

Microsoft.SC-300.v2022-04-16.q116

□□□□:	SC-300
□□□□:	Microsoft Identity and Access Administrator
□□□:	Microsoft
□□ □□ □□□:	116
□□:	v2022-04-16
# □□ □:	2141
# □□ □□□:	1160
https://www.krdump.com/Microsoft.SC-300.v2022-04-16.q116.html	

NEW QUESTION: 1

contoso.com□□□ Azure AD(Azure Active Directory) □□□□ □□□□.
 Azure AD □□ ID □□□ MAU(□□ □□ □□□)□ □□□□ □□□ □□□□ □□□□.
 □□□ □□□□ □□□□?

- A. □□□ □□
- B. □□ □□ □□
- C. □□□ □□
- D. □□□ □□

Answer: C (LEAVE A REPLY)

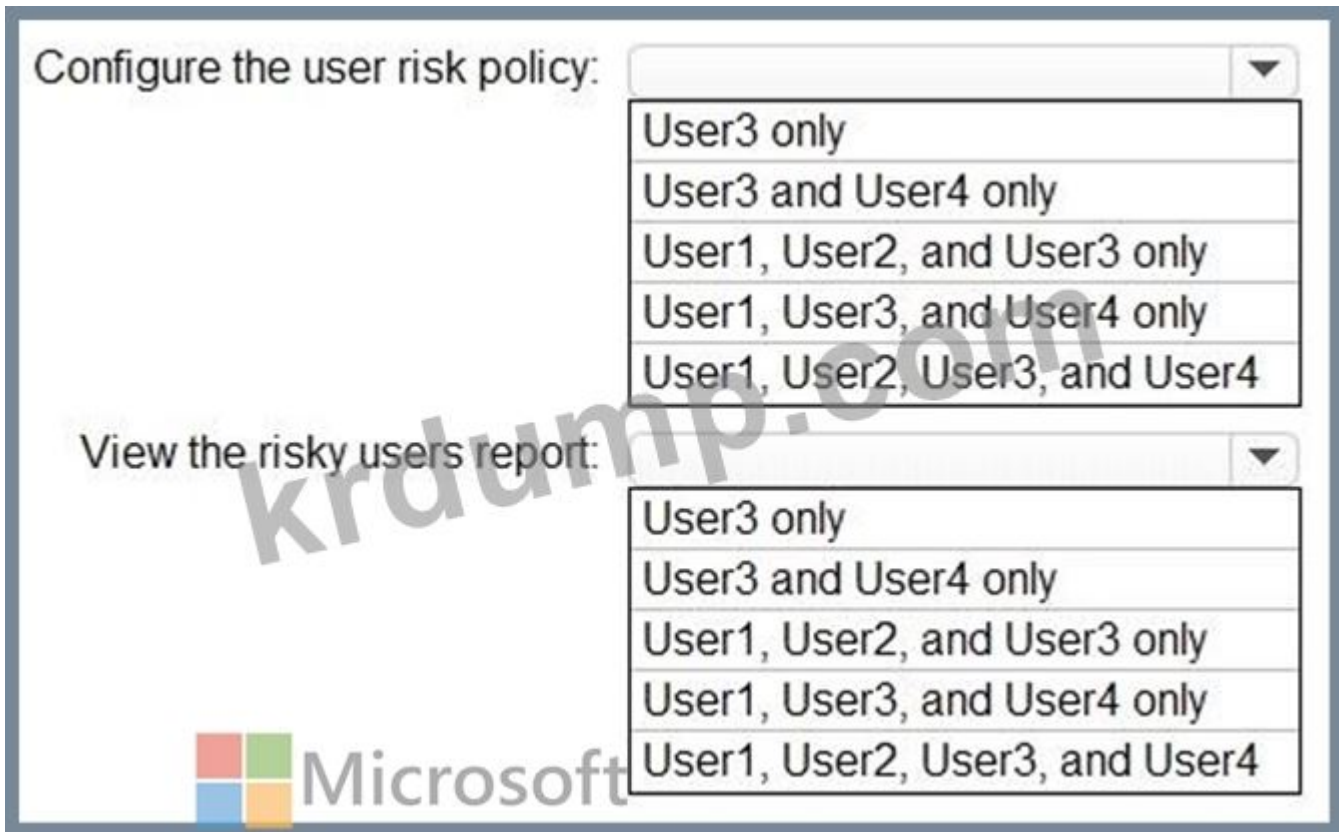
□□:
<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/external-identities-pricing>

NEW QUESTION: 2

□□ □□ □□□ □□□□ □□□□ Azure AD(Azure Active Directory) □□□□ □□□□.

Name	Role
User1	Conditional Access administrator
User2	Authentication administrator
User3	Security administrator
User4	Security operator

Azure AD ID □□□ □□□ □□□□□□.
 □□ □□□□ □□□ □□ □□□ □□□ □ □□ □□ □□□□ □□□ □□□□ □□□□ □ □ □
 □□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□□.
 □□: □ □□□ □□□ 1□□ □□□ □□□□□.



Answer:



□□:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection>

NEW QUESTION: 3

□□□ Contoso.com □□□ Azure AD(Azure Active Directory) □□□□ □□□□. □□□□
Fabrikam, Inc. □□ □□□□ □□□□ □□□□.

Fabrikam Azure AD fabrikam.com litwareinc.com
 Fabrikam Fabrikam
 Fabrikam Fabrikam
 fabrikam.com package1
 Fabrikam?
 Fabrikam: 1

Answer Area

To allow access for users who have fabrikam.com email addresses, configure:

To block access for users who have litwareinc.com email addresses, configure:

- An access package assignment in Identity Governance
- An access package policy in Identity Governance
- A conditional access policy in Azure AD
- The External collaboration settings in Azure AD

Answer:

Answer Area

To allow access for users who have fabrikam.com email addresses, configure:

To block access for users who have litwareinc.com email addresses, configure:

- An access package assignment in Identity Governance
- An access package policy in Identity Governance
- A conditional access policy in Azure AD
- The External collaboration settings in Azure AD

NEW QUESTION: 4

Microsoft 365 E5
 App1
 Microsoft Cloud App Security App1
 4

Actions

- From Microsoft Cloud App Security, create a session policy.
- Publish App1 in Azure Active Directory (Azure AD).
- Create a conditional access policy that has session controls configured.
- From Microsoft Cloud App Security, modify the Connected apps settings for App1.

Answer Area

Answer:

Answer Area

Public App1 in Azure Active Directory (Azure AD).

From Microsoft Cloud App Security, modify the Connect apps settings for App1.

From Microsoft Cloud App Security, create a session policy.

Create a conditional access policy that has session controls configured.

1 - Azure Active Directory(Azure AD) App1.

2 - Microsoft Cloud App Security App1 .

3 - Microsoft Cloud App Security .

4 - .

:

<https://docs.microsoft.com/en-us/cloud-app-security/proxy-deployment-any-app>

<https://docs.microsoft.com/en-us/cloud-app-security/session-policy-aad>

NEW QUESTION: 5

Department1 Azure AD(Azure Active Directory) .

Department1 . (.)

Dashboard > ContosoAzureAD > Department1 Administrative Unit

Department1 Administrative Unit | Users (Preview)

+ Add member Remove member Bulk operations Refresh Columns Preview features Got feedback?

This page includes previews available for your evaluation. View previews →

2 users found

Name	User principal name	User type	Directory synced
<input type="checkbox"/> User1	User1@m365x629615.onmicrosoft.com	Member	No
<input type="checkbox"/> User2	User2@m365x629615.onmicrosoft.com	Member	No

Department1 . (.)

Department1 Administrative Unit | Groups

ContosoAzureAD - Azure Active Directory

+ Add Remove Refresh Columns Preview features Got feedback?

Search groups Add filters

Name	Group Type	Membership Type
<input type="checkbox"/> GR Group1	Security	Assigned
<input type="checkbox"/> GR Group2	Security	Assigned

Department1 (ContosoAzureAD) (Groups)

User Administrator | Assignments

Privileged Identity Management | Azure AD roles

+ Add assignments Settings Refresh Export Got feedback?

Eligible assignments Active assignments Expired assignments

Search by member name or principal name

Name	Principal name	Type	Scope
User Administration			
Admin1	Admin1@m365x67815.onmicrosoft.com	User	Department1 Administrative Unit (Administrative unit)
Admin2	Admin2@m365x67815.onmicrosoft.com	User	Directory

Group2 (ContosoAzureAD) (Groups)

Group2 | Members

Group

+ Add members Remove Refresh Bulk operations Columns Preview features Got feedback

This page includes previews available for your evaluation. View previews ->

Direct members

Name	User type
<input type="checkbox"/> US User3	Member
<input type="checkbox"/> US User4	Member

(ContosoAzureAD) (Groups) (Members)

10:00:00 AM 1/1/2016

Statements

	Yes	No
Admin1 can reset the passwords of User3 and User4.	<input type="radio"/>	<input type="radio"/>
Admin1 can add User1 to Group 2	<input type="radio"/>	<input type="radio"/>
Admin 2 can reset the password of User1.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
Admin1 can reset the passwords of User3 and User4.	<input type="radio"/>	<input checked="" type="radio"/>
Admin1 can add User1 to Group 2	<input type="radio"/>	<input checked="" type="radio"/>
Admin 2 can reset the password of User1.	<input checked="" type="radio"/>	<input type="radio"/>

□□:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units>

NEW QUESTION: 6

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □□□□ □ □□□□ □ □□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □□□ □ □□□□ □□ □□□□ □□ □ □□□ □□ □ □□□ □□ □□ □□□□ □□ □□□□. □ □□□ □□□ □□ □□□ □□ □□□□ □□□ □ □□□□. □□□□□ □□□ □□□ □□ □□□ □□□□ □□□□.

Active Directory □□□□□ □□□□□ Azure AD(Azure Active Directory) □□□□ □□□□. Active Directory□□ □□□ □□□ □□□□□ □□ □□□□□ □□□□ □□ 30□ □□ Azure AD□ □□ □□□ □ □□□ □□□□□□. Active Directory□□ □□□ □□□ □□□□□□ □□□ □□□ □□ Azure AD□ □□□□ □□ □□ □□□.

□□□: □□ □□□ □□□□□. □□□ □□□ □□□□□?

- A. □
- B. □□□

Answer: (SHOW ANSWER)

□□:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn>

NEW QUESTION: 7

□□ □□□ □□□ Azure AD(Azure Active Directory) □□□□ □□□□.

□□: □□1

□□: □□□1, □□□2

□□□: □□□3

2021□ 1□ 15□□ □□□□ □□□ □□ □□□ □□□ □□□□. (□□ □□ □□□□□.)

Create an access review

Access reviews allow reviewers to attest to whether users still need to be in a role.

Review name *

Description

Start date *

Frequency

Duration (in days)

End Never End by Occurrences

Number of times

End date *

Users
Users to review

Scope Guest users only Everyone

Group *

Reviewers
Reviewers

Programs
Link to program
Default Business Flow

Upon completion settings

Advanced settings

[Start](#)



□□□□ □□ □□ □□ Review1 □□□□ □□□□.

User	Date	Do you still need access to Group1?
User1	January 17, 2021	Yes
User2	January 20, 2021	No

□□ □ □□ □□ □□ □□ □□□□. □□□ □□□ □□□□ □□□□□□.
□□: □ □□□ □□□ 1□□ □□□ □□□□.

Statements	Yes	No
On February 5, 2021, User1 can answer the Review1 question again.	<input type="radio"/>	<input type="radio"/>
On January 25, 2021, User2 can answer the Review1 question again.	<input type="radio"/>	<input type="radio"/>
On January 22, 2021, User3 can answer the Review1 question.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
On February 5, 2021, User1 can answer the Review1 question again.	<input checked="" type="radio"/>	<input type="radio"/>
On January 25, 2021, User2 can answer the Review1 question again.	<input checked="" type="radio"/>	<input type="radio"/>
On January 22, 2021, User3 can answer the Review1 question.	<input type="radio"/>	<input checked="" type="radio"/>

□□:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/review-your-access>

NEW QUESTION: 8

User1, User1 □ User3□□□ □ □□ □□□□ □□□ Azure AD(Azure Active Directory) □□□
□ □□ Group1□□□ □□□ □□□□. User2 □ User3□ Group1□ □□□□□.
□□□□□□ □□□ □□□ □□□ □□ Azure AD PIM(Privileged Identity Management)□□ □
□□ □□□□□. (□□ □□□□ □□□ □□ □□□□□.)

Privileged Identity Management | Azure AD roles

Membership | **Setting**

Assignment type ⓘ

- Eligible
- Active

Maximum allowed eligible duration is 3 month(s)

Assignment starts *

01/01/2021 12:00:00 AM

Assignment ends *

01/31/2021 11:59:00 PM

□□ □ □□ □□ □□ □□□ □□ □□□□, □□□ □□□ □□□□ □□□□□. □□: □ □□□ □□□ 1□□ □□□ □□□□.

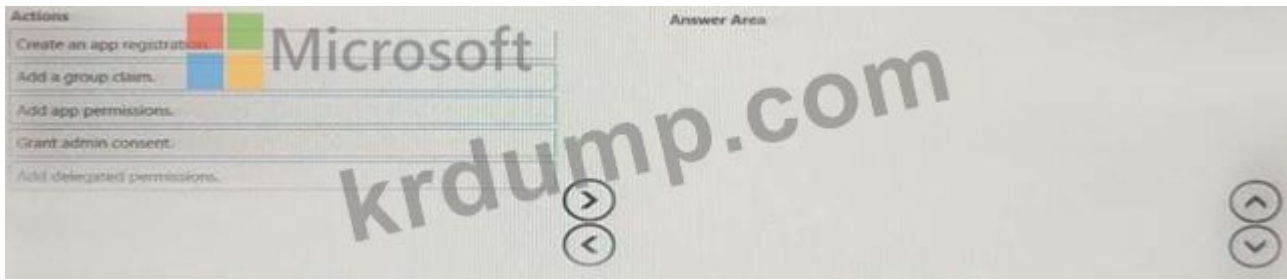
Statements	Yes	No
User1 is assigned the Application administrator role automatically.	<input type="radio"/>	<input type="radio"/>
When User2 requests to be assigned the Application administrator role, only User3 can approve the request.	<input type="radio"/>	<input type="radio"/>
If a request by User1 to be assigned the Application administrator role is approved on January 31, 2021, at 23:00, User1 can use the role until February 1, 2021, at 04:00.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 is assigned the Application administrator role automatically.	<input checked="" type="radio"/>	<input type="radio"/>
When User2 requests to be assigned the Application administrator role, only User3 can approve the request.	<input checked="" type="radio"/>	<input type="radio"/>
If a request by User1 to be assigned the Application administrator role is approved on January 31, 2021, at 23:00, User1 can use the role until February 1, 2021, at 04:00.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION: 9

□□□ contoso.com □□□ Azure AD(Azure Active Directory) □□□□ □□□□. □□□ App1 □□□ □ □□□□ □□ □□□□. App1 □ Microsoft Graph □ □□□□ contoso.com □ □□□□ □□□□ □□ □ □□□ □□□□ □□□. □□ □ □□ □□□ □□□□ □□□□ □□□? □□□□□ □□ □□□□ □□ □□□ □□ □□ □□ □□□□ □□□ □□□ □□□□□□.



Answer:



NEW QUESTION: 10

□□ □□ □□□ □□□ □□□□ Azure AD(Azure Active Directory) □□□□ □□□□.

Name	Type	Membership type
Group1	Security	Assigned
Group2	Security	Dynamic User
Group3	Security	Dynamic Device
Group4	Microsoft 365	Assigned
Group5	Microsoft 365	Dynamic User

□□ □□□ □□ □□□ □□□ □□ □ □□□□?

- A. Group1□
- B. □□1 □ □□4□
- C. Group1 □ Group2□
- D. □□1, □□2, □□4 □ □□5□ □□
- E. □□1, □□2, □□3, □□4 □ □□5

Answer: D (LEAVE A REPLY)

□□ □□□ □□ □□□ □□□ □□□ □ □□□□.

□□:

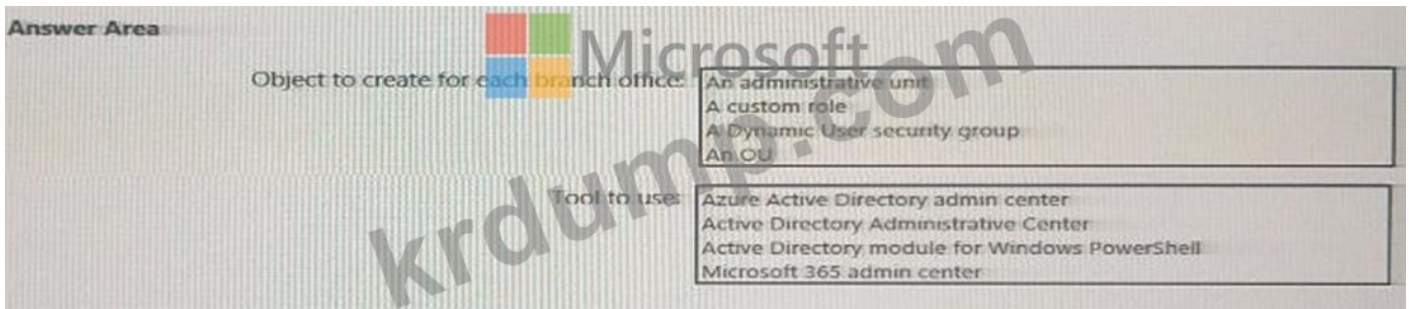
<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

NEW QUESTION: 11

□□□□□ □□□□ □□□□ □□□ □□ □□ □□ □□□ □□□□ □□□.

□□□ □□ □□□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□ □□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.



Answer:



NEW QUESTION: 12

contoso.com Azure AD (Azure Active Directory) .

Azure AD .

.

.

.

.

A.

B.

C.

D.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 13

Microsoft Office 365 Enterprise E3 . 2,500

.

Azure Active Directory Microsoft 365 Enterprise E5

. Office 365 Enterprise E3

.

.

A. Azure Active Directory ID

B. Set-WindowsProductKey cmdlet

C. Azure Active Directory

D. Set-AzureAdUser cmdlet

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 14

contoso.com Azure AD(Azure Active Directory) .
Fabrikam, Inc. .

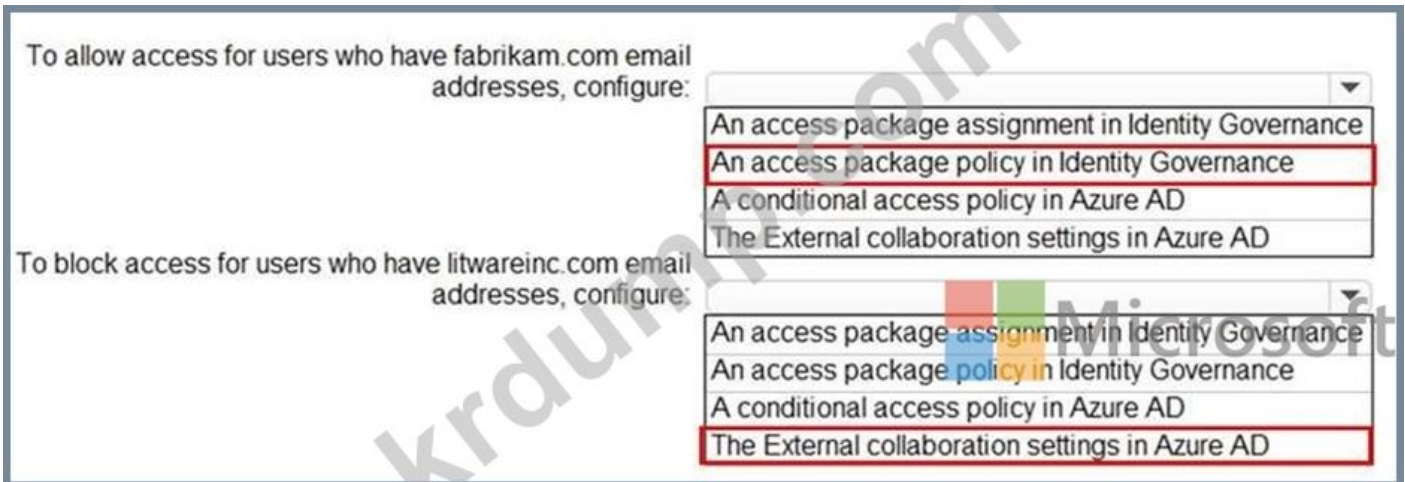
Fabrikam Azure AD fabrikam.com litwareinc.com .
 . Fabrikam .

Fabrikam package1 .
Fabrikam .

fabrikam.com package1 .
 .?
: 1 .



Answer:



:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-request-policy>

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create>

NEW QUESTION: 15

Microsoft 365 .

.

Wi-Fi .

.

MFA(□□□ □□)□ □□□ □□□□□□.
 □□□□ □□ □□□□ □□□ □ □□ MFA □□ □□□ □□□□□□?

- A. □□ □□
- B. □□□
- C. SMS
- D. Microsoft Authenticator □□ □□ □□

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 16

□□ □□ □□□ □□□□ □□□□ Azure AD(Azure Active Directory) □□□□ □□□□.

Name	Type	Directory synced
User1	Member	Yes
User2	Member	No
User3	Guest	No

□□ □□□□ □□ Azure AD□□ □□ □□□ □□ □□ □□□ □□□ □ □□□□? □□□□□□
 □□ □□□□ □□□ □□□ □□□□□□□□.
 □□: □ □□□ □□□ 1□□ □□□ □□□□□.



Answer:



SC-300 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ SC-300 □□! DumpTop
 □ □□ **SC-300** □□ □□□ □□□□□□□, DumpTop SC-300 □□ □□□ □□□□□□□□□
 □□□ □□□□□□□□□. □□□□□ □□□ □□□□ □□ DumpTop SC-300 □□□ □□□□□□.
<https://www.dumptop.com/Microsoft/SC-300-dump.html> (346 Q&As Dumps, **30%OFF Special Discount: KrDump**)

NEW QUESTION: 17

□□□ Microsoft 365 □□□□ □□□□□.
 □□ □□□□ Windows 10□ □□□□ Azure AD(Azure Active Directory) □□□□ □□□ □□□
 □ □□□ □□□□□.

Service1 OAuth Azure AD

 Service1 Azure AD

 Service1 Azure AD

 Azure AD Service1

 ?

Ensure that the users can connect to Service1 without being prompted for authentication:

- An app registration in Azure AD
- Azure AD Application Proxy
- An enterprise application in Azure AD**
- A managed identity in Azure AD

Ensure that the users can access Service1 only from the Azure AD-joined computers:

- Azure AD Application Proxy
- A compliance policy
- A conditional access policy**
- An OAuth policy

Answer:

Ensure that the users **can** connect to Service1 without being prompted for authentication.

