RÉSUMÉ THÉORIQUE – FILIÈRE INFRASTRUCTURE DIGITALE

M213 - Sécuriser un environnement Cloud propriétaire en ligne public

54,5 heures

SOMMAIRE

MODALITÉS PÉDAGOGIQUES

1

LE GUIDE DE SOUTIEN

Il contient le résumé théorique et le manuel des travaux pratiques

2

LA VERSION PDF

Une version PDF est mise en ligne sur l'espace apprenant et formateur de la plateforme WebForce Life

3

DES CONTENUS TÉLÉCHARGEABLES

Les fiches de résumés ou des exercices sont téléchargeables sur WebForce Life

4

DU CONTENU INTERACTIF

Vous disposez de contenus interactifs sous forme d'exercices et de cours à utiliser sur WebForce Life

5

DES RESSOURCES EN LIGNES

Les ressources sont consultables en synchrone et en asynchrone pour s'adapter au rythme de l'apprentissage

PARTIE 1

SE PRÉPARER POUR LA SÉCURITÉ DANS LE CLOUD

Dans ce module, vous allez :

- Connaître les enjeux de sécurité Cloud
- Découvrir des aspects de sécurité Cloud

11 heures

CHAPITRE 1

Identifier les enjeux de sécurité Cloud

Ce que vous allez apprendre dans ce chapitre :

- Identifier les clauses essentielles du contrat fournisseur Cloud
- Le partage de responsabilité dans le Cloud
- Mettre en place une stratégie de sortie du Cloud
- Connaître les normes et les standards de sécurité du Cloud

5,5 heures

CHAPITRE 1

Identifier les enjeux de sécurité Cloud

1. **Clauses du contrat fournisseur Cloud**
2. Responsabilité partagée dans le Cloud
3. Stratégies de sortie du Cloud
4. Normes et standards de sécurité

Importance du contrat fournisseur Cloud

Le contrat de services Cloud que les fournisseurs proposent à leurs clients représente un défi pour les entreprises car il régit des sujets nombreux et variés : techniques, sécuritaires, juridiques, financiers, protection des données personnelles, etc.

Bien que très spécifique au premier abord, ce contrat devient pourtant très vite le croisement entre plusieurs métiers chez les clients : **achats, direction commerciale, informatique, juridique, direction générale** etc. Coordonner ces différents acteurs ou solliciter des spécialités aussi variées au sein d'une entreprise rendent l'analyse du contrat de services Cloud complexe.

Contrairement aux offres classiques d'externalisation, dans lesquelles les prestataires fournissent une réponse personnalisée à un cahier des charges défini par le client, de nombreuses offres de Cloud sont « standards » pour tous les clients et ne répondent pas à un cahier des charges particulier.

Toutefois, le client doit définir ses propres exigences et évaluer si les offres envisagées répondent à l'ensemble des exigences formulées. En effet, si le but du Cloud est d'alléger le client de certaines tâches opérationnelles, il doit s'assurer à priori que le fournisseur suit un niveau d'exigence au moins égal au sien.

PARTIE 1

Les volets du contrat fournisseur Cloud

Ci-après les éléments essentiels devant figurer dans un contrat de prestation de services de Cloud :

1. Localisation
2. SLA et ISO
3. Audit
4. Sécurité
5. Disponibilité

6. Réversibilité/portabilité
7. Sous-traitants
8. Traçabilité
9. Résiliation et élimination
10. Notifications

Détail des clauses du contrat fournisseur Cloud :

1 – Localisation & transfert des données	Compte tenu des contraintes légales, le client doit s'assurer de la localisation et du transit de ses données en limitant la liste des pays (pays ayant des conventions juridiques avec le Maroc comme l'Irlande par exemple) . Dans ce sens, le contrat devrait intégrer une clause permettant au client d'être tenu informé de la localisation de ses données. Cela peut être prévu par une clause stipulant que : "Le fournisseur informe le Client que les Données seront hébergées dans des serveurs localisés dans les pays suivants : [fournir une liste exhaustive des pays hébergeant les serveurs du fournisseur]. En cas de modification des pays destinataires par le fournisseur, ce dernier devra en informer préalablement le Client sans délai et obtenir son consentement écrit. Le cas échéant, le fournisseur devra fournir au Client une liste des pays destinataires mise à jour ".
2 – SLA et ISO	Un SLA (service level agreement) décrit les accords pris entre les deux parties visant à définir les niveaux de qualité du service à fournir et son taux de disponibilité. Demandez également les certificats ISO, car ceux-ci peuvent garantir un certain niveau de performance.
3 – Audit	Il est essentiel que le client conserve la possibilité de s'assurer du respect par le fournisseur de ses obligations à travers des points de contrôle contractuellement organisés. Les audits auront notamment pour vocation de vérifier la conformité aux obligations de sécurité, aux règles régissant le traitement des données personnelles, aux engagements de niveau de service ou aux exigences réglementaires sectorielles le cas échéant applicables en matière d'externalisation. La fréquence, la durée, la définition du périmètre et des modalités, la répartition des coûts ainsi que l'encadrement et le suivi des mesures résultant des vérifications réalisées constituent les points d'attention contractuels.

Détail des clauses du contrat fournisseur Cloud :

4 – Sécurité	Le contrat devra inclure la garantie technique du niveau de sécurité de la plateforme et des équipements sur lesquels les données et applications métiers sont hébergées, ainsi que la mise aux normes des protocoles de sécurité en fonction de l'apparition de nouvelles technologies et des nouveaux usages (authentification, accès sécurisé…). Ainsi, le fournisseur prendra toutes les précautions nécessaires pour assurer la sécurité des données. Les mesures de sécurité concernent la sûreté physique (protection du site, accès sécurisés, système de refroidissement des serveurs, etc.) et la protection des données (chiffrement des données et liaison chiffrée …).
5 – Disponibilité	S'assurer des temps d'arrêt définis par le fournisseur et veiller à ce qu'ils soient planifiés dans le temps, à ce qu'ils soient conformes aux exigences de disponibilité de l'entreprise et qu'ils ne soient pas en conflit avec les heures de travail.
6 – Réversibilité/portabilité	Cet élément contractuel permet de s'assurer de récupérer, à tout moment et dans un format standard, les données hébergées chez le prestataire dont le client doit s'assurer qu'il est bien indépendant. Ainsi, au terme du contrat, vous récupérez l'ensemble de vos données et le fournisseur s'engage à ne conserver aucune copie.
7 - Sous-traitants	S'assurer de savoir si le fournisseur Cloud fait appel à des sous-traitants. Il se peut que ceux-ci gèrent des éléments essentiels du service fourni et qu'ils aient également accès à vos données. Il importe d'avoir une idée précise de leur fiabilité et de leur relation juridique avec le fournisseur.

Détail des clauses du contrat fournisseur Cloud :

8 – Traçabilité	Accès aux journaux de traçabilité des actions effectuées sur les données par le personnel du client et par celui du fournisseur et assurer la remontée de l'information de toute anomalie détectée par le fournisseur.
9 – Résiliation et élimination	S'assurer que le fournisseur Cloud respecte la politique de l'entreprise en matière d'élimination des supports de stockage de données. Les méthodes appliquées pour le nettoyage et la désinfection obligatoires des données doivent être réalisés sous le contrôle et l'approbation de l'entreprise à l'expiration du contrat. Identifier une stratégie de sortie avec des termes qui encadrent la récupération des actifs et des données de l'entreprise dans un laps de temps déterminé.
10 – Notifications	Le fournisseur s'engage à notifier le client pour toute violation des données (fuites de données à caractère personnel, violation de la vulnérabilité des systèmes).

CHAPITRE 1

Identifier les enjeux de sécurité Cloud

1. Clauses du contrat fournisseur Cloud
2. **Responsabilité partagée dans le Cloud**
3. Stratégies de sortie du Cloud
4. Normes et standards de sécurité

Principe de la responsabilité partagée dans le Cloud

Quand vous considérez et évaluez les services Cloud, il est essentiel de comprendre le modèle de responsabilité partagée et de savoir distinguer les tâches de sécurité qui dépendent du fournisseur Cloud de celles qui vous incombent. De plus, de nombreuses entreprises qui envisagent le passage vers Cloud supposent à tort qu'après avoir migré vers le Cloud, leur rôle dans la sécurisation de leurs données est transféré, pour la plupart des responsabilités de sécurité et de conformité, au fournisseur.

Du fait de leur concept, les fournisseurs Cloud doivent assurer la sécurité de certains éléments, tels que l'infrastructure et le réseau, mais les clients doivent être conscients de leurs propres responsabilités. Les fournisseurs peuvent fournir des services pour aider à protéger les données, mais les clients doivent également comprendre leur rôle dans la protection de la sécurité et de la confidentialité de leurs données.

La meilleure illustration de ce problème concerne la mauvaise mise en œuvre d'une politique de mot de passe. En effet, les meilleures mesures de sécurité d'un fournisseur Cloud seront mises en échec si les utilisateurs ne mettent pas des mots de passe complexes.

