متع عقلك فى الكلاود Entra ID Primary Refresh Token (PRT) & Seamless SSO

مقدمة الموضوع

يعتبر كلاً من Primary Refresh Token (PRT) & Seamless SSO آليات لإثبات الهوية الخاصة بالمستخدمين والأجهزة وذلك عند الإتصال بـ Entra IDللدخول على التطبيقات الخاصة بك على مايكروسوفت أزور

يعتبر Primary Refresh Token (PRT)جزء أساسى فى اثبات الهوية لدى Entra ID والذى يدعم ويندوز 10 وأحدث وكذلك ويندوز 2016 وأحدث وكذلك يدعم . iOS, and Android devices

يمكن توصيف PRT بأنه JSON Web Token (JWT)يتم إصداره خصيصاً للأجهزة المسجلة فى. Entra ID

يمكن تشبيه PRT بـ Ticket Granting Ticket (TGT) والذى يحتوى على معلومات المستخدم عند الدخول على جهازه فى بيئة الدومين AD DS

كما تساعدك TGT فى الدخول على جهازك فى الدومين والوصول لموارد الشركة داخل الدومين بدون أن يسألك مرة أخرى عن هويتك تعمل PRT بنفس الطريقة حيث إثبات هويتك يتم بشكل تلقائى عند الدخول على موارد الشركة فى أزور.

يعتبر Seamless SSO مناسب أكثر لأنظمة الويندوز. Windows 7 and Windows 8.1

سيناريوهات استخدام ومزايا Primary Refresh Token (PRT) & Seamless SSO

يعمل PRT مع الحالات الآتية :

Entra AD joined

Hybrid Entra AD joined

Entra AD registered devices

يعمل Seamless SSO فى حالة أن الجهاز Domain Joined مع الأنظمةWindows 7 and Windows 8.1

سؤال هام : هل يمكن استخدام كلا الطريقتين معاً فى نفس الوقت ؟؟؟

الجواب : نعم يمكن استخدامهم فى نفس الوقت ويمكن جمع Seamless SSO مع Managed Authentication والذى يتم فى Entra ID باستخدام آليات مثل Password Hash Synchronization (PHS) or Pass-through Authentication (PTA)

لكن أنتبه دائماً فى حالة استخدامهما معاً الأفضلية تكون لـ Primary Refresh Token (PRT) على حساب!!! Seamless SSO

مزايا إستخدام كلا الطريقتين

: Improved securityحيث يقدم PRT طريقة آمنة لإثبات الهوية وكذلك يحقق SSO عن طريق التطبيقات المستخدمة على جهازك كمتصفحات الويب مثلاً بينما Seamless SSO يحقق طريقة الدخول الآمنة لتطبيقات على أزور باستخدامWindows domain credentials

: Enhanced user experienceتوفر الوقت وتحسن من تجربة الاستخدام لدى المستخدمين حيث أنهم غير مضطرين لإدخال اسم المستخدم وكلمة المرور عدة مرات

: Increased productivityوها الزيادة فى الإنتاجية نابعة من تقليل عدد محاولات الدخول على التطبيقات بفضلSSO

: Flexibilityوالمورنة هنا تتمثل فى استخدامك لكلاً الطريقتين Primary Refresh Token (PRT) & Seamless SSO معاً فى نفس الوقت أو بشكل منفصل وحسب طريقة دخول المستخدم المطلوبة.

بوست هام للسيستم والكلاود أدمين🔥🔥 Azure Entra ID: Admin Roles Explained

كلنا لما بنيجى نبتدى فى الكلاود ونتكلم عن الصلاحيات على أزور بيقابلك صلاحيات ومسؤليات على أزور مثل Global Administrator, User Access Administrator, and Resource Ownerفأنت لازم تكون فاهم الفرق بينهم كويس وأنا جاى النهاردة أبسط لك الموضوع ده ..... كوباية قهوة حلوة ويلا بينا!!!

@فى البداية هأحكى لك قصة جميلة أنت قررت تعمل حساب تجريبى على أزور Azure Free Trial وزى ما أنتوا عارفين بيديلك 200دولار كريدت لمدة شهر ومحتاج بس كإثبات الهوية فيزا فيها 1 دولار مثلاً علشان تعمل الاكاونت بسهولة وتهيص بقى وتتشقلب وتجرب اللى انت عاوزه من لابات.

@بعد 30 يوم لو ما عملتش ترقية للحساب ده لـ PAY AS You GO أو خلصت بسرعة 200 دولار حسابك هيكون Disabled وأقصد بالحساب هنا Subscribtionالخاص بيك .

@مش ده موضوعنا دلوقتى أنت عملت الحساب التجريبى الجميل ده بايميل مثلا اسمه X@hotmail.com وهوب قالك مرحباً وتعالى فى جولة أفرجك على أزور والبورتال الجميلة والقصص دى أنا عاوزك تركز معايا بقى وأنت فى الأول كده ايه الصلاحيات اللى حصلت عليها على أزور بأكاونت الهوتميل بتاعك ده ورقة وقلم وأكتب ورايا يا سيد المهندسين:

---- Global Administrator (1)الرول دى تم اسنادها لليوزر بتاعك تلقائياً وأدخل بنفسك على Entra ID هتلاقى فى المستخدمين حسابك الوحيد فى المستخدمين ومعاك الرول دى اللى ليها صلاحيات على Azure Entra ID tenant المربوط بـ Subscription بتاعك.

---- Owner (2)على مستوى Azure Subscription Level ومعناها لك الصلاحيات المطلقة على جميع الموارد Resources اللى هتعملها بداخله وتقدر تشوف ده لما تروح على Subscriptions ثم تختار I AM وهتلاقيك موجود.

///طيب ما تيجوا نفرق كده بين Global Administrator, User Access Administrator, and Resource Owner///

Global Administrator

@هو أعلى مستوى من الصلاحيات Highest level of administrative privileges على مستوى Entra ID ويقدر يدير ويتحكم فى كل حاجة وتعالى أعطيك أمثلة:

Add, edit, and delete users and groups.

