

Azure Active Directory

Gestion des identités hybrides
(concepts et mise en œuvre)

→ Informatique technique

Fichiers complémentaires
à télécharger



Epsilon Collection logo, featuring a stylized 'E' and the word 'Collection'.

epsilon



Seyfallah TAGREROUT



Les éléments à télécharger sont disponibles à l'adresse suivante :
<http://www.editions-eni.fr>
Saisissez la référence de l'ouvrage **EPAZAD** dans la zone de recherche
et validez. Cliquez sur le titre du livre puis sur le bouton de téléchargement.

Préface

Avant-propos

Chapitre 1
Introduction

- 1. Présentation du livre..... 13
 - 1.1 Le cloud 13
 - 1.2 Les différents modèles du cloud..... 14
 - 1.2.1 IaaS 14
 - 1.2.2 PaaS 16
 - 1.2.3 SaaS 16
 - 1.3 Les modèles de déploiement du cloud 17
 - 1.3.1 Le cloud public 17
 - 1.3.2 Le cloud privé 18
 - 1.3.3 Le cloud hybride 18
 - 1.4 Les enjeux du cloud 19
 - 1.5 Les acteurs sur le marché 20
 - 1.6 Microsoft Azure 22
 - 1.6.1 Ce que propose Microsoft Azure..... 23
 - 1.6.2 Microsoft Azure et les scénarios hybrides..... 24
 - 1.6.3 La gestion des identités hybrides..... 24

2 ————— Azure Active Directory

Concepts et mise en œuvre de la gestion des identités hybrides

Chapitre 2 Azure Active Directory

1. EMS	27
1.1 Azure Active Directory	28
1.2 Azure Information Protection	29
1.3 Cloud App Security	30
1.4 Microsoft Intune	31
1.5 Microsoft Advanced Threat Analytics	31
1.5.1 Azure Advanced Threat Protection	33
1.6 EMS et les licences	33
2. Azure Active Directory	35
2.1 Présentation d'Azure Active Directory	35
2.1.1 Les éditions d'Azure Active Directory	37
2.1.2 Les limites d'Azure Active Directory	38
3. Microsoft et l'identité	39
3.1 Différences entre ADDS et Azure Active Directory	39
3.2 Les identités Microsoft dans le cloud	40
3.2.1 Azure Active Directory	40
3.2.2 ADDS sur une machine virtuelle Azure	41
3.2.3 Azure Active Directory Domain Service	41
4. L'identité hybride	43
4.1 Scénarios d'usage	44
4.1.1 Office 365	44
4.1.2 EMS	45
4.1.3 Application SaaS	45
4.2 Identité hybride et authentification	45
4.2.1 Synchronisation de mot de passe	46
4.2.2 Le Pass-through - Authentification directe	49
4.2.3 La fédération avec Active Directory Federation Services	51
4.2.4 PingFederate	52
4.3 Quel moyen d'authentification ?	53
4.4 Architecture Azure Active Directory	55

5. Débuter avec Azure Active Directory	59
5.1 Préparation du Bac à sable	59
5.1.1 Environnement Azure	60
5.1.2 Machines virtuelles - serveurs	78
5.1.3 Configuration réseau	86
5.1.4 Création du domaine Active Directory.....	92
5.1.5 Création de la structure utilisateurs	109
5.2 Création d'un annuaire Azure Active Directory.....	112
5.2.1 Création d'un tenant Office 365	112
5.2.2 Souscription d'un abonnement EMS E5	121
5.3 Configuration	125
5.3.1 Découverte de l'interface Azure Active Directory Admin center	125
5.3.2 Création d'un compte d'administrateur global.....	143
5.3.3 Ajout d'un domaine public personnalisé.....	149
5.3.4 Personnalisation	153
5.4 Azure Active Directory et PowerShell.....	154
5.4.1 Module MSOnline	154
5.4.2 Module AzureAD	159