Répartition de la responsabilité selon les modèles de services

Le NIST (National Institute of Standards and Technology) définit le Cloud computing comme un modèle de prestation de services qui comprend les caractéristiques essentielles suivantes :

- Libre-service à la demande : les utilisateurs peuvent fournir eux-mêmes des services
- Large accès au réseau : le service est disponible sur n'importe quel support ou appareil, y compris mobile
- Mise en commun des ressources : plusieurs utilisateurs possibles et accès dynamique aux ressources en commun
- Élasticité rapide : les ressources peuvent augmenter ou se réduire aussi rapidement qu'elles sont utilisées ou libérées
- Service mesuré : les services sont facturés en fonction de ce qui est utilisé

Le NIST définit également trois principaux mécanismes de prestation de services Cloud :

- IaaS : l'infrastructure en tant que service;
- PaaS : plateforme en tant que service et;
- SaaS : logiciel en tant que service.

Les responsabilités en ce qui concerne une charge de travail varient selon qu'elle est hébergée sur un logiciel SaaS, une plateforme PaaS, une infrastructure IaaS ou dans un centre de données local.

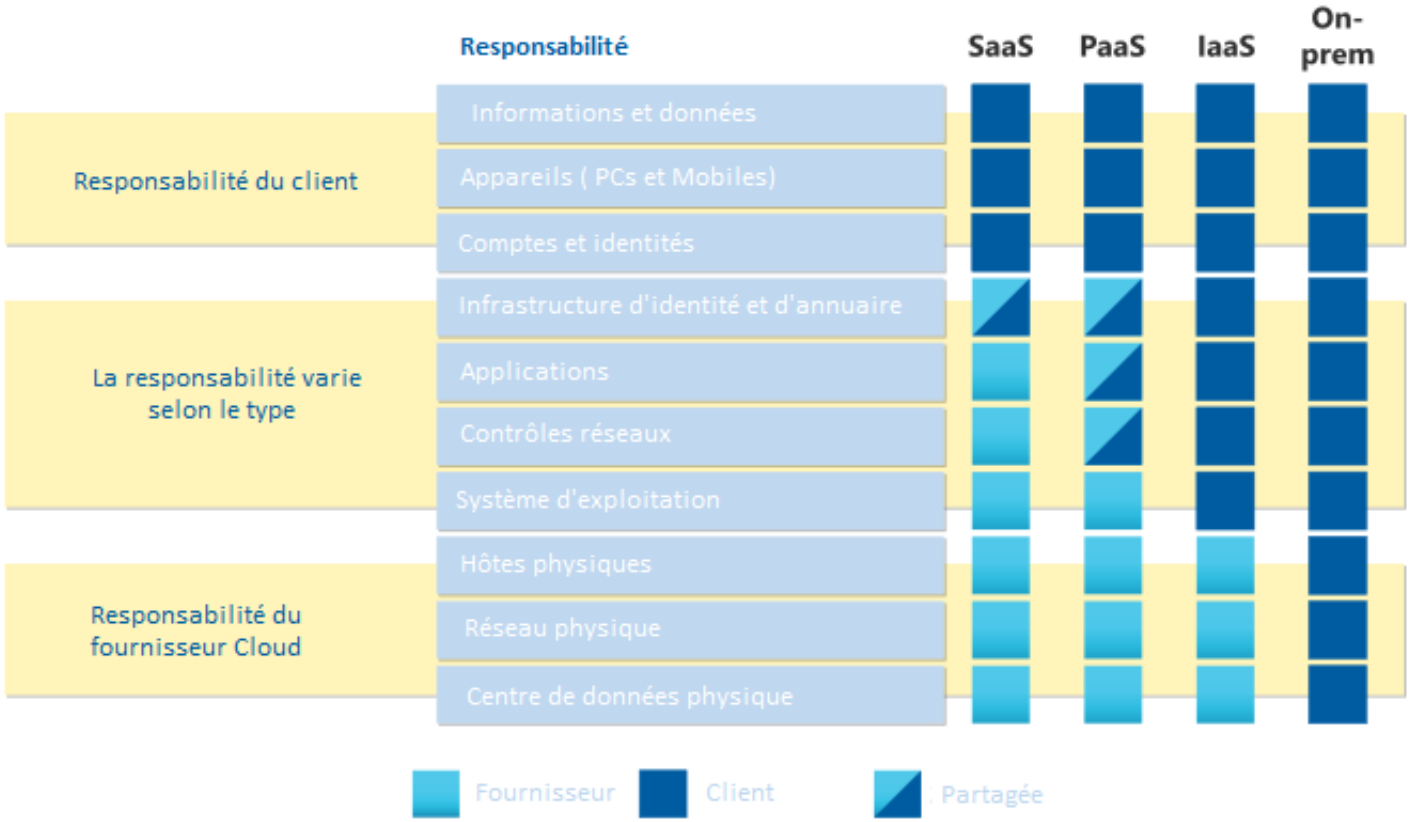
Répartition de la responsabilité selon les modèles de services

Dans un centre de données local, vous êtes propriétaire de la pile entière. Quand vous migrez dans le Cloud, certaines responsabilités sont transférées au fournisseur. Le schéma suivant illustre les domaines de responsabilité entre vous et le fournisseur, selon le type de déploiement de votre pile.

Vous êtes chargé de protéger la sécurité de vos données et des identités, des ressources locales, et des composants du Cloud que vous contrôlez (qui varient selon le type de service).

Quel que soit le type de déploiement, vous conservez toujours les responsabilités suivantes :

- Données
- Points de terminaison
- Comptes
- Gestion de l'accès



PARTIE 1

CHAPITRE 1

Identifier les enjeux de sécurité Cloud

1. Clauses du contrat fournisseur Cloud
2. Responsabilité partagée dans le Cloud
3. **Stratégies de sortie du Cloud**
4. Normes et standards de sécurité

Pourquoi faut-il avoir des stratégies de sortie du Cloud?

Le concept de « **sortie du Cloud** » est simple. Certains l'appellent une « **migration inversée** », mais en termes simples, une stratégie de sortie du Cloud correspond à la mise en place d'un plan d'entreprise pour garantir que les services et les solutions déployés sur le Cloud peuvent être remplacés ou répliqués efficacement, sans interruption significative.

Il existe plusieurs raisons pour lesquelles une entreprise peut envisager une stratégie de sortie du Cloud :

- **Maintenir un niveau plus élevé de continuité et de fiabilité des activités :**

Alors que la plupart des fournisseurs de Cloud public offrent une disponibilité importante sur des services fiables, même les grands acteurs du marché ont connu des pannes importantes ces dernières années. Si cela persiste à l'avenir, l'entreprise doit envisager de créer une solution de reprise après sinistre entre les Cloud publics ou le rapatriement des services en interne.

- **Accéder à l'innovation :**

L'innovation peut aider l'entreprise à mieux répondre à l'évolution des opportunités du marché. Le multi-Cloud consiste à exploiter les capacités uniques de différents Cloud, plutôt que d'aller tout-en-un avec un seul fournisseur de Cloud.

Par exemple, une entreprise peut tirer parti d'une nouvelle technologie de pointe proposée par un fournisseur de Cloud qu'elle n'utilise pas actuellement. Par ailleurs, un fournisseur de Cloud peut arrêter ou ne plus prendre en charge une application ou un service particulier, impactant ainsi l'équipe projet.

Pourquoi faut-il avoir des stratégies de sortie du Cloud?

➢ **Exigences réglementaires :**

Afin de s'aligner avec les exigences légales et les règlementations en vigueurs.

Par exemple, La Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (CNDP) établit des règles sur la manière dont les informations d'identification personnelle doivent être traitées. Si votre fournisseur actuel héberge ce type de données dans des emplacements interdits, l'entreprise aura besoin d'un plan pour déplacer ces données vers un autre fournisseur, car vous êtes considéré comme le propriétaire des données.

➢ **Verrouillage des fournisseurs :**

Avoir une stratégie de sortie du Cloud bien planifiée atténue les pressions liées au verrouillage des fournisseurs. Avoir une stratégie de sortie du Cloud prête à l'emploi vous permet de profiter de meilleurs prix et de remises plus intéressantes en vous donnant plus de poids dans les négociations financières.

Les 4 aspects clés de toute stratégie de sortie du Cloud :

Voici les 4 aspects que vous devrez avoir en vue lors de la construction de votre stratégie de sortie du Cloud :

- ✓ **L'inventaire des plateformes :** Connaître son patrimoine est essentiel. Les stratégies de sortie ne s'appliquent souvent qu'aux fonctions critiques de l'entreprise. Il est donc important de savoir ce que vous avez en cours d'exécution dans quel Cloud – un inventaire Cloud à jour est d'une grande aide.

- ✓ **L'infrastructure open source et portabilité :** Les composants d'infrastructure open source tels que Kubernetes ou les clusters OpenShift ou les bases de données open source peuvent faciliter le passage d'un Cloud à l'autre. Plus vous utilisez de services propriétaires, plus il sera difficile d'adapter votre application pour qu'elle s'exécute dans un nouvel environnement Cloud.

- ✓ **Multi-Cloud dès le début :** Vu les délais important des négociations contractuelles entre les entreprises et les fournisseurs Cloud. Il est plus judicieux d'avoir des contrats établis avec plusieurs fournisseurs Cloud dès le début.