Assign roles to users (e.g., assign other users as administrators)

Manage access to applications (e.g., registering and granting consent for apps)

Configure policies (e.g., Conditional Access, Identity Protection)

Access and configure the entire Azure subscription if given owner permissions on the subscription

مثال : الشركة عندك عاوزة تستخدم Conditional Access policies لاجبار استخدام وتطبيق Multi-Factor Authentication على جميع المستخدمين طبعاً اللى هيعمل الشغلانة دى هو عمنا Global Administrator فينشئ ويطبق البوليسى دى على مستوى. Tenant

User Access Administrator

@هو عبارة عن Azure Role مركزة على إدارة صلاحيات الوصول لموارد أزور Azure resources وبيشتغل على 3 مستويات subscription, resource group, or resource levelوهو ليس له صلاحيات administrative privileges على Entra ID نفسه وتعالى أقولك قدراته ايه:

Grant, remove, or modify access permissions (e.g., assign Reader or Contributor roles) for Azure resources

Manage Role-Based Access Control (RBAC) for subscriptions and resource groups

Resource Owner

@له التحكم الكامل على المورد الذى طبقت هذه الصلاحية عليه وهو مرتبط فقط بالمورد وتعالى أعطيك مثال:

لو أعطيت يوزر Owner على VM فهو فقط له صلاحيات على هذه الماكينة الوهمية فقط وليس أى شيئ آخر فهو يندرج تحت-Privileged Azure built in roles

ومثال آخر أنشأنا Storage Account وجعلنا أحد المستخدمين مثلاً (ديفيلوبر) له صلاحية Resource Owner على هذا الحساب التخزينى فهو يستطيع التحكم فى هذا الحساب التخزينى وفقط وليس له صلاحية فى أى مكان آخر

بوست هام جداً للسيستم والكلاود أدمين Unlocking Hybrid Identity: What Can Be Synced Between ADDS and Entra ID؟ 🔥🔥

السؤال ده متكرر جداً فى المقابلات التقنية وبيلخبط ناس كتير علشان كده بأمر الله تعالى ألخص لك القصة ببساطة ..... كوباية قهوة حلوة ويلا بينا!!!

@زى ما أنتوا عارفين انه كتير من الشركات بتحتاج تعمل Sync يعنى تزامن بين المستخدمين اللى على الدومين ويطلعوا فوق على Entra ID علشان يكون فيه أكسس للخدمات على أزور أو مايكروسوفت 365.

@السؤال اللى بيحير ناس كتير يا ترى ايه اللى ممكن يتنقل تحت من الدومين لفوق على أزور ؟؟؟ والعكس يعنى هل أقدر أعمل يوزرات فوق على أزور ينزلوا تحت على الدومين ؟؟؟

##أنواع الكائنات والمعلومات اللى يمكن نسخها وتزامنها إلى أزور## Synced from On-Prem ADDS to Entra ID

(1) Users :وطبعاً ده الافتراضى اللى كلنا عارفينه وببساطة بنحدد يا يتم نقل الجميع أو OU فيها يوزرات معينة وبيتم نسخ خواصه كذلك مثل UPN, email, display name, and group membershipsويمكن اضافة خصائص أخرى e.g., mobile, title وعن طريق تفعيل Password hash synchronizationيتم نسخ الهاش الخاص بباسوردات المستخدمين ليتم نسخها على . Entra ID

(2) Groups :يتم نسخ المجموعات سواءاً كانت Security groups and distribution lists بعضوياتها كذلك وبالنسبة لتداخل المجموعات nested groupsفلها اعتبارات معينة!!

(3) Contacts :حيث تكون مفيدة لكى تظهر فى قوائم عناوين البريد global address list (GAL) ويمكن نسخ بعض خواصها مثل name, email, and proxy addresses

(4) Devices :حيث تظهر الأجهزة الأعضاء فى الدومين Hybrid Azure AD كذلك على Entra ID ويساعدك على تطبيق بوليسى عليها والتحكم فيها مثلاً من خلال Intune

(5) Custom on-prem attributes :حيث يتم تحديد خصائص اضافية يتم نسخا على Entra ID بمساعدة الأداةEntra Connect

##أنواع الكائنات والمعلومات اللى يمكن نسخها وتزامنها من أزور ## Synced from Entra ID to On-Prem ADDS

(1) Password Writeback :ويمكن الاستفادة منها مع تفعيل SSPR أى عندما يقوم المستخدم بتغيير باسورده على الكلاود يتم نسخها لتحت على الدومين وطبعاً بتحتاج لترخيص من نوع Entra ID Premium P1 أو أعلى.

(2) Device Writeback :ومعناه الأجهزة الورك جروب المسجلة على أزور يتم نسخ الشهادة الرقمية الخاصة بها لتصبح موجودة على الدومين تحت علشان لو عندك خدمات مثل ADFS ومحتاج الناس تدخل على تطبيقات عندك وعاوز تدى صلاحية للنوع ده من الأجهزة وتفرض عليهم بوليسى حسب حالة كل جهاز.

(3) Group Writeback :حيث يمكن استنساخ Microsoft 365 Groups حيث تظهر تحت على الدومين كـ on-prem mail-enabled security groupsوطبعاً محتاج وجود اكسشينج سيرفر

أظن بعد اللى كتبته ليك فوق ده لو حد جه قالك لو عاوزين أو عندنا يوزرات فوق على الكلاود وعاوزينها تنزل تحت على الدومين نعمل ايه ؟؟؟؟ خد بالك يبقى بيوقعك!!!!

بوست هام جداً للكلاود أدمين🔥🔥 Microsoft Entra pass-through authentication

@يسمح للمستخدمين بتسجيل الدخول إلى كل من التطبيقات المحلية والتطبيقات على أزور باستخدام نفس المستخدم وكلمة المرور) <--- الموجودة على DC بتاعك!!!)

@يتم إستخدام هذه الطريقة عندما تريد بعض المؤسسات التي ترغب في فرض سياسات أمان وكلمة مرور Active Directory المحلية الخاصة بها!!

@من المتطلبات الأساسية إنك هتكون عامل Sync لليوزرات اللى عندك فى الدومين ويتم نسخها على Entra ID لكن هنا مش هيتم أخذ الباسوردات!!!

@الإختلاف الجوهرى هنا أن user’s password hash لا يتم نقلها إلى Entra ID لكن يتم إثبات الهوية من!!! On-Premises AD

@وهنا ميزة أساسية وهى كلمات المرور الخاصة بالمستخدمين لا يتم تخزينها على الكلاود بأى شكل ويمكن حماية حسابات المستخدمين بإستخدام بعض المميزات مثل Entra ID Conditional Access policiesوكذلك(Multi-Factor Authentication (MFA

@لا بد أن تعلم أن Authentication Agent والذى يكون موجود فى شبكتك الداخلية يقوم فقط بالإتصال outbound connections معنى هذا أنه لا تحتاج لوجوده فى شبكة منفصلة مثل DMZ

@يفضل تثبيت أكثر من Authentication Agent على سيرفرات عضو فى الدومين لضمان عدم وقوع الخدمة وتوزيع الأحمال redundancy and load balancing !!