Chapitre 3

Gestion des utilisateurs et des groupes

1. Les utilisateurs dans Azure Active Directory	165
1.1 Création des utilisateurs	166
1.1.1 Création des utilisateurs en interface graphique	166
1.1.2 Création des utilisateurs en PowerShell	172
1.2 La gestion des utilisateurs	174
1.2.1 Restauration de mots de passe.....	174
1.2.2 Supprimer un utilisateur	175
1.2.3 Restaurer un utilisateur	177
1.2.4 Donner un rôle à des utilisateurs.....	178
1.2.5 Propriété des utilisateurs Azure Active Directory	186

4 _____ Azure Active Directory

Concepts et mise en œuvre de la gestion des identités hybrides

2. Les groupes dans Azure Active Directory	190
2.1 Types de groupes	190
2.1.1 Groupe de sécurité	190
2.1.2 Groupe Office 365	190
2.2 Type d'appartenance	191
2.2.1 Affecté	191
2.2.2 Utilisateurs dynamiques	192
2.2.3 Appareil dynamique	197
2.3 Création des groupes affectés	201
2.3.1 Création des groupes en interface graphique	201
2.3.2 Création des groupes en PowerShell	202
2.4 La gestion des groupes	204
2.4.1 Vue d'ensemble	211
2.4.2 Propriétés des groupes	213
2.4.3 Ajout et suppression des membres	214
2.4.4 Propriétaire de groupe	216
2.4.5 Appartenance aux groupes	218
2.4.6 Applications	220
2.4.7 Licences	221
2.4.8 Ressources Azure	222
3. La gestion des licences	222
3.1 Présentation des licences	223
3.2 Affectation des licences	223
3.2.1 Affectation de licence à un utilisateur en interface graphique	225
3.2.2 Affectation de licence à un utilisateur en PowerShell ..	229
3.2.3 Affectation de licence à un groupe en interface graphique	240

Chapitre 4

Gestion des appareils et applications

1. Gestion des appareils dans Azure Active Directory	243
1.1 Introduction	243
1.1.1 Le modern Management	244
1.1.2 Paramètres dans Azure Active Directory	247
1.2 Inscription d'appareils - Azure AD Registration.....	249
1.2.1 Comment inscrire un poste Windows 10 dans Azure Active Directory ?.....	250
1.2.2 Propriétés de l'appareil inscrit	254
1.3 Jonction d'appareils - Azure AD Join.....	256
1.3.1 Comment joindre un poste Windows 10 dans Azure Active Directory ?.....	258
1.3.2 Propriétés de l'appareil joint.....	262
1.3.3 Gestion des appareils joints à Azure Active Directory ..	263
1.3.4 Audit et logs	265
1.4 Appareils hybrides dans Azure Active Directory	268
1.4.1 Concept.....	268
1.4.2 Fonctionnement	269

Chapitre 5

Azure Active Directory et les applications

1. Introduction	271
2. Les applications intégrées à Azure Active Directory	272
2.1 Introduction	272
2.2 Les avantages	276
2.3 Les types d'applications	277
3. Intégration d'applications dans Azure Active Directory	277
3.1 Démarches.....	278
3.2 Intégrer une application SaaS	279
3.2.1 Authentification SSO.....	284

6 ————— Azure Active Directory

Concepts et mise en œuvre de la gestion des identités hybrides

3.2.2	Création et ajout des utilisateurs	
Azure Active Directory		295
3.2.3	Ajout de l'utilisateur au niveau de l'application	 295
3.3	Gestion d'une application intégrée	 298
3.4	Signature de jeton SAML	 308
3.5	Configuration des rôles claims dans un jeton SAML	 312
3.6	Fonctionnement du SAML avec Azure Active Directory	 318
4.	Enregistrement d'applications	 320
4.1	Introduction	 320
4.2	Enregistrer une application	 320
5.	Azure Application Proxy	 321
5.1	Présentation	 322
5.2	Fonctionnement d'Azure Application Proxy	 324
5.3	Exemples	 325
5.4	Publication d'applications IIS	 326
5.4.1	Téléchargement et installation du connecteur proxy	.. 327
5.4.2	Intégration de l'application locale	
dans Azure Active Directory		332
5.4.3	Ajout d'un utilisateur au niveau de l'application	 335
5.4.4	Test d'accès à l'application depuis l'extérieur	 336
5.4.5	Test depuis le portail Myapps	 337
5.5	Mode d'authentification	 338