- ✓ **Blocage entreprise :** Même si, d'un point de vue technique, votre application peut facilement être déplacée vers un autre fournisseur Cloud, si vous exécutez des applications Cloud à grande échelle, la configuration des environnements Cloud correspondants en transférant les autorisations et les configurations est extrêmement complexe. Utilisez un système de gouvernance centralisé comme **meshCloud** pour garder vos structures indépendantes des fournisseurs spécifiques.

CHAPITRE 1

Identifier les enjeux de sécurité Cloud

1. Clauses du contrat fournisseur Cloud
2. Responsabilité partagée dans le Cloud
3. Stratégies de sortie du Cloud
4. **Normes et standards de sécurité**

Normes et standards de sécurité applicables dans le Cloud

Les utilisateurs de service Cloud ont un réel besoin d'être rassurés quant à la sécurité des offres Cloud, notamment sur la confidentialité, l'intégrité et la disponibilité de l'information. Etant donnée la diversité des offres (IaaS, PaaS, SaaS ...), le nombre important d'acteurs impliqués dans cet écosystème et la complexité des contrats Cloud, les clients réclament en premier lieu plus de clarté et de lisibilité. La certification des services Cloud d'un fournisseur selon des normes bien établies est un facteur important permettant de renforcer cette confiance.

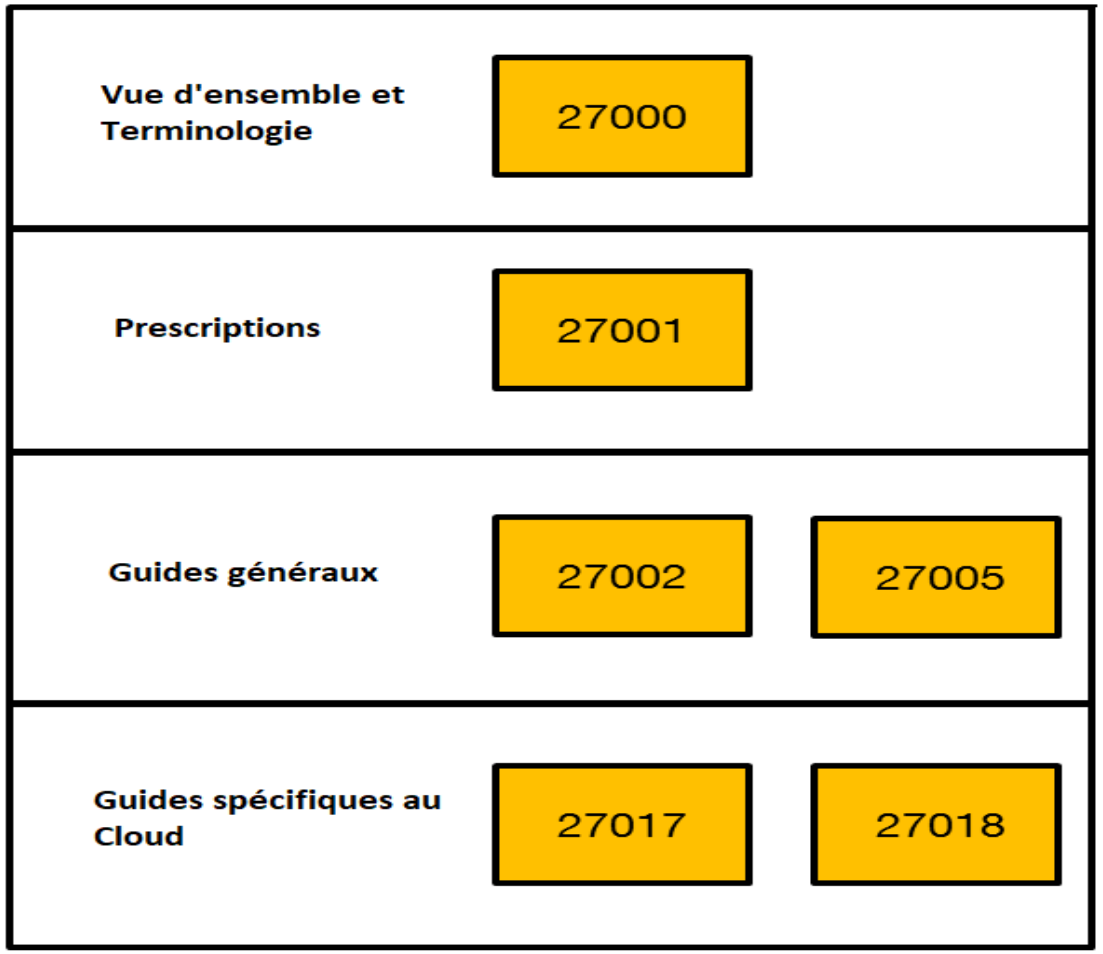
Ci-dessous les normes de sécurité applicable au niveau Cloud :

- **ISO 7498-2** : la norme ISO 7498-2 est un volet sécurité relativement ancien de la norme ISO 7498 plus connue sous le nom de Modèle OSI. Elle définit l'exigence en matière de sécurité sur des thèmes comme : l'identification, les autorisations, la confidentialité, la disponibilité, l'intégrité et la non-répudiation. La sécurité du Cloud peut être guidée par cette norme afin d'être efficace et sécurisée.
- **HIPAA** : Une application de santé qui traite des informations médicales protégées doit respecter la règle de protection de la vie privée et la règle de sécurité prévues par la loi américaine HIPAA (Health Insurance Portability and Accountability Act). Au minimum, la loi HIPAA peut exiger qu'un établissement de soins de santé reçoive impérativement par écrit une garantie du fournisseur de Cloud indiquant que les données PHI reçues ou créées seront protégées.
- **PCI :** La norme de sécurité de l'industrie des cartes de paiement (PCI DSS) concerne les informations propriétaires relatives aux normes de sécurité pour les entreprises, lorsque celles-ci traitent les cartes de crédit venant des plus grands systèmes de paiement par carte comme Visa, MasterCard, American Express, Discover et JCB.
- **RGPD (Règlement général sur la protection des données) :** Conçu pour renforcer la protection des données pour les personnes au sein de l'Union Européenne. Le RGPD exige que les données concernant les personnes (comme « un nom, une adresse postale, une photo, une adresse e-mail, des coordonnées bancaires, des publications sur des réseaux sociaux, des informations médicales ou l'adresse IP d'un ordinateur ») restent sur des serveurs au sein de l'UE et ne soient pas transférées hors de celle-ci.
- **CDMI (Cloud Data Management Interface)** : décrit un format d'échange qui permet de déplacer les données d'un environnement Cloud vers un autre.

PARTIE 1

Normes et standards de sécurité applicables dans le Cloud

- **ISO/IEC 27001 :** la norme ISO 27001 est une norme reconnue à l'échelle internationale pour l'évaluation de la sécurité des environnements informatiques. Cette norme concernant la sécurité de l'information est fondée sur les méthodes de gestion de la sécurité de l'information, de la confidentialité, de l'intégrité et de la disponibilité.
- **ISO/IEC 27017 :** la norme ISO/IEC 27017 est une déclinaison du guide de bonnes pratiques ISO/IEC 27002 traitant spécifiquement le Cloud. Elle propose des contrôles de sécurité supplémentaires pour le Cloud puisque l'ISO/IEC 27002, la norme dont elle découle et qu'elle enrichit, ne couvre pas cet aspect de manière adéquate. Elle la complète de deux manières :
  1. **En précisant les mesures de sécurité existantes dans la norme ISO/IEC 27002** et en distinguant des mesures pour le fournisseur de services Cloud et pour le client de services Cloud.
  2. **En ajoutant des mesures de sécurité manquantes** par rapport à la norme ISO/IEC 27002 et décrites dans l'annexe A de la norme ISO/IEC **27017.**
- **ISO/IEC 27018 :** la norme ISO/IEC 27018 est une norme récente (août 2014) corollaire à ISO 27001 et elle concerne les prestataires des services Cloud public. Elle propose un ensemble de bonnes pratiques pour la protection des informations personnelles identifiables.



Normes et standards de sécurité applicables dans le Cloud

- **CIS* Foundations Benchmarks :** fournissent les meilleures pratiques qui ont été développées pour aider les entreprises à sécuriser les environnements de Cloud public au niveau du compte. Il existe plus de 100 PDF CIS Benchmarks gratuits couvrant plus de 25 familles de produits de fournisseurs tels que les systèmes d'exploitation, les serveurs, les fournisseurs de Cloud, les appareils mobiles, les logiciels de bureau et les appareils réseau.

* **CIS** : Center for Internet Security (fournit des normes de configuration consensuelles et indépendantes des fournisseurs pour le Cloud).

- **NIST* 800-53 :** La publication spéciale 800-53 du NIST couvre les étapes du cadre de gestion des risques qui traitent de la sélection des contrôles de sécurité pour les systèmes d'information fédéraux conformément aux exigences de sécurité de la norme FIPS (Federal Information Processing Standard) 200. Les règles de sécurité couvrent 18 domaines, dont le contrôle d'accès, la réponse aux incidents, la continuité des activités et la reprise après sinistre.

* **NIST :** National Institute of Standards and Technology.