- An app registration in Azure AD
- Azure AD Application Proxy
- An enterprise application in Azure AD**
- A managed identity in Azure AD

Ensure that the users can access Service1 only from the Azure AD-joined computers:

- Azure AD Application Proxy
- A compliance policy
- A conditional access policy**
- An OAuth policy

https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

 https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/require-managed-devices

NEW QUESTION: 18

Identity Governance

□□ □□□ □□ □□□?

- A. □□□□□□ □□□□□□□□ □□ □□□ □□ □□□ □□□□□.
- B. □□□□□ □□□□□.
- C. □□□□□ □□□□□.
- D. □□□□□□ □□□□□□□□ □□ □□□ □□ □□ □□□ □□□□□.

Answer: (SHOW ANSWER)

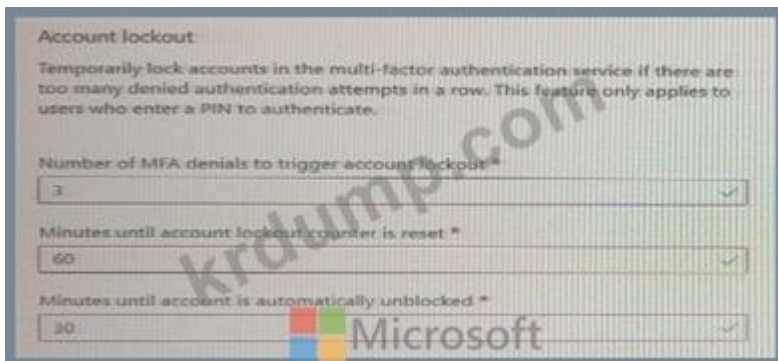
□□:

https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-overview □□ Contoso, Ltd □□□ □□□□ □□□□ □□□□ □□□ □□ □□ □□□ □□□ □□□.

Contoso □ Fabrikam, Inc □□ □□□ □□□ □□□ □□ □□□□. Fabricam □□ fabrikam.com □□□ Azure AD(Azure Active Directory) □□□□ □□□□.

NEW QUESTION: 19

MFA(□□□ □□) □ □□□□ Azure AD(Azure Active Directory) □□□□ □□□□. □□ □□ □□□ □□ □□□ □□ □□□□□.



□□□□ □□□ □□□□ □□□□ □□□ □□□ □□□□ □ □□□ □□□□ □□□ □□□□ □□□ □□□□ □□□ □□□□ □□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□□.



Answer:



NEW QUESTION: 20

□□ □□ □□□ Azure AD(Azure Active Directory) □□□□ □□□□.

Name	Multi-factor auth status	Device
User1	Disabled	Device1
User2	Enabled	Device2
User3	Enforced	Device3

2021 2 1 10:00 AM MFA (Multi-Factor Authentication) status for users.

remember multi-factor authentication on trusted device (learn more)

Allow users to remember multi-factor authentication on devices they trust (between one (1) - 90 days)

Number of days users can trust devices for:

NOTE: For the optimal user experience, we recommend using Conditional Access sign-in frequency to extend session lifetimes on trusted devices, locations, or low-risk sessions as an alternative to "Remember MFA on a trusted device" and "Remember MFA on a trusted device." Be sure to extend the duration to 90 or more days. Learn more about reauthentication prompts.

2021 2 26 10:00 AM Azure AD MFA status for users.

Date	User
February 2, 2021	User1
February 5, 2021	User2
February 21, 2021	User1

2021 2 26 10:00 AM MFA status for users?

A)

Name	Multi-factor auth status
User1	Disabled
User2	Enabled
User3	Enforced

B)

Name	Multi-factor auth status
User1	Enabled
User2	Enabled
User3	Enabled

C)

Name	Multi-factor auth status
User1	Enforced
User2	Enforced
User3	Enforced

D)

Name	Multi-factor auth status
User1	Disabled
User2	Enforced
User3	Enforced

A. C

B. D

C. A

D. B

Answer: D (LEAVE A REPLY)

NEW QUESTION: 21

Azure AD (Azure Active Directory) MFA status for users.

2021 2 26 10:00 AM MFA status for users.

Admin1 2021 2 26 10:00 AM App1 MFA status for users.

Admin1 Azure AD App1 MFA status for users.

Admin1 MFA status for users?

- A. Azure AD Connect on Server 1
- B. Azure AD Connect on Server 2
- C. Azure AD Connect on Server 1 and Server 2
- D. Azure AD Connect on Server 2 and Server 1

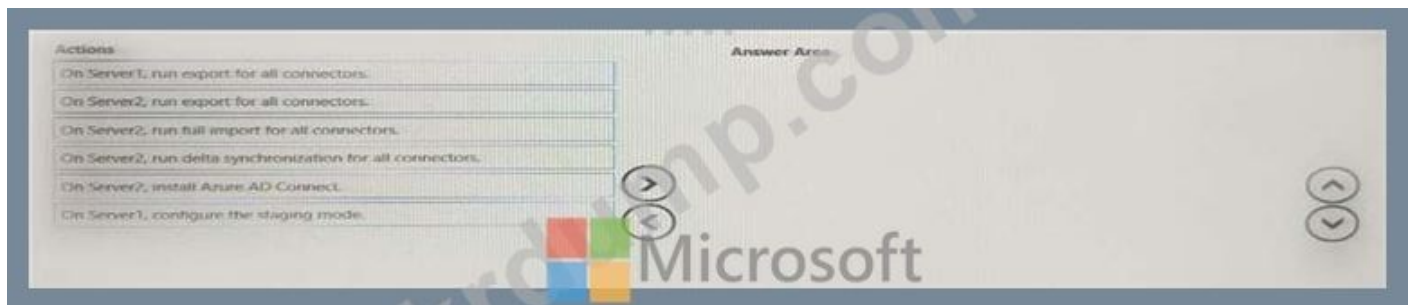
Answer: (SHOW ANSWER)

Answer:

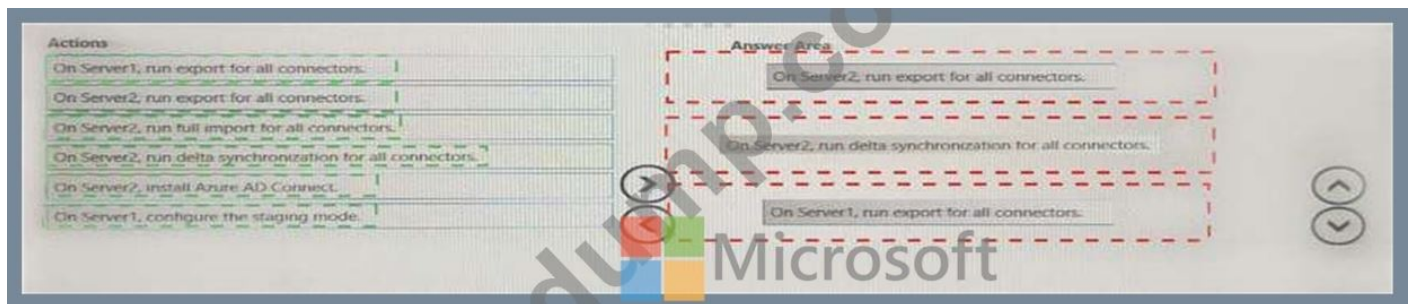
<https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles>

NEW QUESTION: 22

A company has two servers, Server 1 and Server 2, running Windows Server 2019. The company has an Azure AD Connect cloud sync connector for contoso.com. The connector is configured to sync users and groups from the on-premises Active Directory to Azure AD. The connector is currently in staging mode. The administrator wants to run a full import of all connectors on Server 2. Which actions should the administrator perform? (Select all that apply.)



Answer:



NEW QUESTION: 23

A company has a Microsoft 365 subscription. The company has a policy that requires all users to use multi-factor authentication (MFA) when logging in to Microsoft 365. The administrator wants to implement MFA for all users. Which actions should the administrator perform? (Select all that apply.)

- A. Microsoft Authenticator
- B. Windows Hello for Business

- C. Windows Hello
- D. SMS

Answer: (SHOW ANSWER)

Windows 10 can use Windows Hello on a PC. It can use Windows Hello on a PC with a camera, a fingerprint scanner, or a PIN. It can use Windows Hello on a PC with a camera, a fingerprint scanner, or a PIN. It can use Windows Hello on a PC with a camera, a fingerprint scanner, or a PIN.

Windows Hello can be used on a PC with a camera, a fingerprint scanner, or a PIN. It can be used on a PC with a camera, a fingerprint scanner, or a PIN. It can be used on a PC with a camera, a fingerprint scanner, or a PIN.

URL:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods>

<https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview>

NEW QUESTION: 24

Which of the following is a valid Azure AD Connect configuration? (Select two)

- A. Azure AD Connect with PingFederate as the federation provider.
- B. Azure AD Connect with a local Active Directory.
- C. Azure AD Connect with a local Active Directory and a VPN connection.
- D. Azure AD Connect with a local Active Directory and a VPN connection.

Answer: (SHOW ANSWER)

1, Litware, Inc
2

Litware, Inc. and Fabrikam, Inc. are both Active Directory domains. Litware is a member of the Fabrikam domain. Litware has a VPN connection to Fabrikam. Litware has a VPN connection to Fabrikam.

ID:

litware.com is connected to Azure AD (Azure Active Directory) as a federated domain. Active Directory is connected to Azure AD Connect as a local Active Directory. Azure AD Connect is connected to Azure AD as a local Active Directory.

Litware.com is connected to Azure AD as a federated domain. User1 is a user in the Litware.com domain. Azure AD is connected to Litware.com as a local Active Directory.

Fabrikam is connected to Azure AD as a federated domain. Fabrikam is connected to litware.com as a local Active Directory.

URL:

Litware is a member of the Microsoft 365 Enterprise E5 license. Microsoft Cloud App Security is a cloud security solution.

Litware litware.com Azure AD Office 365 Azure Sentinel
Active Directory Office 365 Azure Sentinel
Azure Sentinel Azure AD
Office 365 Azure AD
Office 365 Azure AD

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Litware VPN Azure Office 365 Azure Sentinel
Azure Office 365 Azure Sentinel
Office 365 Azure Sentinel

Litware Office 365 Azure AD

- * Azure AD PIM(Privileged Identity Management)
- * litware.com Azure AD
- * Identity Governance
- * User1 Azure AD

Litware litware.com Active Directory LwLicenses
LwLicenses litware.com Azure AD
LwLicenses Microsoft 365

Litware LWGroup1 Litware Azure AD
Azure AD

Litware Office 365 Azure AD

- * Litware (MFA)
- * MFA Litware Boston Azure AD
- * litware.com
- * MFA
- * Office 365

Litware Litware Azure AD Azure AD
LWGroup1

□□□□ □□ □□

Litware□ Azure Sentinel□ Fusion □□□ □□□□ □□□□□ Azure AD □□□□ □□□□□

Microsoft Office 365 □□□ □□□ □□□□ □□□□ □□□□□ □□□.

NEW QUESTION: 25

Log Analytics □□ □□□ □□□□.

□□□ □□ □□ □□ □□□ □□□□ □□□.

Azure AD□□ □□□ □□□□ □□□□?

- A. □□ □□□
- B. □□ □□
- C. □□ ID
- D. □ □□

Answer: B (LEAVE A REPLY)

□□:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/overview-monitoring>

NEW QUESTION: 26

□□□ Contoso.com□□□ Azure AD(Azure Active Directory) □□□□ □□□□. □□□□

Fabrikam, Inc.□□ □□□□ □□□□ □□□□.

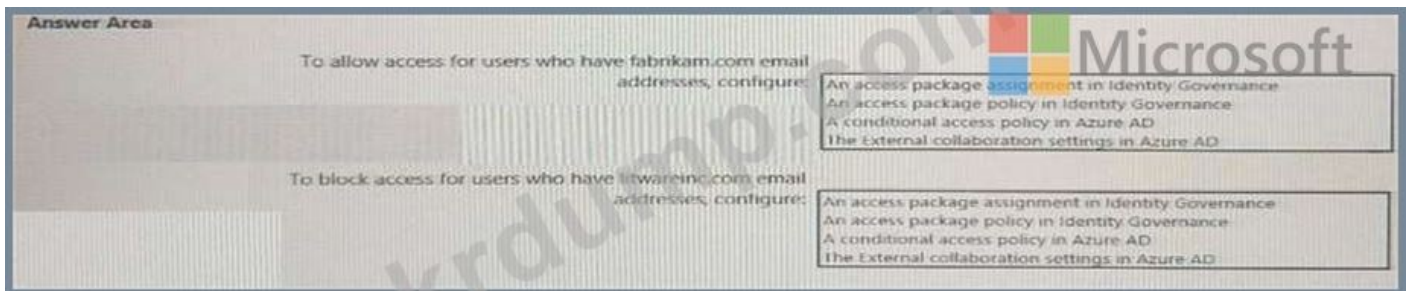
Fabrikam□ Azure AD□ □□□□ fabrikam.com □ litwareinc.com□□□□ □ □□ □□□ □□□ □ □□ □□□□.

Fabrikam□ □□ □□□ □□□ □□□□.

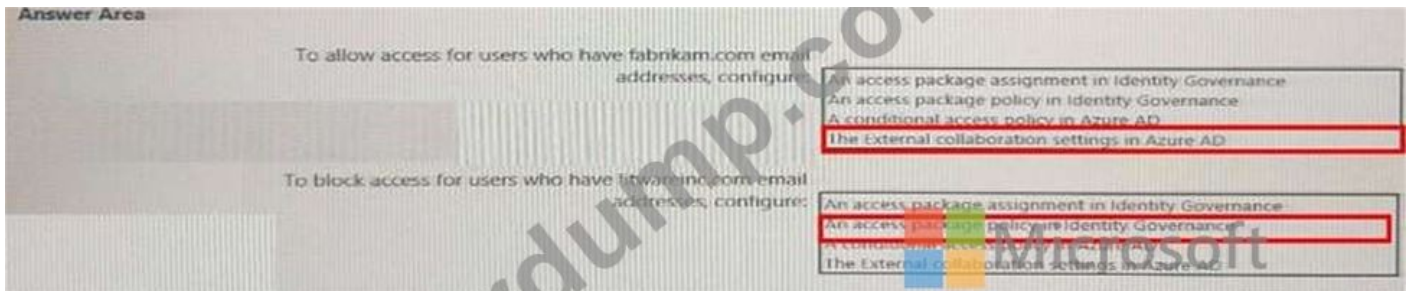
fabrikam.com □□□ □□□ □□ □□□□ package1□ □□□□ □ □□□ □□ □□□.

□□□ □□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.



Answer:



NEW QUESTION: 27

Department1□□□ □□ □□□ □□□ Azure AD(Azure Active Directory) □□□□ □□□□.

Department1 □□ □□□ □□□□ □□□ □□□□ □□□□. (□□□ □□ □□□□□.)

Dashboard > ContosoAzureAD > Department1 Administrative Unit

Department1 Administrative Unit | Users (Preview)

ContosoAzureAD - Azure Active Directory

+ Add member Remove member Bulk operations Refresh Columns Preview features Got feedback?

This page includes previews available for your evaluation. View previews →

Search users Add filters

2 users found

Name	User principal name	User type	Directory synced
<input type="checkbox"/> User1	User1@m365x629615.onmicrosoft.com	Member	No
<input type="checkbox"/> User2	User2@m365x629615.onmicrosoft.com	Member	No

Department1 □□ □□ □□□□ □□□ □□□ □□□□. (□□ □□ □□□□□.)

Dashboard > ContosoAzureAD > Department1 Administrative Unit

Department1 Administrative Unit | Groups

ContosoAzureAD - Azure Active Directory

>> + Add Remove Refresh Columns Preview features Got feedback?

Search groups Add filters

Name	Group Type	Membership Type
<input type="checkbox"/> Group1	Security	Assigned
<input type="checkbox"/> Group2	Security	Assigned

Department1 □□ □□ □□□ □□□ □□□ □□□ □□□ □□□□. (□□ □□ □□□□□.)

Dashboard > ContosoAzureAD > Identity Governance > Privileged Identity Management > ContosoAzureAD >

User Administrator | Assignments

Privileged Identity Management | Azure AD roles

+ Add assignments Settings Refresh Export Got feedback?

Eligible assignments Active assignments Expired assignments

Search by member name or principal name

Name	Principal name	Type	Scope
User Administration			
Admin1	Admin1@m365x629615.onmicrosoft.com	User	Department1 Administrative Unit (Administrative unit)
Admin2	Admin2@m365x629615.onmicrosoft.com	User	Directory

Group2 □ □□□□ Group2 □□□□ □□□□□. (□□2 □□ □□□□□.)



Answer:



NEW QUESTION: 29

□□ □□ □□□ □□□□ □□□□ Azure AD(Azure Active Directory) □□□□ □□□□.

Name	Type	Directory synced
User1	Member	Yes
User2	Member	No
User3	Guest	No

□□ □□□□ □□ Azure AD□□ □□ □□□ □□ □□ □□□ □□□ □ □□□? □□□□□□
 □□ □□□□ □□□ □□□ □□□□□□□□.
 □□: □ □□□ □□□ 1□□ □□□ □□□□□.



Answer:



NEW QUESTION: 30

□□ □□ □□□ □□□□□ □□ □□□ □□□□ □□□.
 DC1□ Azure AD □□ □□ DC □□□□□□ □□□□□□.
 □□□ □□□ □□ □□□? □□□□□□ □□ □□□□ □□□ □□□ □□□□□□□□.
 □□: □ □□□ □□□ 1□□ □□□ □□□□□.

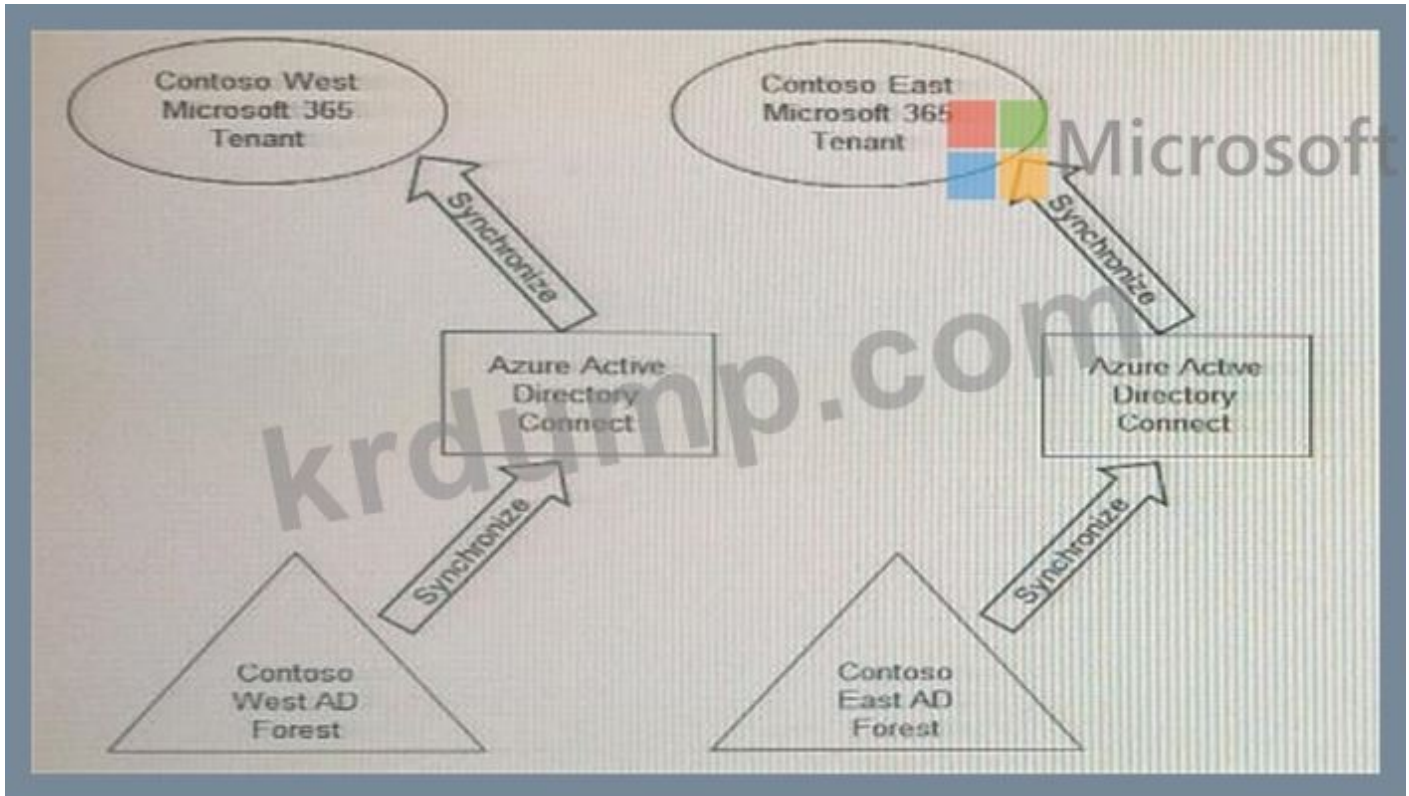


Answer:



NEW QUESTION: 31

Contoso East and Contoso West are Microsoft 365 tenants. Contoso East is a Microsoft 365 ID tenant. Contoso West is a Microsoft 365 ID tenant.



Contoso West is a Microsoft 365 tenant. Contoso East is a Microsoft 365 tenant. Contoso West is a Microsoft 365 tenant. Contoso East is a Microsoft 365 tenant.

Contoso West is a Microsoft 365 tenant?

- A. West is a Microsoft 365 tenant.
- B. Contoso East Active Directory is connected to Contoso West via Azure AD Connect.
- C. Contoso West is connected to Azure AD via Azure AD Connect.
- D. Azure AD Connect is connected to Contoso East via Contoso East Active Directory.

Answer: A (LEAVE A REPLY)

□□□ □□□□□□□□. □□□□ □□□ □□□□ □□ DumpTop SC-300 □□□ □□□□□.
<https://www.dumptop.com/Microsoft/SC-300-dump.html> (346 Q&As Dumps, 30%OFF Special
Discount: **KrDump**)

NEW QUESTION: 32

contoso.com SMTP □□ □□□ □□□□ Microsoft Exchange □□□ □□□□.
□□ □□□□ Azure AD(Azure Active Directory) □□ □□ □□□ □□□ □□ contoso.com □
□ □□ □□□ □□□□□.
□□ □□□ □□□□ □□□ Azure AD □□□□ □□ □□ □□□ □□□ □□□□.
□□□□ Microsoft 365 □□□□ □□ □□ □□□ □□□ □□ contoso.com Azure AD □□□□
□ □□□ □□□ □□□ □□□□ □□ □□□.
□□ PowerShell cmdlet □ □□□□ □□□□?

