MS HYBRID CLOUD MÉRNÖK / TÁMOGATÓ

3. forduló

A kategória támogatója: EURO ONE Számítástechnikai Zrt.

Ismertető a feladathoz

A 3.forduló feladatait a hosszú hétvége miatt kivételesen szerda (11.02.) éjfélig tudod megoldani!

Érdemes ebben a fordulóban is játszanod, mert a következő forduló kezdetekor, 11.03-án 18 órától kiosztjuk az 1.-2.-3. fordulóban megszerzett badgeket!

A verseny közben az alábbi teljesítményeket díjazzuk:

- fordulógyőztes
- átlagnál jobb időeredmény
- átlag feletti pontszám
- hibátlan forduló

Szeretnénk rá felhívni figyelmedet, hogy az egyszer megkapott badge-eket nem vonjuk vissza, akkor sem, ha esetleg az adott fordulóban a visszajelzések alapján változások vannak.

Jó játékot!

Felhasznált idő: 00:00/25:00 **Elért pontszám:** 0/45

1. feladat 0/10 pont

Az adatközpontban található fizikai szerveren egy ASP.NET alkalmazás fut virtuális gépen. A virtuális gép tagja a cég Active Directory tartományának. Korábban már integrálva lett az on-premises Active Directory tartomány az Azure AD szolgáltatással. A cél, hogy amikor a felhasználó az Azure AD felhasználójával egy másik országból szeretné használni az alkalmazást, akkor bejelentkezéskor az Azure MFA-val hitelesítse magát.

Mely funkciókat kell konfigurálni a cél elérésének érdekében?

Válaszok

- [x] Azure AD conditional access policy
  Ez a válasz helyes, de nem jelölted meg.
- [ ] Public Load Balancer
- [ ] Azure Migrate
- [ ] App Service plan
- [ ] Azure AD standard application

- [x] Azure AD enterprise application
  Ez a válasz helyes, de nem jelölted meg.
- [ ] Azure AD tenant restrictions
- [x] Azure AD application proxy
  Ez a válasz helyes, de nem jelölted meg.

Magyarázat

https://learn.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-add-on-premises-application

2. feladat 0/5 pont

Az Azure Active Directory tartományban az alkalmazottak csoporttagságait nem minden esetben frissítik, ezért olyan felhasználók is hozzáférhetnek erőforrásokhoz, akik már nem jogosultak azok eléréséhez.

Hogyan lehetséges havonta automatikusan ellenőrizni, hogy az adott csoportnak csak olyan vendég felhasználók a tagjai, akik még jogosultak a csoporttagságra?

Válasz

- ( ) Conditional Access policies konfigurálásával
- ( ) Tenant Restrictions konfigurálásával
- (•) Azure AD access reviews konfigurálásával
  Ez a válasz helyes, de nem jelölted meg.
- ( ) A csoport tagsági típusát Dynamic Userre kell megváltoztatni
- ( ) Azure AD Privileged Identity Management konfigurálásával
- ( ) Azure AD Identity Protection konfigurálásával

Magyarázat

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

3. feladat 0/10 pont

Az on-premises hálózatban található két Windows Server 2019 operációs rendszert futtató virtuális gép, VM01 és VM02. Az SA01 Storage Accountban korábban létre lett hozva egy fájlmegosztás Share01 néven Azure-ben. VM01 és az SA01 fájlmegosztása között Azure File Sync szolgáltatással szinkronizálódnak a fájlok.

Milyen lépéseket kell végrehajtani ahhoz, hogy VM02 és SA01 között is szinkronizálódjanak a fájlok?

Válaszok

- [x] Telepíteni az Azure File Sync Agentet a VM02 szerverre
  Ez a válasz helyes, de nem jelölted meg.
- [ ] Létrehozni egy Storage Sync Service-t Azure előfizetésben
- [x] Hozzáadni egy server endpointot a sync grouphoz
  Ez a válasz helyes, de nem jelölted meg.
- [x] Regisztrálni VM02-t a Storage Sync Service segítségével
  Ez a válasz helyes, de nem jelölted meg.

