Chapitre 3
Concepts de base

1. Introduction

Les exercices du chapitre précédent ont permis de prendre en main le portail de gestion et de créer et d'organiser des raccourcis, afin de faciliter la navigation dans les menus. C'est une toute première étape.

Dans ce chapitre, le point de départ est la notion d'organisation et de gouvernance dans Azure. Tous les concepts, quels qu'ils soient, sont adossés à cette notion de gouvernance. Tout le début du chapitre est consacré à ce sujet majeur, au cœur de toute l'infrastructure Azure. Puis viennent la présentation et l'explication de la convention de nommage des ressources puis de la politique d'étiquettes. Enfin, il va être temps de créer une première ressource.

Dans la suite du chapitre, les concepts de base sont expliqués : comment mieux protéger ses ressources et éviter une suppression accidentelle ? Que sont les RBAC (contrôle d'accès basé sur un rôle) et que permettent-ils ? Ou même comment choisir sa région d'appartenance, la région sur laquelle déployer ses ressources Azure ?

Puis le chapitre se poursuit par une simulation de calcul des coûts engendrés par le déploiement d'une ressource ou d'un service (ensemble de ressources par exemple).

Le sujet important de la redondance vient clore ce chapitre.

Ces sujets doivent être abordés afin de passer sereinement à la suite. Ce chapitre est dense et aborde de nombreuses notions essentielles utiles pour le démarrage. Il demande une bonne lecture pour être assimilé. Il se prête assez peu aux exercices, il faut passer du temps sur ces points théoriques.

Ces concepts de base ne sont pas les points les plus techniques présents sur Azure mais ils sont très impactants s'ils sont mal mis en œuvre et si ces quelques règles simples ne sont pas respectées. Le point qui suit sur la gouvernance est certainement le moins considéré par les entreprises qui démarrent et même par celles qui ont déjà un grand nombre de charges de travail déployées sur Azure, et cela est bien dommage. C'est certainement cette partie qui demande le plus d'investissement par la suite pour corriger et réaligner son architecture. Alors autant le prendre en compte dès le départ pour démarrer dans des bonnes conditions.

2. Gouvernance

La gouvernance Azure désigne l'ensemble des stratégies, des méthodes et de l'organisation qui permettent de gérer les ressources, la sécurité et la conformité dans l'environnement Azure. C'est une définition assez générique. Derrière cette définition, il y a une organisation assez cadrée et que l'on retrouve souvent sous le terme CAF ou Cloud Adoption Framework (cadre d'adoption du cloud). Le terme est assez rarement utilisé en Français. Il faut donc retenir ce terme de CAF !

Le CAF, c'est un ensemble de bonnes pratiques et de recommandations qu'il faut essayer d'adapter (et d'adopter) dans le cadre de l'entreprise. Lorsque l'on arrive sur le cloud, c'est la partie la plus facile, rien n'existe, respecter les bonnes pratiques dès le départ est une règle de bon sens. Lorsque l'on est déjà sur le cloud et que l'on n'a pas forcément respecté les recommandations, c'est un peu plus difficile, voire beaucoup plus difficile. Plus le temps passé hors d'une implémentation conforme au CAF est élevé, plus les charges de remédiation vont l'être également. Mais la bonne pratique à la cible, c'est qu'il faut essayer de se rapprocher le plus possible de ce Framework.