- A. MsolCompanySettings □□
- B. MsolCompanySettings □□
- C. Mso1DomaininFederationSettings □□
- D. □□□□-Msol federateDomain

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 33

contoso.com SMTP □□ □□□ □□□□ □□□□□ Microsoft Exchange □□□ □□□□.
□□□□ Microsoft 365 □□□□ □□ □□ □□□ □□□ □□ □□ □□ □□□□□ □
□ □□□□□□□.
□□ □□□ □□□□ □□□ Azure AD(Azure Active Directory) □□□□ □□ □□ □□□ □□
□ □□□ □□□.
□□ 4□□ □□□ □□□□ □□□□ □□□? □□□□□ □□ □□□□ □□ □□□ □□ □□
□□ □□□□ □□□ □□□ □□□□□□□□.

Actions	Answer Area
Sign in to the Microsoft 365 admin center.	
Create a self-signed user account in the Azure AD tenant.	
From the Microsoft 365 admin center, add the domain name.	
Respond to the Become the admin message.	
From the Microsoft 365 admin center, remove the domain name.	
Create a TXT record in the contoso.com DNS zone.	

Answer:

Answer Area



Create a self-signed user account in the Azure AD tenant.

Sign in to the Microsoft 365 admin center.

Respond to the Become the admin message.

Create a TXT record in the contoso.com DNS zone.

1 - Azure AD □□□□□ □□ □□□ □□□ □□□□ □□□□.

2 - Microsoft 365 □□ □□□ □□□□□□.

3 - □□□ □□ □□□□ □□□□□.

4 - contoso.com DNS □□□□ TXT □□□□ □□□□.

□□:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/domains-admin-takeover>

NEW QUESTION: 34

User1, User1 □ User3□□□ □ □□ □□□□ □□□ Azure AD(Azure Active Directory) □□□ □ □□ Group1□□□ □□□ □□□□□. User2 □ User3□ Group1□ □□□□□. □□□□□□ □□□ □□□ □□□ □□ Azure AD PIM(Privileged Identity Management)□□ □ □□ □□□□□. (□□ □□□□ □□□ □□ □□□□□□.)

Privileged Identity Management | Azure AD roles

Membership Setting

Assignment type ⓘ

Eligible

Active

Maximum allowed eligible duration is 3 month(s)

Assignment starts *

01/01/2021 12:00:00 AM

Assignment ends *

01/31/2021 11:59:00 PM

00 0 00 00 00 00 000 00 00000, 000 000 0000 00000.
 00: 0 000 000 100 000 0000.

Answer Area

Statements	Yes	No
User1 is assigned the Application administrator role automatically.	<input type="radio"/>	<input type="radio"/>
When User2 requests to be assigned the Application administrator role, only User3 can approve the request.	<input type="radio"/>	<input type="radio"/>
If a request by User1 to be assigned the Application administrator role is approved on January 31, 2021, at 23:00, User1 can use the role until February 1, 2021, at 04:00.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 is assigned the Application administrator role automatically.	<input checked="" type="radio"/>	<input type="radio"/>
When User2 requests to be assigned the Application administrator role, only User3 can approve the request.	<input checked="" type="radio"/>	<input type="radio"/>
If a request by User1 to be assigned the Application administrator role is approved on January 31, 2021, at 23:00, User1 can use the role until February 1, 2021, at 04:00.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION: 35

00: 0 000 000 000000 0000 000 00 0 000000. 0000 0 0000 0
 00 000 000 0 00 000 0000 0000 00000. 00 00 0000 0 000 0
 00 0000 00 0 000 00 00 0000 000 0000 00 0 00000.
 0 000 000 00 000 00 0000 000 0 00000. 000000 000 000 00
 000 0000 00000.
 Microsoft 365 0000 00000.
 1000 000 000 10000 IT 00000 00000.
 0000 00000 000 000 000000. (00 00 000000.)

Create an access review

Access reviews allow reviewers to attest to whether users still need to be in a role.

Review name *

Description

Start date *

Frequency

Duration (in days)

End Never End by Occurrences

Number of times

End date

Users Scope Everyone

Review role membership (permanent and eligible) *
Application Administrator and 72 others

Reviewers

(Preview) Fallback reviewers

Upon completion settings



- A.
- B.

Answer: [\(SHOW ANSWER\)](#)

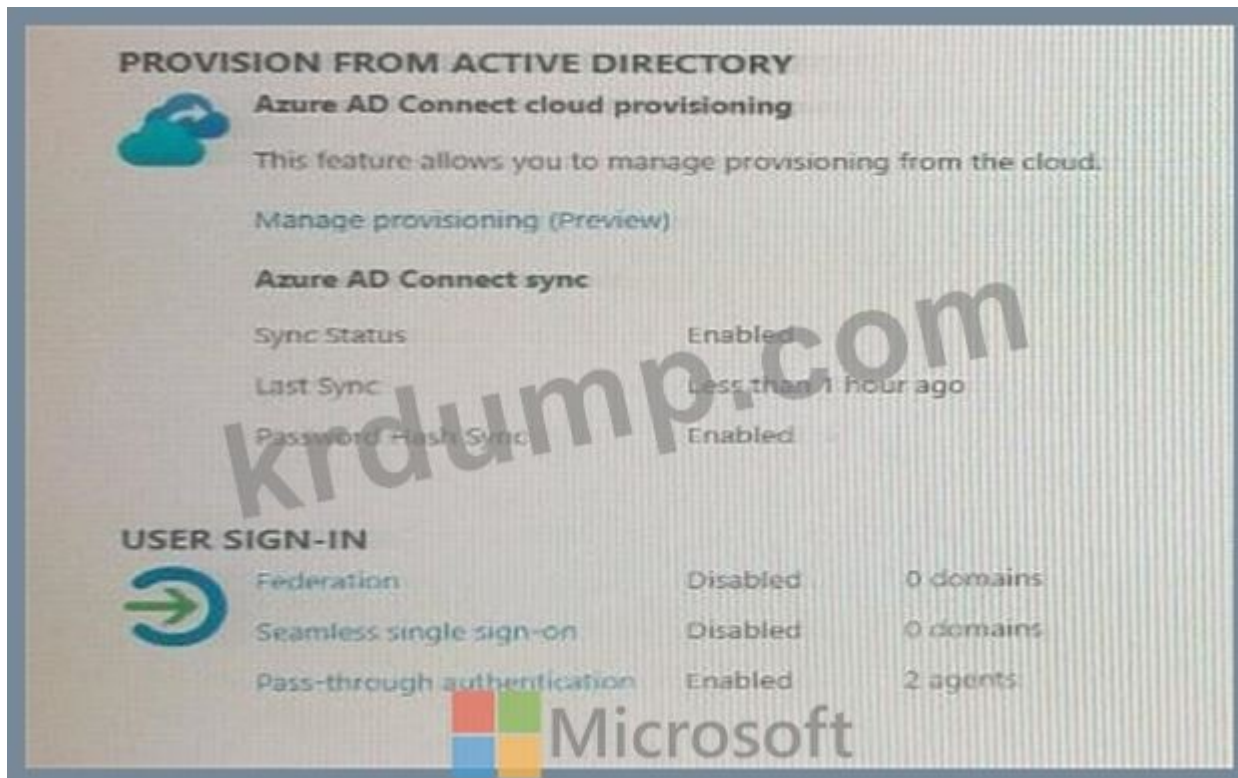
NEW QUESTION: 36

Which users are synced from Active Directory to Azure AD(Azure Active Directory)?

Name	Type	Directory synced
User1	User	No
User2	User	Yes
User3	Guest	No

Which users are synced from Active Directory to Azure AD Connect?

Which users are synced from Active Directory to Azure AD?



Which users are synced from Active Directory to Azure AD?

Which users are synced from Active Directory to Azure AD?

A. User1, User2, User3

B. User1

C. User1 and User2

D. User1 and User3

Answer: B (LEAVE A REPLY)

NEW QUESTION: 37

Which users are synced from Active Directory to Azure AD(Azure Active Directory)?

Name	Role
Admin1	Application administrator
Admin2	Application developer
Admin3	Cloud application administrator
User1	User

App1 □ App2□□ □ □□ □□□□ □□ □□□□□. □□ □□□□ Azure AD□ App1□ □□□ □□.

App1□ □□□□ □□□ □ □□ □□□ Azure AD□ App2□ □□□ □ □□ □□□ □□□□ □ □□.

□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.

Can assign users to App1:

- Admin1 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and User1

Can register App2 in Azure AD:

- Admin1 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and User1

Answer:

Can assign users to App1:

- Admin1 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and User1

Can register App2 in Azure AD:

- Admin1 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and User1

□□:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal-assign-users>

<https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added>

NEW QUESTION: 38

□□ □□ □□□ □□□□ □□□ □□□□□ □□□ □□□ □□□□.

Name	Description
Server1	Domain controller that runs Windows Server 2019
Server2	Server that runs Windows Server 2019 and has Azure AD Connect deployed
Server3	Server that runs Windows Server 2019 and has a Microsoft ASP.NET application named App1 installed
Server4	Unassigned server that runs Windows Server 2019
Firewall1	Hardware firewall connected to the internet that blocks all traffic unless explicitly allowed

Active Directory □□□□□ □□□□□ Azure AD(Azure Active Directory) □□□□ □□□□.

Azure AD□ □□ □□□ □□(MFA)□ □□□□□.

Azure AD □□□□□ App1□ □□□ □ □□□ □□□□ □□□.

□□ □ □□□1□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□ □□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.

Service to install on Server4:

- Azure AD Application Proxy
- The Azure AD Password Protection DC agent
- The Azure AD Password Protection proxy service
- Web Application Proxy in Windows Server

Rule to configure on Firewall1:

- Allow incoming HTTPS connections from Azure AD to Server4.
- Allow incoming IPsec connections from Azure AD to Server4.
- Allow outbound HTTPS connections from Server4 to Azure AD.
- Allow outbound IPsec connections from Server4 to Azure AD.

Answer:

Service to install on Server4:

- Azure AD Application Proxy
- The Azure AD Password Protection DC agent
- The Azure AD Password Protection proxy service
- Web Application Proxy in Windows Server

Rule to configure on Firewall1:

- Allow incoming HTTPS connections from Azure AD to Server4.
- Allow incoming IPsec connections from Azure AD to Server4.
- Allow outbound HTTPS connections from Server4 to Azure AD.
- Allow outbound IPsec connections from Server4 to Azure AD.

□□:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy>

NEW QUESTION: 39

Active Directory □□□□ □□□□□ Azure AD(Azure Active Directory) □□□□ □□□□. □□□□□ □□□□□□ □□□□□ Active Directory □□□□ □□□□ VPN □□□ □□□□ □□□□. VPN □□□ Azure MFA(□□□□ □□)□ □□□□ □□□□. VPN □□□ Azure MFA□ □□□□ □□□□ □□□□ □□□. □□□□□ □□□ □□□□ □□□?

- A. Azure AD □□□□□□ □□□
- B. Azure AD □□ □□ □□□
- C. □□□□ □□ □□(NPS)
- D. □□ □□ □□□

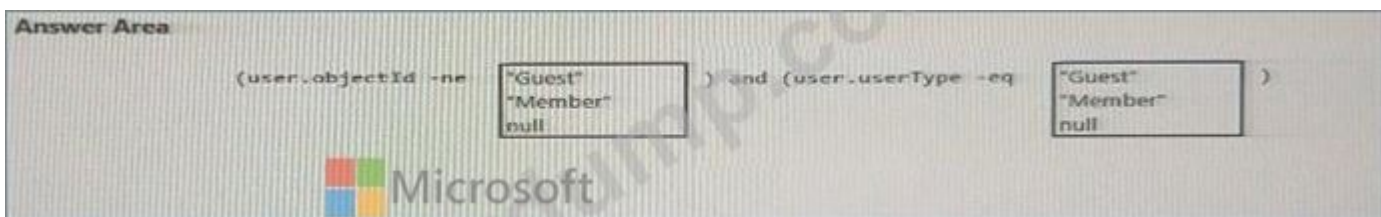
Answer: C (LEAVE A REPLY)

□□/□□:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-nps-extension-vpn>

NEW QUESTION: 40

□□ □□ □□□ □□□□□ LWGroup1 □□□ □□□□ □□□. □□ □□□ □□□ □□□ □□□□ □□□? □□□□□ □□□ □□ □□□ □□□□ □□□□ □□□. □ □□ □ □, □ □ □□ □□ □□ □□□□ □□ □ □□□□. □□□□ □□□ □ □□ □ □□ □□□ □□□□□□ □□□□□ □□ □□□ □□□□. □□: □ □□□ □□□ 1□□ □□□ □□□□.



Answer:

```
Answer Area
(user.objectId -ne "Guest" and (user.userType -eq "Member" or null))
```

NEW QUESTION: 41

Microsoft 365 □□□□ □□□□. Azure AD(Azure Active Directory) □□□□ □-□□□□ Active Directory □□□□ □□□□□□. □□□□□ □□ □□ □□□ □□□ □□□□□□.

Name	Operating system	Configuration
Server1	Windows Server 2019	Domain controller
Server2	Windows Server 2019	Domain controller
Server3	Windows Server 2019	Azure AD Connect

□□□ □□□□□ □□□□ □□□ □ □□□□. Server1 □ Server2□□ Azure AD □□ □□□ □□□□□. Windows Server 2019□ □□□□ Server4□□ □ □□□ □□□□□. □□ □□□ □□□□ □□ Azure AD □□ □□□ □□ □□□□□ □□□□ □□□. Server4□□ □□□ □□□□ □□□?

- A. □□ AD □□□
- B. Azure AD □□□□□□ □□□
- C. □□□□ □□ □□ □□□(PCNS)
- D. Azure AD □□ □□ □□□ □□□

Answer: D (LEAVE A REPLY)

□□: <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premisesdep>

NEW QUESTION: 42

Microsoft 365 □□□□ □□□□. □□□ □□□ □□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□. (□□□ □□□ □□ □ □□□□□.)

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

Require MFA for all users ✓

Assignments

Users and groups ⓘ >

All users

Cloud apps or actions ⓘ >

All cloud apps

Conditions ⓘ >

1 condition selected

Access controls

Grant ⓘ >

0 controls selected

Session ⓘ >

0 controls selected

Enable policy

Report-only On Off

Create

grant access. [Learn more](#)

Block access

Grant access

Require multi-factor authentication ⓘ

Require device to be marked as compliant ⓘ

Require Hybrid Azure AD joined device ⓘ

Require approved client app ⓘ
See list of approved client apps

Require app protection policy ⓘ
See list of policy protected client apps

Require password change (Preview) ⓘ

For multiple controls

Require all the selected controls

Require one of the selected controls

Select

00 00 00 00 000 000 00 000 000 00 0000 0 0 00000. (00 00 0 0 00 00 00000.)

Privileged Identity Management > ContosoAzureAD > User Administrator

Role setting details - User Administrator

Privileged Identity Management | Azure AD roles

Edit

Activation

Setting	State
Activation maximum duration (hours)	8 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	Yes
Approvers	1 Member(s); 0 Group

Assignment

Setting	State
Allow permanent eligible assignment	No
Eligible assignments after	15 day(s)
Eligible assignments after permanent active assignment	No
Expire active assignments after	1 month(s)
Require Azure Multi-Factor Authentication on active assignment	No
Require justification on active assignment	No

Which of the following statements are true? (Select all that apply.)

ContosoAzureAD > Identity Governance > Privileged Identity Management > ContosoAzureAD >

User Administrator | Assignments

Privileged Identity Management | Azure AD roles

+ Add assignments Settings Refresh Export Got feedback?

Eligible assignments Active assignments Expired assignments

Search by member name or principal name

Name	Principal name	Type	Scope	Membership
User Administrator				
Admin1	Admin1@m365x629615.onmicrosoft.com	User	Directory	Direct
Admin2	Admin2@m365x629615.onmicrosoft.com	User	Directory	Direct
Admin3	Admin3@m365x629615.onmicrosoft.com	User	Directory	Direct

Which of the following statements are true? (Select all that apply.)

Admin1 can request activation of the User administrator role for a period of two hours.

Answer Area

Statements	Yes	No
Before Admin1 can perform a task that requires the User administrator role, an approver must approve the activation request.	<input type="radio"/>	<input type="radio"/>
Admin2 can request activation of the User administrator role for a period of two hours.	<input type="radio"/>	<input type="radio"/>
If Admin3 connects to the Azure Active Directory admin center, and then activates the User administrator role, Admin3 will be prompted to authenticate by using multi-factor authentication (MFA) twice.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements

Microsoft

Before Admin1 can perform a task that requires the User administrator role, an approver must approve the activation request. Yes No

Admin2 can request activation of the User administrator role for a period of two hours. Yes No

If Admin3 connects to the Azure Active Directory admin center, and then activates the User administrator role, Admin3 will be prompted to authenticate by using multi-factor authentication (MFA) twice. Yes No

NEW QUESTION: 43

Microsoft 365 .

Azure AD(Azure Active Directory) .

Name	Type
Group1	Security
Group2	Distribution
Group3	Microsoft 365
Group4	Mail-enabled security

Azure AD . Appl . App1
 ?

- A. Group2
- B. 1
- C. 1 4
- D. Group3
- E. 1

Answer: E (LEAVE A REPLY)

NEW QUESTION: 44

User1 Azure AD(Azure Active Directory)
 .

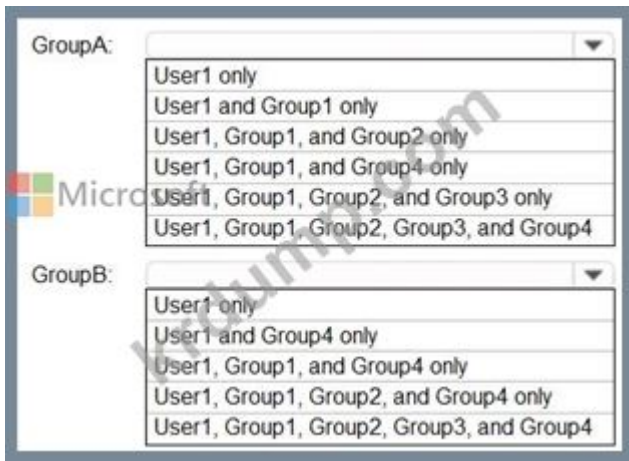
Name	Type	Membership type
Group1	Security	Assigned
Group2	Security	Dynamic User
Group3	Security	Dynamic Device
Group4	Microsoft 365	Assigned

.

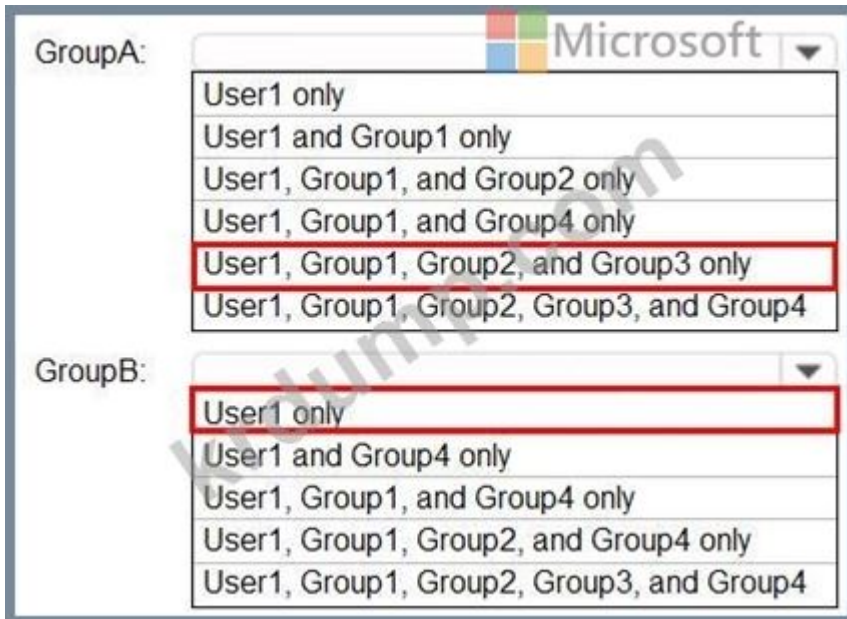
Name	Type	Membership type
GroupA	Security	Assigned
GroupB	Microsoft 365	Assigned

GroupA GroupB ?
 .

: 1 .



Answer:



□□:

<https://bitsizebytes.wordpress.com/2018/12/10/distribution-security-and-office-365-groups-nesting/>

NEW QUESTION: 45

- Microsoft 365 □□□□ □□□□.
- 300□□ □□□□ □□ □ □□□ □□□□. □ □□□□ □□□□ □□□□ □□□□
- □□ □□ □□□□ □□□ □ □□□□. □ □□ □□□□ □□ □□□ □□ □□□□ □
- □□□□.
- □□□ □ □□□□ □□□ □□□□.
- □□ □□□□ Microsoft 365 □□□□ □□□□ □ MFA(□□□□ □□)□ □□□□ □□□□.
- □□□ □□□□ □□□□?
- A. □□□ □□□□ □□
 - B. Microsoft Authenticator □
 - C. □□□□□ Windows Hello □□
 - D. FIDO2 □□

Answer: D (LEAVE A REPLY)

□□/□□:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless

NEW QUESTION: 46

contoso.com□ □□ □□□ □□□ □□□□□ □ Microsoft 365 □□□□ □□□□□. □□□ □□□ □□□ □□□□ Microsoft 365 □□□□ □□ □□□□ □□□ □ □□□ □□□□ □□□.

□□ □□□ □□ □□□?

- A. □□□ □□ □□□ □□□□□□□.
- B. □□ □□□□ □□□□□□□.
- C. □□□ □□(MFA) □□ □□□ □□□□□.
- D. Windows Server Active Directory□ □□ □□ □□□ □□□□□.

Answer: B ([LEAVE A REPLY](#))

□□/□□:

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults

SC-300 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ SC-300 □□! DumpTop □ □□ **SC-300** □□ □□□ □□□□□□□, DumpTop SC-300 □□ □□□ □□□□□□□□ □□□ □□□□□□□□. □□□□□ □□□ □□□□ □□ DumpTop SC-300 □□□ □□□□□.

