

MICROSOFT PUBLIC SECTOR CLOUD DESIGN

Cloud Governance & Security
dans le secteur public suisse



Documents connexes

Nom du document

Microsoft Public Sector Cloud Design

Document : Cloud governance & Security dans le secteur public suisse V1.4

Identification : Governance and Security Guideline Swiss Public Sector_V1.4

Azure Blueprints for Public Sector (ISO 27001)

[Microsoft Docs](#)

© (2021) Microsoft Corporation. All rights reserved. Microsoft, Windows and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries.

The information herein is for informational and discussion purposes only and represents the current view of Microsoft Corporation or any Microsoft Group affiliate as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment or binding offer or acceptance of any warranties, liabilities, wrongdoing etc. on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this document.

Sommaire

1	Objet de ce document	5
2	Contenu et structure.....	5
3	Principes de base	6
3.1	Aménagement de la zone d'atterrissement.....	6
3.2	Rôles et organisation.....	7
3.3	Contrôle des accès (RBAC)	7
3.4	Azure Arc.....	8
3.5	Policies et paramètres de sécurité.....	9
3.5.1	Allowed Location Policy.....	9
3.6	Monitoring.....	10
3.7	Réseau	10
3.7.1	Qu'est-ce qu'un réseau virtuel dans Azure ?	10
3.7.2	Segmentation du réseau	11
3.7.2.1	Groupes de sécurité réseau NSG.....	11
3.7.2.2	Application Security Groups ASGs	11
3.7.2.3	Pare-feu	11
3.7.3	Connexion réseau selon Azure	11
3.8	Active Directory	11
3.9	Key Vault.....	12
3.10	Contrôle des coûts	12
3.11	Security Center.....	13
4	Contrôles ISO 27001.....	14
4.1	A.6.1.2 Cloisonnement des tâches	14
4.2	A.8.2.1 Classification des informations	15
4.3	A.9.1.2 Accès aux réseaux et services réseaux	15
4.4	A.9.2.3 Gestion des droits d'accès privilégiés	16
4.5	A.9.2.4 Gestion des informations secrètes d'authentification des utilisateurs.....	16
4.6	A.9.2.5 Vérification des droits d'accès des utilisateurs	17
4.7	A.9.2.6 Suppression ou modification des droits d'accès	18
4.8	A.9.4.2 Procédures de connexion sécurisées.....	18
4.9	A.9.4.3 Système de gestion des mots de passe	19
4.10	A.10.1.1 Stratégie sur l'utilisation des contrôles de chiffrement	20
4.11	A.12.4.1 Journalisation des événements.....	21
4.12	A.12.4.3 Journaux des administrateurs et des opérateurs	21
4.13	A.12.4.4 Synchronisation des horloges.....	22
4.14	A.12.5.1 Installation de logiciels sur les systèmes d'exploitation.....	22
4.15	A12.6.1 Gestion des vulnérabilités techniques.....	22
4.16	A.12.6.2 Restrictions liées à l'installation de logiciels	23
4.17	A.13.1.1 Contrôles de réseau.....	23
4.18	A.13.2.1 Stratégies et procédures de transfert d'informations	24

Figures

Figure 1 – Blueprint ISO 27001 Shared Services.....	6
Figure 2 – Imbrication RBAC.....	7
Figure 3 – Champs d'application des droits d'accès accordés aux rôles	8
Figure 4 – Vue d'ensemble des fonctions d'Azure Arc.....	8
Figure 5 – Rapport de synthèse sur la conformité.....	9

Avis de non-responsabilité

Ce document reprend les questions souvent posées par nos clients sur l'utilisation des solutions de cloud computing. Il devrait vous permettre de mieux comprendre les contextes techniques et juridiques impliqués par l'utilisation d'une solution d'informatique en nuage. Ce document n'inclut pas un examen spécifique de la situation juridique individuelle. Pour obtenir une évaluation juridique individuelle et définitive sur la recevabilité de l'utilisation des solutions Microsoft Cloud spécifique à votre cas, vous devrez donc recourir séparément à un conseil juridique.



1 OBJET DE CE DOCUMENT

Ce document sert de guide et de recommandation pour la mise en place d'un environnement de plateforme de cloud standardisé ainsi que pour son opérationnalisation. Il prend en compte les risques identifiés dans Microsoft Public Sector Cloud Design. La norme de sécurité ISO 27001 tient lieu de référence pour les mesures et contrôles.

2 CONTENU ET STRUCTURE

Pour réaliser une zone d'atterrissement standardisée dans le cloud public Azure conformément à la norme ISO 27001, nous fournissons des modèles de déploiement des composants requis et recourons à des mécanismes de contrôle. À cet effet, nous prenons d'abord en compte les concepts de base des composants puis les différents contrôles qui en vérifient l'efficacité.

Tout risque qui serait identifié et écarté de Microsoft Public Sector Cloud Design est signalé.

3 PRINCIPES DE BASE

Les modèles ISO 27001 servant à déployer les composants de la zone d'atterrissement s'appuient sur des Azure Blueprints¹ appliqués à un ou plusieurs abonnements. Des groupes de ressources, des autorisations et des stratégies sont créés à cet effet.

- ISO 27001² → Ce blueprint comprend des stratégies générales pour la mise en œuvre de mesures sur des ressources d'application existantes ou à créer.
- ISO 27001 : Services partagés³ → Ce blueprint crée les ressources centrales et partagées qui sont requises pour la prise en charge des opérations de la zone d'atterrissement, autorisations des rôles par défaut comprises.
- ISO 27001 : charges de travail ASE/SQL⁴ → Ce blueprint optionnel fournit un ou plusieurs environnements d'application standardisés et basés sur le web qui s'appuient sur des ressources PaaS du type «App Service» et «SQL DB».

Le compte rendu sur la conformité aux contrôles ISO 27001 s'effectue avec l'aide d'Azure Security Center, qui signale toutes les divergences de contrôle dans les ressources des abonnements associés. Pour ce faire, celui-ci applique une compilation de stratégies où seul est conservé le résultat d'audit par stratégie.

3.1 AMÉNAGEMENT DE LA ZONE D'ATTERRISSAGE

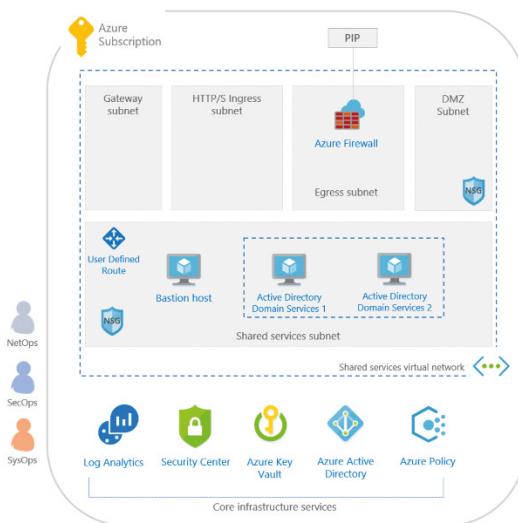


Figure 1 – Blueprint ISO 27001 Shared Services

La zone d'atterrissement basée sur ISO 27001 est une approche architecturale et une mise en œuvre qui fait référence au niveau de l'entreprise. Elle permet de créer et de rendre opérationnelles à grande échelle les zones cibles dans Azure. Elle cadre avec l'Azure Roadmap et le Cloud Adoption Framework⁵ pour Azure.

L'architecture prévoit une zone centrale divisée qui est couverte par un abonnement et d'autres zones dédiées à des applications (telles qu'ISO 27001 : charges de travail ASE/SQL) qui font l'objet d'abonnements spécifiques. Les différents composants de la zone centrale sont décrits dans les chapitres suivants.

En fonction des considérations techniques et des recommandations en aménagement de cette architecture, il est possible d'envisager différents compromis selon le scénario de votre entreprise. Une légère divergence n'est pas exclue mais si vous suivez les recommandations de base, l'architecture cible qui en résultera conduira votre organisation sur la voie d'une évolution durable.