@عملية الإتصال بين Authentication Agent & Entra ID مؤمنة بإستخدام certificate-based authentication ويتم تجديد هذه الشهادات تلقائيًا كل بضعة أشهر بواسطة Entra ID

##ولكى تعلم ما يحدث وراء الكواليس إليك تسلسل هذه العملية كالتالى:

(1يبدأ المستخدم تسجيل الدخول على تطبيق على سبيل المثالOutlook Web App

(2يقومEntra ID ، عند تلقي طلب تسجيل الدخول، بوضع اسم المستخدم وكلمة المرور (المشفرين باستخدام public key of the Authentication Agents)في قائمة الانتظارqueue

(3يتلقى On-premises Authentication Agent اسم المستخدم وكلمة المرور ويقوم بفك التشفير باستخدام private key الخاص به

(4يقوم Agent بالتحقق من اسم المستخدم وكلمة المرور باستخدام Windows APIs والموجه إلى الأكتيف ديركتورى الخاص بنا

(5تقوم وحدة تحكم مجال Active Directory بتقييم الطلب وإرجاع الاستجابة المناسبة (النجاح أو الفشل أو انتهاء صلاحية كلمة المرور أو قفل المستخدم) إلى الوكيلAgent

(6يقوم Agent بارجاع الإستجابة إلى Entra ID ومن ثم تتقرر حالة وطريقة دخول المستخدم على التطبيق

بوست هام جداً للكلاود أدمين🔥🔥 EntraExporter Tool For Entra ID Tenant

@هذه الأداة عبارة عن PowerShell module تستطيع استخراج المعلومات من Entra ID وتعطيك معلومات عن كونفيج الكائنات مثل user accounts, groups, administrative units, organization branding, subscriptions, and policiesوتنشى ملفات من نوع. JSON files

@تعتبر طريقة جميلة لاستنساخ point-in-time أى حفظ جميع التعديلات والخصائص للمعاومات الخاصة بـ Entra ID (Azure AD) configuration

@لا تعتبر باك أب للكائنات على أزور فعلى الرغم من عدم تمكنك من استخدام البيانات الملتقطة Captured Data لإنشاء الكائنات مرة أخرى لكن توفر لك كل المعلومات وهذه تعد بداية رائعة إذا كنت بحاجة إلى استعادة أي شيء أو إعادة تشغيله.

@لعمل تثبيت لتلك الأداة يمكنك استخدام الأمر التالىInstall-Module EntraExporter -Scope Allusers :

ملحوظة : فريق التطوير الخاص بهذه الأداة ينصح باستخدامك لـ PowerShell 7 لتشغيل هذه الأداة بكفاءة!!!

@تعتمد هذه الأداة على Microsoft Graph PowerShell SDK لاستخراج المعلومات من Entra ID وتحتاج لمجموعة متنوعة من الصلاحيات للوصول إلى الكائنات المختلفة والبوليسى على أزور لذا عليك باستخدام الأمر التالى:

Connect-MgGraph -Scopes 'Directory.Read.All', 'Policy.Read.All', 'IdentityProvider.Read.All', 'Organization.Read.All', 'User.Read.All', 'EntitlementManagement.Read.All', 'UserAuthenticationMethod.Read.All', 'IdentityUserFlow.Read.All', 'APIConnectors.Read.All', 'AccessReview.Read.All', 'Agreement.Read.All', 'Policy.Read.PermissionGrant', 'PrivilegedAccess.Read.AzureResources', 'PrivilegedAccess.Read.AzureAD', 'Application.Read.All'

@ثم عليك بتنفيذ الأمر التالى لتتمم عملية الاتصال Connect-EntraExporter :

@ستظهر لك نافذة تكتب فيها اسم المستخدم وكلمة السر ويجب عليك منح الموافقة على الأذونات المطلوبة للوصول إلى البيانات وهتسألنى هنا يا ترى ايه الصلاحيات المطلوبة علشان أقدر اعمل التاسك ده ؟؟؟ والاجابة يا عزيزى فى النقطة السابقة عندما استخدمنا الأمر Connect-MgGraph لاعطاءنا الصلاحيات المطلوبة!!!

@وعلشان تتمكن من استخراج المعلومات Exporting Entra ID Information هتعمل الأمر ده Export-Entra -Path 'C:\EntraID\' -All :

@توقع انتهاء عملية استخراج المعلومات فى خلال 10-15 دقيقة وهتلاقيها فى المجلد اللى قولت له عليه وهتلاقى داخل المجلدات ملفات JSON files اللى تم توليدها باستخدام الأداة وممكن تتفرج على محتويات الملفات باستخدام أى محرر مثل Visual Studio Code

بوست هام جداً للكلاود أدمين🔥🔥 Azure Hybrid Identity Authentication Methods

@كثير من المؤسسات تعتمد نظام هوية مختلط Hybrid Identity لأنه بيكون فيه هدف أساسى وهو استخدام نفس الأكاونت الخاص بالمستخدم للوصول إلى التطبيقات والخدمات الموجودة سواءاً فى الدومين المحلى الخاص بك أو على أزور أو على مايكروسوفت 365.

@يجب أن تكون طرق المصادقة والتأكد من هويات المستخدمين هي القرار الأول للمؤسسة التي ترغب في الانتقال إلى الخدمات السحابية.

السؤال الهام : ما هى طرق إثبات هوية المستخدمين والتى يعتمد عليها Entra ID Hybrid Identity ؟؟

أولاً Password Hash Synchronization : ثانياً Pass-through Authentication : ثالثاًFederated authentication :

#خلونا النهاردة نتكلم بشيئ من التفصيل الممتع والمبسط عن Password Hash Synchronization لذلك كوباية قهوة جميلة كده ، ركز معايا ويلا بينا .....

@يتم إستخدام أداة Microsoft Entra Connect المجانية من مايكروسوفت لعمل نسخ وتزامن User Password Hashes مع Entra ID وتقدر تحملها من هنا

https://www.microsoft.com/en-us/download/details.aspx...