<https://www.dumptop.com/Microsoft/SC-300-dump.html> (346 Q&As Dumps, **30%OFF Special Discount: KrDump**)

NEW QUESTION: 47

Microsoft 365 □□□□ □□□□.

Azure AD(Azure Active Directory) □□□□ □-□□□□□ Active Directory □□□□ □□□□□□□. Emergency1□□□ □□ □□□ □□ □□□ □□ □□□□□. Emergency1□□ Azure AD□ □ □□□ □□□ □□□□□. Emergency1□ Azure AD □□ □□ □ □-□□□□□ □□□ □□□ □□□ □□□□□.

Emergency1□ □□ □ □□□□□ □□ □□□□ □□□ □□□.

□□□ □□□ □□ □□□?

- A. Emergency1□ □□□□□ □□□□□ □□ □□□ □□□□□ Azure Monitor□ □□□□□.
- B. Emergency1□ □□ □□□ □□(MFA)□ □□□□□ □□□ □□□ □□□ □□□□□.
- C. Emergency1□ □□ □□ □□□ □□□ Azure AD PIM(Privileged Identity Management) □□ □□ □□□□□.
- D. Emergency1□ □□□ □□□ □□ □□□□□□ □□□□ □□□ □□ □□□ □□□□□.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 48

contoso.com Azure AD(Azure Active Directory)

Azure AD B2B()

1. : 1

- A.
- B. URL
- C.
- D.
- E.

Answer: A,B (LEAVE A REPLY)

:/:

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/tutorial-bulk-invite>

NEW QUESTION: 49

contoso.com Microsoft 365

contoso.com

User email	User type	Invitation accepted	Shared resource
User1@outlook.com	Guest	No	Enterprise application
User2@fabrikam.com	Guest	Yes	Enterprise application

Azure Active Directory

Collaboration restrictions

- Allow invitations to be sent to any domain (most inclusive)
- Deny invitations to the specified domains
- Allow invitations only to the specified domains (most restrictive)

Delete

TARGET DOMAINS

Outlook.com 

Microsoft SharePoint Online user3@adatum.com

1. : 1

Statements	Yes	No
User1 can accept the invitation and gain access to the enterprise application.	<input type="radio"/>	<input type="radio"/>
User2 can access the enterprise application.	<input type="radio"/>	<input type="radio"/>
User3 can accept the invitation and gain access to the SharePoint site.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 can accept the invitation and gain access to the enterprise application.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can access the enterprise application.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can accept the invitation and gain access to the SharePoint site.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION: 50

ADatum is a Microsoft Azure Active Directory Connect sync agent. Which of the following is a valid command to run to configure the sync agent?

- A. Microsoft Azure Active Directory Connect Set-ADSyncScheduler -SyncCycle Start-ADSyncSyncCycle -CycleType Full
- B. PowerShell Set-ADSyncScheduler -SyncCycle Start-ADSyncSyncCycle -CycleType Full
- C. PowerShell Start-ADSyncSyncCycle -CycleType Full
- D. Microsoft Azure Active Directory Connect Set-ADSyncScheduler -SyncCycle Start-ADSyncSyncCycle -CycleType Full

Answer: A (LEAVE A REPLY)

ADatum

ADatum OU(OU=ADatum) is a Microsoft Azure AD Connect sync agent. Which of the following is a valid command to run to configure the sync agent?

NEW QUESTION: 51

User1 is a Microsoft Azure AD(Azure Active Directory) sync agent. Which of the following is a valid command to run to configure the sync agent?

User1 is a Microsoft Azure AD(Azure Active Directory) sync agent. Which of the following is a valid command to run to configure the sync agent?

Name	Platform	Registered in contoso.com
Device1	Windows 10	Yes
Device2	Windows 10	No
Device3	iOS	Yes

2020-11-05 contoso.com is a Microsoft Azure AD(Azure Active Directory) sync agent. Which of the following is a valid command to run to configure the sync agent?

ADatum: ADatum


ADatum: Contoso ADatum

□□□□ □□ □□□ □□□□□ □□: □□
□□□□ □□ □□□□ □□□□□ □□: □□
□□ □□: □□
□□□: 2020□ 12□ 10□
□□: □□

2020□ 11□ 15□□ User1□ Device3□ □□1□ □□□□□.
□□ □ □□ □□ □□ □□ □□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□□.
□□: □ □□□ □□□ 1□□ □□□ □□□□□.

 Statements	Yes	No
On November 20, 2020, User1 can accept Terms1 on Device1.	<input type="radio"/>	<input type="radio"/>
On December 11, 2020, User1 can accept Terms1 on Device2.	<input type="radio"/>	<input type="radio"/>
On December 7, 2020, User1 can accept Terms1 on Device3.	<input type="radio"/>	<input type="radio"/>

Answer:

 Statements	Yes	No
On November 20, 2020, User1 can accept Terms1 on Device1.	<input checked="" type="radio"/>	<input type="radio"/>
On December 11, 2020, User1 can accept Terms1 on Device2.	<input checked="" type="radio"/>	<input type="radio"/>
On December 7, 2020, User1 can accept Terms1 on Device3.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION: 52

□□□ □□□ □□ □□□ □□ □ □□ □□ □□□ □□□□ □□□.
□□□ □□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□□.
□□: □ □□□ □□□ 1□□ □□□ □□□□□.

To configure user access:

- An access package
- An access review
- A conditional access policy

To enable collaboration with fabrikam.com:

- An accepted domain
- A connected organization
- A custom domain name

Answer:



To configure user access:

- An access package
- An access review
- A conditional access policy

To enable collaboration with fabrikam.com:

- An accepted domain
- A connected organization
- A custom domain name

□□:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-organization>

NEW QUESTION: 53

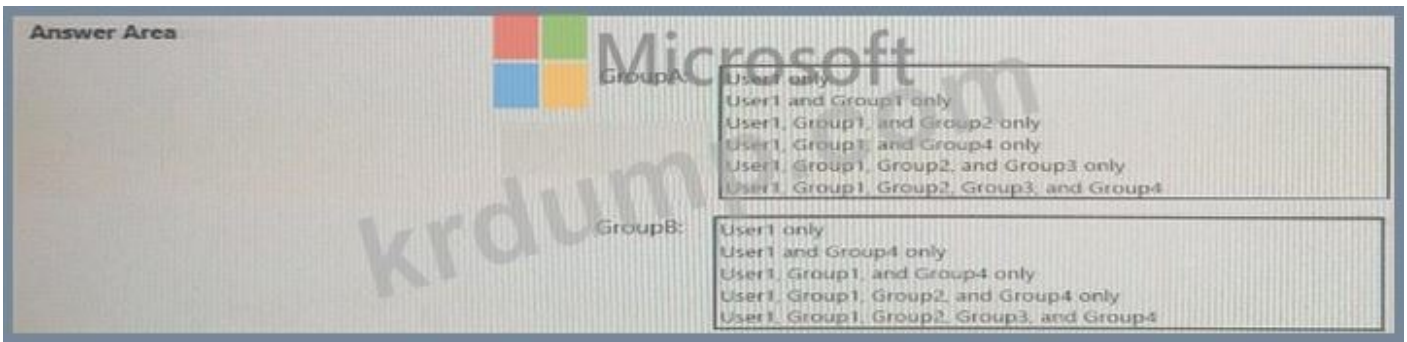
User1□□□ □□□□ □□ □□ □□□ □□□ □□□ Azure AD(Azure Active Directory) □□□ □□□□.

Name	Type	Membership type
Group1	Security	Assigned
Group2	Security	Dynamic User
Group3	Security	Dynamic Device
Group4	Microsoft 365	Assigned

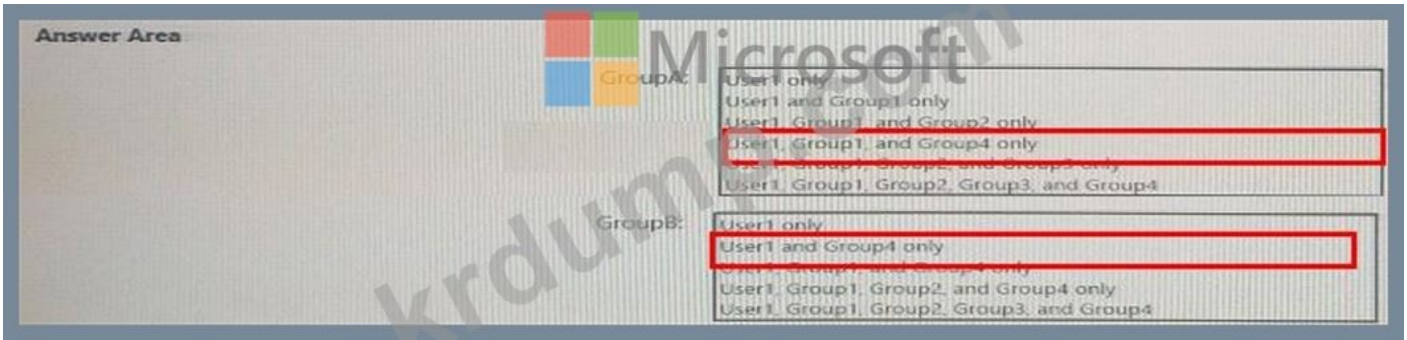
□□□□□ □□ □□ □□□ □□□ □□□□□.

Name	Type	Membership type
GroupA	Security	Assigned
GroupB	Microsoft 365	Assigned

GroupA□ GroupB□ □□ □□□□ □□□ □□□□□? □□□□□ □□□□ □□□ □□□ □ □□□□□. □□; □□□□ □□□ 1□□ □□□ □□□□.



Answer:



NEW QUESTION: 54

User1 Azure AD(Azure Active Directory) .

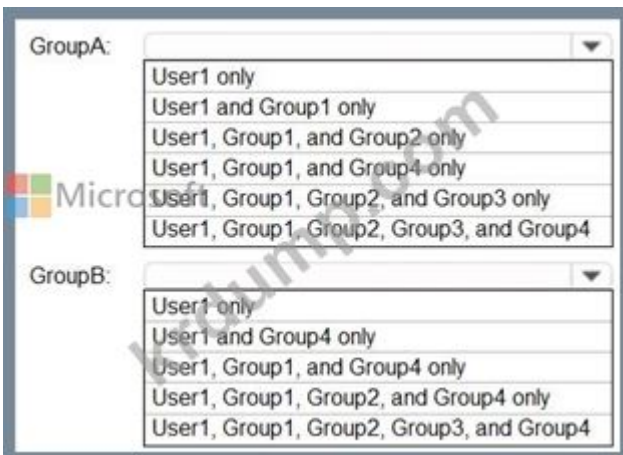
Name	Type	Membership type
Group1	Security	Assigned
Group2	Security	Dynamic User
Group3	Security	Dynamic Device
Group4	Microsoft 365	Assigned

.

Name	Type	Membership type
GroupA	Security	Assigned
GroupB	Microsoft 365	Assigned

GroupA GroupB ? .

: 1 .



Answer:

GroupA:

- User1 only
- User1 and Group1 only
- User1, Group1, and Group2 only
- User1, Group1, and Group4 only
- User1, Group1, Group2, and Group3 only
- User1, Group1, Group2, Group3, and Group4

GroupB:

- User1 only
- User1 and Group4 only
- User1, Group1, and Group4 only
- User1, Group1, Group2, and Group4 only
- User1, Group1, Group2, Group3, and Group4

□□:

<https://bitsizebytes.wordpress.com/2018/12/10/distribution-security-and-office-365-groups-nesting/>

NEW QUESTION: 55

Microsoft 365 E5 □□□□ □□□□.

App1□□□ □□□□ □□ □□□□□.

Microsoft Cloud App Security□ □□□□ App1□ □□□ □□ □□ □□□□□ □□□□□ □□ □.

□□ 4□□ □□□ □□□□ □□□□ □□□? □□□□□ □□ □□□□ □□ □□□ □□ □□ □□ □□□□ □□□ □□□□□□.

Answer:

NEW QUESTION: 56

contoso.com SMTP. Microsoft Exchange. Microsoft 365. Azure AD (Azure Active Directory). 4. contoso.com DNS TXT record.

Actions	Answer Area
Sign in to the Microsoft 365 admin center.	<div style="text-align: center;"> ← → </div>
Create a self-signed user account in the Azure AD tenant.	
From the Microsoft 365 admin center, add the domain name.	
Respond to the Become the admin message.	
From the Microsoft 365 admin center, remove the domain name.	
Create a TXT record in the contoso.com DNS zone.	

Answer:

Answer Area

Create a self-signed user account in the Azure AD tenant.

Sign in to the Microsoft 365 admin center.

Respond to the Become the admin message.

Create a TXT record in the contoso.com DNS zone.

1 - Azure AD tenant.

2 - Microsoft 365 admin center.

3 - Add the domain name.

4 - contoso.com DNS TXT record.

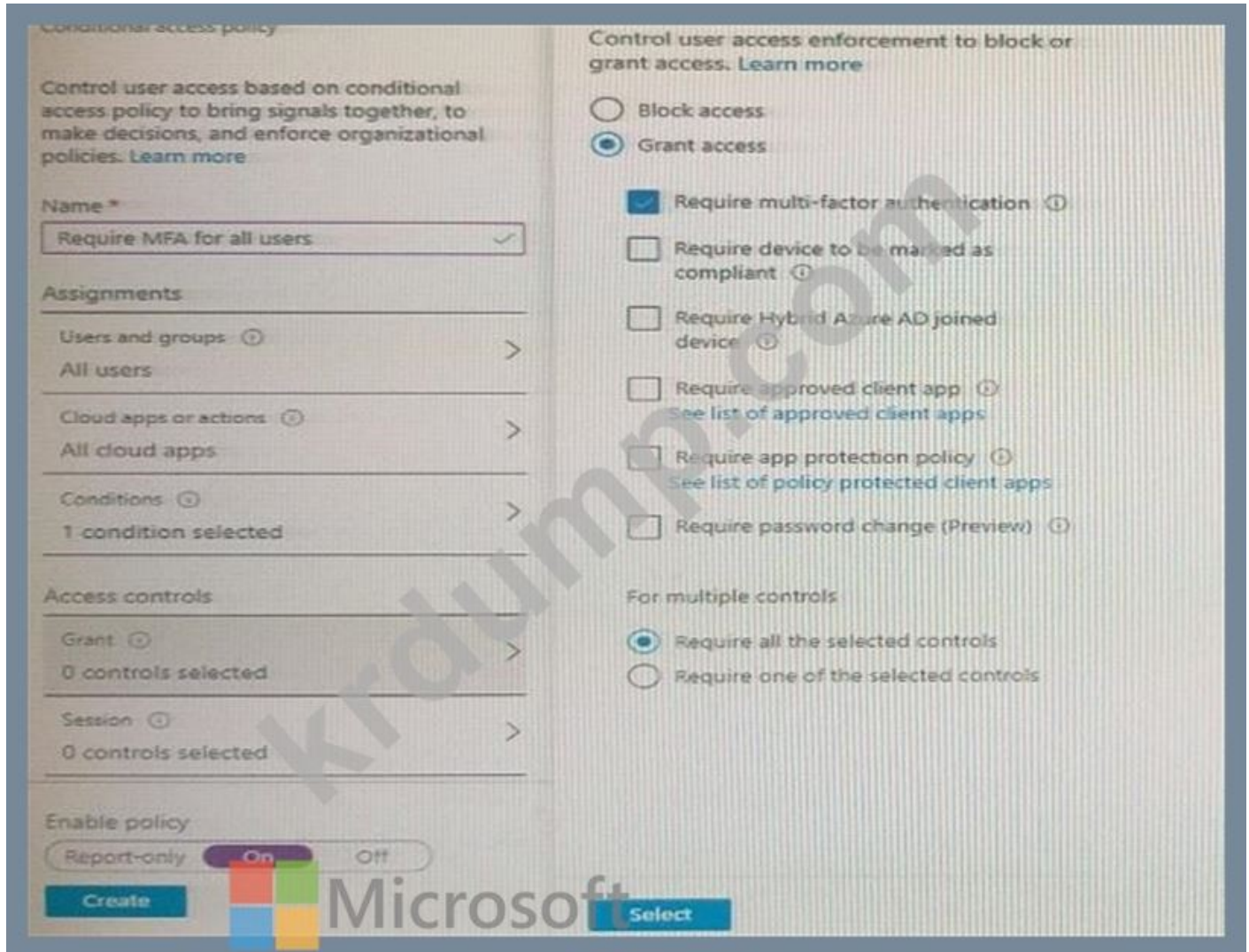
□□:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/domains-admin-takeover>

NEW QUESTION: 57

Microsoft 365 □□□□ □□□□.

□□□ □□□ □□ □□□ □□□ □□ □□□ □□□ □□□□□. (□□□ □□□ □□ □ □□□□□.)



□□ □□ □□ □□ □□□ □□□ □□ □□□ □□□ □□ □□□ □ □□□□□. (□□ □□ □ □□□□□.)

Privileged Identity Management > ContosoAzureAD > User Administrator >

Role setting details - User Administrator

Privileged Identity Management | Azure AD roles

Edit

Activation

Setting	State
Activation maximum duration (hours)	8 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	Yes
Approvers	1 Member(s), 0 Group

Assignment

Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	15 day(s)
Allow permanent active assignment	No
Expire active assignments after	1 month(s)
Require Azure Multi-Factor Authentication on active assignment	No
Require justification on active assignment	No

Which of the following statements are true? (Select all that apply.)

Admin1 can request activation of the User administrator role for a period of two hours.

Admin2: Admin3 can request 100 hours of activation.

Statements	Yes	No
Before Admin1 can perform a task that requires the User administrator role, an approver must approve the activation request.	<input type="radio"/>	<input type="radio"/>
Admin2 can request activation of the User administrator role for a period of two hours.	<input type="radio"/>	<input type="radio"/>
If Admin3 connects to the Azure Active Directory admin center, and then activates the User administrator role, Admin3 will be prompted to authenticate by using multi-factor authentication (MFA) twice.	<input type="radio"/>	<input type="radio"/>

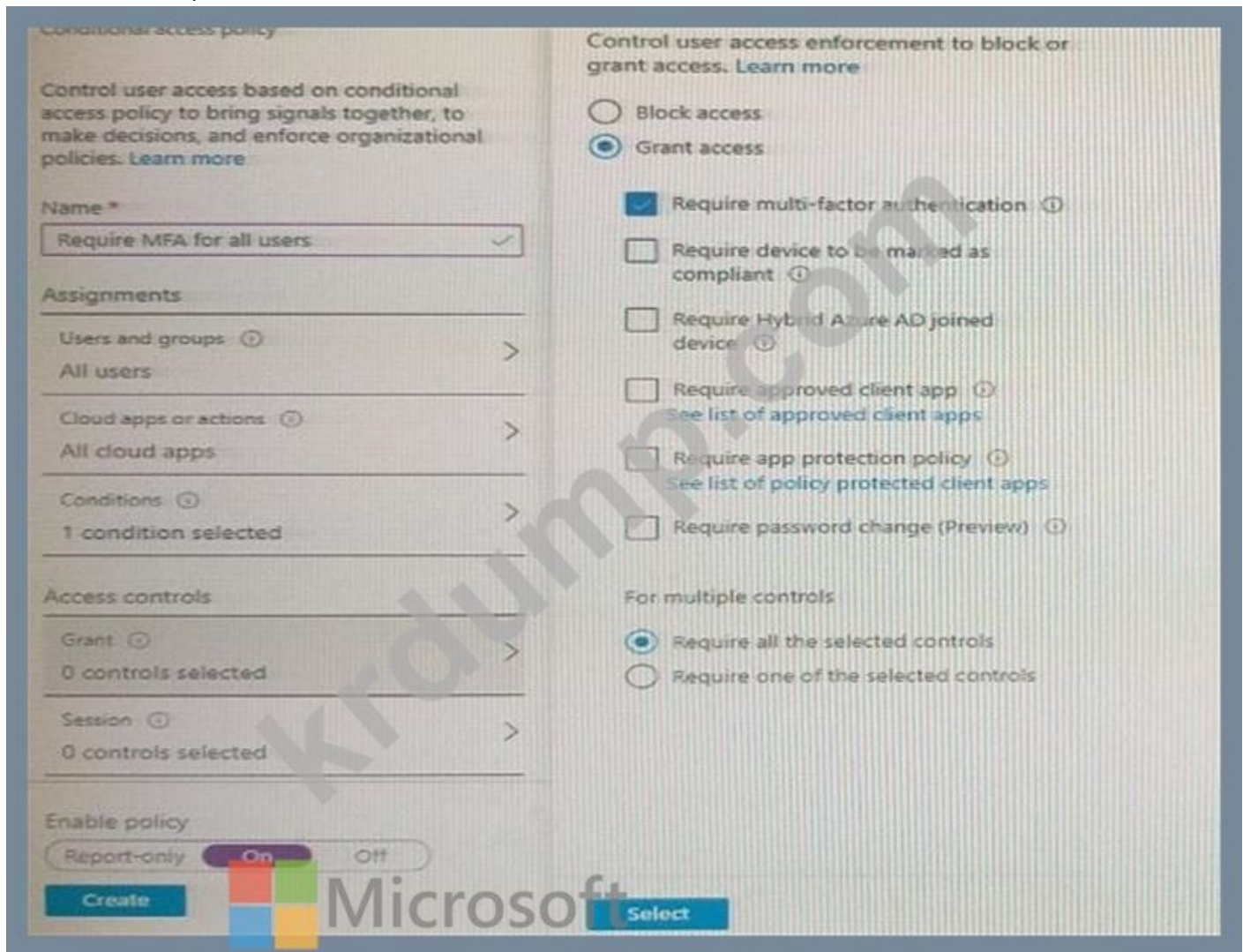
Answer:

Statements	Yes	No
Before Admin1 can perform a task that requires the User administrator role, an approver must approve the activation request.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can request activation of the User administrator role for a period of two hours.	<input type="radio"/>	<input checked="" type="radio"/>
If Admin3 connects to the Azure Active Directory admin center, and then activates the User administrator role, Admin3 will be prompted to authenticate by using multi-factor authentication (MFA) twice.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION: 58

Microsoft 365 Admin Center

□□□ □□□ □□ □□□ □□□ □□ □□□ □□□ □□□□□. (□□□ □□□ □□ □
□ □□□□□.)



□□ □□ □□ □□ □□□ □□□ □□ □□□ □□□ □□ □□□ □ □ □□□□. (□□ □□ □
□ □□ □□ □□□□□.)