CHAPITRE 2

Appréhender des aspects de sécurité Cloud

Ce que vous allez apprendre dans ce chapitre :

- Avoir une idée sur la console de gestion du Cloud
- Assimiler les principes de clés et de secrets
- Sécuriser un compte administrateur
- Connaître la journalisation des événements

5,5 heures

CHAPITRE 2

Appréhender des aspects de sécurité Cloud

1. **Console de gestion du Cloud**
2. Clés et secrets
3. Comptes administrateurs
4. Journalisation des événements

Principe de la console de gestion de sécurité

La console de gestion de la sécurité Cloud correspond à un ensemble d'outils mises à la disposition des clients par les fournisseurs Cloud qui couvrent les deux grands piliers de la sécurité Cloud : la plateforme de protection de charge de travail (**CWPP**) et la gestion de la posture de sécurité Cloud (**CSPM**).

Les outils mis en place répondent à trois besoins essentiels lorsque vous gérez la sécurité de vos ressources et charges de travail dans le Cloud et localement :

Evalue en continu

votre posture de sécurité et ce afin de vous aider à comprendre votre situation actuelle en matière de sécurité et vous permettre ainsi d'améliorer efficacement votre sécurité

Sécurise

vos charges de travail avec des actions pas à pas qui protègent vos charges de travail contre les risques de sécurité connus.

Protège

vos charges de travail en temps réel afin que vous puissiez réagir immédiatement et empêcher les événements de sécurité de se propager.

La gestion de la posture de sécurité Cloud (CSPM)

CSPM désigne l'utilisation de stratégies et de logiciels pour garantir que les ressources Cloud sont auditées, organisées, correctement configurées, maintenues, sécurisées et respectent les normes de conformité.

Selon le **cabinet Gartner**, les outils CSPM sont indispensables à la sécurité du Cloud.

Exemple de solution :

Azure Defender pour le Cloud : il évalue en continu vos ressources, vos abonnements et les entreprise à la recherche de problèmes de sécurité et affiche votre posture de sécurité sous la forme d'un degré de sécurisation, un score agrégé des résultats de sécurité qui vous présente, d'un seul coup d'œil, l'état de votre sécurité actuelle : plus le score est élevé, et plus le niveau de risque identifié est faible.

Lorsque vous ouvrez **Azure Defender** pour le Cloud pour la première fois, il :

1. **Affiche un degré de sécurisation** pour vos abonnements en fonction de l'évaluation de vos ressources connectées, par rapport aux recommandations du Benchmark de sécurité Azure. Lorsque vous avez activé les fonctionnalités de sécurité renforcée, vous pouvez personnaliser les normes utilisées pour évaluer votre conformité, ainsi qu'ajouter d'autres réglementations (telles que NIST et Azure CIS) ou des exigences de sécurité spécifiques à votre entreprise. Vous pouvez également appliquer des recommandations et évaluer votre score sur la base des standards des bonnes pratiques de sécurité de base d'autres fournisseurs (AWS, …).

2. **Fournit des recommandations en matière de sécurité renforcée** en fonction des erreurs de configuration et des faiblesses de sécurité identifiées. Utilisez ces recommandations de sécurité pour renforcer la posture de sécurité des ressources Azure, hybrides et Multi-Cloud de votre entreprise.

Comment fonctionne CSPM

La gestion de la posture de sécurité du Cloud fournit des ressources permettant d'identifier les faiblesses de sécurité liées à la configuration, aux opérateurs et aux utilisateurs pour les activités à risque. La détection s'étend pour atteindre les ressources locales et celles s'exécutant sur d'autres Cloud.

En cas de détection, des suggestions ou une assistance peuvent être présentées pour prendre des mesures correctives en fonction des configurations. Il est également possible de définir des exigences en matière de stratégie pour des groupes de ressources, de faire appliquer les stratégies et de corriger et consigner automatiquement toute violation de sécurité.

Le CSPM permet d'avoir une vue complète de l'infrastructure Cloud d'une entreprise. Cette information fournira une visibilité en donnant :

- Une synthèse des problèmes liés au SaaS, au IaaS et au PaaS pour réduire les risques et garantir la conformité
- Un score de sécurité et de risque
- Des recommandations concrètes
- Une carte indiquant la provenance de l'activité suspecte de l'utilisateur

Toute action ou paramètre sur une ressource qui pourrait potentiellement causer un risque de sécurité est un problème. La gestion de la posture de sécurité du Cloud aidera à détecter les ressources mal configurées et les activités menaçant la sécurité afin de fournir aux administrateurs de la sécurité la visibilité nécessaire pour trier et résoudre les problèmes de sécurité du Cloud.

Avantages CSPM

1. **Automatiser la résolution des problèmes de sécurité :** Automatisez la correction des menaces de sécurité pour les problèmes simples et complexes en utilisant les actions de remédiations de sécurité pour aider à optimiser l'intervention des ressources de l'équipe sécurité.
2. **Obtenir une vue d'ensemble de la posture en matière de risque :** Évaluer et visualiser l'état de sécurité et de risque Cloud à l'aide d'une interface utilisateur de type console et d'interfaces programmables telles que les API Cloud, les interfaces de ligne de commande, les kits de développement logiciel (SDK), etc.
3. **Automatiser l'application des politiques de sécurité du Cloud :** Prévenir les erreurs de configuration de la sécurité du Cloud en appliquant dès le premier jour les exigences de la stratégie de sécurité pour les données critiques de l'entreprise et réduire le risque de sécurité tout au long du cycle de vie du Cloud.
4. **Adopter une bibliothèque de stratégies avec les bonnes pratiques de sécurité :** Bénéficier d'une expertise en matière de sécurité intégrée pour protéger les ressources grâce à un service de sécurité Cloud intégré et à une bibliothèque de stratégies de sécurité pour aider à configurer et à protéger les charges de travail.
5. **Renforcez la sécurité par compartiment :** Déplacer la responsabilité de la sécurité dans le système d'exploitation invité, l'application et les couches de données avec une application approfondie de la sécurité Cloud intégrée pour remplir les obligations de sécurité.

La plateforme de protection de charge de travail (CWPP)

Selon le cabinet **Gartner**, une plateforme de protection de la charge de travail du Cloud (**CWPP**) est définie comme une offre de sécurité centrée sur la charge de travail, destinée à répondre aux exigences spécifiques de protection des charges de travail dans les environnements hybrides, multi-Cloud et de data center.

De plus, **Gartner** affirme que les CWPP offrent un contrôle et une visibilité cohérents pour les machines physiques, les machines virtuelles, les conteneurs et les charges de travail sans serveur, quel que soit l'emplacement.

En général, les outils CWPP permettent de sécuriser toutes les ressources de l'entreprise, que ce soit celles disponibles chez différents fournisseurs Cloud ou sur le site du client.

Exemple de solution :

Azure Defender pour le Cloud offre des alertes de sécurité optimisées par les renseignements sur les menaces Microsoft. Il inclut également une série de protections avancées et intelligentes pour vos charges de travail. Les protections des charges de travail sont fournies au travers de plans Microsoft Defender spécifiques selon le type de ressources incluses dans vos abonnements.

Par exemple, vous pouvez activer Microsoft Defender pour le stockage afin de recevoir des alertes sur les activités suspectes liées à vos ressources de stockage.

Etant donnée qu'Azure Defender pour le Cloud est un service natif Azure, de nombreux services Azure sont surveillés et protégés sans devoir être déployés, mais vous pouvez également ajouter des ressources locales ou venant d'autres Cloud publics.

La plateforme de protection de charge de travail (CWPP)

La protection des ressources sur le Cloud ce fait à travers des connecteurs natifs pour le fournisseur Cloud (exemple : Azure Defender pour le Cloud Azure).

Ainsi, il permet de détecter les menaces pesant sur les ressources suivantes :

Services PaaS

- Détecte les menaces ciblant les différents services de données Cloud (exemple : Azure App Service, Azure SQL, Stockage Microsoft Azure).
- Détecte les anomalies dans les journaux d'activité des applications Cloud.

Services de données

- Inclut des fonctionnalités qui permettent de classer automatiquement vos données.
- Fournit des évaluations pour les vulnérabilités potentielles sur les services de stockage, ainsi que des recommandations pour les atténuer.

Services Réseaux

- Aide à limiter votre exposition aux attaques par force brute.
- A l'aide de l'accès juste-à-temps à la machine virtuelle, vous renforcez ainsi votre réseau en empêchant les accès inutiles.
- Vous permet de définir des stratégies d'accès sécurisées sur les ports sélectionnés, juste pour les utilisateurs autorisés, les adresses IP ou les plages d'adresses IP sources autorisées et pour une durée limitée.

La plateforme de protection de charge de travail (CWPP)

La protection s'étend pour atteindre les ressources locales et celles s'exécutant sur d'autres Cloud, ce qui vous permet de protéger vos différents serveurs et vous aide à vous concentrer sur l'essentiel, à savoir bénéficier de renseignements personnalisés sur les menaces et d'alertes hiérarchisées en fonction de votre environnement.