- [ ] Hozzáadni egy cloud endpointot a sync grouphoz

Magyarázat

https://learn.microsoft.com/en-us/azure/storage/file-sync/file-sync-deployment-guide?tabs=azure-portal%2Cproactive-portal

4. feladat 0/15 pont

A cég felhasználói számára minden irodában biztosítva van internet hozzáférés. Az irodákban található hálózati konfiguráció az alábbi:

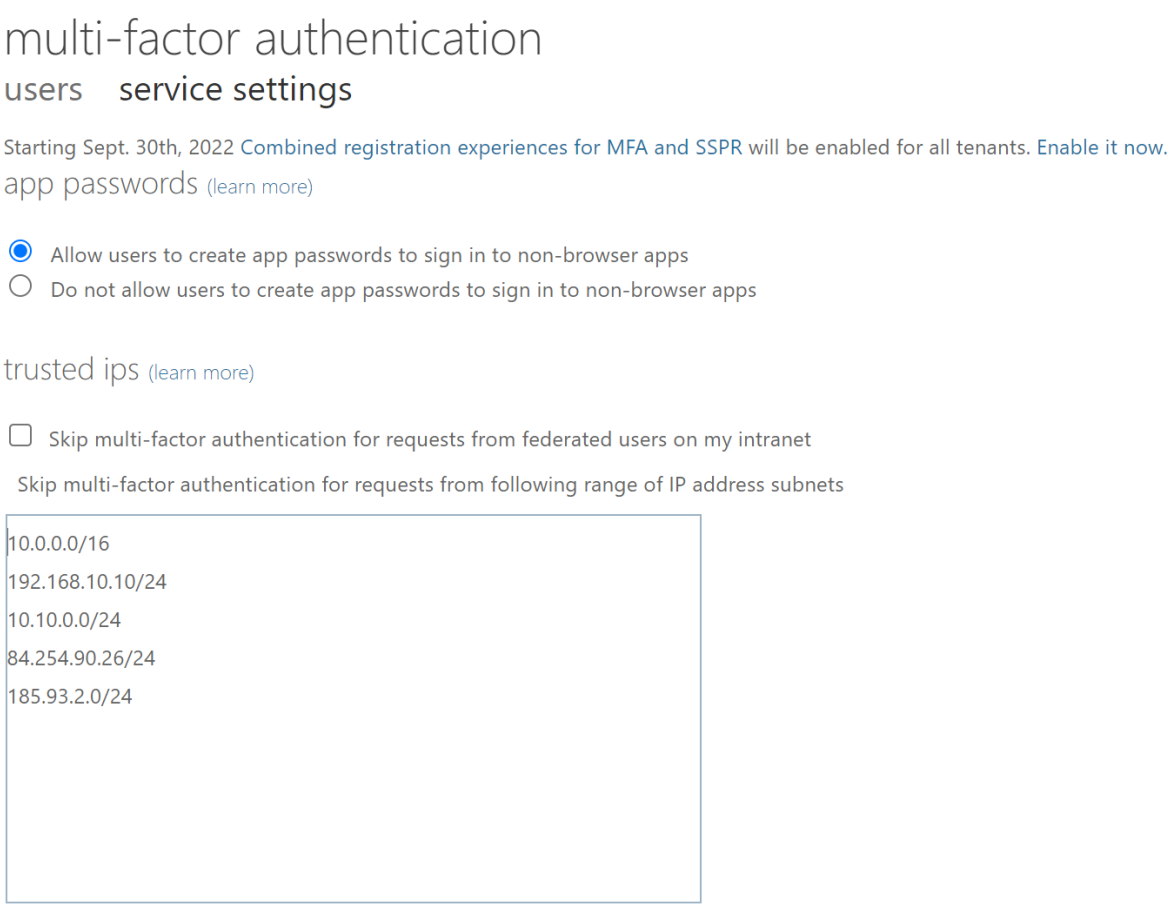
City	Private IP range	Public IP range
Budapest	10.0.0.0/16	185.43.205.0/24
London	192.168.10.0/24	178.20.31.0/24
Paris	10.10.0.0/24	185.93.2.0/24
Zurich	10.20.0.0/16	84.254.90.0/24

A biztonsági szabályzat miatt a cég több irodájába is többfaktoros hitelesítést állítottatok be az Azure Portalt használó alkalmazásfejlesztők számára. Minden fejlesztőhöz Application Developer szerepkör van hozzárendelve.