Privileged Identity Management > ContosoAzureAD > User Administrator >

Role setting details - User Administrator

Privileged Identity Management | Azure AD roles

Edit

Activation

Setting	State
Activation maximum duration (hours)	8 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	Yes
Approvers	1 Member(s), 0 Group

Assignment

Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	15 day(s)
Allow permanent active assignment	No
Expire active assignments after	1 month(s)
Require Azure Multi-Factor Authentication on active assignment	No
Require justification on active assignment	No

Which of the following statements are true? (Select all that apply.)

Admin1 can request activation of the User administrator role for a period of two hours.

Admin2 can request activation of the User administrator role for a period of two hours.

Statements	Yes	No
Before Admin1 can perform a task that requires the User administrator role, an approver must approve the activation request.	<input type="radio"/>	<input type="radio"/>
Admin2 can request activation of the User administrator role for a period of two hours.	<input type="radio"/>	<input type="radio"/>
If Admin3 connects to the Azure Active Directory admin center, and then activates the User administrator role, Admin3 will be prompted to authenticate by using multi-factor authentication (MFA) twice.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
Before Admin1 can perform a task that requires the User administrator role, an approver must approve the activation request.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can request activation of the User administrator role for a period of two hours.	<input type="radio"/>	<input checked="" type="radio"/>
If Admin3 connects to the Azure Active Directory admin center, and then activates the User administrator role, Admin3 will be prompted to authenticate by using multi-factor authentication (MFA) twice.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION: 59

Which of the following statements are true? (Select all that apply.)

Name	Type
User1	User
Guest1	Guest
Identity1	Managed identity

Azure AD PIM (Privileged Identity Management) is used to manage access to Azure AD resources. Which of the following is a valid PIM role assignment?

- A. Guest1 as ID
- B. User1 as Guest1
- C. User1 as Identity1
- D. User1 as Identity1

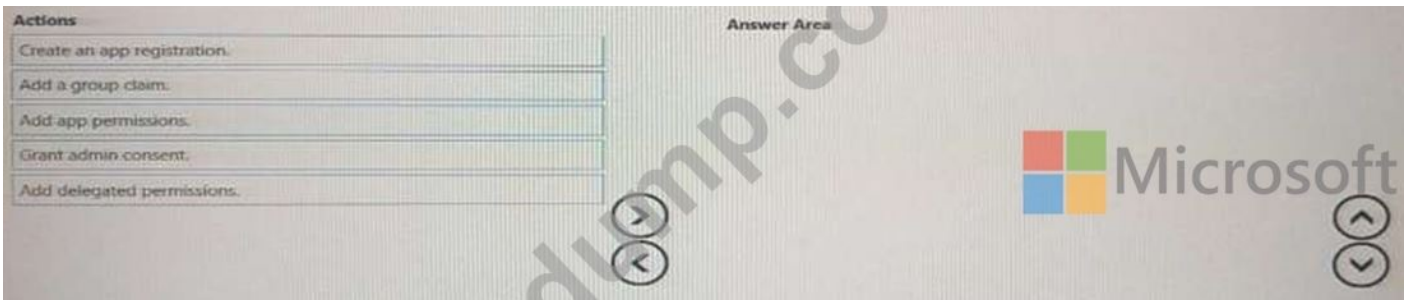
Answer: C (LEAVE A REPLY)

NEW QUESTION: 60

contoso.com is an Azure AD (Azure Active Directory) tenant. An application named App1 is registered in the tenant. App1 uses the Microsoft Graph API to access resources in the tenant. Which of the following is a valid permission for App1 to use the Microsoft Graph API?

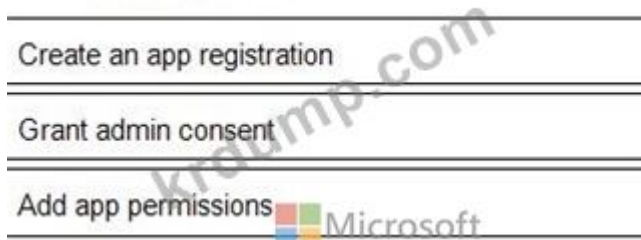
App1 needs to be granted the following permissions:

- 1. App1 needs to be granted the permission to read the user profile.
- 2. App1 needs to be granted the permission to read the user profile and the user's contacts.
- 3. App1 needs to be granted the permission to read the user profile and the user's calendar.
- 4. App1 needs to be granted the permission to read the user profile and the user's calendar and the user's contacts.



Answer:

Answer Area



- 1 - Add app permissions
- 2 - Grant admin consent
- 3 - Create an app registration

<https://docs.microsoft.com/en-us/graph/auth/auth-concepts>

NEW QUESTION: 61

Which of the following is a valid Azure AD role assignment?

□□□□ □□ □□□ □□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□ □□ □□□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.

The users must first:

Microsoft

- Provide consent for any app to access the data of Contoso.
- Register for multi-factor authentication (MFA).
- Register for self-service password reset (SSPR).

You must configure:

Microsoft

- A sign-in risk policy
- A user risk policy
- An Azure AD Password Protection policy

Answer:

The users must first:

Microsoft

- Provide consent for any app to access the data of Contoso.
- Register for multi-factor authentication (MFA).
- Register for self-service password reset (SSPR).

You must configure:

Microsoft

- A sign-in risk policy
- A user risk policy
- An Azure AD Password Protection policy

□□

The users must first:

Microsoft

- Provide consent for any app to access the data of Contoso.
- Register for multi-factor authentication (MFA).
- Register for self-service password reset (SSPR).

You must configure:

Microsoft

- A sign-in risk policy
- A user risk policy
- An Azure AD Password Protection policy

□□:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies>

SC-300 <https://www.dumptop.com/Microsoft/SC-300-dump.html> (346 Q&As Dumps, **30%OFF Special Discount: KrDump**)

NEW QUESTION: 62

Scenario: A company is planning to migrate its on-premises Active Directory to Azure AD. The company has the following environment:

Name	Description
Server1	Domain controller that runs Windows Server 2019
Server2	Server that runs Windows Server 2019 and has Azure AD Connect deployed
Server3	Server that runs Windows Server 2019 and has a Microsoft ASP.NET application named App1 installed
Server4	Unassigned server that runs Windows Server 2019
Firewall1	Hardware firewall connected to the internet that blocks all traffic unless explicitly allowed

The company wants to ensure that the migration process is successful. The company has the following requirements:

- Active Directory must be migrated to Azure AD (Azure Active Directory).
- Azure AD must be configured with Multi-Factor Authentication (MFA).
- Azure AD must be configured with App1.
- Server4 must be configured with the service to install on Server4.
- Rule to configure on Firewall1 must be configured.

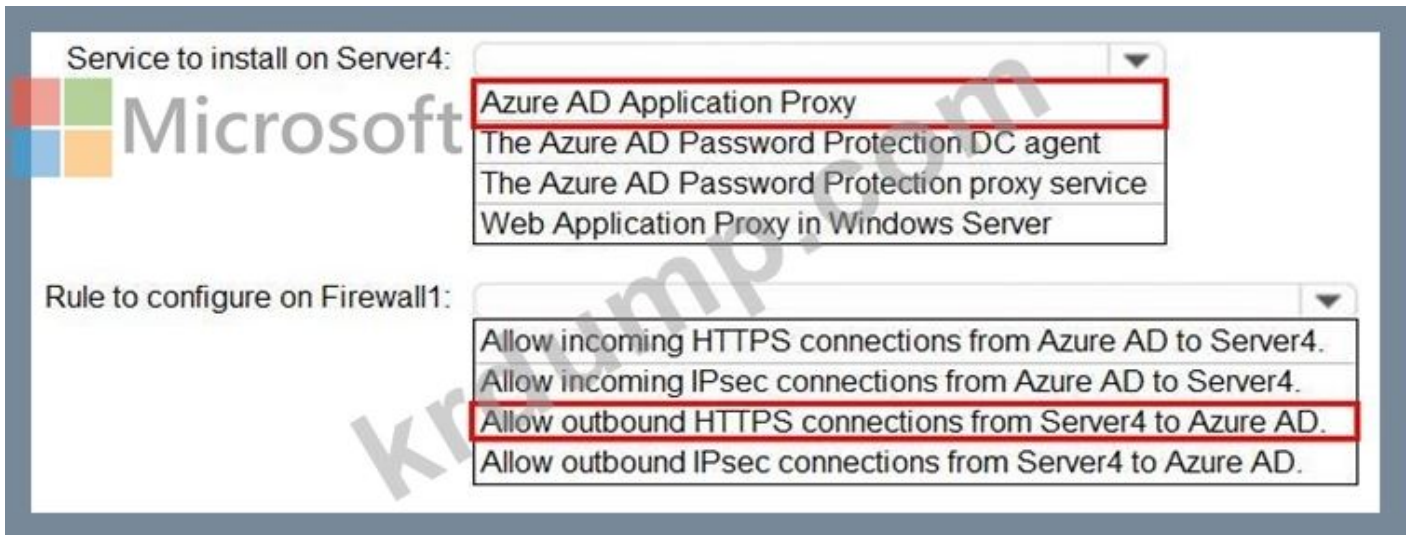
Service to install on Server4:

- Azure AD Application Proxy
- The Azure AD Password Protection DC agent
- The Azure AD Password Protection proxy service
- Web Application Proxy in Windows Server

Rule to configure on Firewall1:

- Allow incoming HTTPS connections from Azure AD to Server4.
- Allow incoming IPsec connections from Azure AD to Server4.
- Allow outbound HTTPS connections from Server4 to Azure AD.
- Allow outbound IPsec connections from Server4 to Azure AD.

Answer:

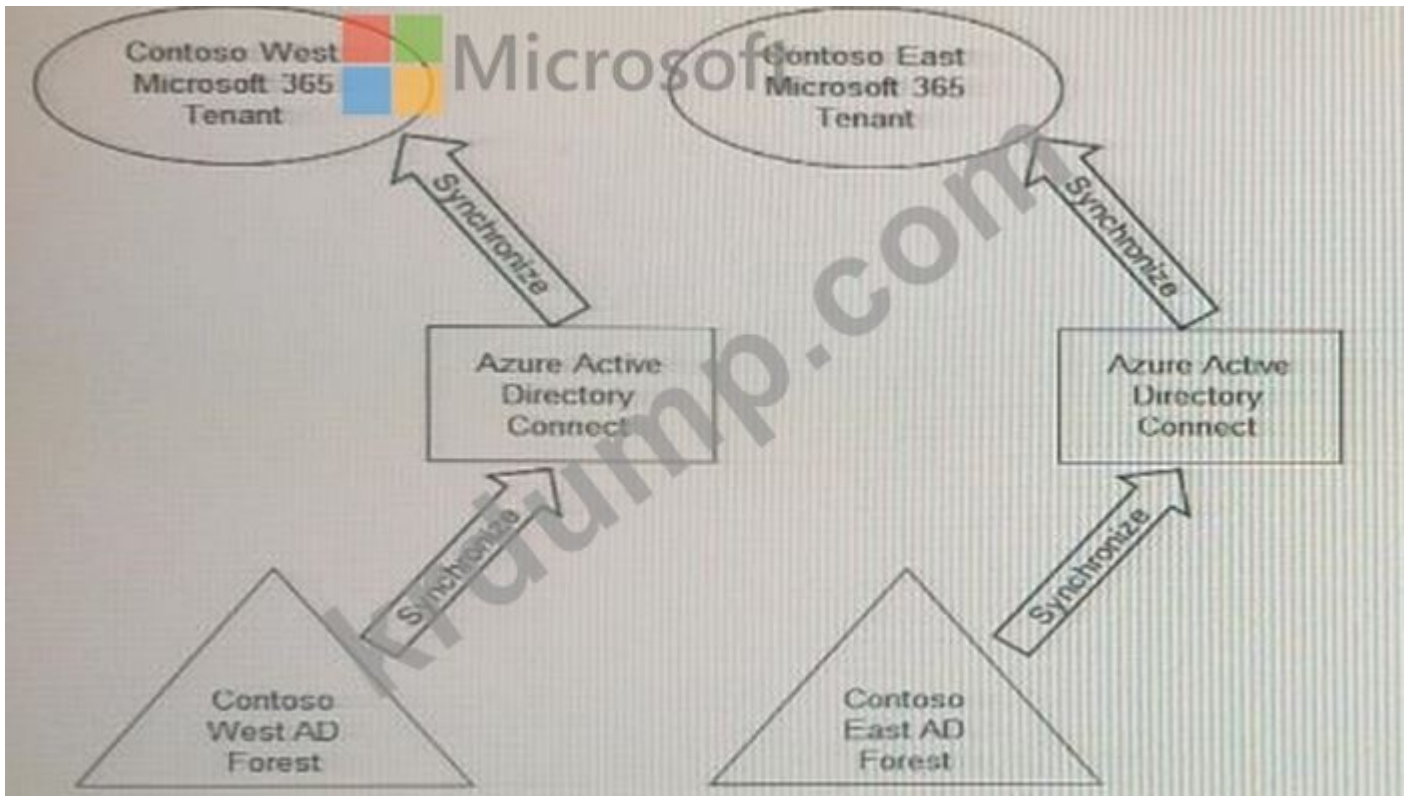


□□:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy>

NEW QUESTION: 63

□□□□ Contoso East □ Contoso West □□ □ □□ □□□□ □□□□. □ □□□ □□ Microsoft 365 ID □□□□□ □□ □□□□ □□ □□□□.



Contoso West □□□□ Microsoft SharePoint Online □□□□ □□ □□□ □□□ Contoso East □□□ □□□□□ □□□□ □□□. □□□□□ □□ Microsoft 365 □□□□□ □□□□ □□□ □□□.

□□□ □□□ □□ □□□?

A. West □□□□ □□ Contoso East □□□□ □□ □□□ □□□ □□□□.

B. Contoso East Active Directory □□□□□ Contoso West □□□□ □□□□□□ Contoso East □□ □□ Azure AD Connect □□□ □□□□□.

C. Contoso West Azure AD Connect Contoso East Active Directory

D. Azure AD Connect Contoso East Contoso East Active Directory Contoso West

Answer: A (LEAVE A REPLY)

NEW QUESTION: 64

Boston MFA. How can you ensure that users in Boston can access the application from their mobile devices?

- A. IP address range
B. IP address range
C. IP address range and IP address
D. IP address range and IP address

Answer: A (LEAVE A REPLY)

NEW QUESTION: 65

Microsoft 365 Exchange Online. How can you ensure that users can access their email from their mobile devices?

- A. Exchange Online
B. Exchange Online
C. Exchange Online and Exchange Online
D. Exchange Online and Exchange Online

Answer: C (LEAVE A REPLY)

URL:

https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

NEW QUESTION: 66

Microsoft 365 HighRiskCountries. How can you ensure that users can access their email from their mobile devices?



Answer:

Answer Area

Configure [redacted] countries by using:

Configure Sign-in frequency by using:

- A cloud app or action
- A condition
- A grant control
- A session control

- A cloud app or action
- A condition
- A grant control
- A session control

NEW QUESTION: 67

Azure AD(Azure Active Directory) [redacted] App1 [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted].

Save Discard Delete Got feedback? Yes No

Enabled for users to sign-in? Yes No

Name * App1

Homepage URL https://app1.m365x629615.onmicrosoft.com/

Logo AP

Select a file

User access URL https://myapps.microsoft.com/signin/App1/09d158d6-d29d-40de-b0d...

Application ID 09d158d6-d29d-40de-b0d0-321fd0630665

Object ID 03709d22-7e61-4007-a2a0-04dbdff269cd

Terms of Service Url Publisher did not provide this information

Privacy Statement Url Publisher did not provide this information

Reply URL https://contoso.com/App1/login

User assignment required? Yes No

App1 [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted].

Answer Area

[answer choice] can access App1 from the homepage URL

App1 will appear in the Microsoft Office 365 app launcher for [answer choice]

- All users
- No one
- Only users listed on the Owners blade
- Only users listed on the Users and groups blade

- all users
- no users
- only users listed on the Owners blade
- only users listed on the Users and groups blade

Answer:

Answer Area

[answer choice] can access App1 from the homepage URL

App1 will appear in the Microsoft Office 365 app launcher for [answer choice]

- All users
- No one
- Only users listed on the Owners blade
- Only users listed on the Users and groups blade

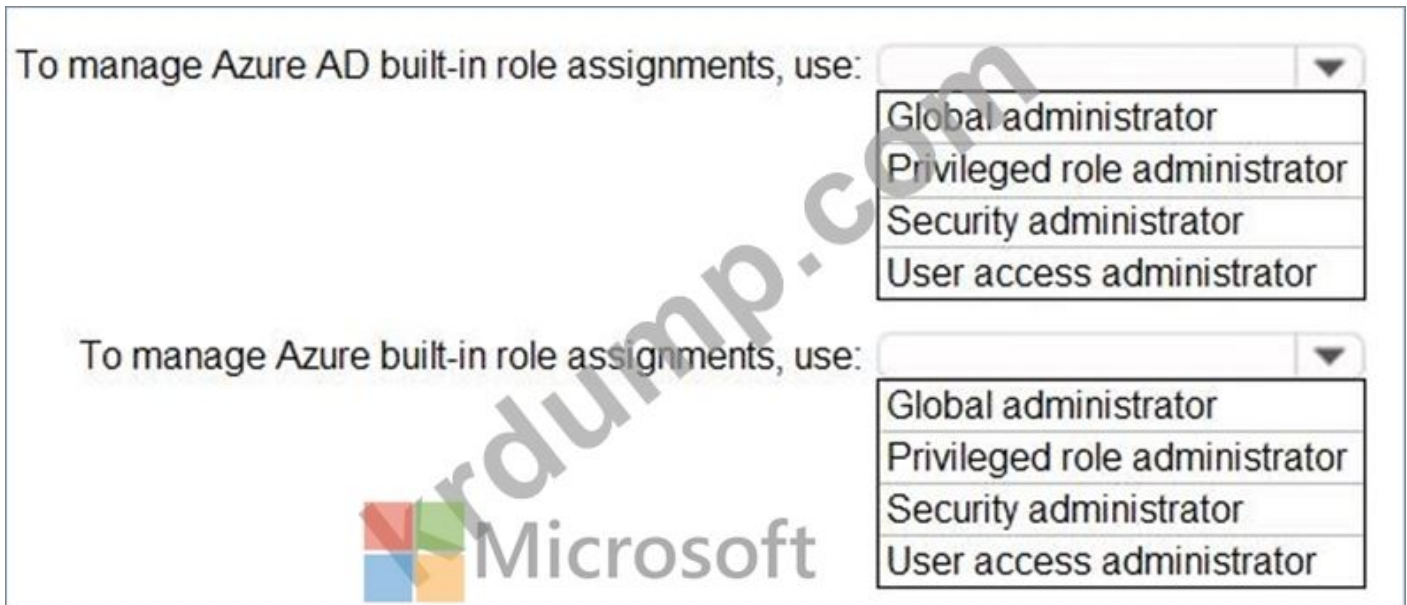
- All users
- no users
- only users listed on the Owners blade
- only users listed on the Users and groups blade

NEW QUESTION: 68

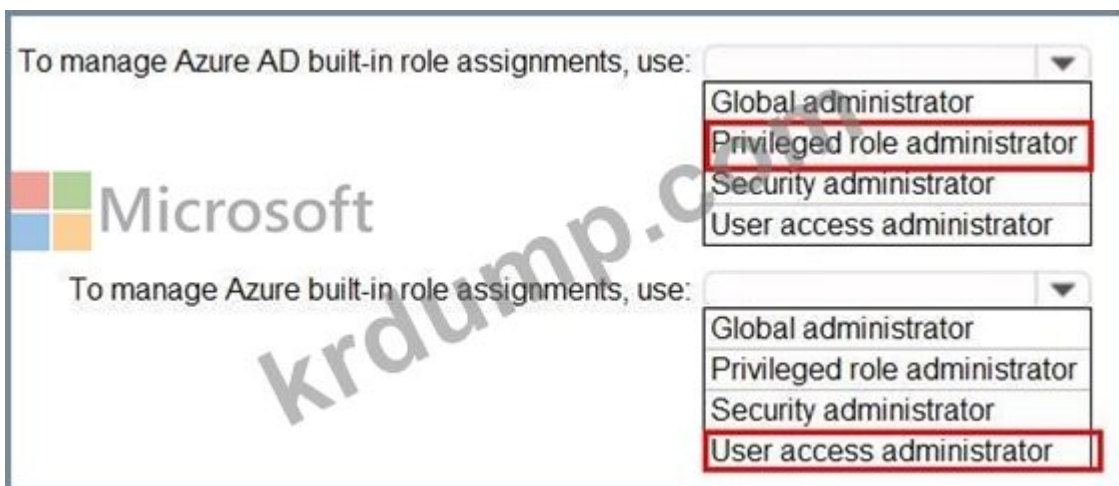
□□ □□□ □□□□ □ □□□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□.

□□□ □□□□□□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.



Answer:



□□:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal>

<https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

NEW QUESTION: 69

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □□□□ □ □□□□ □□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □□□ □□ □□□□ □□ □ □□□ □□ □ □□□ □□ □ □□□ □□ □ □□□.

□ □□□ □□□ □□ □□□ □□ □□ □□□□ □□□ □ □□□□. □□□□□ □□□ □□□ □□ □□□ □□□□ □□□□.

Microsoft 365 □□□□ □□□□.

10□□ □□□ □□□ 100□□ IT □□□□ □□□□.

□□□□ □□□□ □□□ □□□ □□□□□□. (□□ □□ □□□□□.)

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □□□□ □ □□□□ □ □□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □□□ □ □□ □□□□ □□ □ □□□ □□ □ □□□ □□ □□ □□□□ □□□ □□□□ □□ □ □□□□. □□□□ □□□ □□ □□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□□□ □□□ □□□ □□ □□□□ □□□□.

Microsoft 365 □□□□ □□□□.

10□□ □□□ □□□ 100□□ IT □□□□ □□□□.

□□□□ □□□□ □□□ □□□ □□□□□□. (□□ □□ □□□□□.)

Create an access review

Access reviews allow reviewers to attest to whether users still need to be in a role.

Review name *

Description

Start date *

Frequency

Duration (in days)

End Never End by Occurrences

Number of times

End date

Users

Scope Everyone

Review role membership (permanent and eligible) *
Application Administrator and 72 others

Reviewers

Reviewers

(Preview) Fallback reviewers

✓ Upon completion settings

Megan Bowen [redacted].
[redacted].
[redacted].
[redacted]?