@وبهذا، يمكنك تسجيل الدخول إلى خدمات Azure AD باستخدام نفس المستخدم ونفس كلمة المرور التي تستخدمها لتسجيل الدخول إلى Active Directoryالمحلي الخاص بك

@يمكنك استخدام هذه الميزة لتسجيل الدخول بنفس حساب المستخدم وكلمة المرور للوصول إلى خدمات متنوعة سواءاً على أزور أو Microsoft 365

@تعتبر هذه الطريقة من المتطلبات الأساسية لـ Identity Protection and Microsoft Entra Domain Services

@تساعد مزامنة كلمة المرور على تقليل عدد كلمات المرور التي يحتاج المستخدمون لديك إلى الاحتفاظ بها بكلمة مرور واحدة فقط

@تتم هذه العميلة عن طريق أخذ user's password hash من الأكتيف ديركتورى لدينا ثم تشفيرها وإرسالها إلىEntra ID

@يتم تشغيل عملية مزامنة Hash لكلمات المرور كل دقيقتين بإستخدام password hash synchronization agent ولا يمكنك تعديل وتيرة هذه العملية وعند حدوث التزامن يتم عمل Overwrite للباسورد الموجود على الكلاود

@عند دخول المستخدم يتم إرسال password hash مع أسم المستخدم وهنا يقوم Entra ID بعمل مقارنة للتأكد من تطابق Hash وفى حالة التأكد يتم دخول المستخدم لخدمات Azure

@يمكن للمستخدام عند الدخول على تطبيقات الكلاود اختيار Keep me signed in (KMSI) check box وهذا الاختيار يعمل على إعداد session cookieبحيث يتجاوز عملية اثبات الهوية مرة أخرى لمدة 180 يوم ويمكن لـ Microsoft Entra administrator التحكم فى سلوك هذا الخيار بالتفعيل أو التعطيل!!

@لك أن تعلم أنه SHA256 password data stored in Microsoft Entra ID هى أعلى أماناً من الباسوورد المخزنة لديك فى Local AD

بوست هام جداً لمهندسين الشبكات والسيستم أدمين Enhanced Security Admin Environment (ESAE)

🔥🔥

###ما هى ESAE Forest ؟###

@تعتبر أسلوباً معيارياً نقوم فيه بتخصيص فورست إدارية تحتوى على حسابات ذات صلاحية عالية مثل (مستخدمين ومجموعات ومحطات العمل).

@يتم عمل علاقة ثقة بين هذه ESAE forest وبين فورست أخرى تحتوى على موارد Resources (Production Forest) نريد إدارتها بشكل أحادى الإتجاه One-way Trust ومعنى ذلك أن الحسابات التى سنقوم بتعيينها من داخل ESAE forest تستطيع الوصول إلى الموارد داخل Production Forestلكن العكس غير صحيح لا تستطيع حسابات Production Forest الوصول إلى. ESAE forest

###مميزات### ESAE forests

: Locked-down accounts (1ومعنى ذلك أن حسابات المستخدمين التى سيتم الإستعانة بهم من داخل ESAE forest يتم إعطائهم صلاحية عالية داخل Production Forestوهى فى الأساس Standard nonprivileged user accounts ومثال على ذلك المستخدم العادى ده ممكن يبقى عضو فى Domain Adminsداخل Production Forest بحيث لو تم كشفه بواسطة هاكر وقتها لن يستطيع القيام بأى شيئ يمثل خطورة داخل. ESAE forest

: Selective authentication (2ومعنى هذا أن علاقة الثقة اللى حضرتك ناوى تعملها بين الاثنين فورست دول مش مفتوحة على البحرى كده واللى بنسميها Forest Wide لكنها هتكون محددة جداً Selective ومعنى ذلك أنه سيتم تحديد أجهزة معينة داخل Production Forest هى فقط اللى المستخدمين عندنا من ESAE forestيقدروا يشتغلوا عليها.

: Simple way to improve security (3إستخدامنا لـ ESAE forest يعتبر تحسن جوهرى ملحوظ فى عوامل الأمان التى نستطيع تقديمها إلى Production Forestحيث أن حسابات المستخدمين ذات الصلاحيات العادية هى فقط المخزنة بداخل Production Forest لكن الحسابات ذات الصلاحيات العالية privileged administrative accounts فقط مخزنة داخل ESAE forest وبما أنهم مخزنين فى فورست منفصلة نستطيع تطبيق أعلى درجات الحماية والأمان عليهم.

###متطلبات وإعتبارات تنفيذ### ESAE forests

@لا تقم بتثبيت تطبيقات أو خدمات غير ضرورية داخل ESAE forests فقط تشمل حسابات المستخدمين ذو الصلاحية العالية.

@يفضل أن تحتوى ESAE Forest على single-domain حيث ليس هناك أى إحتياج لعمل أكثر من دومين داخل هذه الفورست.

@كما قلنا سابقاً استخدم علاقة ثقة أحادية الإتجاه one-way trusts بحيث فى حالة اختراق الحسابات لا يستطيع أحد من Production الوصول عندنا وتخريب. ESAE Forest

@يجب تأمين نظام التشغيل داخل ESAE Forest من حيث التحديثات الأمنية والتوصيات الهامة والتقنيات التى ترفع درجات الحماية وإليك أمثلة عليها Secure Boot, BitLocker volume encryption, Credential Guard, and Device Guard

بوست هام لمهندسى الشبكات والمبتدئين فى الكلاود🔥🔥 Azure Role-based Access Control (RBAC)

@إدارة وتعيين الصلاحيات للوصول لموارد أزور من أهم الوظائف التى تسعى الشركات التى لديها تطبيقات وخدمات على الكلاود من أجل تحسينها وزيادة الأمان الخاص بها ويمكنك تلخيص ذلك فى 3 أسئلة هامة:

WHO (1)؟؟ من يمتلك حق الوصول لموارد أزور وهنا نقصد التحقق من هوية المتصلين

WHAT (2)؟؟ وماذا تستطيع أن تفعل ؟؟ أى صلاحية الوصول لهذه الموارد وحدود قدراتك

WHERE (3)؟؟ ما هى المناطق التى تستطيع الوصول إليها (نطاق صلاحيتك)!!