Chapitre 6

Gestion des identités hybrides

1.	Introduction	 339
2.	Extension d'un Active Directory local	
vers Azure Active Directory		340
2.1	Pourquoi étendre ses utilisateurs	
vers Azure Active Directory ?		341
2.2	Les attributs Active Directory stockés	
dans Azure Active Directory		342

2.3	Avant d'étendre son Active Directory	344
2.4	L'outil IdFix	350
3.	Azure Active Directory Connect	354
3.1	Présentation d'AAD Connect	354
3.2	Architecture	354
3.3	Topologies avec AAD Connect	355
4.	Avant d'installer AAD Connect	357
4.1	Prérequis Azure Active Directory	357
4.2	Prérequis ADDS	358
4.3	Prérequis serveur AAD Connect	358
4.4	Prérequis du serveur SQL	360
4.5	Prérequis des comptes d'administration et comptes de services	360
4.6	Prérequis réseau	361
5.	Installation de AAD Connect	365
5.1	Installation personnalisée	368
5.2	Configuration Express Settings	387
5.3	Validation et configuration supplémentaire	387
5.4	Activation de la synchronisation avec le hash Sync	395
5.5	Vérification de l'état de la synchronisation	400
6.	Active Directory Fédération Service	404
6.1	Installation d'ADFS	404
6.1.1	Prérequis	408
6.1.2	Installation ADFS interne	412
6.1.3	Installation du Web Application Proxy	427
7.	AAD Connect et les options d'authentification	437
7.1	Synchronisation de hachage de mot de passe	438
7.1.1	Configuration	438
7.1.2	Validation	441
7.2	Le Pass-through	443
7.2.1	Prérequis	443
7.2.2	Configuration	444

8 **Azure Active Directory**

Concepts et mise en œuvre de la gestion des identités hybrides

7.2.3	Validation	446
7.3	La fédération avec ADFS	448
7.3.1	Configuration	448
7.3.2	Vérification	451
8.	Gestion d'AAD Connect	452
8.1	Personnalisation de la synchronisation	452
8.1.1	Filtrage des OU	453
8.1.2	Fonctionnalités en options	456
8.1.3	Azure APP	457
8.1.4	Azure AD Attributs	458
8.2	Gestion des appareils hybrides	458
8.2.1	Prérequis	459
8.2.2	Configuration Hybrid Azure AD	460
8.2.3	Configuration Device WriteBack	467
8.2.4	Opérations au niveau des appareils	472
8.3	Le mode Staging	475
8.3.1	Introduction	475
8.3.2	Configuration	476
9.	AAD Connect Health	479
9.1	AAD Connect Health pour AADS	480
9.1.1	Installation	480
9.2	AAD Connect Health ADFS	485
9.2.1	Installation	486
9.3	AAD Connect Health Sync	489
9.3.1	Administration	490
10.	Résumé	494
10.1	Méthode d'authentification	495

Chapitre 7 Gestion de la synchronisation

1. AAD Connect	497
1.1 Présentation des outils	498
1.1.1 Import du module PowerShell.....	499
1.1.2 Architecture de synchronisation	504
1.2 Synchronisation des utilisateurs	508
1.3 Le filtrage.....	510
1.3.1 Éditeur de règles de synchronisation.....	516
1.3.2 Création de règle de synchronisation positive	519
1.4 Connecteur space	534
1.4.1 Connecteur space Active Directory.....	535
1.4.2 Connecteur space Azure Active Directory	544
1.5 Métaverse	544
1.5.1 Métaverse Designer	545
1.5.2 Metaverse Search	548
1.5.3 Propriétés des objets.....	552
2. Opérations et configurations.....	557
2.1 AAD Connect Scheduler	557
2.1.1 Configuration et opérations	558
2.1.2 Changement de mots de passe du compte de service AD Sync.....	565
2.1.3 Prévention des suppressions accidentelles	568
2.1.4 Statistiques	571
3. Problématique.....	572
3.1 Cas réel d'entreprise	572
3.1.1 Explication	573
3.1.2 Démonstration	574