¹ <https://docs.microsoft.com/fr-ch/azure/governance/blueprints/overview>

² <https://docs.microsoft.com/fr-ch/azure/governance/blueprints/samples/iso-27001-2013>

³ <https://docs.microsoft.com/fr-ch/azure/governance/blueprints/samples/iso27001-shared>

⁴ <https://docs.microsoft.com/fr-ch/azure/governance/blueprints/samples/iso27001-ase-sql-workload>

⁵ <https://docs.microsoft.com/fr-ch/azure/cloud-adoption-framework/>

3.2 RÔLES ET ORGANISATION

Seul un personnel compétent et habilité à accomplir les tâches qui lui sont confiées saura correctement mettre en place une plateforme de cloud qui réponde aux objectifs bien définis de l'entreprise. Pour être efficace, ce modèle de fonctionnement doit s'appuyer sur une organisation bien structurée dans laquelle les différentes responsabilités sont rattachées à des rôles prédefinis, qui sont à leur tour attribués à des équipes formées et à des membres du personnel bien identifiés.

Le service informatique a généralement sa propre structure qu'il suffira d'adapter aux nouvelles circonstances et tâches d'une plateforme de cloud comme Azure. Les fonctions de cloud suivantes présentent les disciplines qui sont requises pour favoriser l'adoption du cloud et qui doivent être affectées à des rôles bien ancrés dans l'organisation.

- Cloud Strategy → Adaptation des nouvelles conditions techniques aux besoins de l'entreprise
- Cloud Governance → Détection des risques d'entreprise et définition des mesures de la conformité
- Cloud Platform Operations → Entretien et exploitation de la zone d'atterrissement de la plateforme de cloud et de ses services basiques
- Cloud Application Operations → Mise en œuvre et exploitation des applications qui ont migré et des nouvelles solutions en cloud
- Cloud Competence Center → Élaboration, mise en place et conseil dans le domaine des nouvelles approches et technologies de cloud
- Cloud Automation → Accélération de l'adoption du cloud et de ses nouveaux processus
- Cloud Data → Élaboration et définition des flux de données de l'entreprise vers et depuis le cloud ainsi qu'enrichissement analytique des données dans le cloud via des architectures définies
- Cloud Security → Protection des informations et exécution des tâches liées à la sécurité dans le cloud

La migration vers le cloud nécessite généralement le recours à toutes ces fonctions et disciplines mais les différents rôles sont plus ou moins impliqués selon le stade de développement. Plus l'adaptation progresse et prend de l'ampleur, plus ces rôles et leurs responsabilités sont définis et à ancrer dans une matrice RACI.

3.3 CONTRÔLE DES ACCÈS (RBAC)

Le contrôle des accès RBAC «Role Based Access Control» d'Azure vous permet de répartir les tâches de gestion de votre organisation entre les différentes équipes et de donner aux différents comptes d'utilisateurs uniquement l'accès aux ressources Azure dont ils ont besoin pour accomplir leurs tâches. Au lieu d'accorder des droits d'accès illimités à tous les comptes de votre abonnement ou de vos ressources, il est préférable de limiter les droits d'accès à certaines actions d'un domaine spécifique (groupe de gestion ; abonnement ; groupe de ressources).

En termes de stratégie des droits d'accès, l'expérience a montré qu'il vaut mieux accorder aux utilisateurs le moins de droits possibles pour l'exécution de leurs tâches. Évitez de confier des rôles relativement étendus dans des domaines vastes, même si cela peut sembler au début plus pratique. Quand vous créez des rôles utilisateur, veillez donc à n'inclure que les droits d'accès indispensables. En restreignant les rôles et les domaines, vous limitez les ressources qui sont exposées à des risques en cas de compromission d'un gardien principal de sécurité.

Le diagramme ci-dessous propose une imbrication des éléments en termes de droits d'accès :

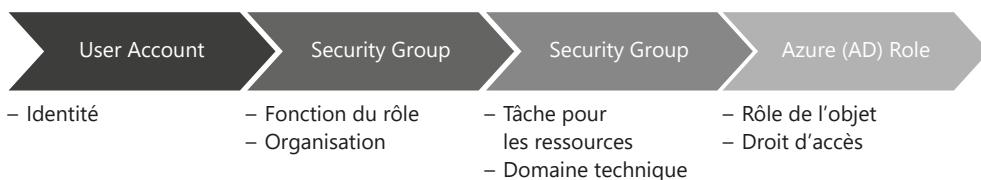


Figure 2 – Imbrication RBAC

	Role				
	Reader	Resource-specific	Custom	Contributor	Owner
Scope	Management group				
	Observers	Users managing resources			Admins
	Resource group				
	Resource	Automated processes			

Le schéma suivant montre les domaines éventuels pour lesquels un utilisateur est susceptible d'obtenir un droit d'accès via son affectation à un groupe.

Figure 3 – Champs d'application des droits d'accès accordés aux rôles

3.4 AZURE ARC

En règle générale, les ressources informatiques ne migrent pas toutes d'un seul coup dans le cloud. Il se peut même que certaines ressources migrent vers les centres de données d'un autre fournisseur en vue d'une stratégie multi-cloud. Pour de tels scénarios hybrides et multi-cloud, Azure Arc propose des options centrales de gestion. Les clients peuvent alors également utiliser les offres de sécurité et de conformité pour les ressources qui ne sont pas ou pas encore dans Azure.

Cas d'application et scénarios

- Visibilité centrale sur une large gamme de ressources (Windows, Linux, Kubernetes)
- Organisation et inventaire de toutes les ressources dans les groupes de gestion, les abonnements, les groupes de ressources ou les balises
- Développement de l'automatisation et gestion de la configuration
- Gestion des stratégies de sécurité
- Gestion des accès avec contrôle des accès basé sur les rôles et Azure Lighthouse
- Approvisionnement de bases de données (SQL, PostgreSQL) dans des clusters Kubernetes, localement ou dans un autre cloud
- Recherche dans plusieurs environnements via Azure Resource Graph

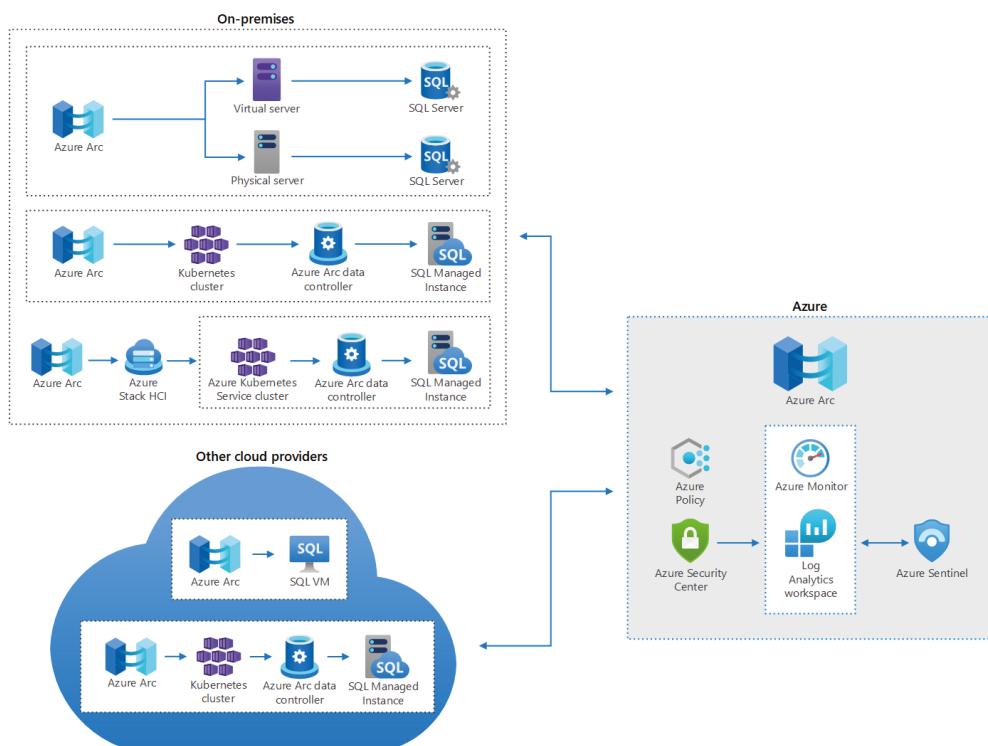


Figure 4 – Vue d'ensemble des fonctions d'Azure Arc

3.5 POLICIES ET PARAMÈTRES DE SÉCURITÉ

Azure Policy aide à appliquer les normes organisationnelles et à évaluer la conformité selon les besoins. Via son tableau de bord de conformité, ce service donne une vue agrégée permettant d'évaluer la situation générale de l'environnement et de lancer une exploration en vue d'une évaluation granulaire par ressource et stratégie. Il vous aide également à mettre vos ressources en conformité grâce à une maintenance en bloc des ressources existantes et une maintenance automatique des nouvelles ressources.