- A. [redacted]
- B. [redacted]

Answer: B ([LEAVE A REPLY](#))

[redacted]:

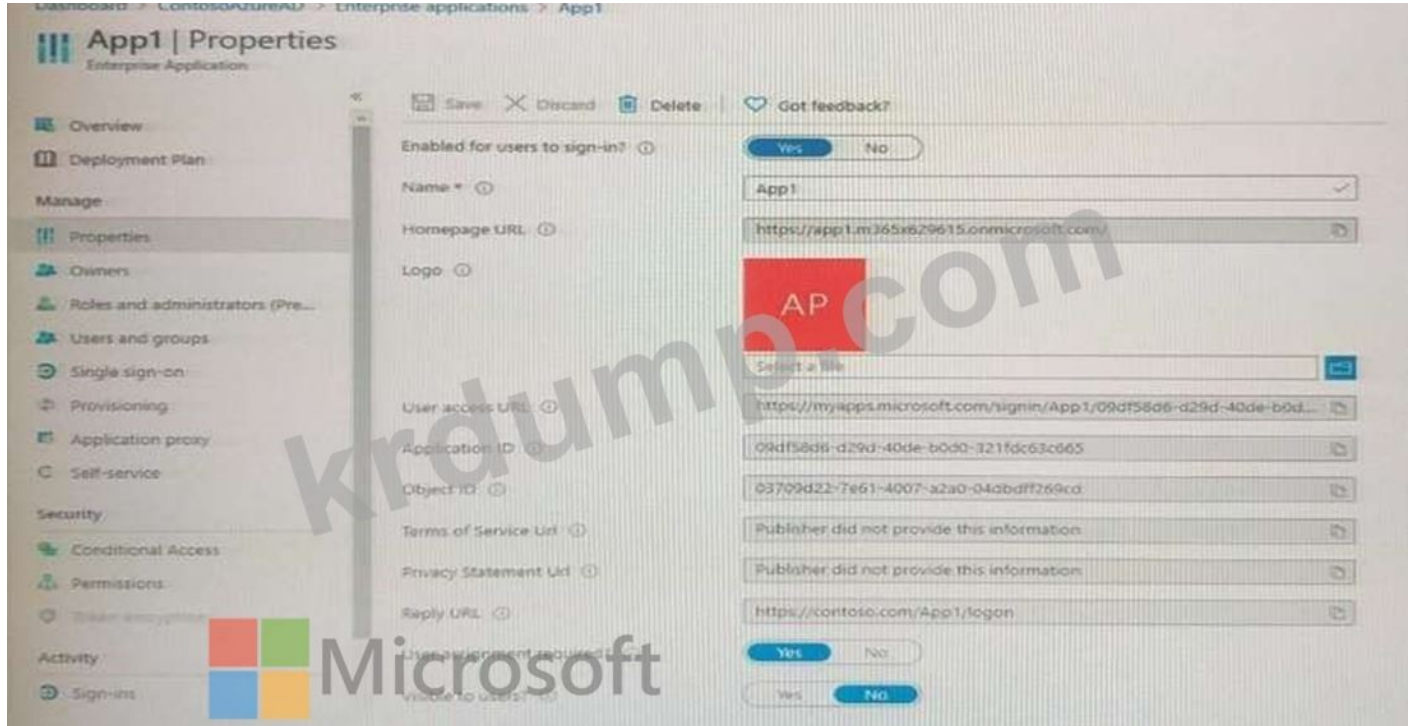
<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

NEW QUESTION: 71

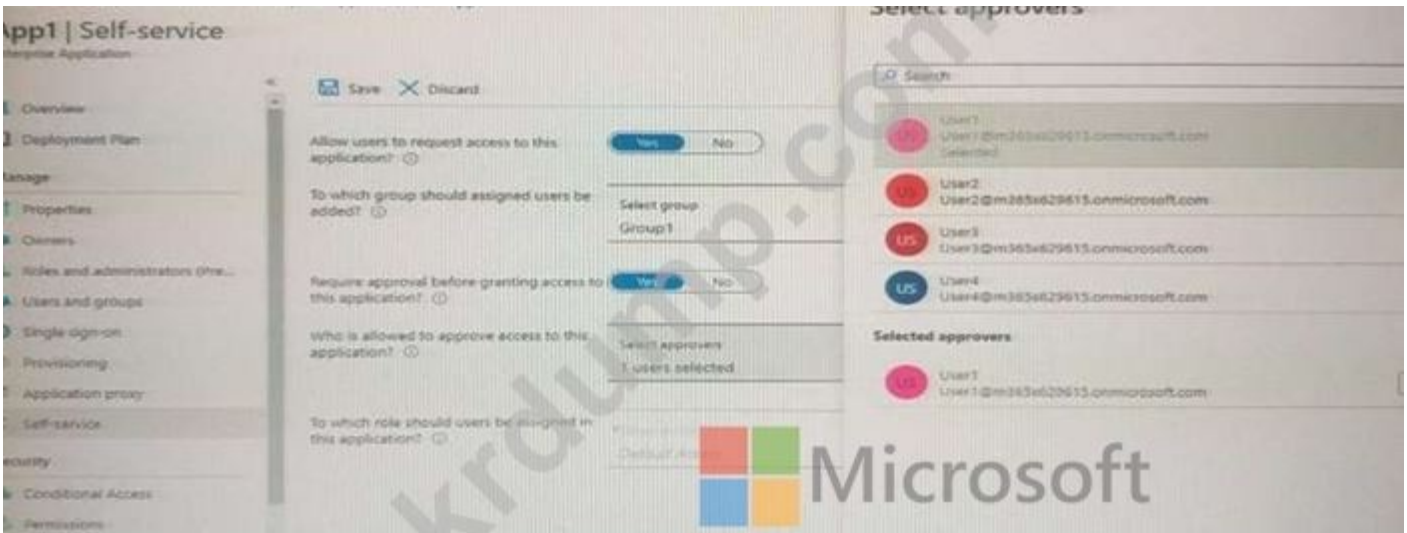
Group! [redacted] Microsoft 365 [redacted]. Group1 [redacted].
([redacted])



App1 [redacted] App1 [redacted]. (App1 [redacted].)



App1 [redacted] App1 [redacted] (App1 [redacted].)



contoso.com Microsoft 365 Enterprise application.
 Group1: Group1 100 users assigned.



Answer:



NEW QUESTION: 72

contoso.com Microsoft 365 Enterprise application.
 Group1: Group1 100 users assigned.
 Group2: Group2 50 users assigned.

User email	User type	Invitation accepted	Shared resource
User1@outlook.com	Guest	No	Enterprise application
User2@fabrikam.com	Guest	Yes	Enterprise application

Azure Active Directory Group1: Group1 100 users assigned.
 Group2: Group2 50 users assigned.

Collaboration restrictions

- Allow invitations to be sent to any domain (most inclusive)
- Deny invitations to the specified domains
- Allow invitations only to the specified domains (most restrictive)

 Delete

TARGET DOMAINS

Outlook.com  Microsoft

Microsoft SharePoint Online □□□□□ □□□□□ user3@adatum.com□ □□□□ □□□□□.
 □□ □ □□ □□ □□ □□ □□ □□□□□. □□□ □□□ □□□□ □□□□□□.
 □□: □ □□□ □□□ 1□□ □□□ □□□□□.

Statements	Yes	No
User1 can accept the invitation and gain access to the enterprise application.	<input type="radio"/>	<input type="radio"/>
User2 can access the enterprise application.	<input type="radio"/>	<input type="radio"/>
User3 can accept the invitation and gain access to the SharePoint site.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 can accept the invitation and gain access to the enterprise application.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can access the enterprise application.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can accept the invitation and gain access to the SharePoint site.	<input type="radio"/>	<input checked="" type="radio"/>

□□

Statements

Yes

No

User1 can accept the invitation and gain access to the enterprise application.

User2 can access the enterprise application.

User3 can accept the invitation and gain access to the SharePoint site.

Box 1:

outlook.com User1

Box 2:

outlook.com User2
User2

Box 3: No

outlook.com User3

NEW QUESTION: 73

Azure AD(Azure Active Directory) App1
App1

Enabled for users to sign-in? Yes No

Name

Homepage URL

Logo 

User access URL

Application ID

Object ID

Terms of Service Url

Privacy Statement Url

Reply Url

User assignment required? Yes No

Visible to users? Yes No

□□□□ □□□ □□□□ □□□□ □□□ □□□ □□□□ □ □□□ □□□□ □□□ □□□□
□□.
□□: □ □□□ □□□ 1□□ □□□ □□□□.

[answer choice] can access App1 from the homepage URL.

- All users
- No one
- Only users listed on the Owners blade
- Only users listed on the Users and groups blade

App1 will appear in the Microsoft Office 365 app launcher for [answer choice].

- all users
- no one
- only users listed on the Owners blade
- only users listed on the Users and groups blade

Answer:

[answer choice] can access App1 from the homepage URL.

- All users
- No one
- Only users listed on the Owners blade
- Only users listed on the Users and groups blade

App1 will appear in the Microsoft Office 365 app launcher for [answer choice].

- all users
- no one
- only users listed on the Owners blade
- only users listed on the Users and groups blade

□□:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal>

NEW QUESTION: 74

Litware □□□□ □□ Azure AD □□□□ □□□ □□□□ □□□. □□□□ □□□□ □□ □□ □ □□□□ □□□.

□□□ □□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.

Azure AD Connect settings to modify:

- Directory Extensions
- Domain Filtering
- Optional Features

Assign Azure AD licenses to:

- An Azure Active Directory group that has only nested groups
- An Azure Active Directory group that has the Assigned membership type
- An Azure Active Directory group that has the Dynamic User membership type

Answer:



NEW QUESTION: 75

contoso.com is a Microsoft 365 tenant. You need to ensure that all users in the tenant can use Microsoft 365 apps. You need to configure the tenant to support Microsoft 365 apps. What should you do?

- A. Configure the tenant to support Microsoft 365 apps.
- B. Configure the tenant to support Microsoft 365 apps.
- C. Configure the tenant to support Microsoft 365 apps.
- D. Windows Server Active Directory is not supported.

Answer: (SHOW ANSWER)

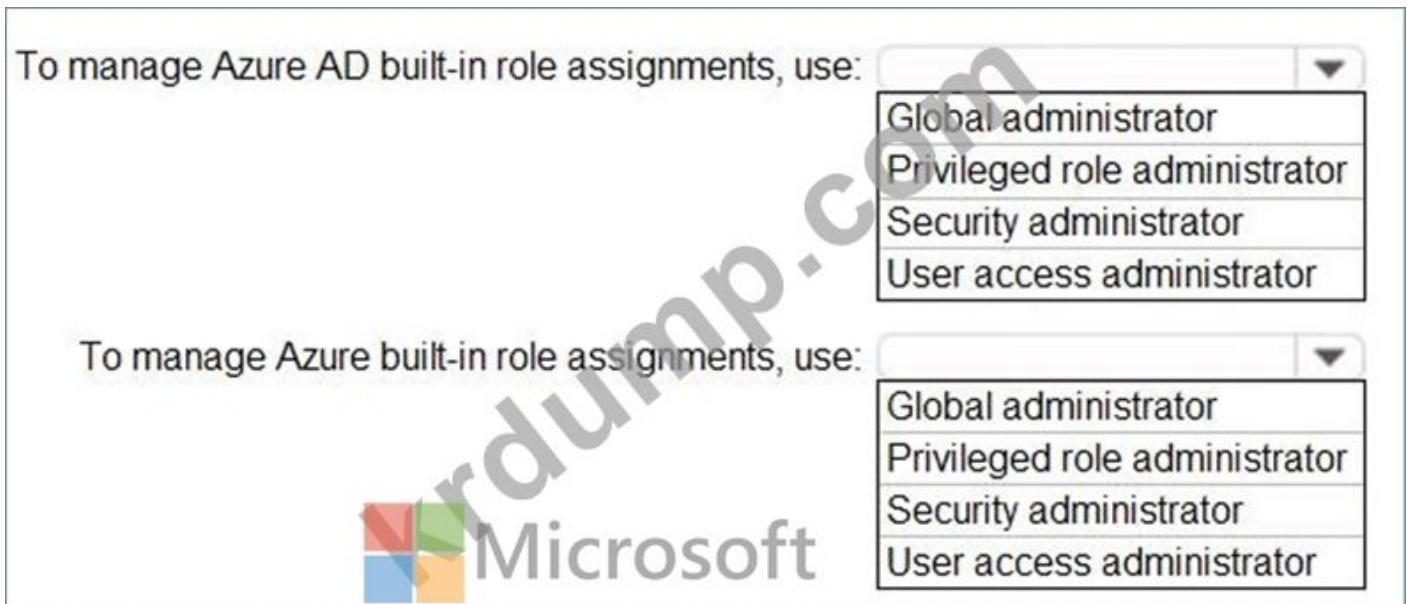
☐☐:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>

NEW QUESTION: 76

You are configuring an Azure AD tenant. You need to ensure that all users in the tenant can use Microsoft 365 apps. You need to configure the tenant to support Microsoft 365 apps. What should you do?

- ☐☐: ☐ ☐☐☐ ☐☐☐ 1☐☐ ☐☐☐☐☐☐☐.



Answer:



□□:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal>

<https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

SC-300 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ SC-300 □□! DumpTop
 □ □□ **SC-300** □□ □□□ □□□□□□, DumpTop SC-300 □□ □□□ □□□□□□□□
 □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop SC-300 □□□ □□□□□.
<https://www.dumpst.com/Microsoft/SC-300-dump.html> (346 Q&As Dumps, **30%OFF Special Discount: KrDump**)

NEW QUESTION: 77

contoso.onmicrosoft.com □ □□□ □□□ □□□□ □ Microsoft 365 □□□□ □□□□.
 □□□ □□ □□□ □□ contoso.com □ □□□□□.
 □ Microsoft 365 □□□□ □□ □□□ □□□□ contoso.com □ □□□□ □□□.
 □□ 4□□ □□□ □□□□ □□□□ □□□? □□□□□ □□ □□□□ □□ □□□ □□ □□
 □□ □□□□ □□□ □□□ □□□□□□□.

Actions

- Delete the contoso.onmicrosoft.com domain
- Register a custom domain name of contoso.com.
- Set the domain to primary.
- Create a new TXT record in DNS.
- Verify the domain name.

Answer Area

Microsoft

Krdump.com

Navigation arrows: left, right, up, down

Answer:

□□



□□:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-organization>

NEW QUESTION: 79

Azure AD(Azure Active Directory) □ □ □ □ App1 □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □.
App1 □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □.

[answer choice] can access App1 from the homepage URL.

▼

- All users
- No one
- Only users listed on the Owners blade
- Only users listed on the Users and groups blade

App1 will appear in the Microsoft Office 365 app launcher for [answer choice].

▼

- all users
- no one
- only users listed on the Owners blade
- only users listed on the Users and groups blade

Answer:

[answer choice] can access App1 from the homepage URL.

▼

- All users
- No one
- Only users listed on the Owners blade
- Only users listed on the Users and groups blade

App1 will appear in the Microsoft Office 365 app launcher for [answer choice].

▼

- all users
- no one
- only users listed on the Owners blade
- only users listed on the Users and groups blade

□□:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal>

NEW QUESTION: 80

Microsoft 365 □□□□ □□□□.

□□ □□□□ □□□□□□ □□□□ □□□ □□□□.

□□□□ Wi-Fi □□□□ □□ □□□ □□□ □□ □□ □□□□ □□ □□□□□□.

□□ □□□□ □□□□ □□ □□□□ □□□□ □□□□ □ □□ □□ □□□□□□ □□□ □□ □□□.

MFA(□□□□ □□)□ □□□ □□□□□□.

□□□□ □□ □□□□ □□□ □ □□ MFA □□ □□□ □□□□□□?

- A. Microsoft Authenticator □□ □□ □□
- B. □□ □□
- C. □□
- D. SMS

Answer: A (LEAVE A REPLY)

□□:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-authenticator-app#verification-code-from-mobile-app>

NEW QUESTION: 81

□□□□ □□□ □□ Azure AD(Azure Active Directory) □□ □□□ □□□□□. (□□ □□ □□ □□□.)

Custom smart lockout

Lockout threshold ⓘ ✓

Lockout duration in seconds ⓘ ✓

Custom banned passwords

Enforce custom list ⓘ Yes No

Custom banned password list ⓘ Contoso
 Litware
 Tailwind
 project
 Zettabyte
 MainStreet

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ Yes No
 Enforced Audit

□□ □□□□□ □□□□ □□□□.

* □□□□litw@re

* T@ilw1nd

* C0nt0s0

□□ □□□□□ □□□□□?

A. Pr0jectlitw@re □ T@ilw1nd □□

B. C0nt0s0□

C. C0nt0s0, Pr0jectlitw@re □ T@ilw1nd

D. C0nt0s0 □ T@ilw1nd □□

E. C0nt0s0 □ Pr0jectlitw@re □□

Answer: C (LEAVE A REPLY)

□□/□□:

<https://blog.enablingtechcorp.com/azure-ad-password-protection-password-evaluation>

NEW QUESTION: 82

Microsoft 365 □□□□ □□□□.

Azure AD(Azure Active Directory)□□ □□ □□□ □□□□□.

□□ □□□ □□□□ □□□□ □□□□ □□□□ □ □□□ □□ □□□. □□ □□□

□ □□□□ □□□□ □□□.

□□□ □□□□ □□□?

A. Microsoft Cloud App Security□ □□□ □□□□□.

B. Microsoft Endpoint Manager□ □□ □□.

C. Azure AD□ □□□ □□□ □□

D. Microsoft Endpoint Manager□ □□ □□ □□

Answer: C (LEAVE A REPLY)

□□:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use>

NEW QUESTION: 83

Azure AD(Azure Active Directory) □□□□ □□□□.

□□□ □□□ □□□□ □□□□□ Azure AD □□□ □□□ □□□□ □□□.

Azure AD□ □□□ □□□ □□□□ □□ □□ □□□□□?

A. 365□

B. 30□

C. 14□

D. 90□

Answer: B (LEAVE A REPLY)

NEW QUESTION: 84

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □□□□ □ □□□□ □

□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □□□ □

□□ □□□□ □□ □ □□□ □□ □□ □□□□ □□□ □□□□ □□ □ □□□□.

□ □□□ □□□ □□ □□□ □□ □□□□ □□□ □ □□□□. □□□□□ □□□ □□□ □□

□□□ □□□□ □□□□.

Microsoft 365 □□□□ □□□□.

□□ □□□□ Microsoft 365 □□□□ □□□□ □ MFA(□□□□ □□)□ Microsoft Authenticator

□□ □□□□ □□□.

□□ □□□□ □□□ □□□ □□□□ □□ Microsoft Authenticator □□□ MFA □□□□□ □□

□□ □□□□□.

□□□□ □□□□ □□ MFA □□□ □□□□ □□□□ □□□□ □□□□ □□□.

□□□: Azure Portal□□ MFA(□□□□ □□)□ □□ □□ □□□ □□□□□.

□□□ □□□ □□□□□□?

A. □

B. 000

Answer: B (LEAVE A REPLY)

00 00 000 0000 000.

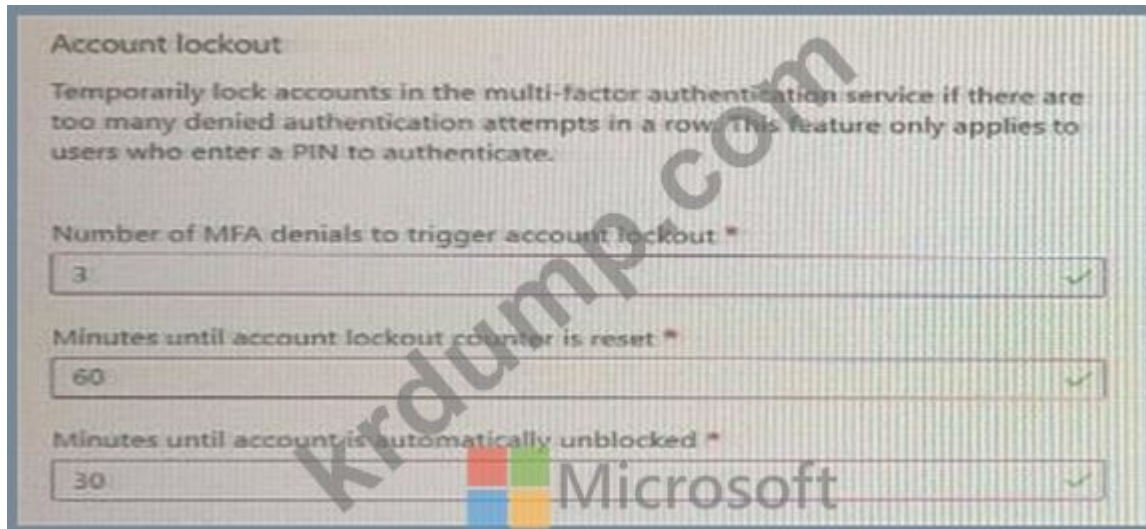
00:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings>

NEW QUESTION: 85

MFA(000 00)0 0000 Azure AD(Azure Active Directory) 0000 0000.

00 00 000 00 000 00 000000.

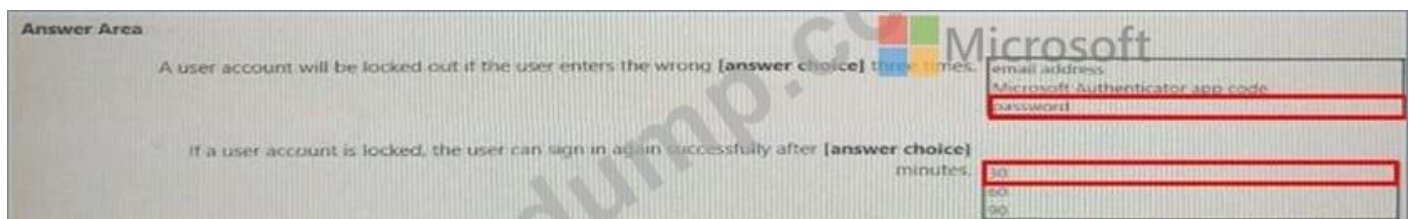


0000 000 0000 0000 000 000 0000 0 000 0000 000 0000
00.

00: 0 000 000 100 000 0000.



Answer:



NEW QUESTION: 86

00: 0 000 000 000000 0000 000 00 0 000000. 0000 0 0000 0
00 000 000 0 00 000 0000 0000 0000. 00 00 0000 0 000 0
00 0000 00 0 000 00 0000 000 0000 00 0 0000.
0 000 000 00 000 00 0000 000 0 0000. 000000 000 000 00
000 0000 0000.

Azure Monitor0 0000 Azure AD(Azure Active Directory) 00 0000 000000.

NEW QUESTION: 89

□□ □□ □□□ □□□□ □□□□ Azure AD(Azure Active Directory) □□□□ □□□□.