10 ————— Azure Active Directory

Concepts et mise en œuvre de la gestion des identités hybrides

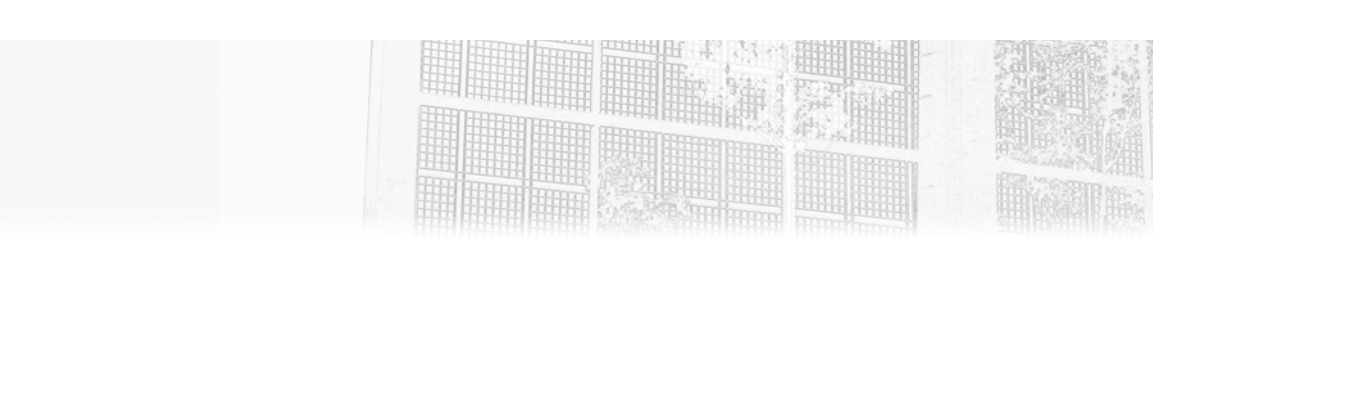
Chapitre 8

Azure Active Directory, sécurité et collaboration

1. Introduction	581
2. Accès conditionnel	582
2.1 Introduction	582
2.1.1 Conditions	584
2.1.2 Exemple MFA pour le portail Azure	585
3. Azure Active Directory Identity Protection	607
3.1 Introduction	607
3.1.1 Activation	609
3.1.2 Administration	612
4. Azure MFA	629
4.1 Introduction	630
4.1.1 Configuration	632
4.1.2 Test	636
5. Azure Active Directory smart lockout	642
5.1 Introduction	642
5.1.1 Configuration	643
5.2 Protection des mots de passe d'Active Directory local.	646
5.2.1 Introduction	647
5.2.2 Prérequis	648
5.2.3 Mise en place	650
6. Collaboration	658
6.1 Azure B2B	658
6.1.1 Invitation e-mail	659
7. Gestion de mot de passe	663
7.1 Le self-service	664
7.1.1 Configuration	664
7.1.2 Test	669
8. Azure Active Directory Secure Score	674
8.1 Fonctionnement	674