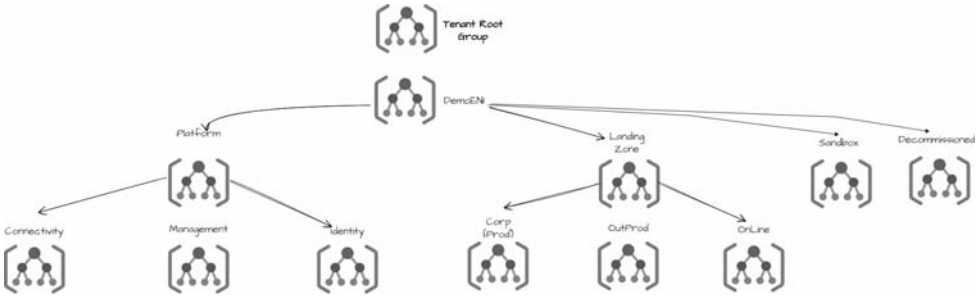
Ce n'est pas une notion purement technique, mais plutôt un cadre organisationnel. Il y a assez peu de composants pour déployer ce socle de base de la gouvernance. Sous sa forme la plus simple, on retrouve des groupes de managements appelés groupe de gestion (ou Management groups), des abonnements (ou subscriptions). Ce sont deux types de conteneurs organisationnels qui ne sont pas à proprement parler des ressources Azure. Ces conteneurs ne sont pas facturés, ils servent à organiser (gouverner) les environnements.

Si au départ, ce n'est pas un point technique, ne pas s'appuyer sur l'arborescence de ces conteneurs rend l'utilisation d'Azure beaucoup plus compliquée. Il n'est pas inutile de le dire plusieurs fois tellement ce point est structurant Avec un bon démarrage conforme au CAF, le travail se fait de manière globale, de manière industrielle. Sans, ce n'est pas la même charge.

Avant d'aller plus loin dans cet exemple, un peu plus d'informations.

Les groupe de management, ce sont les conteneurs de plus haut niveau. Ils se trouvent tout au sommet de l'arborescence. Ils peuvent contenir d'autres groupes de management et des abonnements Azure. Le CAF propose une arborescence type pour ces MG (groupes de management). Sous le MG Tenant Root Group qui est un MG obligatoire et précréé par Azure, on doit trouver un MG intermédiaire qui, normalement, porte le nom de l'organisation. C'est DemoENI dans le schéma suivant. Puis on sépare son organisation avec, d'un côté, les ressources de plateforme, c'est-à-dire le cœur de l'organisation où vont se trouver toutes les ressources du socle partagé de l'entreprise (ressource cœur de réseau, cœur de l'administration et cœur de l'identité). D'un autre côté, les ressources applicatives, ce que l'on retrouve communément sous le terme de zone d'atterrissage Azure (ou Landing Zone). Puis, de manière plus anecdotique, deux MG, l'un pour les ressources et abonnements décommissionnés (c'est-à-dire qui sont amenés à être supprimés), et l'autre pour les environnements de bac à sable.

Ce qui se présente sous la forme d'un schéma de ce genre :



Une arborescence organisationnelle conforme au CAF

Voilà à quoi ressemble une hiérarchie, une arborescence organisationnelle conforme au CAF. Ce n'est finalement pas très compliqué, c'est une arborescence à quatre niveaux, mais qui, avec un peu d'habitude, reste très lisible. La question est de savoir à quoi cela sert. Ce n'est fait de cette manière pour des raisons esthétiques, bien évidemment.

Pour vraiment maîtriser cette partie, deux autres schémas avec l'ajout de composants/ressources qui donnent de la valeur au modèle. Dans le premier, deux notions complémentaires sont ajoutées.

– La notion de RBAC, contrôle d'accès basé sur les rôles (ou *Role-Based Access Control*) traités en détail dans le chapitre Identité et accès. Pour l'instant, pour comprendre le schéma, il faut retenir que ce sont les RBAC qui vont définir les droits d'accès.
– La notion de stratégie (ou Policy) Azure traitée dans le chapitre Bonnes pratiques. Pour l'instant, il faut retenir que les stratégies sont une aide à l'administration, des « garde-fous » qui aident les administrateurs à garantir la conformité des ressources. C'est un peu plus fin que cette simple définition, mais c'est pour l'instant suffisant pour comprendre le schéma.