A fejlesztők MFA állapota az alábbi:

- Developer01: Disabled
- Developer02: Enabled
- Developer03: Enforced

Az MFA konfigurálásakor a multifactor authentication trusted IPs fülön az alábbi IP címeket konfiguráltátok:



Melyik állítás igaz az alábbiak közül?

Válaszok

- [ ] Developer01 felhasználótól többfaktoros hitelesítés lesz kérve az Azure Portalra történő bejelentkezéskor, amennyiben azt a budapesti irodából teszi meg.
- [ ] Developer01 felhasználótól többfaktoros hitelesítés lesz kérve az Azure Portalra történő bejelentkezéskor, amennyiben azt a 178.17.31.16 IP címről teszi meg.
- [ ] Developer01 felhasználótól többfaktoros hitelesítés lesz kérve az Azure Portalra történő bejelentkezéskor, amennyiben azt a párizsi irodából teszi meg.
- [x] Developer02 felhasználótól többfaktoros hitelesítés lesz kérve az Azure Portalra történő bejelentkezéskor, amennyiben azt a budapesti irodából teszi meg.
  Ez a válasz helyes, de nem jelölted meg.
- [ ] Developer02 felhasználótól többfaktoros hitelesítés lesz kérve az Azure Portalra történő bejelentkezéskor, amennyiben azt a zürichi irodából teszi meg.
- [x] Developer02 felhasználótól többfaktoros hitelesítés lesz kérve az Azure Portalra történő bejelentkezéskor, amennyiben azt a londoni irodából teszi meg.
  Ez a válasz helyes, de nem jelölted meg.
- [x] Developer03 felhasználótól többfaktoros hitelesítés lesz kérve az Azure Portalra történő bejelentkezéskor, amennyiben azt a 10.0.0.10 IP címről teszi meg.
  Ez a válasz helyes, de nem jelölted meg.
- [ ] Developer03 felhasználótól többfaktoros hitelesítés lesz kérve az Azure Portalra történő bejelentkezéskor, amennyiben azt a 84.254.90.45 IP címről teszi meg.
- [x] Developer03 felhasználótól többfaktoros hitelesítés lesz kérve az Azure Portalra történő bejelentkezéskor, amennyiben azt a londoni irodából teszi meg.
  Ez a válasz helyes, de nem jelölted meg.

Magyarázat

https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates

https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#trusted-ip

5. feladat 0/5 pont

Egy saját fejlesztésű alkalmazást telepítettél Azure-be, amely a felhasználók hitelesítését Azure AD-val oldja meg. Az alkalmazást három különböző Azure Tenant felhasználói is szeretnék használni. A felhasználóknak kötelező MFA-t használniuk az alkalmazásba történő bejelentkezéskor.

A felsorolt opciók közül miket kell konfigurálnod, hogy a fentebb említett követelmények teljesüljenek?

Válaszok

- [ ] Azure application security group
- [ ] Azure AD managed identities
- [x] Azure AD conditional access policy
  Ez a válasz helyes, de nem jelölted meg.
- [ ] B2B direct connect
- [ ] a Microsoft Intune app protection policy
- [x] Azure AD guest accounts
  Ez a válasz helyes, de nem jelölted meg.
- [ ] Identity Experience Framework policy

Magyarázat

https://learn.microsoft.com/en-us/azure/active-directory/external-identities/what-is-b2b

https://learn.microsoft.com/en-us/azure/active-directory/external-identities/b2b-tutorial-require-mfa

© 2023 Human Priority Kft.

KÉSZÍTETTE cone

Megjelenés

Világos