Par exemple, si vous avez connecté un compte Amazon Web Services (AWS) à un abonnement Microsoft Azure, vous pouvez activer l'une de ces protections :

1. Les **fonctionnalités de Defender pour le Cloud** s'étendent à vos ressources AWS. Ce plan sans agent évalue vos ressources AWS conformément aux recommandations de sécurité spécifiques à AWS. Celles-ci sont incluses dans votre niveau de sécurité. Les ressources sont également évaluées par rapport à leur conformité aux standards intégrés spécifiques à AWS (AWS CIS, AWS PCI DSS et AWS Foundational Security Best Practices). La page d'inventaire des ressources de Defender pour le Cloud est une fonctionnalité multi-Cloud qui vous permet de gérer vos ressources AWS avec vos ressources Azure.

2. **Microsoft Defender pour Kubernetes** étend sa détection des menaces contre les conteneurs et ses défenses avancées à vos **clusters Amazon EKS Linux**.

3. **Microsoft Defender pour les serveurs** ajoute la détection des menaces et les défenses avancées à vos instances EC2 Linux et Windows. Ce plan comprend la licence intégrée de Microsoft Defender pour point de terminaison, des bases de référence de sécurité et des évaluations au niveau de l'OS, l'analyse de l'évaluation des vulnérabilités, les contrôles d'application adaptatifs (AAC), le monitoring de l'intégrité des fichiers (FIM), etc.

CHAPITRE 2

Appréhender des aspects de sécurité Cloud

1. Console de gestion du Cloud
2. **Clés et secrets**
3. Comptes administrateurs
4. Journalisation des événements

Principe des clés et des secrets

Un secret est un élément pour lequel vous voulez contrôler étroitement l'accès. Il peut s'agir de clés d'API, de mots de passe, de certificats, de clés de chiffrement, les jetons OAuth et d'autres données sensibles nécessaires à l'exécution de vos applications.

Pour éviter les fuites de sécurité, il faut procéder au stockage des clés et des secrets dans un magasin sécurisé (exemple : Clés API, Chaînes de connexion de base de données, Clés de chiffrement des données, Clés SSH ou Mots de passe).

En effet, les informations sensibles ne doivent pas être stockées dans **le code ni dans la configuration de l'application**. Un attaquant qui parviendrait à accéder en lecture au code source ne doit pas pouvoir prendre connaissance de secrets spécifiques à l'application et à l'environnement.

Stockez l'ensemble des clés et des secrets d'application dans un service de coffre de clés managé (KMS). Le stockage des clés de chiffrement dans un magasin managé limite encore l'accès et les applications ou ressources qui désirent accéder aux secrets doivent s'authentifier à l'aide d'identités managées.

Les différents fournisseurs Cloud proposent différents outils qui permettent la gestion des clés et des secrets :

Fournisseurs	AWS	Google Cloud	Azure
Gestion des Clés	AWS KMS	Cloud KMS	Azure Key Vault
Gestion des secrets	AWS Secrets Manager	Secret Manager	Azure Key Vault

Fonctionnement des clés et des secrets (Azure Key Vault)

Toute personne disposant d'un abonnement Azure peut créer et utiliser des coffres de clés. Bien qu'Azure Key Vault procure des avantages aux développeurs et aux administrateurs de sécurité, il peut être implémenté et géré par l'administrateur d'une entreprise qui gère d'autres services Azure.

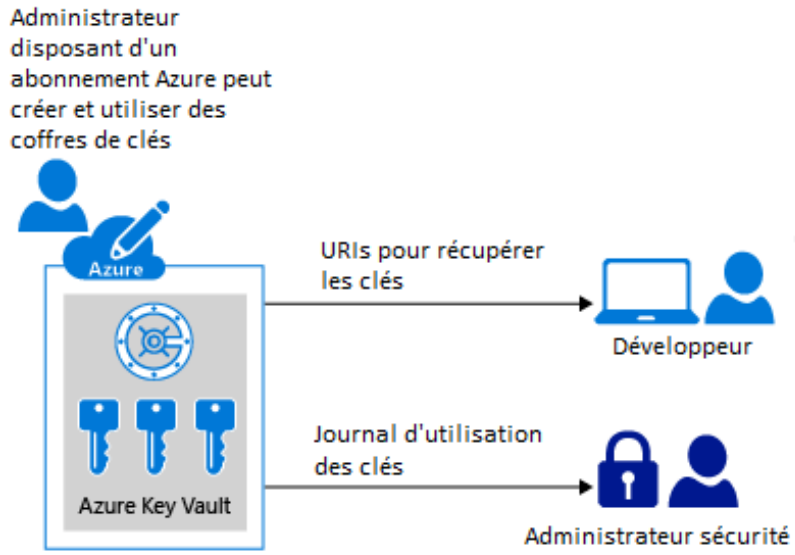
Par exemple, cet administrateur peut se connecter avec un abonnement Azure, créer un coffre pour l'entreprise dans lequel il va stocker les clés et avoir la responsabilité des tâches opérationnelles suivantes :

- créer ou importer une clé ou un secret ;
- supprimer ou effacer une clé ou un secret ;
- autoriser des utilisateurs ou des applications à accéder au coffre de clés, afin qu'ils puissent gérer ou utiliser les clés et les clés secrètes ;
- configurer l'utilisation de la clé (par exemple, signer ou chiffrer) ;
- surveiller l'utilisation de clés.

Cet administrateur donne ensuite aux développeurs les URI à appeler à partir de leurs applications.

Cet administrateur donne également les informations de journalisation sur l'utilisation de la clé à l'administrateur de sécurité.

Les développeurs peuvent également gérer les clés directement à l'aide d'API.



Source Microsoft

PARTIE 1

Meilleures pratiques de gestion des clés et des secrets

La rotation des clés et des secrets

Les secrets sont souvent stockés dans la mémoire de l'application en tant que variables d'environnement ou paramètres de configuration pendant tout le cycle de vie de l'application, ce qui les rend sensibles à une exposition indésirable. Pour réduire les vecteurs d'attaque, les secrets nécessitent une rotation et sont sujets à une date d'expiration. Le processus doit être automatisé et exécuté sans aucune intervention humaine. Leur stockage dans un magasin géré simplifie ces tâches opérationnelles en gérant la rotation des clés.

Étant donné que les secrets sont sensibles à la fuite ou à l'exposition, il est important de les renouveler souvent, au moins tous les 60 jours.

Accès et isolement réseau

Vous pouvez réduire l'exposition de vos coffres en spécifiant les adresses IP qui y ont accès. Configurez votre pare-feu de manière à n'autoriser que les applications et les services connexes à accéder aux secrets du coffre afin de réduire la capacité des attaquants à accéder aux secrets.

En outre, les applications doivent utiliser le droit d'accès minimal en ne disposant que de l'accès en lecture des secrets.

Surveillance

Pour surveiller l'accès à vos secrets et leur cycle de vie, activez la journalisation. Utilisez les services de monitoring proposé par le fournisseur Cloud pour surveiller sur la même plateforme toutes les activités liées aux secrets dans tous vos coffres. Vous pouvez aussi utiliser les services de détection d'événements (comme Azure Event Grid) pour surveiller le cycle de vie des secrets.

CHAPITRE 2

Appréhender des aspects de sécurité Cloud

1. Console de gestion du Cloud
2. Clés et secrets
3. **Comptes administrateurs**
4. Journalisation des événements

Les recommandations de sécurité pour les comptes « administrateurs »

La sécurité est une priorité pour les entreprises qui utilisent le Cloud. L'un des aspects clés de la sécurité en matière de gestion des ressources du Cloud est l'**identité** et l'**accès**.

Les comptes administrateurs sont des comptes à hauts privilèges, ayant accès à toutes les fonctionnalités des services et ressources Cloud. Ils sont les plus ciblés par les attaquants et nécessitent une authentification forte pour réduire le risque de compromission.

Ci-après les recommandations de sécurité concernant les comptes administrateurs établies pour les volets suivants :

- GESTION DES HABILITATIONS
- AUTHENTIFICATION MULTI-FACTEURS
- PROTECTION DU CHANGEMENT DE MOT DE PASSE
- SURVEILLER L'ACTIVITÉ
- PRÉPARER LA RÉCUPÉRATION D'UN COMPTE

Gestion des habilitations

La gestion des habilitations a pour finalité de protéger l'accès aux ressources du système d'information (SI) et de permettre de retrouver a posteriori qui était habilité à quoi. Dans un environnement Cloud, une telle action devra aussi être faite, et ce d'une manière périodique afin de maîtriser l'équilibre entre sécurité et productivité.

Dans ce sens, au niveau du workflow de gestion des habilitations, il est important de :

- **Exiger la validation en deux étapes pour les comptes administrateurs :** la validation en deux étapes permet de protéger le compte contre tout accès non autorisé.
- **Ne pas partager les comptes administrateurs entre les utilisateurs :** Configurez pour chaque administrateur un compte identifiable qui lui soit propre. En effet, si plusieurs administrateurs utilisent le même compte pour se connecter à la console d'administration, par exemple admin@example.com, il n'est pas possible d'identifier celui qui a effectué les actions répertoriées dans le journal d'audit.
- **Ne pas utiliser les comptes administrateurs pour des activités quotidiennes.**

Authentification multi-facteurs

L'authentification multi-facteurs (MFA) nécessite à un individu de présenter un minimum de deux formes d'authentification avant que l'accès ne soit accordé. Dans ce sens, il est important de :

- **Exiger MFA pour les administrateurs :** Les comptes auxquels sont affectés les droits d'administration sont ciblés par les attaquants, il faut alors exiger l'authentification MFA sur ces comptes afin de réduire le risque de compromission de ces comptes.