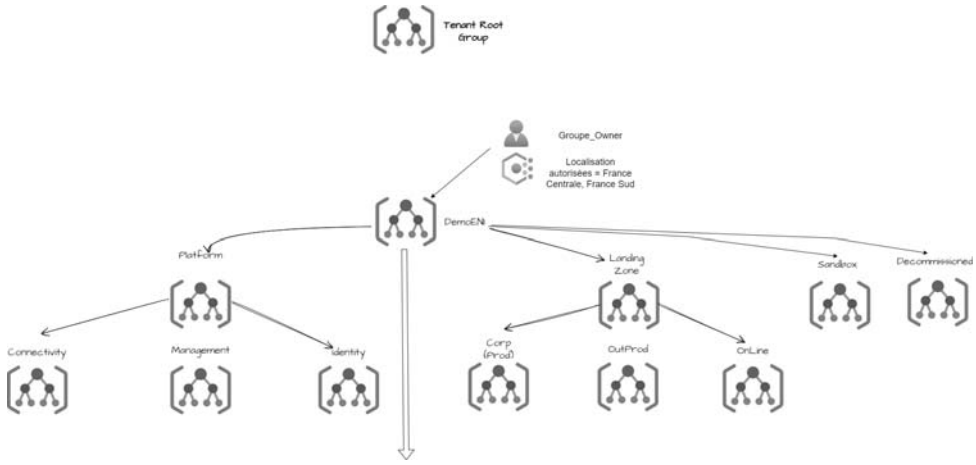
Remarque

Le terme Azure Policy ou Policy est très communément utilisé sur Azure. Sa version française, stratégie, l'est peu. Pour cette raison, il sera question de Policy tout au long de ce chapitre.

Ci-dessous, RBAC et Policy sont ajoutés. Au sommet de l'arborescence (juste en dessous, en fait), c'est-à-dire sur le MG *DemoENI* qui est le MG intermédiaire. En termes de gouvernance, c'est l'ajout d'un groupe de sécurité avec un rôle Owner (propriétaire) et une stratégie Azure qui autorise les déploiements uniquement sur les régions France Centre et France Sud. Ce positionnement sur le MG *DemoENI* garantit que tout ce qui se trouve plus bas va hériter de ces RBAC et de cette stratégie.

Remarque

La notion d'héritage est une notion de base. Tout ce qui se trouve au niveau supérieur va redescendre sur les niveaux inférieurs. Dans le schéma ci-dessous, par exemple, ce qui est placé sous DemoENI va redescendre en bas de l'arborescence en partant de DemoENI. Ce qui se trouve sur Landing Zone va redescendre en bas de l'arborescence en partant de Landing Zone, etc.



RBAC et Policy au plus haut niveau.