@الآن تستطيع أن تقول أن Azure RBAC هو نظام مبنى بداخل Azure Resource Managerيمكنك من إدارة الوصول والصلاحيات لموارد أزور الخاصة بك.

##إليك بعض الأمثلة لتعرف ماذا الذى يمكنك فعله باستخدام## Azure RBAC

*بداخل الاشتراك الخاص بك subscription يمكنك تعيين شخص ليتحكم فى VMs وشخص آخر للتعامل مع Virtual Networks

*تسمح لـ DBA groupبإدارة الوصول إلى قواعد بيانات SQL databases

*تسمح لشخص معين بإدارة جميع الموارد بداخل Resource Group مثلVMs - Subnets - Web Sites

*تسمح لتطبيق ما Application بالوصول لجميع الموارد الموجودة بداخلResource Group

@تعيين الصلاحيات والمسؤوليات ونسميه Role Assignment ينقسم إلى ثلاثة عناصر:

: Security principal (1)مثل user, group, service principal, or managed identity وهو الذى يطلب الوصول لموارد أزور

: Role definition (2)مجموعة من الصلاحيات Actions التى يستطيع المستخدم القيام بها مثل read, write, and delete والجدير بالذكر هنا أنه مصطلح Roles أى الأدوار (الوظائف) التى تمتلك الصلاحيات وقد تكون صلاحيات بمستويات عالية مثل Owner أو متخصصة مثل virtual machine reader .

ملحوظة : يمتلك أزورالعديد من built-in roles مثل Virtual Machine Contributorوالذى يمكن من خلاله إنشاء وإدارة VMs واذا كانت هذه الوظائف الجاهزة غير مناسبة لك يمكنك إنشاء ما يسمى بـ .Azure custom roles

: Scope (3)وهى مجموعة الموارد التى ينطبق عليها الصلاحيات وهناك أربعة مستويات مبنية على علاقات parent-child وهى:

Management Group - Subscription - Resource Group - Resource

@هناك أيضاً Role assignments وهى العملية التى تمكننا من وصل Role Definition ليتم ربطه بـ user, group, service principal, or managed identityوتطبيقه على Scope

@يمكنك تعيين الصلاحيات باستخدام الأدوات التالية.Azure portal, Azure CLI, Azure PowerShell, Azure SDKs, or REST APIs

##سؤال هام Where is Azure RBAC data stored : ؟؟##

يتم تخزين كل ما يختص بالصلاحيات وتعيين المسؤوليات بشكل Globally حتى يمكنك تعيينها على الموارد على أزور أياً كانت المنطقة

@استخدامك لـ Azure RBAC مجانى ومشمول ضمن الاشتراك الخاص بك.

بوست مهم لمهندسين الكلاود والسيكيورتىMicrosoft Entra Password Protection for on-premises

ده ضمن موضوعات الكورس القوى جداًAZ-801 Configuring Windows Server Hybrid Advanced Services

@كلنا عارفين انه يمكن فرض السياسات الأمنية الخاصة بباسوردات المستخدمين فى الدومين بطريقة من اثنين:

---- Domain Password Policyودى بتكون واحدة على مستوى الدومين بالكامل

-------- Fine-Grained Password Policyودى بتكون بوليسى مفصلة وتربطها على جروبات من المستخدمين لو حبيت

@بس فيه زيادة بقى يا ترى لو عاوزين نمنع المستخدمين من استخدام كلمات سر شائعة او سهلة التخمين او ما يكونش فيها من اسم الشركة او القطاع اللى شغال فيه هنعملها ازاى بقى ؟؟؟؟

#أشهر الباسوردات اللى بتودى الناس فى داهية وتضرب حساباتهم @!FerrariRed - P@ssw0rd1234 - !Welcome01 والقائمة طويلة من الباسوردات العبثية اللى عاوزين نمنعها!!!!

@مايكروسوفت بطريقة جميلة عملت لك الحل ويمكن تطبيقه على الدومين كنترولر عادى جدا بدون ما يكون عندك Hybrid identity أو تكون عامل Syncلحسابات الناس على الكلاود وده باستخدامMicrosoft Entra Password Protection

@ببساطة مايكروسوفت هتقدم لك Global List والقائمة دى لاشهر الباسوردات سهلة التخمين ومحدثة باستمرار وتمنع الناس من استخدمها وكمان قدمت لك Custom List فصلها انت على مزاجك وضيف كلمات السر الغير مرغوب فى استخدامها!!

@طيب يا ترى ايه نوع الترخيص اللى أنا محتاجه علشان استفيد بالميزة الحلوة أوى دى :

---- Cloud-only usersحسابات الناس على الكلاود فقط محتاجين Microsoft Entra ID Free للتمتع بـ global banned password list أما لو عاوز القائمة المخصصة كمان فلازم يكون عندك Microsoft Entra ID P1 or P2

---- Users synchronized from on-premises AD DSودى بتنطبق سواء عامل تزامن او لا هتحتاج Microsoft Entra ID P1 or P2 سواءا لكلا القائمتينGlobal List / Custom List

@طيب يا ترى ايه السوفتوير اللازم علشان استفيد بالميزة الجميلة دى ؟؟؟

---- AzureADPasswordProtectionDCAgentSetupوده بينزل على DC عندك وبيطلب ريستارت

----- AzureADPasswordProtectionProxySetupوده بينزل على سيرفر عضو فى دومين ولا يحتاج ريستارت

وطبعاً فيه شوية أوامر باورشيل لازم تتعمل علشان تربط السيرفرين دول معEntra ID Password Protection

@طيب ما تيجوا نشوف آلية عمل الميزة الرائعة دى فى سيناريو سهل كده:

(1اليوزر بيطلب تغيير الباسوورد وبيتبعت الطلب ده طبعاً للدومين كنترولر وساعتها DC Agent password filter dll بيقوم بفحص الباسورد دى ويشوف يا ترى هل مطابقة للشروط اللى أنا عاملها ؟ هل هى ضمن الباسوردات الممنوعة ؟؟

(2كل ساعة تقريبا بيقوم DC Agent ده اللى على الدومين كنترولر وعن طريق Service Connection Point بيعرف مين هو Microsoft Entra Password Protection Proxy Serviceوده المسئول عن تحميل أحدث باسوورد بوليسى من Entra ID فبياخد القائمة دى منه وتتخزن على سيرفر DCفى SYSVOL وده بيسمح ليها بالاستنساخ على جميع سيرفراتDCs

(3ساعتها DC وعنده أحدث ليستة بيشوف يا ترى باسوورد حضرتك (العبقرية !!) مطابقة للشروط ولا لا فغذا كانت مطابقة هيقولك ماشى تم التغيير ويتسجل طبعاً فى Event Viewer أما يا ويلك لو كانت مش مطابقة للشروط هيرفض التغيير ويسجلها برضه كمحاولة فاشلة!!!