Azure Policy est souvent utilisé dans le cadre de la mise en œuvre de la gouvernance pour la cohérence des ressources, le respect des réglementations, la sécurité, les coûts et la gestion. Les définitions de stratégie applicables à ces cas d'application courants sont déjà intégrées à votre environnement Azure pour vous faciliter les premiers pas.

Azure Policy n'implique pas forcément une restriction des actions mais assure que l'état des ressources est conforme aux règles de votre entreprise, quelle que soit la personne qui a effectué les modifications ou en a l'autorisation.

Pour obtenir un aperçu de l'état actuel des stratégies, il est possible de recourir à la vue d'ensemble d'Azure Policies qui renseigne sur le statut actuel des stratégies déployées.

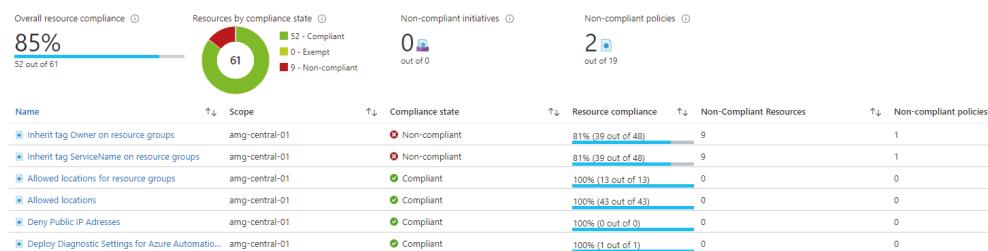


Figure 5 – Rapport de synthèse sur la conformité

Recommandations :

- Commencez avec un effet d'audit plutôt qu'un effet de refus pour suivre l'impact de la définition de votre stratégie sur votre environnement. Si vous avez déjà des scripts en place pour mettre automatiquement à l'échelle vos applications, la définition d'un effet de refus peut entraver ces tâches d'automatisation déjà en place.
- Il est recommandé de créer des définitions au niveau le plus élevé, comme au niveau du groupe de gestion ou de l'abonnement. Une définition créée au niveau du groupe de gestion peut être affectée à un groupe d'abonnement ou de ressources au sein de ce groupe de gestion.
- Nous recommandons de créer et d'affecter des définitions d'initiative également pour une seule définition de stratégie. Exemple : vous avez une définition de stratégie policyDefA que vous créez sous la définition d'initiative initiativeDefC. Si vous créez ultérieurement une autre définition de stratégie pour la stratégieDefB dont les objectifs sont similaires à ceux de la stratégieDefA, vous pourrez l'ajouter à l'initiativeDefC afin de la suivre ensemble.
- Dès que vous avez créé une affectation d'initiative, les définitions de stratégie ajoutées à l'initiative font également partie des affectations de cette initiative.
- L'évaluation d'une affectation d'initiative implique l'évaluation de toutes les stratégies regroupées dans cette initiative. Il est donc préférable de ne pas inclure dans une initiative une stratégie que vous devez évaluer séparément.

3.5.1 Allowed Location Policy

Des stratégies intégrées permettent d'assurer que les ressources Azure sont uniquement déployées à des emplacements précis :

- Allowed locations
- Allowed locations for resource groups

Ces stratégies nous permettent d'empêcher le déploiement de ressources dans d'autres régions.

3.6 MONITORING

Azure Monitor vous aide à maximiser la disponibilité et la performance de vos applications et services. Cette solution complète collecte, analyse et traite les données de télémétrie de vos environnements cloud et locaux. Ces informations vous permettent de comprendre comment fonctionnent vos applications et d'identifier activement les problèmes.

Azure Monitor peut collecter les données provenant de différentes sources, allant de votre application à tous les systèmes d'exploitation et services dont vous dépendez et à la plateforme elle-même. Azure Monitor collecte les données provenant de tous les niveaux suivants :

- Application monitoring data
- Guest OS monitoring data
- Azure resource monitoring data
- Azure subscription monitoring data
- Azure tenant monitoring data

Les données du journal et les métriques de la plupart des ressources Azure peuvent être envoyées via Diagnostic Settings à une gestion centrale des données telle que Log Analytics Workspace. L'agent Log Analytics est à déployer pour les machines virtuelles Azure, le déploiement pouvant s'effectuer via le Security Center.

Scénarios de monitoring :

- Assurer l'absence de problèmes dans le système.
- Suivre la disponibilité du système et de ses composants.
- Gérer la performance pour empêcher une baisse inattendue du débit en cas d'une hausse de surcharge.
- Assurer que le système respecte les SLA (Service Level Agreements) signés avec le client.
- Protéger la vie privée et la sécurité du système, des utilisateurs et de leurs données.
- Suivre les opérations effectuées à des fins de contrôle ou à des fins juridiques.
- Surveiller l'utilisation quotidienne du système et identifier les tendances qui pourraient entraîner des problèmes si elles ne sont pas traitées.
- Suivre les problèmes qui surviennent depuis le premier rapport jusqu'à analyse des véritables raisons, rectification, mises à jour du logiciel qui en résultent et déploiement.
- Suivre le déroulement des opérations et débogage des versions du logiciel.

3.7 RÉSEAU

Les services de réseau Azure offre une multitude de fonctions réseau qui peuvent s'utiliser seules ou ensemble.

3.7.1 Qu'est-ce qu'un réseau virtuel dans Azure ?

Azure Virtual Network (VNET) est le module de base pour votre réseau privé d'Azure. VNET permet à de nombreux types de ressources d'Azure (comme des ordinateurs Azure virtuels) de communiquer entre elles mais aussi avec Internet et des réseaux locaux. VNET est similaire à un réseau classique que vous exploitez dans votre centre de données mais il offre les avantages supplémentaires de l'infrastructure d'Azure, tels que l'évolutivité, la disponibilité et l'isolation.

Azure vous propose différentes approches pour établir votre réseau. Il est recommandé d'élaborer une topologie de type « hub and spoke » qui offre notamment comme avantages une réduction des coûts, l'isolation de la charge de travail et le contournement des limitations techniques des abonnements Azure.

[Hub-spoke network topology in Azure - Azure Reference Architectures | Microsoft Docs](#)

3.7.2 Segmentation du réseau

La segmentation est un modèle dans lequel vous prenez votre empreinte réseau et créez des périmètres définis par logiciel à l'aide d'outils disponibles dans Azure. Vous définissez ensuite les règles qui régissent le trafic en provenance / à destination de ces périmètres de façon à avoir des postures de sécurité différentes selon les parties de votre réseau. Cette solution est intéressante quand vous placez différentes applications (ou parties d'une application donnée) dans ces périmètres car vous pouvez régir la communication entre ces entités segmentées. Ce modèle présente encore un autre avantage : si une partie de la pile d'applications est compromise, vous pourrez mieux contenir l'impact de cette violation de sécurité, et l'empêcher de se répandre latéralement dans le reste de votre réseau. C'est un principe clé du modèle Confiance Zéro de Microsoft qui offre à votre organisation une solution de sécurité de premier rang.

Azure propose à cet effet les outils suivants :

3.7.2.1 Groupes de sécurité réseau NSG

Les NSG sont des mécanismes de contrôle d'accès destinés à réguler le trafic entre les ressources au sein d'un réseau virtuel et avec des réseaux externes (Internet, autres réseaux virtuels, etc.). Il est possible dans les NSG d'appliquer une stratégie de segmentation plus différentiée en créant des périmètres pour un sous-réseau, un groupe de machines virtuelles ou même une machine virtuelle unique.