- **Désactiver la mémorisation de la MFA :** Il faut aussi veiller à éviter de donner aux utilisateurs la possibilité de se souvenir de l'authentification sur leurs appareils. La mémorisation de la MFA pour les appareils et les navigateurs vous permet de donner aux utilisateurs la possibilité de contourner MFA pendant un nombre de jours défini après la réussite de la connexion à l'aide de MFA.

- **Adopter une politique de gestion des mots de passe :** Il faut veiller à implémenter une politique de gestion des mots de passe comprenant la complexité, une certaine longueur des mots de passe ainsi que leur expiration périodique.

Protection du changement de mot de passe

Pour sécuriser le changement du mot de passe et éviter qu'il soit fait par une personne malveillante, il faut s'assurer que les deux autres formes d'identification sont nécessaires avant de permettre la réinitialisation du mot de passe. La configuration de la double identification avant d'autoriser la réinitialisation du mot de passe garantit la confirmation de l'identité de l'utilisateur via deux formes d'identification distinctes. Avec une double vérification d'identité, un attaquant devrait compromettre les deux formulaires d'identité avant de pouvoir réinitialiser par malveillance le mot de passe d'un utilisateur.

Il faut aussi s'assurer que :

- Tous les utilisateurs vont recevoir à leurs adresses de messagerie principale et secondaire un courrier électronique les informant que leur propre mot de passe a été réinitialisé via le portail du service de réinitialisation de mot de passe en libre-service.

- Tous les administrateurs sont avertis si un autre administrateur réinitialise son mot de passe.

Surveiller l'activité

Surveiller l'activité des administrateurs et les risques de sécurité potentiels est un élément important pour intervenir à temps.

Dans ce sens, il faut prévoir de :

- **Configurer des alertes par e-mail destinées à l'administrateur :** Surveillez l'activité des administrateurs et les risques de sécurité potentiels en configurant des alertes par e-mail destinées aux administrateurs pour signaler certains événements, par exemple des tentatives de connexion suspectes, des appareils mobiles compromis ou des modifications effectuées par un autre administrateur.

- **Consultez le journal d'audit de la console d'administration :** Ouvrez le journal d'audit de la console d'administration pour afficher l'historique de chaque tâche effectuée dans la console d'administration, l'administrateur qui l'a exécutée, la date et l'adresse IP avec laquelle l'administrateur s'est connecté.

Préparer la récupération d'un compte

Les administrateurs doivent ajouter des options de récupération à leur compte administrateur.

Dans ce sens, il faut prévoir de :

- **Ajouter des options de récupération aux comptes administrateurs :** Si un administrateur oublie son mot de passe, il peut choisir différents moyens de transmission du nouveau mot de passe par appel vocal, SMS ou e-mail. Pour ce faire, un numéro de téléphone et une adresse e-mail de récupération sont, en général, requis pour le compte.

- **Enregistrer les codes de secours à l'avance:** Si un administrateur perd sa clé de sécurité ou son téléphone (sur lequel il peut recevoir le code pour la validation en deux étapes), il peut se connecter à l'aide d'un code de secours. Les administrateurs doivent générer et imprimer des codes de secours à utiliser en cas de besoin. Conservez-les dans un endroit sécurisé.

CHAPITRE 2

Appréhender des aspects de sécurité Cloud

1. Console de gestion du Cloud
2. Clés et secrets
3. Comptes administrateurs
4. **Journalisation des événements**

Principe de la journalisation des événements

Les fournisseurs Cloud offrent un large éventail d'options de journalisation et d'audit de sécurité configurables pour vous aider à identifier les failles dans vos mécanismes et vos stratégies de sécurité.

En effet, les applications Cloud sont complexes, et se composent de nombreux éléments mobiles. L'enregistrement des données peut fournir des aperçus sur vos applications et vous aider à :

- Détecter des problèmes antérieurs et éviter des problèmes futurs.
- Améliorer les performances et la maintenabilité des applications.
- Automatiser des actions qui nécessitent autrement une intervention manuelle.

Les journaux des événements sont classés par type :

- **Journaux de ressources** : Fournissent des aperçus sur les opérations effectuées dans une ressource. Par exemple, l'obtention d'un secret à partir d'un coffre de clés ou l'exécution d'une requête sur une base de données. Le contenu des journaux de ressources varie en fonction du service et du type de ressource.

- **Journal d'activité :** Fournit des informations sur les opérations effectuées sur chaque ressource dans l'abonnement à partir de l'extérieur en plus des mises à jour sur des événements Service Health. Le journal d'activité vous permet de déterminer la *nature*, l'*auteur* et le *moment* de toute opération d'écriture (PUT, POST, DELETE) effectuée sur les ressources dans votre abonnement. Il n'y qu'un seul journal d'activité par abonnement.

Liste des journaux d'événements

Le tableau suivant liste les principaux types de journaux des événements disponibles dans le Cloud Azure :

Catégorie de journal	Type de journal	Usage	Intégration
Journaux d'activité	Événements de plan de contrôle sur les ressources d'Azure Resource Manager.	Fournissent des informations sur les opérations qui ont été effectuées sur les ressources de votre abonnement.	API REST, Azure Monitor
Journaux de ressources Azure	Données fréquentes sur les opérations des ressources Azure Resource Manager de l'abonnement.	Fournissent des aperçus sur les opérations que votre ressource réalise elle-même.	Azure Monitor
Compte-rendu Azure Active Directory	Journaux d'activité et rapports.	Signalent les activités de connexion des utilisateurs et fournissent des informations sur l'activité système relative à la gestion des utilisateurs et des groupes.	API Graph
Machines virtuelles et services Cloud	Services du journal des événements Windows et Syslog Linux.	Capturent les données système et les données de journalisation sur les machines virtuelles, puis les transfèrent vers un compte de stockage de votre choix.	Windows (avec stockage Diagnostics Azure) et Linux dans Azure Monitor

Source Microsoft

Liste des journaux d'événements

Catégorie de journal	Type de journal	Usage	Intégration
Azure Storage Analytics	Journalisation du stockage, fournit les données de métriques d'un compte de stockage.	Fournit des informations sur les demandes de trace, analyse les tendances d'utilisation et diagnostique les problèmes de votre compte de stockage.	API REST ou bibliothèque cliente
Journaux de flux du groupe de sécurité réseau (NSG)	Format JSON, affiche les flux entrants et sortants, par règle.	Affiche des informations sur le trafic IP entrant et sortant via un groupe de sécurité réseau.	Azure Network Watcher
Application Insights	Journaux d'activité, exceptions et diagnostics personnalisés.	Fournit un service de monitoring des performances de l'application (APM) aux développeurs web sur de nombreuses plateformes.	API REST, Power BI
Traitement des données/alertes de sécurité	Alertes de Microsoft Defender pour le Cloud, alertes des journaux d'activité Azure Monitor.	Fournit des alertes et des informations sur la sécurité.	API REST, JSON

Source Microsoft

PARTIE 2

ADOPTER UNE INFRASTRUCTURE CLOUD SÉCURISÉE

Dans ce module, vous allez :

- Renforcer la sécurité des VM
- Sécuriser le réseau
- Gérer les identités
- Protéger les données

38 heures

CHAPITRE 1

Renforcer la sécurité des VM

Ce que vous allez apprendre dans ce chapitre :

- Connaître la gestion des correctifs
- Désactiver l’accès Internet
- Désactiver les ports d’accès RDP/SSH
- Comprendre Bastion

8 heures

CHAPITRE 1

Renforcer la sécurité des VM

1. **Gestion des correctifs**
2. Accès internet
3. Désactivation de l’accès RDP/SSH
4. Bastion

La sécurité des VM

Suivant le type de service IaaS pour le Cloud, vous pouvez utiliser des machines virtuelles pour déployer un large éventail de solutions informatiques, et ce en toute flexibilité. Le service prend en charge Microsoft Windows, mais aussi Linux pour différentes distributions. Vous pouvez ainsi déployer n'importe quelle application et n'importe quel langage sur quasiment n'importe quel système d'exploitation.

Une machine virtuelle vous donne la flexibilité de la virtualisation sans devoir acheter le matériel physique qui exécute la machine virtuelle, ni en assurer la maintenance. Vous pouvez créer et déployer vos applications en ayant la certitude que vos données sont protégées au sein de centres de données hautement sécurisés.

Un ensemble de fonctionnalités de sécurité sont implémentées automatiquement par les fournisseurs Cloud. Toutefois, le client, à travers la configuration des machines virtuelles, peut compromettre et impacter le niveau de sécurité de la ressource. Ci-dessous certains volets importants relatifs à la sécurité des VM :

- Stratégie de gestion des correctifs
- Accès Internet
- Désactivation de l'accès RDP/SSH
- Bastion

Principe de gestion des correctifs

Il est essentiel de disposer d'un processus efficace de gestion des mises à jour et des correctifs pour assurer le bon fonctionnement des opérations, résoudre les problèmes de sécurité et réduire les risques de menaces accrus en matière de cybersécurité.