##أنا كنت حريص أبسط الموضوع قدر الإمكان لكن فيه تفاصيل كتير واللاب العملى بتاعه ممتع جدا !!!

بوست هام جداً للمبتدئين فى الكلاودMicrosoft Entra Hybrid Join

###مقدمة الموضوع###

@كما تكلمنا سابقاً لكى تجعل المستخدمين يتمتعوا بتجربة استخدام مميزة فى الوصول لتطبيقاتك على أزور وبأقل مجهود عندك أسلوبين علشان تحقق SSO بالنسبة لأجهزة المستخدمين.

------ Primary Refresh Token (PRT)ودى مناسبة لويندوز 10 وأحدث وويندوز 2016 وأحدث

-------- Seamless SSOودى مناسبة Windows 7 and Windows 8.1

@علشان تعمل الكلام ده لا بد أن يكون Device الخاص بالمستخدم مسجل على Entra ID بشكل من ثلاثة:

--------- Entra Registered Deviceودى باختصار كده وعلى عجالة المستخدم بيقوم بإضافة حساب Work or school account من لوحة التحكم على السيستم عنده وده مش هيغير طريقة اللوجين ويخليه يستخدم الحساب اللوكال الخاص به وتنفع فى سيناريو BYOD وتستخدم مع أنظمة تشغيل مختلفة Windows - MAC - IOS - Android

--------- Entra Joined Deviceودى باختصار كده المستخدم بيقوم بإضافة حساب Work or school account من لوحة التحكم على السيستم عنده وبيغير فى طريقة اللوجين والمستخدم بيخش بحساب Microsoft Account ومناسبة الطريقة دى لويندوز 11/10 باصدارات مختلفة ما عدا Home ما تنفعش معانا واليوزر بيستقبل عند الدخول PRT ودنيته حلوة وبيتمتع بـ SSO على تطبيقات الشركة على أزور

----- Entra Hybrid Joinودى بقى المستخدم مش مضطر يعمل أى حاجة أنا باعتبارى كلاود أدمين فى الشركة أقدر من خلال Sync اللى بيحصل بين On-Premises AD DCوبين Entra ID باستخدام الأداة Entra Connect انى انقل حسابات الكمبيوتر Computer Accounts الخاصة بالمستخدمين لتصبح مسجلة مباشرة على Entra ID Devices وهتتمتع بـ SSO من خلال استقبالها PRT مع دخول المستخدم بحسابه Work Account على جهازه

###ما هى متطلبات تفعيل ميزة### Entra hybrid join

@أن يكون اصدار Microsoft Entra Connect الخاص بك 1.1.819.0 or later ودائماً حمل أحدث اصدار من الموقع الرسمى

@لا بد أن تحدد organizational units (OUs) أو Container الذى سيقوم Entra Connect بعمل تزامن حسابات أجهزة المستخدمين لتصبح مسجلة على أزور

@محتاجين صلاحية Global Administrator على أداة Entra Connect وكمان صلاحية Enterprise administrator على الدومين كنترولر لأنه هيقوم بتسجيل Service Connection Point (SCP) وفيها Endpoint اللى الأجهزة هتكتشفها علشان تسجل فى أزور

@لازم تتأكد انه أجهزة الشركة المراد تسجليها على أزور يكون ليها وصول على الإنترنت وتصل للعناوين الآتية:

https://enterpriseregistration.windows.net

https://login.microsoftonline.com

https://device.login.microsoftonline.com

https://autologon.microsoftazuread-sso.com (If you use or plan to use seamless SSO)

@هتقوم بتفعيل الخطوات دى على أداة Entra Connect

Start Microsoft Entra Connect, and then select Configure.

In Additional tasks, select Configure device options, and then select Next.

In Connect to Microsoft Entra ID, enter the credentials of a Global Administrator for your Microsoft Entra tenant.

In Device options, select Configure Microsoft Entra hybrid join, and then select Next.

In Device operating systems, select the operating systems that devices in your Active Directory environment use, and then select Next.

In SCP configuration, for each forest where you want Microsoft Entra Connect to configure the SCP, complete the following steps, and then select Next.

Select the Forest.

Select an Authentication Service.

Select Add to enter the enterprise administrator credentials.

In Ready to configure, select Configure.

In Configuration complete, select Exit.

ملحوظة هامة جداً : أحياناً الجهاز بتاعك مش بيظهر على Entra ID Devices وده بسبب إنه فيه Attribute لازم تبص عليه فى AD وأسمه userCertificate ولو قيمته <notset>مش هيتنقل خالص وهى مسألة وقت لو الجهاز واصل له نت ومزبط كل حاجة

بوست هام جداً لمهندسي الشبكات والسيكيورتى والكلاود Modern Authentication vs. Basic Authentication

#مقدمة الموضوع#

إدارة عمليات إثبات الهوية وصلاحيات الوصول للخدمات والتطبيقات بشكل آمن للمستخدمين والأجهزة من أولويات الأمان فى الشبكات الحديثة لأى مؤسسة وهناك نوعان من طرق إثبات الهوية هنتكلم عنهم فى البوست ده Basic Authentication وما يحيط به مشاكل وثغرات أمنية والنوع الأحدث والأكثر أمناً وهو Modern Authentication وما يقدمه لنا من مميزات ..... ركز معايا بقى وهات القهوة بتاعتك ويلا بينا!!!

##دردشة سريعة عن## Basic Authentication

@يمتاز هذا النوع بالبساطة حيث يتم تخزين Username and password فى حقل واحد بداخل Header الخاص بطلب إثبات الهوية باستخدام الفورمات base64 encoding ولذلك من الطبيعى أن يتم استخدام بروتوكول SSL لتشفير ذلك header ولحماية اليوزر والباسوورد الخاص بك بس ده لا يمنع إنه هيسبب أخطار أمنية منها:

1)هتلاحظ وجود Authentication headers مع كل طلب خصوصا لو انت بتراقب المحادثة بين كلاينت وسيرفر مما يعرضها للخطر ومعرفة محتواه !!