Conclusion

1. Introduction	681
2. L'identité hybride	682
3. La gestion des appareils	684
4. Modern management	684
5. Sécurité	685
6. Ce que nous avons abordé	686
6.1 Le design d'une architecture hybride	687
6.2 L'extension vers Azure Active Directory	687
6.2.1 AAD Connect	687
6.2.2 Méthode d'authentification	688
6.3 Gestion de l'hybridation	688
6.3.1 Utilisateurs	688
6.3.2 Ordinateurs	688
6.4 Azure Active Directory, la sécurité et la collaboration	689
6.4.1 L'accès conditionnel	689
6.4.2 Azure B2B	689
6.4.3 Azure Active Directory Application Proxy	689
6.4.4 Azure Active Directory Password Protection	690
6.4.5 Azure Active Directory MFA	690
6.4.6 Azure Active Directory Identity Protection	690
Index	691



Chapitre 6

Gestion des identités hybrides

△ 1. Introduction

Jusqu'à présent, nous nous sommes majoritairement focalisés sur une infrastructure *full cloud* Azure Active Directory pour la gestion, entre autres, des comptes utilisateurs. Bien entendu, ce genre de configuration ne convient pas si l'entreprise dispose d'un annuaire Active Directory local et souhaite accéder à des applications ou services cloud tels qu'Office 365 (SharePoint Online, Exchange Online, OneDrive Online, Microsoft Teams, etc.) avec ses utilisateurs locaux.

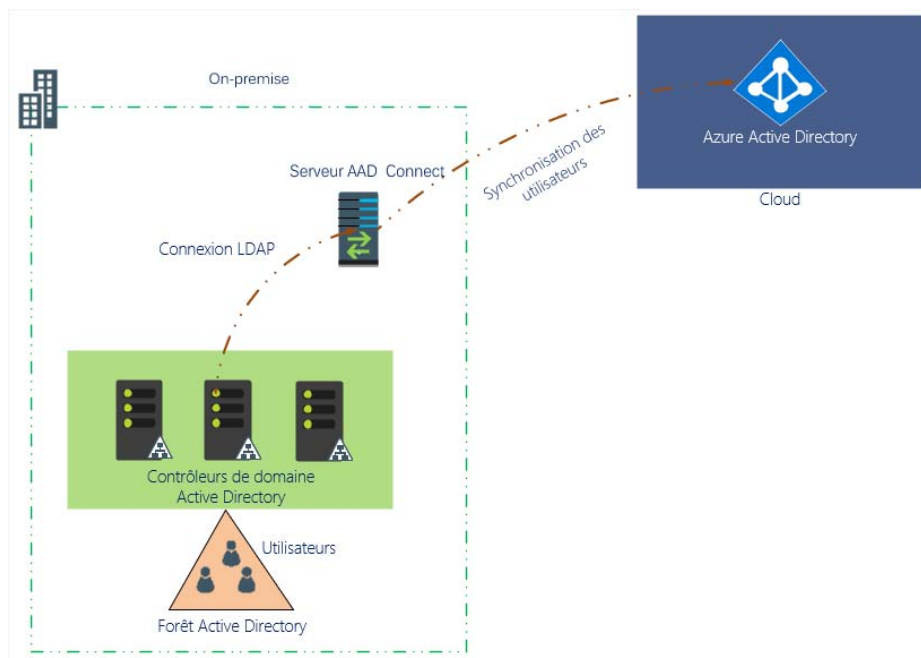
Dans ce cas, il faut étudier la mise en œuvre d'une solution hybride permettant à un utilisateur, dont l'identité est contenue dans l'annuaire Active Directory local, d'accéder aux ressources internes de l'entreprise et de disposer d'une identité dans le cloud (et plus précisément dans Azure Active Directory) pour consommer et s'authentifier auprès des services cloud et applications Office 365.

Cette configuration revient à synchroniser les utilisateurs d'un Active Directory local avec l'annuaire Azure Active Directory dans le cloud. C'est ce qui revient à dire qu'avec Azure Active Directory, nous accédons à plusieurs applications avec une **seule et unique identité**.

Avec Azure Active Directory, notre façon de gérer l'identité change et devient hybride. La gestion des identités ne s'effectue plus seulement en local, mais également, pour les comptes synchronisés, dans le cloud. De nouvelles méthodes d'authentification à administrer apparaissent permettant d'accéder, à l'aide d'une seule identité, aux services cloud et applications SaaS. Nous verrons plus loin dans ce chapitre la gestion de ces authentifications ainsi que les différentes méthodes permettant l'extension d'un Active Directory local vers Azure Active Directory.