3.7.2.2 Application Security Groups ASGs

Les ASG fournissent des mécanismes de contrôle similaires aux NSG mais sont référencés avec un contexte d'application. Un ASG vous permet de regrouper un ensemble de machines virtuelles sous une balise d'application. Il peut définir des règles de trafic des données qui sont ensuite appliquées à chacune des machines virtuelles sous-jacentes.

3.7.2.3 Pare-feu

Le pare-feu Azure est un service natif du cloud qui peut être déployé dans les réseaux virtuels ou dans des déploiements d'Azure Virtual WAN Hubs afin de filtrer le trafic échangé entre des ressources cloud, Internet et l'environnement local. Vous créez des règles ou des stratégies (à l'aide du pare-feu Azure ou d'Azure Firewall Manager) en spécifiant l'autorisation / le refus du trafic avec des contrôles de couche 3 à 7. Pour améliorer le filtrage et la protection des utilisateurs, vous pouvez également filtrer le trafic provenant d'Internet à l'aide du pare-feu Azure ou de solutions tierces. Vous dirigerez à cet effet l'ensemble ou une partie du trafic vers des fournisseurs de sécurité tiers.

3.7.3 Connexion réseau selon Azure

Il existe deux manières de connecter les sites locaux avec le réseau Azure :

- ExpressRoute ([Azure ExpressRoute Overview: Connect over a private connection | Microsoft Docs](#))
- Site à site VPN ([Informations sur la passerelle VPN Azure | Microsoft Docs](#))

La principale différence entre ces deux technologies est qu'ExpressRoute établit la connexion via une connexion backbone de Microsoft privée et payante tandis que VPN passe par l'Internet public. Ces connexions sont toutefois toutes les deux chiffrées.

3.8 ACTIVE DIRECTORY

Dans le cas où des serveurs membres de domaine Windows continuent à être exploités dans Azure en tant que machines virtuelles IaaS, blueprint ISO 27001 prévoit dans la zone centrale d'Active Directory Domain Controllers qui assurent l'authentification et l'autorisation Kerberos au sein du réseau virtuel. En se servant d'une connexion sur site via une passerelle VPN ou ExpressRoute dans le Gateway Subnet, les contrôleurs de domaine reproduisent et synchronisent les données avec l'Active Directory existant.

Un service Bastion est également disponible pour assurer un accès à distance sécurisé à ces machines virtuelles sans adresse IP publique.

3.9 KEY VAULT

Pour tout type de chiffrement de données avec des clés gérées par le client (CMK), Azure Key Vault s'associe à un HSM (module de sécurité matériel, localement ou en tant que service de gestion Azure). Il stocke les clés de chiffrement, les mots de passe et les certificats pour ne les transmettre qu'aux applications qui y sont autorisées par leurs comptes de service. Le facteur de risque humain inhérent à la manipulation de ces éléments de sécurité est ainsi éliminé et la sécurité est renforcée puisque ces « secrets » ne doivent pas être saisis manuellement ou enregistrés ouvertement dans un code.

3.10 CONTRÔLE DES COÛTS

Azure Cost Management propose des outils qui vous permettent de planifier, analyser et réduire vos dépenses et d'ainsi maximiser les profits que vous tirez du cloud. Grâce à ce contrôle des coûts, il est possible d'optimiser la solution en cloud pour réduire les coûts et mieux profiter des avantages offerts par le cloud.

- La fonction **Analyse des coûts** vous aide à analyser les coûts. Différentes visualisations permettent d'afficher de diverses façons les coûts cumulés.
- La fonction **Budgets** permet de configurer différents types d'alertes qui vous avertiront en cas de dépassement d'une certaine valeur limite.
- La fonction **Recommendations** vous aide à identifier les ressources peu ou pas utilisées et à prendre ainsi les mesures qui en éviteront le gaspillage.

Pour la gestion des coûts, il est possible de classifier les différentes ressources afin d'y affecter les coûts, ce qui peut se faire par le biais d'un balisage où chaque ressource est associée à ses métadonnées.

Le balisage est le meilleur procédé qui permette de comprendre les données dans le cadre du rapport sur les coûts. Il est essentiel à tout environnement bien géré mais constitue aussi la première étape vers la gouvernance d'un environnement.

Une norme de balisage doit d'abord être définie afin d'assurer un suivi précis des informations sur les coûts au niveau des unités opérationnelles, environnements et projets. La deuxième étape consiste à garantir une application cohérente de cette norme de balisage. En utilisant Azure Policy, nous pouvons assurer que toutes les ressources sont réellement affectées à une balise. Pour ce faire, ce balisage fait l'objet d'un héritage automatique ou des balises sont automatiquement déployées selon certains indicateurs.

3.11 SECURITY CENTER

Azure Security Center joue un rôle important dans votre stratégie de la gouvernance. Il aide à surveiller la posture de sécurité dans Azure :

- Il offre une vue homogène de la sécurité pour toutes les charges de travail.
- Il collecte, recherche et analyse des données de sécurité provenant de diverses sources, dont également les pare-feu et autres solutions partenaires.
- Il fournit des recommandations de sécurité permettant de résoudre concrètement les problèmes avant qu'ils ne puissent être exploités.
- Il peut servir à appliquer les stratégies de sécurité à vos charges de travail cloud hybrides afin de garantir le respect des normes de sécurité. Les normes ISO 27001 peuvent ainsi être déployées via Azure Security Center.

De nombreuses fonctions de sécurité, telles que les stratégies et recommandations de sécurité, sont disponibles gratuitement. Certaines des fonctions avancées, comme l'accès à la machine virtuelle juste-à-temps et la prise en charge des charges de travail hybrides, sont disponibles au niveau standard du Security Center. L'accès juste-à-temps à la machine virtuelle peut contribuer à réduire l'exposition du réseau aux attaques en contrôlant l'accès aux ports de gestion des machines virtuelles Azure.

Azure Security Center vous permet de renforcer votre posture de sécurité. Ce service vous aide à identifier et à effectuer les tâches de renforcement recommandées en tant que meilleures pratiques de sécurité et à les implémenter sur vos machines, services de données et applications. Il assure également la gestion et l'application de vos stratégies de sécurité ainsi que la conformité de vos machines virtuelles Azure, des serveurs autres qu'Azure et des services PaaS Azure. Security Center vous offre les outils dont vous avez besoin pour obtenir une vue d'ensemble sur vos charges de travail et en particulier sur votre espace de sécurité réseau.



4 CONTRÔLES ISO 27001

Chacun des contrôles suivants est lié à une ou plusieurs définitions de stratégie d'Azure. Ces stratégies peuvent vous aider à évaluer la **conformité** avec le contrôle mais souvent, il n'existe pas de correspondance exacte ou parfaite entre un contrôle et une ou plusieurs stratégies. Ainsi, la **conformité** aux stratégies d'Azure se réfère uniquement aux stratégies elles-mêmes ; elle ne garantit pas que vous êtes entièrement conforme à toutes les exigences d'un contrôle. En outre, la norme de conformité comprend des contrôles qui, pour l'instant, ne sont traités par aucune définition de stratégie d'Azure. La conformité aux stratégies d'Azure ne représente donc qu'une partie de votre conformité globale. Les associations entre les contrôles et les définitions de stratégie d'Azure applicables à cet exemple de conformité blueprint peuvent changer au fil du temps.

Les chapitres suivants dressent la liste des contrôles ISO 27001 pour lesquels Microsoft a instauré des stratégies appropriées dans le Security Center aux fins d'une évaluation technique. D'autres mesures et contrôles potentiels, qui découlent de l'évaluation des risques de Microsoft Public Sector Cloud Design, sont proposés en complément des basiques.

4.1 A.6.1.2 CLOISONNEMENT DES TÂCHES

Les fonctions et les domaines de responsabilité antagonistes doivent être séparés afin de réduire les possibilités d'une modification ou utilisation abusive non autorisée ou involontaire des actifs de l'organisation.