Name	Type	Directory synced
User1	Member	Yes
User2	Member	No
User3	Guest	No

□□ □□□□ □□ Azure AD□□ □□ □□ □□ □□ □□ □□ □□ □□□□? □□□□□□
 □□ □□□□ □□□ □□□ □□□□□□□□.
 □□: □ □□□ □□□ 1□□ □□□ □□□□□.

Answer:

NEW QUESTION: 90

□□□ □□□ □□□ □□□□ □□ □□ □□ □□□ □□□□ □□□□.
 □□□□ □□ □□□ □□ □□ □□□ □□□□ □□□□? □□□□□□ □□ □□□□ □□□□ □□□ □□
 □ □□□□□□□.
 □□: □ □□□ □□□ 1□□ □□□ □□□□□.

Answer:

Answer Area:

The users must first:

- Provide consent for any app to access the data of Contoso.
- Register for multi-factor authentication (MFA).
- Register for self-service password reset (SSPR).

You must configure:

- A sign-in risk policy.
- A user risk policy.
- An Azure AD Password Protection policy.

NEW QUESTION: 91

User1, User1, User3, Group1, Azure AD(Azure Active Directory), Group1, User2, User3, Group1, Azure AD PIM(Privileged Identity Management), Group1.

Role setting details - Application Administrator

Privileged Identity Management | Azure AD roles

Edit

Activation	
Setting	State
Activation maximum duration (hours)	5 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
Require approval to activate	Yes
Approvers	0 Member(s), 1 Group(s)
Assignment	
Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	3 month(s)
Allow permanent active assignment	No
Expire active assignments after	1 month(s)
Require Azure Multi-Factor Authentication on activation	No
Require justification on active assignment	Yes

Group1, User1, User3, Group1, Azure AD(Azure Active Directory), Group1, User2, User3, Group1, Azure AD PIM(Privileged Identity Management), Group1.



Which of the following statements are true?
Select all that apply.

Statements	Yes	No
User1 is assigned the Application administrator role automatically.	<input type="radio"/>	<input type="radio"/>
When User2 requests to be assigned the Application administrator role, only User3 can approve the request.	<input type="radio"/>	<input type="radio"/>
If a request by User1 to be assigned the Application administrator role is approved on January 31, 2021, at 23:00, User1 can use the role until February 1, 2021, at 04:00.	<input type="radio"/>	<input type="radio"/>

Answer:

SC-300 DumpTop SC-300! DumpTop
SC-300, DumpTop SC-300
<https://www.dumptop.com/Microsoft/SC-300-dump.html> (346 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

NEW QUESTION: 92

Which of the following are valid Azure AD(Azure Active Directory) objects?

- * Device1
- * User1, User2, User3, User4, User5
- * Group1, Group2, Group3, Group4, Group5

Name	Type	Membership type	Members
Group1	Security	Assigned	User1, User3, Group2, Group3
Group2	Security	Dynamic User	User2
Group3	Security	Dynamic Device	Device1
Group4	Microsoft 365	Assigned	User4
Group5	Microsoft 365	Dynamic User	User5

Which of the following groups are Microsoft Office 365 Enterprise E5 licensed?

- A. Group1 and Group4
- B. Group1, Group2, Group3, Group4 and Group5
- C. Group1 and Group2
- D. Group1
- E. Group1, Group2, Group4 and Group5

Answer: C (LEAVE A REPLY)

Source:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced>

NEW QUESTION: 93

Group1 is a Security group in an Azure Active Directory tenant. Group1 is a member of Group2, which is a Microsoft 365 group. (Group1 is not a member of Group3.)

```
PS C:\> Get-AzureADGroup -searchstring "group1" | Get-AzureADGroupowner

ObjectID                               DisplayName  UserPrincipalName                UserType
-----
a7f7d405-636f-4493-b971-5c2b7a131b1c Admin        admin@M365x629615.onmicrosoft.com Member

PS C:\> Get-AzureADGroup -searchstring "group1" | Get-AzureADGroupMember | ft displayname

DisplayName
-----
User1
User4
Group3
```

App1 is a Microsoft 365 group in an Azure Active Directory tenant. App1 is a member of Group1, which is a Security group. (App1 is not a member of Group2.)

App1 | Self-service

Enterprise application

- Overview
- Deployment Plan
- Manage
 - Properties
 - Owners
 - Roles and administrators (Pre...
 - Users and groups
 - Single sign-on
 - Provisioning
 - Application proxy
 - Self-service
- Security
 - Conditional Access
 - Permissions

Save Discard

Allow users to request access to this application? Yes No

To which group should assigned users be added? Select Group Group1

Require approval before granting access to this application? Yes No

Who is allowed to approve access to this application? Select approvers 1 users selected

To which role should users be assigned in this application? * Default Access

Select approvers

Search

- User1
User1@m365x629615.onmicrosoft.com
Selected
- User2
User2@m365x629615.onmicrosoft.com
- User3
User3@m365x629615.onmicrosoft.com
- User4
User4@m365x629615.onmicrosoft.com

Selected approvers

- User1
User1@m365x629615.onmicrosoft.com

□□ □ □□ □□ □□ □□□□. □□□ □□□ □□□□ □□□□□□.
□□: □ □□□ □□□ 1□□ □□□ □□□□.

Answer Area

Statements

Yes

No

The members of Group3 can access App1 without first being approved by User1.

After you configure self-service for App1, the owner of Group1 is User1.

App1 appears in the Microsoft Office 365 app launcher of User4.

Answer:

Answer Area

Statements

Yes

No

The members of Group3 can access App1 without first being approved by User1.

After you configure self-service for App1, the owner of Group1 is User1.



App1 appears in the Microsoft Office 365 app launcher of User4.

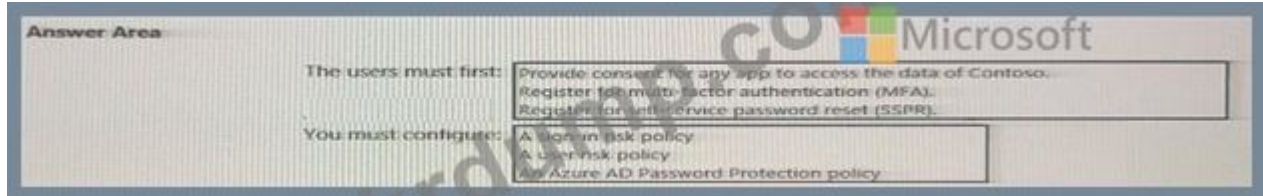
NEW QUESTION: 94

□□□ □□□ □□□ □□□□ □□ □□ □□ □□□□ □□□□.

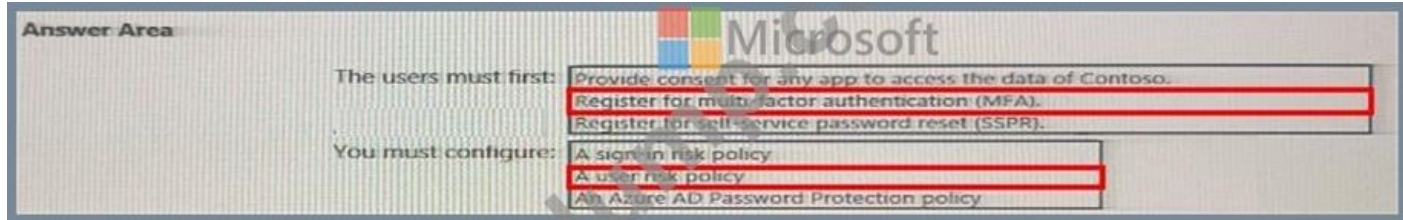
□□□□ □□ □□□ □□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□

□ □□□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.



Answer:



NEW QUESTION: 95

Microsoft 365 □□□□ adatum.com□□□□ Active Directory □□□□ □□□□.

Express □□□ □□□□ Azure AD Connect□ □□□□□.

□□ □□ □□□ □□□□□ SSPR(□□ □□□ □□ □□□)□ □□□□ □□□.

□□□□ □□□□□ □□□□□ □□□ □ □□□ □□□□□ □□ □□□ □ □□ □□ □□□

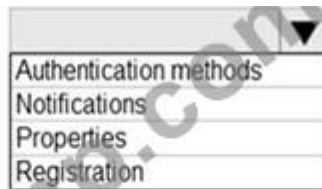
□□□□□ □□□□ □□□□□ □□□.

□□□ □□□□ □□□ □□□□ □□□□ □□□ □□ □□□ □□□□□ □□□.

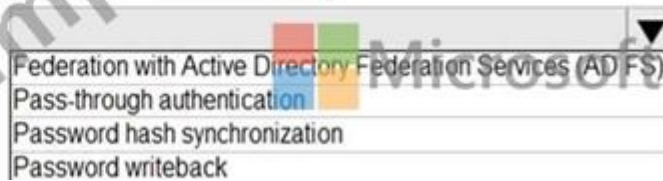
□□□ □□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.

From the Password reset blade in the Azure Active Directory admin center, configure:

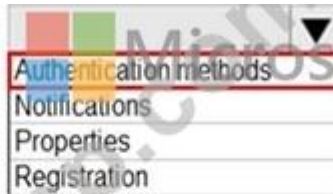


From Azure AD Connect, enable:

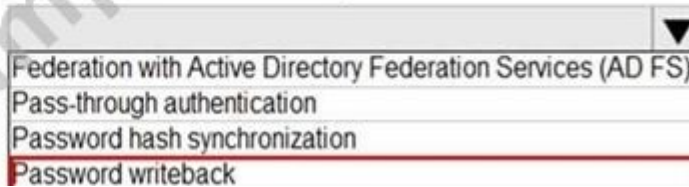


Answer:

From the Password reset blade in the Azure Active Directory admin center, configure:



From Azure AD Connect, enable:



□□:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment>

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-security-questions>

NEW QUESTION: 96

□□□ □□ □□□ □□ □□ □□ □□□ □□□□ □□□.

□□□ □□□ □□ □□□?

A. Azure AD Connect□□ PingFederate□□ □□□□□□ □□□□□□.

B. Azure AD □□ □□□ □□□□□.

C. Azure AD Connect□□ □□ □□ □□□□ □□□□□□.

D. Azure AD□□ □□ □□ □□□ □□□□□.

Answer: C (LEAVE A REPLY)

□□:

<https://docs.microsoft.com/en-us/azure/security/fundamentals/steps-secure-identity>

□□ 1, Litware, Inc

ID □□

□□□□□□ litware.com□□□ Azure AD(Azure Active Directory) □□□□ □□□ litware.com

□□□ Active Directory □□□□□ □□□□ □□□□. Azure AD Connect□ □□ □□□ □□□

□ □□ □□ □□□□ □□□□□□ □□□□.

Litware.com□□ □□ □□□□□□ □□□ □□□□ User1□□□ □□□□ □□□□. Litware□

Azure AD □□□□□□ □□□□ □□□□□.

Fabrikam□□ fabrikam.com□□□ Azure AD □□□□ □□□□. Fabrikam□ □□□□

litware.com □□□□ □□□ □□□ □□□□ litware.com□ □□□□ □□□□□□.

□□□□ □□

Litware□ □□ □□□□ Microsoft 365 Enterprise E5 □□□□□ □□□□ □□□□. Microsoft Cloud App Security□ □□ □□ □□ □□ □□ □□□□□□.

Litware□□ litware.com Azure AD □□□□ □□□□ Azure □□□□ □□□□. □□□□ Azure Active Directory □□□ □ Office 365 □□□□ □□□□ Azure Sentinel □□□□□ □□□□ □ □□□. Azure Sentinel□ □□ Azure AD □□□□ □□ □ □□ □□□ □□□□□.

□□□□□ □□

□□□□□ □□□□□□ □□ □□ □□□ □□□ □□□□□.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

□ Litware □□□ □□ □□□□ □□ □□□□□. □ □□□□ □□□ □ VPN □□□ □□□□ Azure □□□ □□ □□□□□ □□□□□. □□ □□□□□ □□□ □□□□□ □□□□ □□□ □□ □□□□□.

□□ □□

Litware□ □□ □□ □□ □□□ □□□□□.

- * Azure AD PIM(Privileged Identity Management)□ □□□□ □□ □□ □□ □□□ □□□□□.
- * □□□ □□ □□□□□ litware.com Azure AD □□□□ □□□□□□□□ □□□□ □□□□ □□-
- * Identity Governance□ □□ □□□ □□ □□□□ □ □□□ □□ □□□□□ □□□□□.
- * User1□ Azure AD□□ □□□□□□□ □□□□□□□ □□ □ □□□ □□□□□. □□ □□ □ □□ □□□□□.

□□□□ □□ □□

Litware□ □□ litware.com Active Directory □□□□□ LWLicenses□□ □□□ □□ □□□ □□ □□□□□□. Litware□ LWLicenses □□ □□ □□□□□ Azure AD □□□□ □□□ □□□□ □□□□. LWLicenses□ □□ □□□ □□ □□ □□□□ □□□ □□□□□ □□□□□ Microsoft 365 □□□ □□□□ □□□□□ □□□.

□□ □□ □□

Litware□ LWGroup1□□□ □□□ □□□□ □□□. □ □□□□ Litware□ □□ □□ Azure AD □□□ □□□ □□□□□ □□ Azure AD □□□ □□□ □□□□□.

□□ □□ □□

Litware□ □□ □□ □□ □□□ □□□□□.

- * □□ Litware □□□□ □□ □□□ □□(MFA)□ □□□□□.
- * □□□□ MFA□ □□□□□ Litware□ Boston □□□□□ Azure AD□ □□□□ □□ □□□□□.
- * litware.com □□□□□ □□ □□□ □□□□ □□□ □□□□□.
- * □□□□□ □□□□□□□□ □□□□ □ MFA□ □□□□□.
- * □□□□□ □□□ □□ □□ □□□□ □□□□ □□□□□.

□□□ □□ □□

Litware□ Litware□ □□ □□ Azure AD □□□ □□□ □□□□□ □□ Azure AD □□□ □□□ □□□□ LWGroup1□□□ □□□ □□□□ □□□.

□□□□ □□ □□

Litware□ Azure Sentinel□ Fusion □□□ □□□□ □□□□□ Azure AD □□□□ □□□□□ Microsoft Office 365 □□□ □□□ □□□□ □□□□ □□□□□ □□□.

NEW QUESTION: 97

□□ □□□ □□□□ □ □□□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □ □□.

□□□ □□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.

The screenshot shows two dropdown menus. The top one is titled "To manage Azure AD built-in role assignments, use:" and lists: Global administrator, Privileged role administrator, Security administrator, and User access administrator. The bottom one is titled "To manage Azure built-in role assignments, use:" and lists the same four roles. A Microsoft logo is visible at the bottom of the screenshot.

Answer:

The screenshot shows a "You must configure:" section with a list of requirements: Assign a sign-in risk policy, Assign a user risk policy, and Assign an Azure AD Password Protection policy. Above this, a "The users must first:" section lists: Provide consent for any app to access the data of Contoso, Register for multi-factor authentication (MFA), and Register for self-service password reset (SSPR). A Microsoft logo is visible on the left.

□□



☐☐:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal>

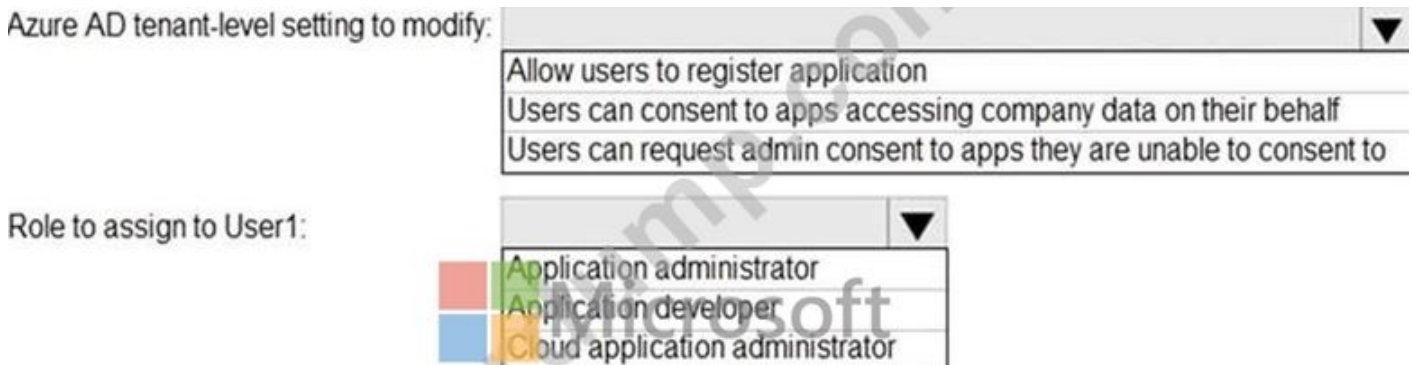
<https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

NEW QUESTION: 98

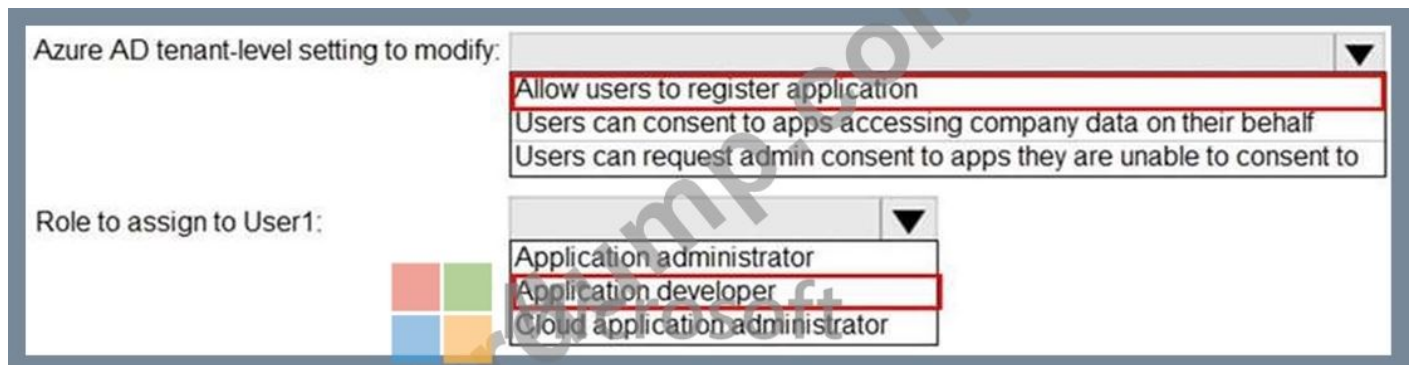
☐☐ ☐☐ ☐☐☐ ☐☐☐☐☐ Azure AD ☐☐ ☐ ☐☐☐ ☐☐☐☐ ☐☐☐.

☐☐☐ ☐☐☐ ☐☐ ☐☐☐? ☐☐☐☐☐ ☐☐ ☐☐☐☐ ☐☐☐ ☐☐☐ ☐☐☐☐☐☐☐.

☐☐: ☐ ☐☐☐ ☐☐☐ 1☐☐ ☐☐☐☐ ☐☐☐☐.



Answer:



☐☐:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles>

NEW QUESTION: 99

contoso.com ☐☐☐ Microsoft 365 ☐☐☐☐ ☐☐☐☐.

☐☐☐ ☐☐☐ ☐☐☐☐ ☐☐☐☐☐☐☐☐☐.

contoso.com

User email	User type	Invitation accepted	Shared resource
User1@outlook.com	Guest	No	Enterprise application
User2@fabrikam.com	Guest	Yes	Enterprise application

Azure Active Directory

Collaboration restrictions

- Allow invitations to be sent to any domain (most inclusive)
- Deny invitations to the specified domains
- Allow invitations only to the specified domains (most restrictive)

Delete

TARGET DOMAINS

Outlook.com  Microsoft

Microsoft SharePoint Online user3@adatum.com

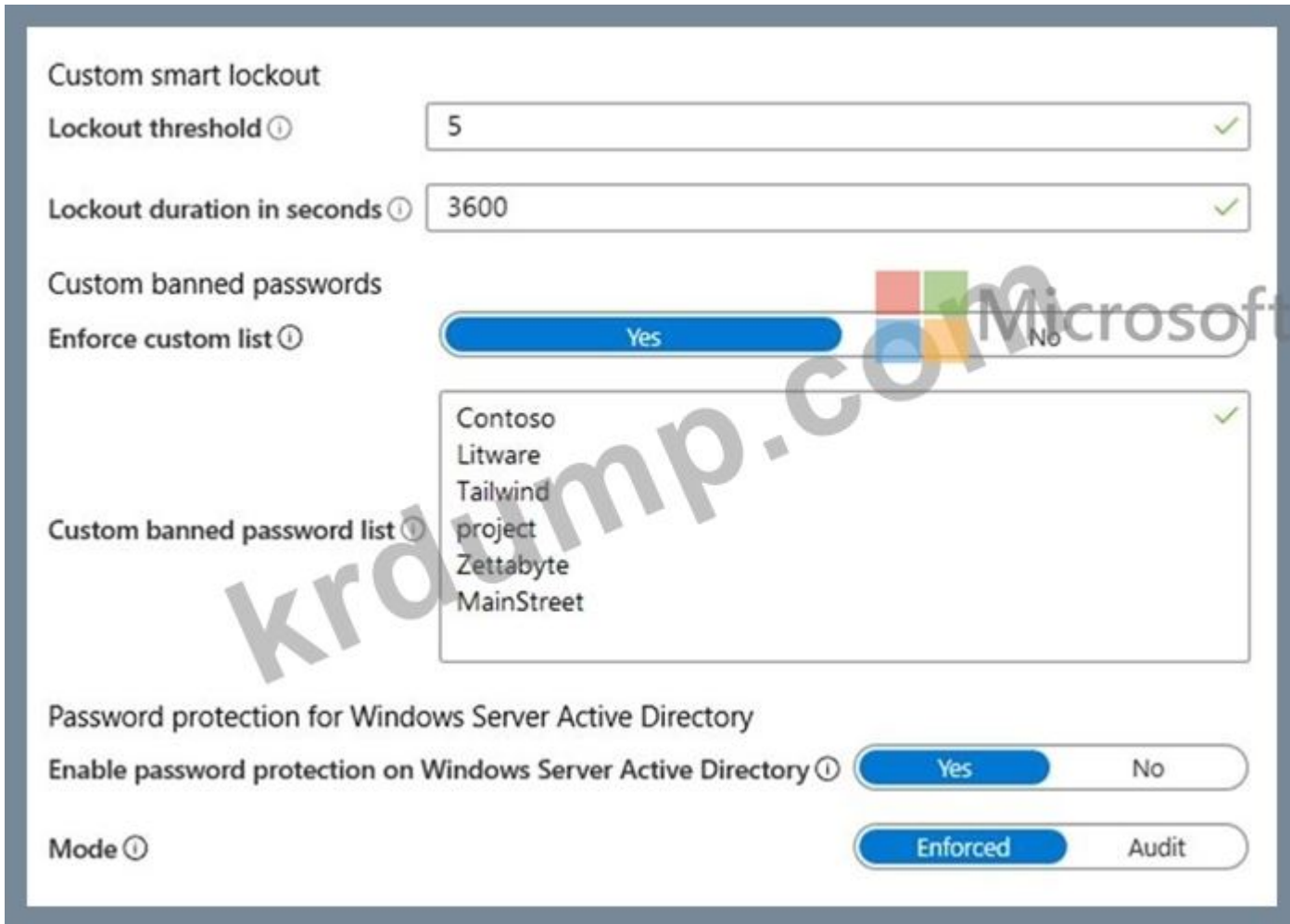
Statements	Yes	No
User1 can accept the invitation and gain access to the enterprise application.	<input type="radio"/>	<input type="radio"/>
User2 can access the enterprise application.	<input type="radio"/>	<input type="radio"/>
User3 can accept the invitation and gain access to the SharePoint site.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 can accept the invitation and gain access to the enterprise application.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can access the enterprise application.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can accept the invitation and gain access to the SharePoint site.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION: 100

Which of the following is a valid password for a user in an Azure AD (Azure Active Directory) tenant? (Select all that apply.)