Toutefois, la gestion des mises à jour des correctifs nécessite une attention constante et continue du fait de la rapide évolution des technologies et de l'émergence constante de nouvelles menaces de sécurité.

Les fournisseurs Cloud offrent un ensemble d'outils et de ressources qui peuvent faciliter la gestion de la tâche complexe que représentent le suivi et l'application des mises à jour et des correctifs sur des machines dans le Cloud et le Cloud hybride.

Ci-dessous un exemple des différents outils qui permettent la gestion des correctifs :

Fournisseurs	AWS	Google Cloud	Azure
Patch Management	AWS Systems Manager (Module Patch Manager)	VM Manager	Azure Update Management

CHAPITRE 1

Renforcer la sécurité des VM

1. Gestion des correctifs
2. **Accès internet**
3. Désactivation de l’accès RDP/SSH
4. Bastion

PARTIE 2

Désactiver l'accès internet d'une VM sur le Cloud Azure

Afin de désactiver l'accès internet pour une machine virtuelle au niveau d'Azure, il suffit de bloquer les flux au niveau du composant Network Security Group (NSG) attaché à la carte réseau de la machine virtuelle.

1 – Se connecter au portail Azure : https://portal.azure.com/;

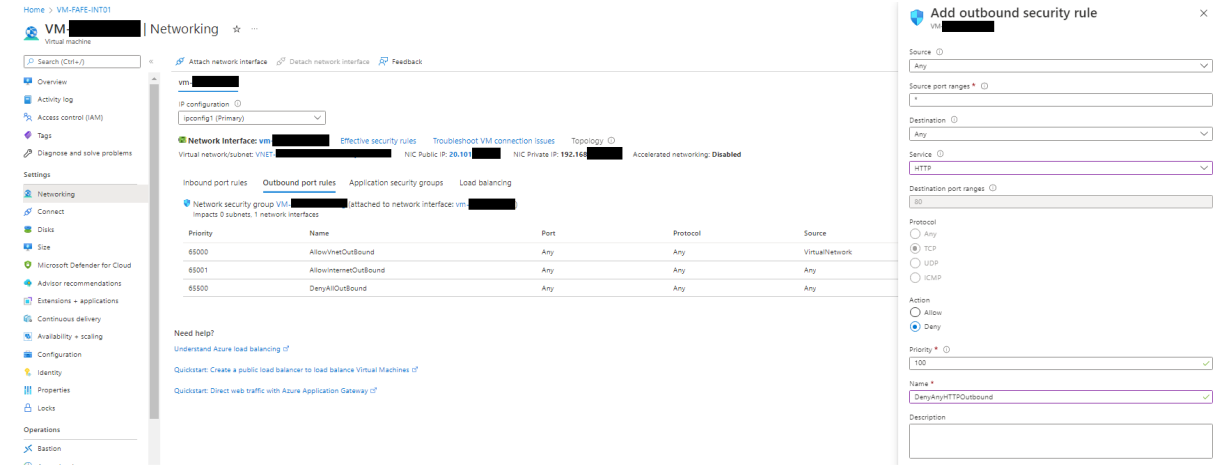
2 – Sélectionner une machine virtuelle;

3 – Au niveau du menu vertical présent à gauche, choisir l'onglet Réseau (Networking);

4 – Choisir « Règles des ports sortants » (Outbound port rules), les différentes règles des flux en sorties sont affichées;

5 – Sélectionner « ajouter une nouvelle règle de sécurité » en renseignant les informations suivantes :

Source : Any **Source port ranges :** * **Destination :** Service Tag **Destination Service tag :** Internet **Service :** HTTP **Protocol :** TCP **Action :** Deny **Priorité :** 100	**Source** : Any **Source port ranges :** * **Destination :** Service Tag **Destination Service tag :** Internet **Service :** HTTPS **Protocol :** TCP **Action :** Deny **Priorité :** 101



CHAPITRE 1

Renforcer la sécurité des VM

1. Gestion des correctifs
2. Accès internet
3. **Désactivation de l’accès RDP/SSH**
4. Bastion

Principe de désactivation de l'accès RDP/SSH

Il est possible d'atteindre les machines virtuelles à l'aide des protocoles RDP (Remote Desktop Protocol) pour Windows et SSH (Secure Shell) pour les machines Linux. Ces protocoles permettent de gérer des machines virtuelles à partir d'emplacements distants. Ils sont souvent utilisés par les centres de données informatiques.

Cependant, ils peuvent être sources de problèmes de sécurité quand ils sont utilisés sur internet. En effet, les attaquants peuvent recourir à des techniques de force brute pour accéder aux machines virtuelles. Lorsqu'ils y parviennent, ils peuvent utiliser votre machine virtuelle comme point de départ pour le piratage d'autres machines sur votre réseau virtuel, voire attaquer des appareils en réseau en dehors.

De ce fait, il est recommandé de désactiver l'accès direct des protocoles RDP et SSH à vos machines virtuelles Azure depuis internet. Cela fait, vous disposez d'autres options vous permettant d'accéder à ces machines virtuelles à des fins de gestion à distance.

Voici quelques scénarios et les options mises à disposition par le fournisseur Cloud Azure pour pallier cette action et vous permettre un accès sécurisé :

Scénarios de désactivation de l'accès RDP/SSH

Scénario 1 : Autorisez un utilisateur unique à se connecter à un réseau virtuel Azure via internet.

L'expression **VPN de point à site** est synonyme de connexion du client/serveur VPN pour un accès à distance. Une fois la connexion point à site établie, l'utilisateur peut avoir recours au protocole RDP ou SSH pour se connecter aux machines virtuelles situées sur le réseau virtuel Azure auquel cet utilisateur est connecté via le VPN point à site. Cela suppose que l'utilisateur dispose des autorisations requises pour atteindre ces machines virtuelles.
Le VPN point à site est plus sécurisé qu'une connexion RDP ou SSH directe, car l'utilisateur doit s'authentifier deux fois pour pouvoir se connecter à une machine virtuelle. L'utilisateur doit d'abord s'authentifier (et être autorisé) pour établir la connexion VPN point à site. Il doit ensuite à nouveau s'authentifier (et être autorisé) pour établir la session RDP ou SSH.

Scénarios de désactivation de l'accès RDP/SSH

Scénario 2 : Permettez aux utilisateurs de votre réseau local de se connecter aux machines virtuelles de votre réseau virtuel Azure.

Un **VPN de site à site** connecte un réseau dans son ensemble à un autre réseau, par le biais d'internet. Vous pouvez utiliser un VPN de site à site pour connecter votre réseau local à un réseau virtuel Azure. Les utilisateurs de votre réseau local se connectent à l'aide du protocole RDP ou SSH via la connexion VPN de site à site. Vous n'avez pas à autoriser un accès RDP ou SSH direct via internet.

Scénario 3 : Pour proposer une fonctionnalité similaire à la connexion VPN de site à site, utilisez une liaison réseau étendu dédiée.

Utilisez le service **ExpressRoute**. Ce service fournit des fonctionnalités similaires au VPN de site à site. Les principales différences entre ces deux architectures sont les suivantes :

- La liaison réseau étendu (WAN) dédiée ne transite pas par internet.
- Les liaisons WAN dédiées sont généralement plus stables et plus performantes.

PARTIE 2

Désactiver l'accès internet d'une VM sur le Cloud Azure

Afin de désactiver l'accès internet pour une machine virtuelle au niveau d'Azure, il suffit de bloquer les flux au niveau du composant Network Security Group (NSG) attaché à la carte réseau de la machine virtuelle.

1 – Se connecter au portail Azure : https://portal.azure.com/;

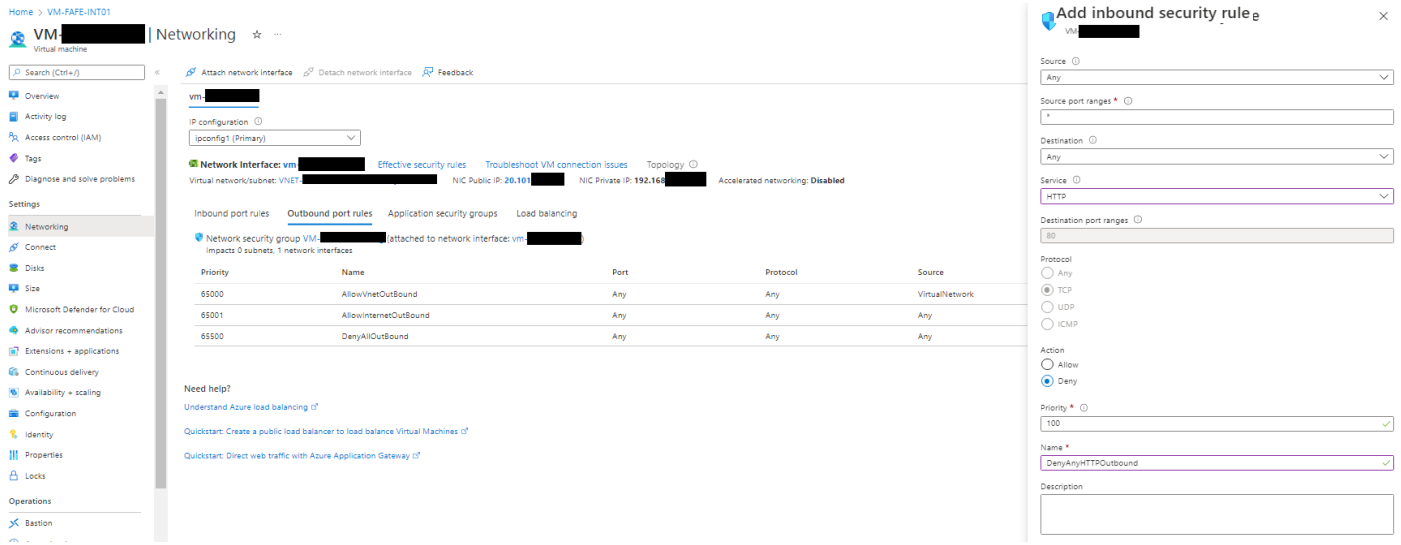
2 – Sélectionner une machine virtuelle;