Documentation sur le contrôle ISO :

<https://www.isms.online/iso-27001/annex-a-6-organisation-information-security/>

Contenu blueprint

Si vous avez seulement un propriétaire d'abonnements Azure, vous n'avez aucun risque de redondance administrative. Au contraire, un nombre élevé de propriétaires d'abonnements augmente le risque d'une infraction provenant d'un compte utilisateur compromis. Ce blueprint vous aide à maintenir un nombre approprié de propriétaires d'abonnements Azure en attribuant deux définitions de stratégie Azure qui en vérifient le nombre. La gestion des autorisations pour propriétaires d'abonnements peut vous aider à mettre en place un cloisonnement approprié des tâches.

- 3 propriétaires maximum devaient être définis pour votre abonnement.
- Plus d'un propriétaire devrait être associé à votre abonnement.

Mesures et stratégies complémentaires

- Limiter à un minimum le nombre d'administrateurs globaux existants pour les cas d'urgence (recommandation: 2 à 3)
- Mettre en œuvre le concept des rôles sans recourir à une administration globale ou au propriétaire de l'abonnement.

4.2 A.8.2.1 CLASSIFICATION DES INFORMATIONS

Les informations doivent être classées en fonction des exigences légales, des critères de valeur, de criticité et de sensibilité à une divulgation ou modification non autorisée, et au mieux d'une manière reflétant l'activité opérationnelle sans l'entraver ou la gêner.

Documentation sur le contrôle ISO : <https://www.isms.online/iso-27001/annex-a-8-asset-management/>

Contenu blueprint

Le service Azure « SQL Vulnerability Assessment » vous aide à détecter des données sensibles qui sont enregistrées dans votre base de données, et fournit des recommandations sur la classification de ces données.

- Les failles de sécurité de vos bases de données SQL devraient être supprimées.

Mesures et stratégies complémentaires

- Les ressources qui comprennent des données devraient être classifiées avec des balises de ressources.
- Azure Purview permet d'établir une classification générale des contenus des données des ressources prises en charge et de les saisir dans un catalogue de données en vue de leur dépistage.

4.3 A.9.1.2 ACCÈS AUX RÉSEAUX ET SERVICES RÉSEAUX

Le principe de l'accès minimal est l'approche générale : elle est privilégiée pour la protection et préférée à un accès illimité et à des droits de super-utilisateur sans examen approfondi.

Documentation sur le contrôle ISO : <https://www.isms.online/iso-27001/annex-a-9-access-control/>

Contenu blueprint

Azure met en œuvre le contrôle d'accès basé sur les rôles (Azure RBAC) pour gérer les droits d'accès aux ressources Azure. Ce blueprint vous aide à contrôler l'accès aux ressources Azure en attribuant des définitions de stratégie Azure. Ces stratégies vérifient l'utilisation des types et configurations de ressources qui peuvent être plus facilement accessibles. La compréhension des ressources qui violent ces stratégies peut vous aider à prendre les mesures correctives garantissant que l'accès aux ressources Azure est limité aux utilisateurs autorisés.

- Ajouter une identité managée affectée par le système pour activer les attributions de la configuration d'invité sur les machines virtuelles sans identité
- Ajouter une identité managée affectée par le système pour activer les attributions de la configuration d'invité sur les machines virtuelles avec une identité affectée par l'utilisateur
- Surveiller les ordinateurs Linux qui autorisent des connexions à distance via des comptes sans mot de passe
- Surveiller les ordinateurs Linux qui utilisent des comptes sans mots de passe
- Surveiller des ordinateurs virtuels qui n'utilisent aucun support de données géré
- Déployer une extension pour la configuration de l'invité Linux pour activer les attributions de la configuration de l'invité sur les machines virtuelles Linux
- Les comptes de stockage devraient migrer vers de nouvelles ressources d'Azure Resource Manager
- Les machines virtuelles devraient migrer vers de nouvelles ressources d'Azure Resource Manager

Mesures et stratégies complémentaires

- Autoriser des droits d'accès aux composants des réseaux virtuels uniquement à des rôles (groupes) responsables.
- Empêcher la libre création de ressources d'adresses IP publiques.

4.4 A.9.2.3 GESTION DES DROITS D'ACCÈS PRIVILÉGIÉS

L'attribution et l'utilisation des droits d'accès privilégiés doivent être strictement contrôlées compte tenu des droits supplémentaires généralement accordés sur les informations et les systèmes qui les contrôlent.

Documentation sur le contrôle ISO : <https://www.isms.online/iso-27001/annex-a-9-access-control/>

Contenu blueprint

Ce blueprint vous aide à limiter et contrôler les droits d'accès privilégiés en attribuant des définitions de stratégie Azure permettant de vérifier des comptes dotés d'autorisations de propriétaire et/ou d'écriture qui sont externes ou qui n'ont pas d'authentification multifacteur (MFA) activée. Le contrôle d'accès basé sur les rôles d'Azure (Azure RBAC) vous aide à gérer les droits d'accès aux ressources Azure. Ce blueprint attribue également des définitions de stratégie Azure en vue de vérifier l'utilisation de l'authentification Azure Active Directory pour le serveur SQL et Service Fabric. L'utilisation de l'authentification Azure Active Directory permet de simplifier la gestion des droits et de centraliser la gestion des identités des utilisateurs des bases de données et autres services Microsoft. Ce blueprint attribue également une définition de stratégie Azure pour vérifier l'utilisation des règles RBAC Azure personnalisées. Savoir où les règles RBAC Azure personnalisées sont mises en œuvre vous aide à en vérifier la bonne mise en œuvre car ces règles sont sujettes aux erreurs.

- Il est recommandé de déployer un administrateur Azure Active Directory pour le serveur SQL.
- Audit sur l'utilisation des règles RBAC personnalisées
- Les comptes externes dotés de droits de propriétaire devraient être supprimés de votre abonnement.
- Les comptes externes dotés de droits d'écriture devraient être supprimés de votre abonnement.
- La MFA devrait être activée pour les comptes dotés de droits d'écriture sur vos abonnements
- La MFA devrait être activée pour les comptes dotés de droits de propriétaire pour vos abonnements
- Les clusters Service Fabric devraient utiliser uniquement Azure Active Directory pour l'authentification des clients.

Mesures et stratégies complémentaires

- Mise en œuvre de Privileged Identity Management (PIM) d'Azure AD pour l'activation des rôles et droits d'utilisation privilégiés en fonction du temps et des autorisations.
- Mise en œuvre d'Entitlement Management d'Azure AD pour la tenue du cycle de vie des identités et des accès.

4.5 A.9.2.4 GESTION DES INFORMATIONS SECRÈTES D'AUTHENTIFICATION DES UTILISATEURS

Les informations secrètes d'authentification sont une porte d'accès à des biens précieux. Généralement, elles comprennent par exemple des mots de passe, des clés de chiffrement et doivent donc être contrôlées par un procédé formel de gestion ainsi que rester confidentielles pour l'utilisateur.

Documentation sur le contrôle ISO : <https://www.isms.online/iso-27001/annex-a-9-access-control/>

Contenu blueprint

Ce blueprint attribue trois définitions de stratégie Azure en vue de vérifier les comptes pour lesquels l'authentification multifacteur n'est pas activée. L'authentification multifacteur aide à assurer la sécurité des comptes même en cas de compromission d'une partie des informations d'authentification. En surveillant les comptes pour lesquels l'authentification multifacteur n'est pas activée, vous êtes en mesure d'identifier ceux qui sont plus susceptibles d'être compromis. Ce blueprint attribue également deux définitions de stratégie Azure qui vérifient les autorisations de fichier de mots de passe de la machine virtuelle Linux afin d'avertir si elles sont mal établies. Cette configuration vous permet de prendre les mesures correctives permettant d'assurer que les authentificateurs ne sont pas compromis.