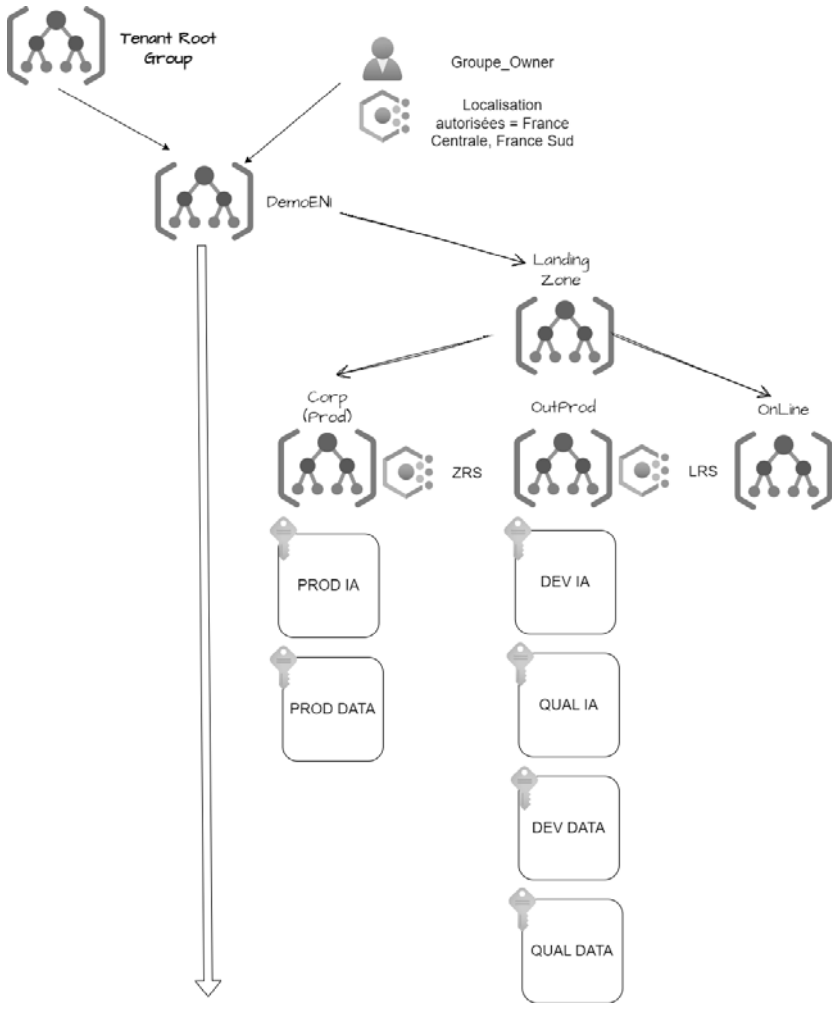
Dernier schéma pour aller au bout du raisonnement : les MG sont des conteneurs organisationnels qui sont peuplés par d'autres MG, comme ci-dessus, avec Connectivity qui est placé dans Plaform, lui-même placé dans DemoENI.

Mais ce sont également des abonnements qui sont placés sous les MG. L'abonnement, c'est aussi un conteneur d'organisation qui va accueillir d'autres conteneurs organisationnels, les groupes de ressources.

Remarque

Par abus de langage, on parle souvent des ressources de l'abonnement. Mais ce sont en fait les ressources qui sont dans les groupes de ressources de l'abonnement. Dans le portail, sur un abonnement, il n'y aura jamais d'autres ressources que des groupes de ressources. Il n'est pas possible de créer une ressource directement dans l'abonnement.

Avec cet exemple complet dans le schéma suivant, on trouve des abonnements différents dans *OutProd* qui symbolise l'environnement hors production et *Corp* qui symbolise les environnements de production. Le schéma est un peu simplifié pour être plus clair. Les abonnements dans le MG Corp héritent de tout ce qui vient de *DemoENI => Landing Zone => Corp*. Dans cet exemple, les RBAC Groupe_Owner, la stratégie de déploiement en France uniquement plus une nouvelle stratégie positionnée sur le MG Corp qui oblige à déployer des ressources uniquement avec une redondance de zone (ZRS). Du côté des abonnements positionnés sous le MG *OutProd*, même chose pour ce qui est hérité de *DemoENI => Landing Zone*, mais avec, cette fois, au niveau du MG *OutProd*, une stratégie différente et une obligation de déploiement dans un mode de redondance locale (LRS).

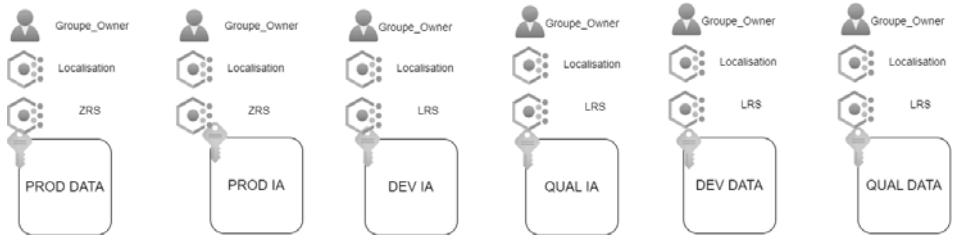


Détail de l'arborescence dans la Landing Zone

Cet exemple est parfait pour illustrer l'intérêt de cette hiérarchie et les avantages que cela apporte. Avec, la gestion est globale et l'héritage est utilisé pour traiter un ensemble.