Which of the following is a valid password for a user in an Azure AD (Azure Active Directory) tenant? (Select all that apply.)

* Litw@re

* T@ilw1nd

* C0nt0s0

Which of the following is a valid password for a user in an Azure AD (Azure Active Directory) tenant? (Select all that apply.)

A. Pr0jectlitw@re T@ilw1nd

B. C0nt0s0

C. C0nt0s0, Pr0jectlitw@re T@ilw1nd

D. C0nt0s0 T@ilw1nd

E. C0nt0s0 Pr0jectlitw@re

Answer: C (LEAVE A REPLY)

Source:

<https://blog.enablingtechcorp.com/azure-ad-password-protection-password-evaluation>

NEW QUESTION: 101

Microsoft 365 tenant. Which of the following is a valid password for a user in an Azure AD (Azure Active Directory) tenant? (Select all that apply.)

Which of the following is a valid password for a user in an Azure AD (Azure Active Directory) tenant? (Select all that apply.)

* Litw@re

* □□□□ □□□ □□□□ □□□□□□.

* □□□□ □□□□□□□□ □□□□ □ □□□ □□ □□□□ □□ □□ □□□ □ □□□□ □□□□.

□□□□ □□□□ □□□□? □□□□□□ □□ □□□□ □□□□ □□□□ □□□□□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□□.

Answer Area

To classify leaked credentials as high-risk, use:

- Azure Active Directory (Azure AD) Identity Protection
- Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
- Identity Governance
- Self-service password reset (SSPR)

To trigger remediation, use:

- Client apps not using Modern authentication
- Device state
- Sign-in risk
- User location
- User risk

To mitigate the risk, select:

- Apply app enforced restrictions
- Block access
- Grant access but require app protection policy
- Grant access but require multi-factor authentication
- Grant access but require password change

Answer:

To classify leaked credentials as high-risk, use:

- Azure Active Directory (Azure AD) Identity Protection
- Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
- Identity Governance
- Self-service password reset (SSPR)

To trigger remediation, use:

- Client apps not using Modern authentication
- Device state
- Sign-in risk
- User location
- User risk

To mitigate the risk, select:

- Apply app enforced restrictions
- Block access
- Grant access but require app protection policy
- Grant access but require multi-factor authentication
- Grant access but require password change

NEW QUESTION: 102

□□□□ □□□ □□□ □□□□ □□ □□ □□ □□□□ □□□□ □□□.

□□□□ □□ □□□ □□ □□ □□□ □□□□ □□□□? □□□□□□ □□ □□□□ □□□ □□ □□□□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□□.

Answer Area

The users must first:

- Provide consent for any app to access the data of Contoso.
- Register for multi-factor authentication (MFA).
- Register for self-service password reset (SSPR).

You must configure:

- A sign-in risk policy
- A user risk policy
- An Azure AD Password Protection policy

Answer:

The users must first:

- Provide consent for any app to access the data of Contoso.
- Register for multi-factor authentication (MFA).
- Register for self-service password reset (SSPR).

You must configure:

- A sign-in risk policy
- A user risk policy
- An Azure AD Password Protection policy

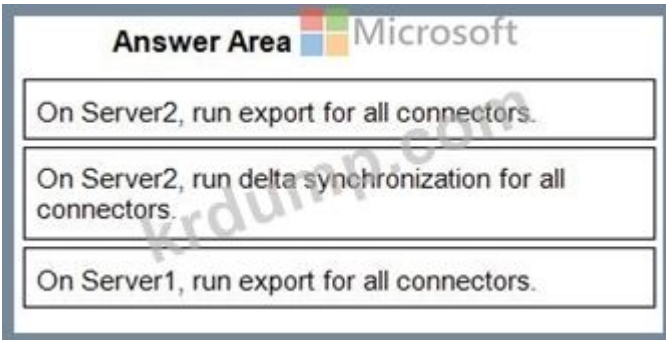
NEW QUESTION: 103

□□□□□□ Azure AD Connect □ □□□□□ contoso.com □□□□ Azure AD (Azure Active Directory) □□□□ □□□□ contoso.com □□□□ Active Directory □□□□□□ □□□□ □□□□□.

Attire AD Connect Server 1 is a Windows Server 2019. Azure AD Connect is installed on Server1. The following actions are performed:



Answer:



- 1 - Server2 run export for all connectors.
- 2 - Server2 run delta synchronization for all connectors.
- 3 - Server1 run export for all connectors.

NEW QUESTION: 104

contoso.com SMTP is configured in Microsoft Exchange. Microsoft 365 is configured. Azure AD (Azure Active Directory) is configured. 4 users are configured. The following actions are performed:

Actions	Answer Area
Sign in to the Microsoft 365 admin center.	<div style="text-align: center;"> ⏪ ⏩ </div>
Create a self-signed user account in the Azure AD tenant.	
From the Microsoft 365 admin center, add the domain name.	
Respond to the Become the admin message.	
From the Microsoft 365 admin center, remove the domain name.	
Create a TXT record in the contoso.com DNS zone.	

Answer:

Answer Area
Create a self-signed user account in the Azure AD tenant
Sign in to the Microsoft 365 admin center
Respond to the Become the admin message
Create a TXT record in the contoso.com DNS zone

1 - Azure AD

2 - Microsoft 365

3 -

4 - contoso.com DNS TXT

:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/domains-admin-takeover>

NEW QUESTION: 105

Microsoft 365 .

Windows 10 Azure AD(Azure Active Directory) .

Service1 . Service1 OAuth Azure AD . Service1 Azure AD .

Service1 .

Azure AD Service1 .

.

? .


: 1 .

Ensure that the users can connect to Service1 without being prompted for authentication:

- An app registration in Azure AD
- Azure AD Application Proxy
- An enterprise application in Azure AD
- A managed identity in Azure AD

Ensure that the users can access Service1 only from the Azure AD-joined computers:

- Azure AD Application Proxy
- A compliance policy
- A conditional access policy
- An OAuth policy



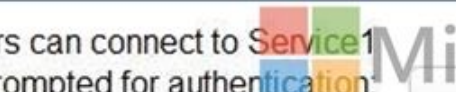
Answer:

Ensure that the users can connect to Service1 without being prompted for authentication:

- An app registration in Azure AD
- Azure AD Application Proxy
- An enterprise application in Azure AD**
- A managed identity in Azure AD

Ensure that the users can access Service1 only from the Azure AD-joined computers:

- Azure AD Application Proxy
- A compliance policy
- A conditional access policy**
- An OAuth policy



□□:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added>

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/require-managed-devices>

NEW QUESTION: 106

□□ □□ □□□ □□□ □□□□ Azure Active Directory(Azure Azure) □□□□ □□□□.

* Device1□□□ □□

* User1, User2, User3, User4, User5□□ □□□ □□□

* Group1, Group2, Group3, Ciroup4, Group5□□ 5□□ □□

□□□ □□ □□ □□ □□□□□.

NEW QUESTION: 108

User1 Azure AD(Azure Active Directory) .

Name	Type	Membership type
Group1	Security	Assigned
Group2	Security	Dynamic User
Group3	Security	Dynamic Device
Group4	Microsoft 365	Assigned

.

Name	Type	Membership type
GroupA	Security	Assigned
GroupB	Microsoft 365	Assigned

GroupA GroupB ?

: 1

Answer:

:

<https://bitsizebytes.wordpress.com/2018/12/10/distribution-security-and-office-365-groups-nesting/>

NEW QUESTION: 109

□□□□□ Azure AD(Azure Active Directory) □□□□ □□□□□ □□□□□ Active Directory □□□□ □□□□ □□□□. □□□□□ □□ □□ □□□ □□□□□ □□□□□.

Name	Type	Directory synced
User1	User	No
User2	User	Yes
User3	Guest	No

□□ □□□□ □□□□ □□□□□.

Azure AD Connect □ □□ □□□ □□ Azure AD □□ □□□□□.

PROVISION FROM ACTIVE DIRECTORY

Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

Manage provisioning (Preview)

Azure AD Connect sync

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

USER SIGN IN

Federation	Disabled	0 domains
Seamless single sign-on	Disabled	0 domains
Pass-through authentication	Enabled	2 agents

□□□□□ □□□□□ □□□□□□ □□□ □□□□□.

□□ □□□□ Azure AD □ □□□□ □ □□□□?

- A. □□□ 1 □ □□□ 3□
- B. □□□ 1 □□
- C. □□□1, □□□2, □□□3
- D. □□□ 1 □ □□□ 2□

Answer: A (LEAVE A REPLY)

□□:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-current-limitations>

Boston. How do you verify that the MFA policy is applied to the correct IP addresses? How do you verify that the policy is applied to the correct IP addresses?

- A. IP address range 10.10.10.0/24
- B. IP address range 10.10.10.0/24
- C. IP address range 10.10.10.0/24 and IP address range 10.10.10.0/24
- D. IP address range 10.10.10.0/24 and IP address range 10.10.10.0/24

Answer: B (LEAVE A REPLY)

Q:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

Q1, Litware, Inc

ID

litware.com Azure AD (Azure Active Directory) litware.com Active Directory. Azure AD Connect litware.com

Litware.com User1. Litware.com Azure AD

Fabrikam fabrikam.com Azure AD Fabrikam

litware.com litware.com

Litware.com Microsoft 365 Enterprise E5 Microsoft Cloud App Security

Litware.com litware.com Azure AD Azure Active Directory Office 365 Azure Sentinel Azure Sentinel Azure AD

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Litware.com VPN Azure Office 365 Azure Sentinel Azure Sentinel Azure AD

Litware.com

* Azure AD PIM (Privileged Identity Management)

* litware.com Azure AD

* Identity Governance is a cloud-based service that helps organizations manage their identities and access to resources. It provides a central location for managing user identities and their access to various applications and services.

* User1 is a user in the Azure AD tenant. The user is a member of the Litware\Azure AD\Users group. The user is also a member of the Litware\Azure AD\Users group.

Litware is a company that uses Azure AD for authentication and authorization. The company has a domain named litware.com. The company has a group named LWLicenses in Azure AD. The group is a security group. The group is used to manage licenses for Microsoft Office 365. The group is a member of the Litware\Azure AD\Users group.

Litware\Azure AD\Users is a group in Azure AD. The group is a security group. The group is used to manage users in the Azure AD tenant. The group is a member of the Litware\Azure AD\Users group.

Litware\Azure AD\Users is a group in Azure AD. The group is a security group. The group is used to manage users in the Azure AD tenant. The group is a member of the Litware\Azure AD\Users group.

* Litware is a company that uses Azure AD for authentication and authorization. The company has a domain named litware.com. The company has a group named LWLicenses in Azure AD. The group is a security group. The group is used to manage licenses for Microsoft Office 365. The group is a member of the Litware\Azure AD\Users group.

* Litware is a company that uses Azure AD for authentication and authorization. The company has a domain named litware.com. The company has a group named LWLicenses in Azure AD. The group is a security group. The group is used to manage licenses for Microsoft Office 365. The group is a member of the Litware\Azure AD\Users group.

* Litware is a company that uses Azure AD for authentication and authorization. The company has a domain named litware.com. The company has a group named LWLicenses in Azure AD. The group is a security group. The group is used to manage licenses for Microsoft Office 365. The group is a member of the Litware\Azure AD\Users group.

* Litware is a company that uses Azure AD for authentication and authorization. The company has a domain named litware.com. The company has a group named LWLicenses in Azure AD. The group is a security group. The group is used to manage licenses for Microsoft Office 365. The group is a member of the Litware\Azure AD\Users group.

* Litware is a company that uses Azure AD for authentication and authorization. The company has a domain named litware.com. The company has a group named LWLicenses in Azure AD. The group is a security group. The group is used to manage licenses for Microsoft Office 365. The group is a member of the Litware\Azure AD\Users group.

* Litware is a company that uses Azure AD for authentication and authorization. The company has a domain named litware.com. The company has a group named LWLicenses in Azure AD. The group is a security group. The group is used to manage licenses for Microsoft Office 365. The group is a member of the Litware\Azure AD\Users group.

NEW QUESTION: 111

Which of the following is a valid Azure AD (Azure Active Directory) group name? (Select all that apply.)

Group1

Group 1

Group_1

Group.1

New

Conditional access policy

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

Assignments

- Users and groups ⓘ
Specific users included >
- Cloud apps or actions ⓘ
All cloud apps >
- Conditions ⓘ
0 conditions selected >
- Access controls
- Grant ⓘ
0 controls selected >
- Session ⓘ
0 controls selected >

Control user access based on users and groups assignment for all users, specific groups of users, directory roles, or external guest users. [Learn more](#)

Include Exclude

- None
- All users
- Select users and groups

- All guest users (preview) ⓘ
- Directory roles (preview) ⓘ
- Users and groups

Select ⓘ >

1 user

 User1
user1@sk200922outlook.onm... ⓘ



Enable policy

Report-only On Off

Create

□□□□ □□□ □□□□ □□□□ □□□ □□□ □□□□ □ □□□ □□□□ □□□ □□□□
□□.
□□: □ □□□ □□□ 1□□ □□□ □□□□.

To ensure that User1 is prompted for multi-factor authentication (MFA) when accessing Cloud apps, you must configure the [answer choice].

- Conditions settings
- Enable policy setting
- Grant settings
- Sessions settings
- Users and groups setting

To ensure that User1 is prompted for authentication every eight hours, you must configure the [answer choice].

- Conditions settings
- Enable policy setting
- Grant settings
- Sessions settings
- Users and groups setting



Answer:

To ensure that User1 is prompted for multi-factor authentication (MFA) when accessing Cloud apps, you must configure the [answer choice].

- Conditions settings
- Enable policy setting
- Grant settings
- Sessions settings
- Users and groups setting

To ensure that User1 is prompted for authentication every eight hours, you must configure the [answer choice].

- Conditions settings
- Enable policy setting
- Grant settings
- Sessions settings
- Users and groups setting

□□

To ensure that User1 is prompted for multi-factor authentication (MFA) when accessing Cloud apps, you must configure the [answer choice].

- Conditions settings
- Enable policy setting
- Grant settings
- Sessions settings
- Users and groups setting

To ensure that User1 is prompted for authentication every eight hours, you must configure the [answer choice].

- Conditions settings
- Enable policy setting
- Grant settings
- Sessions settings
- Users and groups setting

□□:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-u>

NEW QUESTION: 112

□□ □ □□ □□□ □□ Azure AD(Azure Active Directory) □□□□ □□□□. □□□□□ □□ □□ □□□ □□□□ □□□□□.

Name	Role
Admin1	Application administrator
Admin2	Application developer
Admin3	Cloud application administrator
User1	User

App1 □ App2□□ □ □□ □□□□ □□ □□□□□. □□ □□□□ Azure AD□ App1□ □□□ □□.

App1□ □□□□ □□□ □ □□ □□□ Azure AD□ App2□ □□□ □ □□ □□□ □□□□ □ □□.

□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.

Can assign users to App1

- Admin1 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and User1

Can register App2 in Azure AD

- Admin1 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and User1

Answer:

Can assign users to App1:

- Admin1 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and User1

Can register App2 in Azure AD:

- Admin1 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and User1

□□

Can assign users to App1:

Microsoft

- Admin1 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and User1

Can register App2 in Azure AD:

- Admin1 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and User1

□□:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal-assign-users>

<https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added>

NEW QUESTION: 113

Microsoft 365 E5 □□□□ □□□□.

App1□□□ □□□□ □□ □□□□□.

Microsoft Cloud App Security□ □□□□ App1□ □□□ □□ □□ □□□□□ □□□□□ □□ □.

□□ 4□□ □□□ □□□□ □□□□ □□□? □□□□□ □□ □□□□ □□ □□□ □□ □□ □□ □□□□ □□□ □□□ □□□□□□.

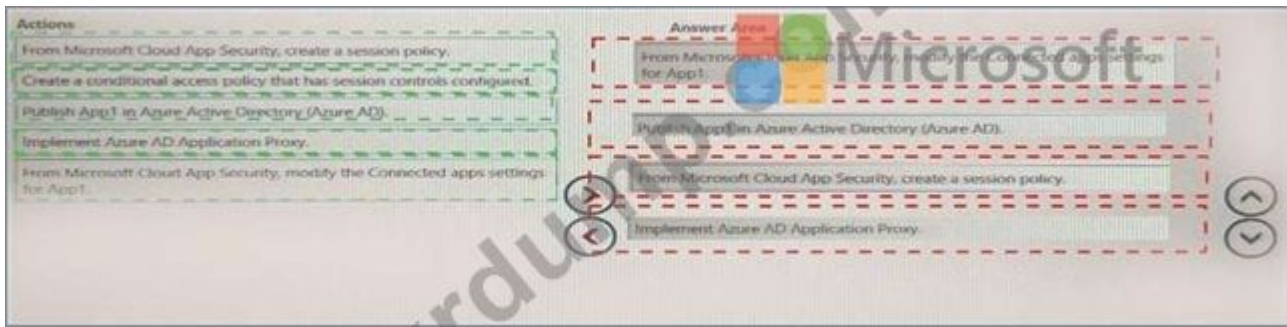
Actions

- From Microsoft Cloud App Security, create a session policy.
- Create a conditional access policy that has session controls configured.
- Publish App1 in Azure Active Directory (Azure AD).
- Implement Azure AD Application Proxy.
- From Microsoft Cloud App Security, modify the Connected apps settings for App1.

Answer Area

Microsoft

Answer:



NEW QUESTION: 114

User1, User1, User3, Group1, Azure AD(Azure Active Directory), Group1, User2, User3, Group1, Azure AD PIM(Privileged Identity Management), Group1.

Role setting details - Application Administrator
Privileged Identity Management | Azure AD roles

Edit

Activation	
Setting	State
Activation maximum duration (hours)	5 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
Require approval to activate	Yes
Approvers	0 Member(s), 1 Group
Assignment	
Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	3 month(s)
Allow permanent active assignment	No
Expire active assignments after	1 month(s)
Require Azure Multi-Factor Authentication on activation	No
Require justification on active assignment	Yes

Group1, User2, User1, Group1.

Add assignments

Privileged Identity Management | Azure AD roles

Membership Setting

Assignment type

Eligible

Active

Maximum allowed eligible duration is 3 month(s).

Assignment starts *

01/01/2021 12:00:00 AM

Assignment ends *

01/31/2021 11:59:00 PM

□□ □ □□ □□ □□ □□□ □□ □□□□, □□□ □□□ □□□□ □□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.

Answer Area

Microsoft

Statements	Yes	No
User1 is assigned the Application administrator role automatically.	<input type="radio"/>	<input type="radio"/>
When User2 requests to be assigned the Application administrator role, only User3 can approve the request.	<input type="radio"/>	<input type="radio"/>
If a request by User1 to be assigned the Application administrator role is approved on January 31, 2021, at 23:00, User1 can use the role until February 1, 2021, at 04:00.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Microsoft

Statements	Yes	No
User1 is assigned the Application administrator role automatically.	<input checked="" type="radio"/>	<input type="radio"/>
When User2 requests to be assigned the Application administrator role, only User3 can approve the request.	<input checked="" type="radio"/>	<input type="radio"/>
If a request by User1 to be assigned the Application administrator role is approved on January 31, 2021, at 23:00, User1 can use the role until February 1, 2021, at 04:00.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION: 115

Azure AD(Azure Active Directory) □ □□□ App1 □□□□ □□□ □□ □□□□ □□ □□□□.

App1 □ □□ □□□ □□ □□□□□.

[answer choice] can access App1 from the homepage URL.

- All users
- No one
- Only users listed on the Owners blade
- Only users listed on the Users and groups blade

App1 will appear in the Microsoft Office 365 app launcher for [answer choice].

- all users
- no one
- only users listed on the Owners blade
- only users listed on the Users and groups blade


Answer:

[answer choice] can access App1 from the homepage URL.

- All users
- No one
- Only users listed on the Owners blade
- Only users listed on the Users and groups blade

App1 will appear in the Microsoft Office 365 app launcher for [answer choice].

- all users
- no one
- only users listed on the Owners blade
- only users listed on the Users and groups blade



□□:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal>

NEW QUESTION: 116

□□ □□ □□□ □□□ □□□□ Azure AD(Azure Active Directory) □□□□ □□□□.

Name	Type	Membership type
Group1	Security	Assigned
Group2	Security	Dynamic User
Group3	Security	Dynamic Device
Group4	Microsoft 365	Assigned
Group5	Microsoft 365	Dynamic User

□□ □□□ □□ □□□ □□□ □□ □ □□□□?

A. Group1□

- B. □□1 □ □□4□
- C. Group1 □ Group2□
- D. □□1, □□2, □□4 □ □□5□ □□
- E. □□1, □□2, □□3, □□4 □ □□5

Answer: D ([LEAVE A REPLY](#))

□□
□□ □□□ □□ □□□ □□□ □□□ □ □□□□.
□□:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

SC-300 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ SC-300 □□! DumpTop
□ □□ **SC-300** □□ □□□ □□□□□□, DumpTop SC-300 □□ □□□ □□□□□□□□
□□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop SC-300 □□□ □□□□□.
<https://www.dumptop.com/Microsoft/SC-300-dump.html> (346 Q&As Dumps, **30%OFF** Special
Discount: **KrDump**)