2. Extension d'un Active Directory local vers Azure Active Directory

Comme expliqué à plusieurs reprises, l'extension d'un Active Directory local consiste à synchroniser des utilisateurs de l'Active Directory local vers Azure Active Directory. Voici une illustration qui montre ce concept d'hybridation d'identité :



Dans une infrastructure à identité hybride, nous possédons au moins les composants suivants :

- un annuaire Active Directory
- un serveur AAD Connect
- des utilisateurs/groupes d'utilisateurs - OU
- un annuaire Azure Active Directory

■ Remarque

Volontairement, nous n'avons pas indiqué ici de ferme AD FS, car il s'agit de lister les éléments minimums afin de synchroniser des utilisateurs locaux vers Azure Active Directory.

Sur l'illustration précédente, nous remarquons que le serveur Azure Active Directory Connect se connecte à la forêt Active Directory via l'un des contrôleurs de domaine et effectue une synchronisation avec Azure Active Directory en fonction des règles et filtrage d'OU imposés. Avec cette configuration précise, certains utilisateurs posséderont à la fois un compte au sein de l'annuaire Active Directory local et dans l'annuaire Azure Active Directory, d'où le nom « identité hybride ».

2.1 Pourquoi étendre ses utilisateurs vers Azure Active Directory ?

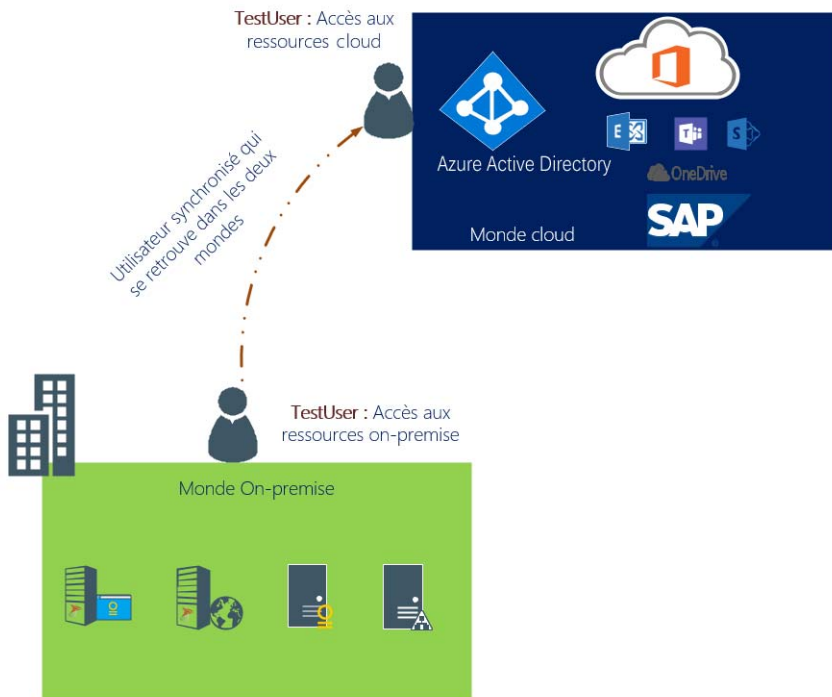
Même si nous avons déjà répondu à cette question, il est très important de comprendre ce que cela représente, et dans quel but on choisit d'étendre un Active Directory vers Azure Active Directory.

Comme évoqué à plusieurs reprises, le cloud est un monde complètement à part. Microsoft offre plusieurs services : les services Office 365, Azure ou encore des applications SaaS. Ces services nécessitent, comme tout service, une authentification sécurisée qui s'appuie pour cela sur l'annuaire Azure Active Directory. Une entreprise qui souhaite bénéficier de ces services et les proposer à ses utilisateurs ne va pas leur proposer un compte et un mot de passe pour chaque application et service, en plus de leur compte local Active Directory. Cela deviendrait lourd à gérer pour les utilisateurs et pour les administrateurs.