- Ajouter une identité managée affectée par le système pour activer les attributions de la configuration d'invité sur les machines virtuelles sans identité
- Ajouter une identité managée affectée par le système pour activer les attributions de la configuration d'invité sur les machines virtuelles avec une identité affectée par l'utilisateur
- Surveiller les ordinateurs Linux qui n'ont pas les autorisations de fichier de mots de passe définies sur 0644
- Déployer une extension pour la configuration de l'invité Linux pour activer les attributions de la configuration de l'invité sur les machines virtuelles Linux.
- La MFA doit être activée pour les comptes dotés de droits d'écriture sur vos abonnements
- La MFA devrait être activée pour les comptes dotés de droits de propriétaire pour vos abonnements.
- La MFA devrait être activée pour les comptes d'abonnement dotés de droits de lecture.

4.6 A.9.2.5 VÉRIFICATION DES DROITS D'ACCÈS DES UTILISATEURS

Les propriétaires d'informations et de systèmes doivent régulièrement vérifier les droits d'accès des utilisateurs dans le cadre de changements de personne (intégration, changement de rôle et départ) mais aussi d'audits plus importants des accès aux systèmes. Les droits d'accès privilégiés doivent être vérifiés à intervalles plus fréquents vu qu'ils impliquent un risque plus élevé.

Documentation sur le contrôle ISO : <https://www.isms.online/iso-27001/annex-a-9-access-control/>

Contenu blueprint

Le contrôle d'accès basé sur les rôles d'Azure (Azure RBAC) vous aide à gérer les droits d'accès aux ressources dans Azure. Vous pouvez via le portail Azure vérifier qui a accès aux ressources d'Azure et à leurs autorisations. Ce blueprint attribue quatre définitions de stratégie Azure afin de vérifier les comptes qui sont à examiner en priorité, notamment les comptes inactifs et les comptes externes dotés d'autorisations élevées.

- Les comptes obsolètes devraient être supprimés de vos abonnements.
- Les comptes obsolètes dotés de droits de propriétaire devraient être supprimés de vos abonnements.
- Les comptes externes dotés de droits de propriétaire devraient être supprimés de vos abonnements.
- Les comptes externes dotés de droits d'écriture devraient être supprimés de vos abonnements.

Mesures et stratégies complémentaires

- Il est recommandé de vérifier régulièrement à l'aide d'Access Review d'Azure AD les autorisations des rôles existants afin d'assurer qu'aucun accès non autorisé ne peut plus avoir lieu.

4.7 A.9.2.6 SUPPRESSION OU MODIFICATION DES DROITS D'ACCÈS

Il convient de supprimer les droits d'accès aux informations et aux installations de traitement des informations de tous les collaborateurs et utilisateurs externes dont l'emploi, le contrat ou l'accord prend fin (ou si nécessaire, adapter ces droits en cas de changement de rôle).

Documentation sur le contrôle ISO : <https://www.isms.online/iso-27001/annex-a-9-access-control/>

Contenu blueprint

Le contrôle d'accès basé sur les rôles d'Azure (Azure RBAC) vous aide à gérer les droits d'accès aux ressources dans Azure. Azure Active Directory et Azure RBAC vous permettent d'actualiser les rôles d'utilisateur pour les adapter aux modifications intervenues dans l'organisation. Les comptes peuvent être, si nécessaire, rendus inaccessibles à la connexion (ou supprimés), ce qui supprime aussi immédiatement les droits d'accès aux ressources Azure. Ce blueprint attribue deux définitions de stratégie Azure pour examiner un compte inactif susceptible d'être supprimé.

- Les comptes obsolètes devraient être supprimés de vos abonnements.
- Les comptes obsolètes dotés de droits de propriétaire devraient être supprimés de vos abonnements.

Mesures et stratégies complémentaires

- Il est recommandé de vérifier régulièrement à l'aide d'Access Review d'Azure AD les autorisations des rôles existants afin d'empêcher tout accès qui n'est plus autorisé.

4.8 A.9.4.2 PROCÉDURES DE CONNEXION SÉCURISÉES

L'accès aux systèmes et applications doit être contrôlé par une procédure de connexion sécurisée afin que l'identité de l'utilisateur soit prouvée. Au-delà du mot de passe classique, cette procédure peut inclure, en fonction du risque, l'authentification multifactor, la biométrie, les cartes à puce et autres moyens de chiffrement,

La connexion sécurisée doit être conçue de manière à ne pas être facilement contournable ; elle doit également assurer que toutes les informations d'authentification sont transmises et stockées sous une forme chiffrée qui empêche leur interception et leur utilisation abusive.

Documentation sur le contrôle ISO : <https://www.isms.online/iso-27001/annex-a-9-access-control/>

Contenu blueprint

Ce blueprint attribue trois définitions de stratégie Azure visant à vérifier les comptes pour lesquels l'authentification multifactor n'est pas activée. L'authentification multifactor d'Azure offre une sécurité supplémentaire car elle requiert une deuxième forme d'authentification et assure une solide authentification. En surveillant les comptes pour lesquels l'authentification multifactor n'est pas activée, vous êtes en mesure d'identifier ceux qui sont plus susceptibles d'être compromis.

- La MFA doit être activée pour les comptes dotés de droits d'écriture sur vos abonnements
- La MFA devrait être activée pour les comptes dotés de droits de propriétaire pour vos abonnements.
- La MFA devrait être activée pour les comptes d'abonnement dotés de droits de lecture

Mesures et stratégies complémentaires

- Grâce à Conditional Access d'Azure AD, différentes limites de connexion devraient pouvoir être mises en place suite à l'évaluation des risques liés aux applications et aux utilisateurs.
- Les comptes de stockage ne devraient pas permettre un accès anonyme.

4.9 A.9.4.3 SYSTÈME DE GESTION DES MOTS DE PASSE

L'objectif d'un système de gestion des mots de passe est d'assurer que les mots de passe répondent systématiquement aux exigences de qualité.

Documentation sur le contrôle ISO : <https://www.isms.online/iso-27001/annex-a-9-access-control/>