Pour vraiment valider la compréhension de ce sujet, ce même modèle avec ces six abonnements sans hiérarchie, c'est-à-dire dans un modèle « à plat ».

Il n'y a plus de modèle avec une arborescence hiérarchique, il ne peut exister sans MG car un abonnement ne peut pas contenir d'autres abonnements. Placer le groupe de sécurité *Groupe_Owner* sur ces six abonnements, c'est maintenant le faire six fois. Placer la stratégie de localisation en France, c'est le faire six fois également. La stratégie de prod ZRS, deux fois et pour terminer, la stratégie de OutProd quatre fois. C'est-à-dire qu'il faut réaliser l'opération 18 fois pour placer les choix de gouvernance.



Une structure plate (non arborescente) n'offre pas toutes les possibilités d'une structure avec arborescence conforme au CAF

Pour rappel, dans un modèle hiérarchique gouverné, ce même résultat est obtenu en quatre opérations. C'est donc le modèle CAF qu'il faut choisir pour plus d'efficacité, plus de cohérence (avec un risque d'erreur beaucoup plus faible) et la possibilité de profiter de l'héritage pour tous les nouveaux abonnements qui, dès qu'ils sont placés dans le bon MG, vont récupérer un ensemble de paramètres cohérents et définis à l'avance.

Remarque

Si ce modèle conforme au CAF n'est pas choisi dès le départ, il n'est pas impossible de se réaligner, mais c'est une opération qui prend énormément de temps et qui peut présenter des risques faibles à moyens. Corriger les déviances à terme est bien plus contraignant que de fixer les limites dès le départ.

3. Convention de nommage

Ce point sur la convention de nommage ainsi que la section suivante consacrée à l'étiquetage des ressources sont des sujets sur lesquels on ne passe pas assez de temps lorsque l'on découvre Azure. Pourtant, ils sont au centre de l'organisation des ressources et apportent beaucoup.

Il faut être exigeant sur le sujet. Le cloud offre des mécanismes de délégation et étant donné la facilité des déploiements, il permet de déléguer rapidement des opérations. Une convention de nommage doit être proposée pour garantir une plus grande homogénéité et rendre l'identification d'un composant plus facile.

Remarque

Il est tout à fait possible de partir de zéro et de créer sa propre convention de nommage. Il existe différentes propositions sur Internet pour simplifier cette tâche. Dans cet ouvrage, la convention retenue est celle proposée par l'éditeur Microsoft à l'adresse https://docs.microsoft.com/fr-fr/azure/cloud-adoption-framework/ready/azure-best-practices/resource-naming, puis à cette adresse https://docs.microsoft.com/fr-fr/azure/cloud-adoption-framework/ready/azure-best-practices/resource-abbreviations. Elle est simple à mettre en œuvre et couvre de très nombreux besoins.

Les propositions faites dans ce lien sont à base d'abréviations pour préfixer les ressources. Dans la pratique, identifier une machine virtuelle dont le nom commence par vm est beaucoup plus facile que des nommages non conventionnels du type *machinetest*, *virttest* ou *001compute*. Ce sujet est plus complexe qu'il n'y paraît. Comme il l'est également On-premises. Définir la convention demande parfois plusieurs réunions et relectures.

Il n'est pas possible de tout faire lorsqu'il s'agit de nommer une ressource et les règles sont différentes selon les ressources. Ainsi, un compte de stockage ne peut contenir que des lettres minuscules et des chiffres, et la longueur doit être comprise entre 3 et 24 caractères.

Un disque managé, quant à lui, peut contenir de 1 à 80 caractères et des caractères alphanumériques, des soulignements et traits d'union (caractères _ et -).

Lorsque la convention n'est pas adaptée à la ressource, il n'est pas possible de valider la création et un message est affiché en erreur avec un rappel des règles.