342 ————— Azure Active Directory

Concepts et mise en œuvre de la gestion des identités hybrides

La nécessité d'étendre un annuaire Active Directory local est alors démontrée. En faisant cela, l'utilisateur peut accéder aux services cloud et non cloud avec la même identité. Il s'agit d'un enjeu crucial pour les grandes entreprises.



2.2 Les attributs Active Directory stockés dans Azure Active Directory

Bien sûr, vous l'avez compris, en synchronisant un utilisateur, ses attributs vont se dupliquer dans le cloud, et plus principalement dans l'annuaire Azure Active Directory. À la nuance près qu'une partie seulement des attributs seront synchronisés : ceux nécessaires a minima pour l'authentification auprès des services et applications cloud.

Beaucoup d'entreprises européennes s'interrogent sur l'emplacement du stockage de leurs données pour des questions de législation, refusant par exemple de les entreposer dans des datacenters aux États-Unis.

Il faut savoir que l'emplacement de stockage des données, en ce qui concerne les offres cloud Microsoft, dépend de l'adresse fournie lors de l'inscription au service Office 365 ou Azure Active Directory pour mieux répondre aux problématiques légales de certains pays européens concernant la localisation de leurs données.

Un site de Microsoft très bien fait explique tout cela : <https://www.microsoft.com/en-us/trustcenter/privacy/where-your-data-is-located>

■ Remarque

La plupart des attributs des utilisateurs des entreprises européennes sont stockés dans les datacenters en Europe, à l'exception des attributs utilisateurs listés ci-dessous qui demeurent entreposés dans les datacenters aux USA :

- givenName
- Name
- UserPrincipalName
- Domain
- PasswordHash
- SourceAnchor
- AccountEnabled
- PasswordPolicies
- StrongAuthenticationRequirement
- ApplicationPassword
- PUID

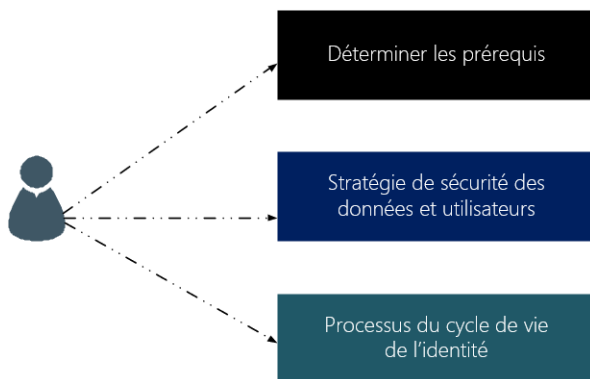
Ces attributs permettent l'authentification et le fonctionnement des utilisateurs. Aucune donnée personnelle des utilisateurs n'est stockée.

2.3 Avant d'étendre son Active Directory

Tout d'abord, il est important de définir les besoins, d'analyser l'existant et de choisir la bonne stratégie. Cette étape d'étude est très importante, et il est préférable de la mettre en œuvre dans chaque projet.

Cette étape regroupe :

- la détermination des prérequis
- la stratégie de sécurité des données et utilisateurs
- le processus du cycle de vie de l'identité



Détermination des prérequis

Cette phase est importante car il s'agit de déterminer les besoins métiers de l'entreprise et de connaître sa stratégie sur le court et le long terme vis à vis du cloud.

Plusieurs points sont à prendre en compte dans cette partie :

- Pourquoi une architecture hybride et pour quels besoins ?
- Pourquoi se diriger vers le cloud ? Connaître et définir la stratégie de l'entreprise.
- Lister les moyens d'authentification utilisés actuellement dans l'entreprise, ce qui permet de définir les besoins techniques pour intégrer une architecture hybride avec Azure Active Directory.