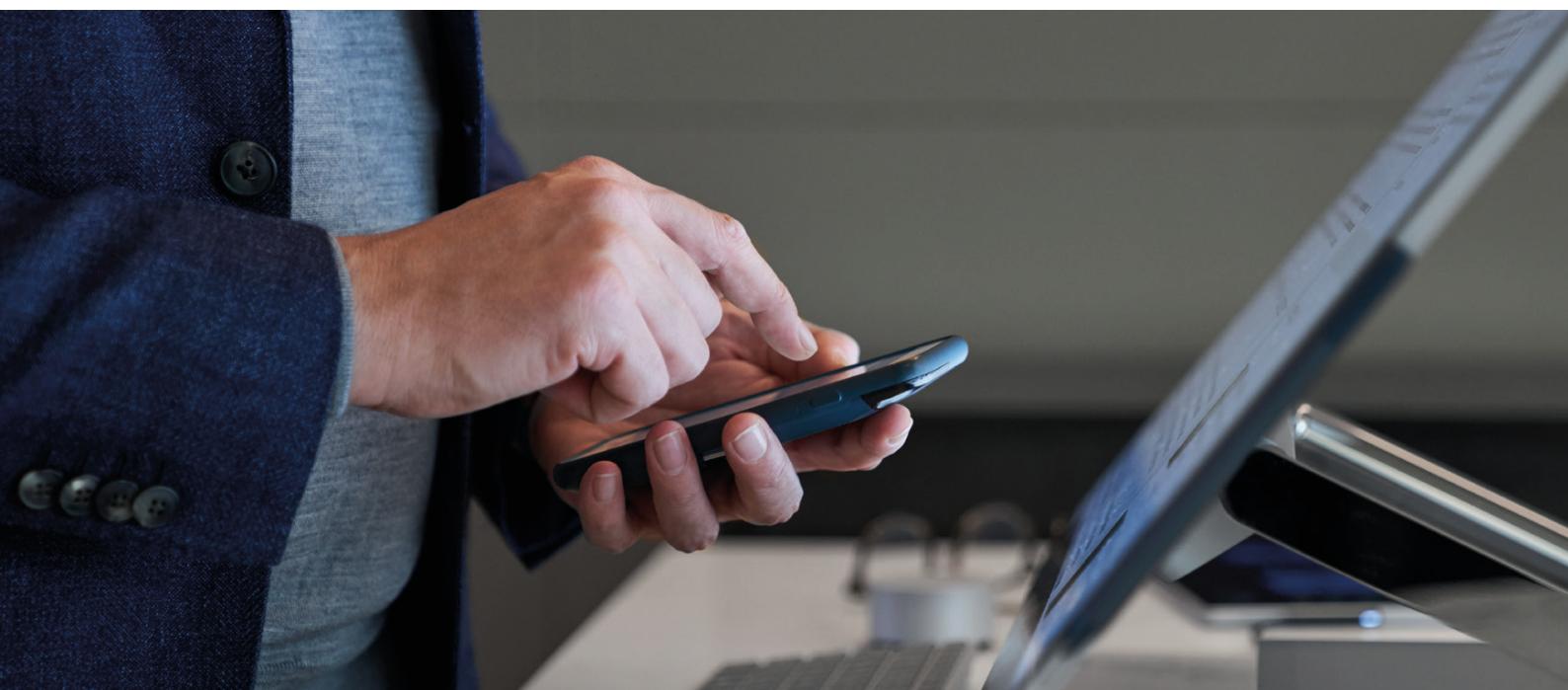
Contenu blueprint

Ce blueprint vous aide à imposer des mots de passe robustes en attribuant des définitions de stratégie Azure qui vérifient les machines virtuelles Windows ne respectant pas la robustesse minimale des mots de passe et autres exigences. En connaissant les machines virtuelles qui ne respectent pas la stratégie sur la robustesse des mots de passe, vous saurez prendre les mesures correctives permettant de garantir que tous les mots de passe de tous les comptes utilisateurs des machines virtuelles sont conformes avec la stratégie.

- Ajouter une identité managée affectée par le système pour activer les attributions de la configuration d'invité sur les machines virtuelles sans identité
- Ajouter une identité managée affectée par le système pour activer les attributions de la configuration d'invité sur les machines virtuelles avec une identité affectée par l'utilisateur
- Surveiller les ordinateurs Windows qui autorisent une réutilisation des 24 mots de passe précédents
- Surveiller les ordinateurs Windows qui n'appliquent pas aux mots de passe un âge maximal de 70 jours
- Surveiller les ordinateurs Windows qui n'appliquent pas aux mots de passe un âge minimal d'un jour
- Surveiller les ordinateurs Windows où le réglage de la complexité des mots de passe n'est pas activé
- Surveiller les ordinateurs Windows où une longueur minimale de 14 signes n'est pas définie pour les mots de passe
- Déployer une extension pour la configuration de l'invité Windows afin d'activer les attributions de la configuration de l'invité sur les machines virtuelles Windows

Mesures et stratégies complémentaires

- Les mots de passe d'Azure AD doivent répondre aux exigences en termes de longueur et de caractères
- Mise en place de Password Protection d' Azure AD pour empêcher les mots de passe de mauvaise qualité tirés de dictionnaires



4.10 A.10.1.1 STRATÉGIE SUR L'UTILISATION DES CONTRÔLES DE CHIFFREMENT

Utilisation correcte et efficace de la cryptographie afin de protéger la confidentialité, l'authenticité et/ou l'intégrité des informations.

Documentation sur le contrôle ISO : <https://www.isms.online/iso-27001/annex-a-10-cryptography/>

Contenu blueprint

Ce blueprint vous aide à appliquer votre stratégie sur l'utilisation des contrôles cryptographiques en attribuant 13 définitions de stratégie Azure qui imposent des contrôles cryptographiques spécifiques et vérifient si de faibles paramètres cryptographiques sont utilisés. En comprenant où les configurations cryptographiques de vos ressources Azure risquent de ne pas être optimales, vous pouvez prendre les mesures correctives permettant d'assurer une configuration de vos ressources conforme à votre stratégie sur la sécurité des informations. En particulier, les stratégies attribuées par ce blueprint exigent le chiffrement des comptes de stockage Blob et Data Lake ; exigent le chiffrement transparent des données des bases de données SQL ; vérifient l'absence de chiffrement des comptes de stockage, des bases de données SQL, des disques durs des machines virtuelles et des variables des comptes Automation ; vérifient les connexions non sécurisées aux comptes de stockage, applications fonctionnelles, applications Web, applications API et à Redis Cache ; vérifient le faible chiffrement des mots de passe des machines virtuelles ; et vérifient les communications Service Fabric non chiffrées.

- Les applications fonctionnelles doivent être uniquement accessibles via HTTPS
- Les applications Web devraient être uniquement accessibles via HTTPS
- Les applications API devraient être uniquement accessibles via HTTPS
- Déployer les conditions nécessaires à la vérification des machines virtuelles Windows qui ne stockent pas les mots de passe à chiffrement réversible
- Afficher les résultats d'audit des machines virtuelles Windows qui n'enregistrent pas de mots de passe
- Le chiffrement du disque dur devrait être appliqué aux machines virtuelles
- Les variables du compte Automation devraient être chiffrées
- Seules les connexions sécurisées à votre cache Azure pour Redis devraient être activées
- Le transfert sécurisé vers les comptes de stockage devrait être activé
- Pour les clusters Service Fabric, la propriété ClusterProtectionLevel devrait être définie sur EncryptAndSign
- Le chiffrement transparent des données des bases de données SQL devrait être activé

Mesures et stratégies complémentaires

- Le chiffrement des comptes de stockage devrait être activé
- Les comptes de stockage devraient être uniquement accessibles via HTTPS
- TLS 1.2 devrait être systématiquement utilisé sur les comptes de stockage

4.11 A.12.4.1 JOURNALISATION DES ÉVÉNEMENTS

Il convient de créer, conserver et réviser régulièrement des journaux d'événements qui enregistrent les activités des utilisateurs, les exceptions, les erreurs et les événements liés à la sécurité des informations.

Documentation sur le contrôle ISO : <https://www.isms.online/iso-27001/annex-a-12-operations-security/>

Contenu blueprint

Ce blueprint vous permet d'assurer que les événements du système sont consignés en attribuant sept définitions de stratégie Azure qui vérifient les réglages de la journalisation sur des ressources Azure. Les journaux de diagnostic permettent de visualiser les opérations effectuées au sein des ressources Azure.

- Intervention d'audit de l'agent Dependency - Image de la machine virtuelle (OS) non répertoriée
- Déploiement d'audit de l'agent Dependency dans les jeux de mise à l'échelle des machines virtuelles
 - Image de la machine virtuelle (OS) non répertoriée
- Déploiement d'audit de l'agent Log Analytics - Image de la machine virtuelle (OS) non répertoriée
- Intervention d'audit de l'agent Log Analytics dans les jeux de mise à l'échelle des machines virtuelles
 - Image de la machine virtuelle (OS) non répertoriée
- Paramètre de diagnostic de l'audit
- L'intervention d'audit devrait être activée sur le serveur SQL

Mesures et stratégies complémentaires

- Azure Policies permet non seulement de vérifier si les ressources concernées disposent également des options de journalisation nécessaires mais aussi d'appliquer immédiatement ces dernières.

4.12 A.12.4.3 JOURNAUX DES ADMINISTRATEURS ET DES OPÉRATEURS

Les activités des administrateurs et des opérateurs du système doivent être consignées et les journaux doivent être protégés et régulièrement examinés. Un degré de journalisation plus élevé devrait être envisagé pour les comptes privilégiés tels qu'administrateurs et opérateurs du système.

Documentation sur le contrôle ISO : <https://www.isms.online/iso-27001/annex-a-12-operations-security/>

Contenu blueprint

Ce blueprint vous permet d'assurer que les événements du système sont consignés en attribuant des définitions de stratégie Azure qui vérifient les réglages de la journalisation sur des ressources Azure. Les journaux de diagnostic permettent de visualiser les opérations effectuées au sein des ressources Azure.