2)كمان الباسوردات بيتعمل ليها Cache على أغلب المتصفحات فده برضه بيعرضنا لجانب آخر من الثغرات الأمنية.

3)في الأساس يعتبر الاعتماد على فحص أسماء المستخدمين وكلمات المرور من خلال السيرفر مباشرة طريقة قديمة وغير مناسبة لحماية البيانات.

##دردشة سريعة عن## Modern Authentication

@فى النوع ده بيتم استخدام ما يسمى بـ Established Protocolsمعنى هذا أنه سيتم الفصل بين Identity Provider والمنوط به إثبات الهوية عن Service Providerواللى عنده الخدمة او التطبيق اللى اليوزر بيحاول يأكسس عليه.

@علشان اقرب لك الصورة تخيل بقى إنه اللى مسئول عن إثبات الهوية بتاعتك) Entra ID اللى كان اسمه قبل كده (!! Azure AD وما يقدمه لك من عناصر أمان لحسابات المستخدمين بكلمات المرور ودعم استخدام MFA لاستخدام أكثر من طريقة فى الدخول وأيضاً نستطيع تطبيق بوليسى على المستخدمين لمزيد من التحكم.

@فيبقى انت بتوجه الطلب بتاعك لسيرفر الويب اللى عليه التطبيق يقوم السيرفر يعمل لك Redirect تروح تكلم Entra ID وساعتها هو اللى هيتأكد من يوزر وباسوورد وكمان MFA بتاعتك لو طلبها وبعد ما يتأكد يقوم يعطيك Access Token علشان تروح تقدمها للويب سيرفر وبعد ما تقدم التذكرة دى للويب سيرفر ويتأكد منها يقوم الويب سيرفر باعت ليك Cookie يتخزن عندك فى المتصفح علشان تتمتع بـتجربة SSO ولا يسألك مرة ثانية أنت مين!!!

**عارف سؤال هييجى فى بالك دلوقتى !! منين الويب سيرفر يتأكد إنه Token اللى جت دى من Entra ID مش من حتة تانية ؟؟؟

الجواب : المفروض تكون عامل Federation بين سيرفر الويب أو التطبيق بتاعك وبين Entra ID وده هيخلي سيرفرك يكون عليه Key اللى بيستخدمه Entra IDفى إنه يعمل توقيعه الخاص Signature على التوكن بتاعتك وساعتها هيتأكد إنه فعلاً توكن شرعى مش ملعوب فيه.

@وأزيدك من الشعر بيت كمان سيرفر الويب بتاعك المفروض بيكون عليه Key مختلف يعمل توقيع بيه على معلومات وصولك للسيرفر اللى بيبعتها ليك علشان لو حد فكر انه يستخدمها ويلعب فيها هتتكشف والسيرفر هيرفضها .

##أمثلة على البروتوكولات الشائعة المستخدمة مع## Modern Authentication

: (WS-Federation (Web Services Federation @يتأكد من إثبات هوية المستخدم عن طريق web-based services لذلك يضمن للمستخدم إنه يكون مثبت هويته على عدة تطبيقات فى نفس الوقت.

: (Security Authentication Markup Language (SAML @بيقوم توصيل كلاً من Identity Provider مع Service Provider ويطلب التأكد من هوية المستخدم وبيدينا مرونة أكبر وإزاى بيحصل التشفير بينهم.

: (Open Authorization (OAuth @بنسميه بروتوكول تفويض مثلاً نستخدم حساب الجى ميل بتاعنا أو الفيس بوك للوصول لمواقع معينة ليها Trust مع GMAIL OR Facebook وكمان فيه بروتوكول رابع متطور عنه اسمه OpenID Connect (OICD)

موضوع هام جداً للمبتدئين فى الكلاودDifference between Azure AD B2B and B2C

Azure AD B2B ###أو المعروفة باسم### B2B Collaboration

@هى ميزة بداخل Microsoft Entra External ID والتي تتيح لك دعوة المستخدمين Guest Users للتعاون مع مؤسستك عن طريق إرسال دعوة Invitationعن طريق الايميل) وهذا ما يميزها فى المقام الأول عن. (B2C

@يتم إنشاء حساب لهذا Guest داخل Entra ID Users ويكون على شكل (User Object) ويكون هذا المستخدم الضيف مسجل بايميل خارجى جوجل أو ياهو أو أى مزود خدمة آخر لنعطيهم صلاحيات على التطبيقات الموجودة بداخل المؤسسة على أزور.feeling excited —.

@لا بد أن تعلم أنه هذا المستخدم بياناته وكلمة السر الخاصة به ليست مخزنة على أزور لكنه مجرد وسيلة لتعريفه بداخل أزور ويسهل علينا تعيين الصلاحيات له.

@يمكنك مشاركة تطبيقات وخدمات شركتك بشكل آمن مع مستخدمين خارجيين ، مع الحفاظ على السيطرة على بيانات شركتك الخاصة .

@يقوم المستخدمون الضيوف بتسجيل الدخول إلى تطبيقاتك وخدماتك باستخدام هوياتهم الخاصة بالعمل أو المدرسة أو حسابات مواقع التواصل الإجتماعى.

@يمكنك بمنتهى السهولة وعبر بوابة Azure ثم Entra ID ثم من Users نختار Create a new guest user وتحدد الايميل الذى سيتم ارسال الدعوة له.

@استخدم السياسات Policies لمشاركة تطبيقاتك وخدماتك بشكل آمن ويمكن باستخدام Conditional Access policies فرض استخدام المصادقة متعددة العوامل MFA بحيث نجبر المستخدمين Guest على استخدام أكثر من عنصر للتحقق من الهوية.

Azure Active Directory B2C

@تمكن من التعاون بين أزور والعملاء business-to-customer حيث يمكن لعملائك استخدام هويات حساباتهم الاجتماعية أو المؤسسية أو المحلية المفضلة للحصول على إمكانية تسجيل الدخول الموحد إلى تطبيقاتك . Single Sign-On

@هذه الميزة قادرة على دعم ملايين المستخدمين ومليارات عمليات المصادقة يوميًا ، فهى تعتني بأمان منصة المصادقة وسلامتها ، ومراقبة التهديدات والتعامل معها تلقائيًا أى الحماية من هجمات مثل Dos Attacks وكذلك brute force attacks والتى تعتمد على محاولة تخمين معلومات الدخول.