- Surveillance du paramètre de diagnostic
- La surveillance dans le serveur SQL doit être activée
- La surveillance dans le serveur SQL doit être activée
- L'agent Dependency doit être activé pour les images répertoriées de la machine virtuelle.
- L'agent Dependency doit être activé dans les groupes de mise à l'échelle de la machine virtuelle pour les images répertoriées de la machine virtuelle.
- L'agent Log Analytics doit être activé pour les images répertoriées de la machine virtuelle.
- L'agent Log Analytics doit être activé dans les groupes de mise à l'échelle de la machine virtuelle pour les images répertoriées de la machine virtuelle

Mesures et stratégies complémentaires

- Surveillance des journaux de connexion et d'audit d'Azure AD

4.13 A.12.4.4 SYNCHRONISATION DES HORLOGES

Au sein d'une organisation ou d'une zone de sécurité, les horloges de tous les principaux systèmes de traitement des informations doivent être synchronisées sur une seule source de temps de référence.

Documentation sur le contrôle ISO : <https://www.isms.online/iso-27001/annex-a-12-operations-security/>

Contenu blueprint

Ce blueprint vous permet d'assurer que les événements du système sont consignés en attribuant des définitions de stratégie Azure qui vérifient les réglages de la journalisation sur des ressources Azure. Les journaux Azure s'appuient sur des horloges internes synchronisées pour assurer la corrélation temporelle des enregistrements sur les événements de toutes les ressources.

- Surveillance du paramètre de diagnostic
- La surveillance dans le serveur SQL doit être activée
- L'agent Dependency doit être activé pour les images répertoriées de la machine virtuelle
- L'agent Dependency doit être activé dans les groupes de mise à l'échelle de la machine virtuelle pour les images répertoriées de la machine virtuelle
- L'agent Log Analytics doit être activé pour les images répertoriées de la machine virtuelle
- L'agent Log Analytics doit être activé dans les groupes de mise à l'échelle de la machine virtuelle pour les images répertoriées de la machine virtuelle

4.14 A.12.5.1 INSTALLATION DE LOGICIELS SUR LES SYSTÈMES D'EXPLOITATION

Des procédés doivent être mis en place pour contrôler l'installation de logiciels sur les systèmes d'exploitation.

Documentation sur le contrôle ISO : <https://www.isms.online/iso-27001/annex-a-12-operations-security/>

Contenu blueprint

Le contrôle adaptatif d'application est une solution d'Azure Security Center vous permettant de contrôler quelles applications peuvent être exécutées sur vos machines virtuelles hébergées dans Azure. Ce blueprint attribue une définition de stratégie Azure qui surveille le jeu des applications autorisées. Cette capacité vous aide à contrôler l'installation de logiciels et les applications sur les machines virtuelles Azure.

- Le contrôle adaptatif d'application visant à définir les applications sûres doit être activé sur les ordinateurs

4.15 A12.6.1 GESTION DES VULNÉRABILITÉS TECHNIQUES

Il convient de recueillir en temps utile les informations sur les vulnérabilités techniques des systèmes d'information utilisés, d'évaluer l'exposition de l'organisation à ces vulnérabilités et de prendre les mesures appropriées pour faire face aux risques impliqués.

Documentation sur le contrôle ISO : <https://www.isms.online/iso-27001/annex-a-12-operations-security/>

Contenu blueprint

Ce blueprint vous aide à gérer les vulnérabilités des systèmes d'information en attribuant des définitions de stratégie Azure qui surveillent les mises à jour du système manquantes ainsi que les vulnérabilités du système d'exploitation, de SQL et des machines virtuelles dans Azure Security Center. Azure Security Center propose des fonctionnalités de création de rapports qui vous permettent de voir en temps réel l'état de sécurité des ressources déployées.

- Une solution d'évaluation des vulnérabilités doit être installée sur vos ordinateurs virtuels
- Surveiller la protection manquante Endpoint Protection dans Azure Security Center
- Les risques de sécurité encourus par les bases de données SQL doivent être résolus
- Les mises à jour du système devraient être installées sur vos ordinateurs
- Les risques de sécurité pour vos ordinateurs devraient être éliminés

4.16 A.12.6.2 RESTRICTIONS LIÉES À L'INSTALLATION DE LOGICIELS

L'installation de logiciels doit faire l'objet de règles qui sont à définir et à mettre en œuvre par l'utilisateur. Ce contrôle porte sur la réduction de la capacité des utilisateurs à installer des logiciels, notamment sur les terminaux locaux (postes de travail, ordinateurs portables, etc.).

Documentation sur le contrôle ISO : <https://www.isms.online/iso-27001/annex-a-12-operations-security/>

Contenu blueprint

Le contrôle adaptatif d'application est une solution d'Azure Security Center vous permettant de contrôler quelles applications peuvent être exécutées sur vos machines virtuelles hébergées dans Azure. Ce blueprint attribue une définition de stratégie Azure qui surveille le jeu des applications autorisées. Les restrictions sur l'installation de logiciels peuvent vous aider à minimiser la probabilité d'introduire des vulnérabilités logicielles.

- Le contrôle adaptatif d'application visant à définir les applications sûres doit être activé sur les ordinateurs

Mesures et stratégies complémentaires

- Les interfaces secondaires de Source Control Management (SCM) (Kudu, intégration GitHub, etc.) des ressources prises en charges sont à sécuriser.

4.17 A.13.1.1 CONTRÔLES DE RÉSEAU

Les réseaux doivent être gérés et contrôlés pour protéger les informations au sein des systèmes et applications.

Documentation sur le contrôle ISO : <https://www.isms.online/iso-27001/annex-a-13-communications-security/>

Contenu blueprint

Ce blueprint vous aide à gérer et à contrôler les réseaux en attribuant une définition de stratégie Azure qui surveille les groupes de sécurité réseau dotés de règles permissives. Les règles trop permissives risquent de permettre un accès non souhaité au réseau et doivent être revues. Dans ce blueprint sont également attribuées trois définitions de stratégie Azure en vue de surveiller les points de terminaison, applications et comptes de stockage non protégés. Les points de terminaison et applications qui ne sont pas protégés par un pare-feu ainsi que les comptes de stockage à accès non limité sont susceptibles de laisser un accès non souhaité aux informations contenues dans le système d'information.

- L'accès via un point de terminaison accessible sur Internet devrait être limité.
- Les comptes de stockage devraient limiter l'accès réseau.

Mesures et stratégies complémentaires

- Attribution forcée de NSG sur des sous-réseaux en vue de limiter le trafic autorisé.
- Attribution forcée de tables de routage sur des sous-réseaux en vue de contrôler le trafic des données sortant via un pare-feu.
- Mise en œuvre de points de terminaison privés pour tous les services PaaS pris en charge en vue de limiter aux réseaux privés la communication réseau entre les composants d'application
- Utilisation de fonctionnalités de réseau sécurisées pour publier des applications web sur Internet ou y accéder depuis Internet :
 - Application Gateway (pour les applications web)
 - Azure Front Door (pour les applications web multi-régions)
 - Load Balancer (pour une IP publique pour applications)
 - NAT Gateway (IP publique pour le trafic Internet sortant)
 - Bastion Host (pour l'accès à distance du bureau aux machines virtuelles)

4.18 A.13.2.1 STRATÉGIES ET PROCÉDURES DE TRANSFERT D'INFORMATIONS

Des stratégies, procédures et contrôles de transmission formels doivent être mis en place pour protéger le transfert d'informations s'effectuant via tous types d'installations de communication

Documentation sur le contrôle ISO : <https://www.isms.online/iso-27001/annex-a-13-communications-security/>

Contenu blueprint

Le blueprint vous aide à assurer la sécurité du transfert d'informations avec les services Azure en attribuant deux définitions de stratégie Azure qui visent à vérifier les connexions non sécurisées aux comptes de stockage et à Redis Cache.

- Pour Azure Redis Cache, seules les connexions sécurisées doivent être activées.
- Le transfert sécurisé dans les comptes de stockage devrait être activé.

Mesures et stratégies complémentaires

- Le transfert uniquement via HTTPS devrait être activé dans App Services.
- Le transfert uniquement via HTTPS devrait être activé dans Front Door.
- Le transfert uniquement via HTTPS devrait être activé dans Application Gateway.





Merci
Danke
Grazie
Engraziel