@تعتبر خدمة منفصلة عن Entra ID حيث يتم إنشاء قاعدة حسابات المستخدمين الخاصة بها فهو يسمح للشركات ببناء تطبيقات مخصصة للعملاء، ثم السماح لأي شخص بالتسجيل وتسجيل الدخول إلى تلك التطبيقات دون أي قيود على حساب المستخدم.

@تعتبر هذه الميزة white-label authentication solution ومعنى ذلك أنه يمكنك تخصيص تجربة المستخدم User Experience مع علامتك التجارية بحيث تمتزج بسلاسة مع تطبيقات الويب والهاتف المحمول الخاصة بك.

@قم بتخصيص كل صفحة يتم عرضها بواسطة Azure AD B2C عندما يقوم المستخدمون بالتسجيل وتسجيل الدخول وتعديل معلومات ملفاتهم الشخصية عن طريق تخصيص HTML, CSS, and JavaScript بحيث تبدو تجربة استخدام Azure AD B2C كأنها جزء اصيل من تطبيقاتك.

@تستخدم هذه الميزة بروتوكولات اثبات الهوية المعروفة مثل OpenID Connect, OAuth 2.0, and Security Assertion Markup Language (SAML)وتتكامل بشكل رائع مع غالبية التطبيقات الحديثة.

بوست هام جدا لمهندسى الشبكاتADDS vs AAD Domain Services

ده ضمن موضوعات الكورس🔥🔥 AZ-800: Administering Windows Server Hybrid Core Infrastructure

@سأناقش الأنواع التالية ، والاختلافات بينهم وحالات الاستخدام الخاصة بهم

1- Active Directory Domain Services اختصاراً ADDS

2- Azure Active Directory Domain Services بقى اسمه!!! Entra Domain Services

Active Directory Domain Services (ADDS)

@هذا هو Active Directory التقليدي الخاص بك، والذي يشار إليه أيضًا باسم Domain Controller أوDC ، والذي قمت بتثبيته في شركتك.

@قد تقوم بتثبيت تلك الميزة على خادم فعلي أو إفتراضي Physical Server /Virtual Machine وتقوم بتثبيته باستخدام أحدث نظام تشغيل Windows Serverثم تثبيت. ADDS

@يمكنك إنشاء (المستخدمين - حسابات الكمبيوتر - المجموعات - السياسات الأمنية .....) والكثير من الخدمات المرتبطة بها مثلDNS

@يعتمد على بروتكولات مثل LDAP, Kerberos and NTLM authentication

@يمكنك إستخدام هذا النوع فى غالبية الشركات مثلاً لديك شركة تضم مستخدمين وأجهزة كمبيوتر وترغب في توحيد سياسات المصادقة والترخيص والأمن ومركزيتها ويعتبر هذا النهج التقليدى

@ويمكنك إستنساخ الكثير من المعلومات الموجودة فى سيرفرك مثل (حسابات المستخدمين وكلمات السر - الأجهزة) لتصبح متاحة على منصة أزور السحابية لتستطيع التعامل مع تطبيقاتك السحابية والإستفادة من ميزة Single Sign On (SSO)

Azure Active Directory Domain Services (Azure ADDS)

@هو مشابه لما عليه On-premise ADDS كما تكلمنا عليه فى الأعلى لكنك لن تقلق أو ينشغل بالك بالآتى:

Forest/Domain levels - FSMO roles - Upgrades/Patching

@هو يعتبر Active Directory as a Service والذى تقدمه مايكروسوفت لك بشكل جاهز وبخطوات بسيطة وسهلة بدون أن تقلق لإمكانيات السيرفر أو التحديثات الأمنية وخلافه من الأمور التى تقلق مدراء الشبكات

@المفاجأة هنا أنه يقدم الدعم للبروتوكولات التقليدية مثل LDAP, NTLM, and Kerberos authentication مما يتيح لك نقل أعباء العمل التقليدية إلى السحابة بدون مشكلة

@يمكنك عمل إنضمام لجميع الأجهزة الإفتراضية VMs على السحابة لتصبح عضو فى Azure ADDS

@يمكنك التحكم فى الأجهزة بإستخدام Group Policy

@مثال عملى لهذا السيناريو أن تريد مؤسستك الانتقال بنسبة 100% إلى Azure وتريد مزيدًا من التحكم في الأجهزة الافتراضية الموجودة على Azure Cloudوترغب في الاحتفاظ بكائنات نهج المجموعة (GPO) للأجهزة الافتراضية وما إلى ذلك من موقع مركزي

@وترغب أيضًا في نقل تطبيقاتك القديمة الداخلية التي تستخدم مصادقة LDAP أو Kerberos إلى السحابة دون الحاجة إلى إعادة كتابتها عندها سيكون Azure ADDSمناسبًا لهذه المتطلبات

بوست هام جداً بعنوانMicrosoft Entra Pass-Through Authentication

ده ضمن موضوعات الكورس🔥🔥 AZ-800: Administering Windows Server Hybrid Core Infrastructure

@لو عاوز تفهم أنواع Authentication المختلفة والمستخدمة مع MS Entra ID هيكون ده أحد السيناريوهات.

@فكرته إنك بتجبر أى حد من المستخدمين اللى عندك لما يتصل على أبلكيشن على الكلاود هيتم التأكد من هويته من خلال سيرفرات ADDS اللى عندك فى الداتا سنتر وده بسبب Agent اللى هيكون وسيط بينك وبينEntra ID

@يمكن استخدامه مع جميع تطبيقات الويب all web browser–based applications والمدعومة منMicrosoft Entra ID

@يمكن استخدامه كذلك مع تطبيقات الأوفيس User sign-ins to Office applications والتى تدعمmodern authentication

@ويمكن استخدامه مع الأوت لوك User sign-ins to Microsoft Outlook وبدعم الكثير من بروتوكولات الايميل مثل Exchange ActiveSync, Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP), and Internet Message Access Protocol (IMAP)

@يمكن استخدامه مع تطبيق السكايب للمحادثات الصوتية والفيديو User sign-ins to Skype for Business والذى يدعم modern authentication

@وكل هذا يكون عن طريق Authentication Agent يتم تنصيبه على الداتا سنتر عندك على سيرفر أو أكثر لو بتدور على High Availability وميزته الجميلة إنه بيدعم فقط Outbound Connections يعنى مش محتاج تخليه فىperimeter network