3 – Au niveau du menu vertical présent à gauche choisir l'onglet Réseau (Networking);

4 – Choisir « Règles des ports entrant » (Inbound port rules), les différentes règles des flux en sorties sont affichées;

5 – Sélectionner « ajouter une nouvelle règle de sécurité » en renseignant les informations suivantes :

Source : Any **Source port ranges :** * **Destination :** Any **Service :** RDP **Protocol :** TCP **Action :** Deny **Priorité :** 102	**Source** : Any **Source port ranges :** * **Destination :** Any **Service :** SSH **Protocol :** TCP **Action :** Deny **Priorité :** 103



Bonnes pratiques pour renforcer la sécurité des VM

Surveillez et limitez la connectivité internet directe des machines virtuelles. Les attaquants analysent en permanence des plages IP de Cloud public pour détecter les ports de gestion ouverts et tentent des attaques « faciles » comme l'identification de mots de passe courants et des vulnérabilités non corrigées connues.

Le tableau suivant répertorie les meilleures pratiques contribuant à protéger les utilisateurs contre ces attaques :

Bonne pratique : empêcher une exposition involontaire du routage et de la sécurité du réseau.
Détail : utiliser **RBAC** pour garantir que seul le groupe central de mise en réseau possède l'autorisation d'accès aux ressources réseau.

Bonne pratique : identifier les machines virtuelles exposées qui autorisent l'accès à partir de « n'importe quelle » adresse IP source et y remédier.
Détail : utiliser les outils de défense (comme Microsoft Defender pour le Cloud). Defender pour le Cloud vous recommande de restreindre l'accès via des points de terminaison accessibles sur internet si l'un de vos groupes de sécurité réseau possède une ou plusieurs règles de trafic entrant autorisant l'accès à partir de « n'importe quelle » adresse IP source. Defender pour le Cloud vous recommande de modifier ces règles de trafic entrant, afin de restreindre l'accès aux adresses IP source qui en ont réellement besoin.

Bonne pratique : restreindre les ports de gestion (RDP, SSH).
Détail : L'accès juste-à-temps (JAT) aux machines virtuelles peut être utilisé pour verrouiller le trafic entrant vers vos machines virtuelles Azure, ce qui réduit l'exposition aux attaques et facilite la connexion aux machines virtuelles en cas de besoin. Lorsque l'accès JAT est activé, Defender pour le Cloud verrouille le trafic entrant vers vos machines virtuelles Azure en créant une règle de groupe de sécurité réseau. Vous sélectionnez les ports de la machine virtuelle pour lesquels le trafic entrant sera verrouillé. Ces ports sont contrôlés par la solution JAT.

CHAPITRE 1

Renforcer la sécurité des VM

1. Gestion des correctifs
2. Accès internet
3. Désactivation de l’accès RDP/SSH
4. **Bastion**

Principe du service Bastion

Un Bastion est un service PaaS que vous déployez et qui vous permet de vous connecter à une machine virtuelle à l'aide de votre navigateur et du portail du fournisseur.

Le service Bastion est un service PaaS complètement managé par la plateforme que vous provisionnez au sein de votre réseau virtuel. Il fournit une connectivité RDP/SSH sécurisée et fluide à vos machines virtuelles, directement à partir du portail du fournisseur Cloud via HTTP TLS.

Quand vous vous connectez via un Bastion, vos machines virtuelles n'ont pas besoin d'adresse IP publique, d'agent ou de logiciel client spécial.

Un Bastion fournit une connectivité RDP et SSH sécurisée à toutes les machines virtuelles du réseau virtuel dans lequel il est provisionné. Il protège donc vos machines virtuelles contre l'exposition des ports RDP/SSH au monde extérieur, tout en fournissant un accès sécurisé à l'aide de RDP/SSH.

Ci-dessous un exemple des différents services Bastion offerts par les fournisseurs Cloud :

Fournisseurs	AWS	Google Cloud	Azure
Service Bastion	AWS Bastion	Google Bastion	Azure Bastion

PARTIE 2

Architecture Azure Bastion

Azure Bastion est déployé sur un réseau virtuel et prend en charge l'appairage de réseaux virtuels. Plus précisément, Azure Bastion gère la connectivité RDP/SSH aux machines virtuelles créées dans les réseaux virtuels locaux ou homologués.

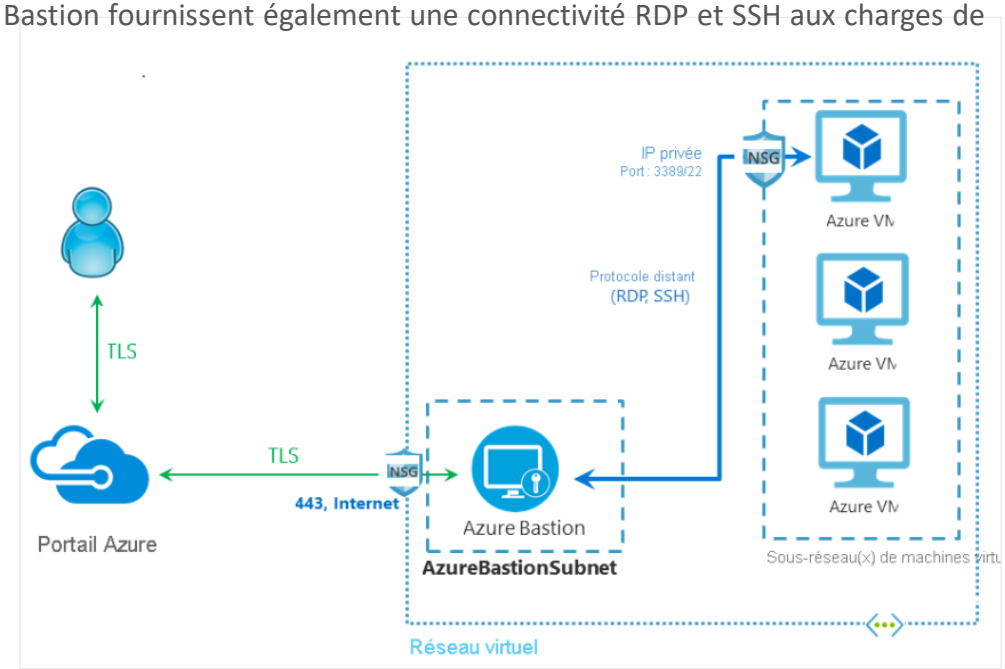
RDP et SSH font partie des moyens fondamentaux par lesquels vous pouvez vous connecter à vos charges de travail exécutées dans Azure.

L'exposition des ports RDP/SSH sur internet est déconseillée car considérée comme une surface de menace importante. Cela est surtout dû aux vulnérabilités du protocole. Pour contenir cette surface de menace, vous pouvez déployer des hôtes Bastion (également appelés serveurs de saut) du côté public de votre réseau périphérique.

Les serveurs hôte Bastion sont conçus et configurés pour faire face aux attaques. Les serveurs Bastion fournissent également une connectivité RDP et SSH aux charges de travail situées derrière le bastion, ainsi qu'à l'intérieur du réseau.

Cette figure représente l'architecture d'un déploiement Azure Bastion. Dans ce diagramme :

- L'hôte Bastion est déployé dans le réseau virtuel qui contient le sous-réseau AzureBastionSubnet avec un préfixe minimum /26.
- L'utilisateur se connecte au portail Azure à l'aide de n'importe quel navigateur HTML5.
- L'utilisateur sélectionne la machine virtuelle à laquelle se connecter.
- D'un simple clic, la session RDP/SSH s'ouvre dans le navigateur.
- Aucune adresse IP publique n'est requise sur la machine virtuelle Azure.



Source Microsoft

Principaux avantages

Avantage	Description
RDP et SSH par le biais du portail fournisseur Cloud	Vous pouvez accéder directement à la session RDP et SSH directement dans le portail du fournisseur Cloud via une expérience fluide en un seul clic.
Session à distance sur TLS et traversée de pare-feu pour RDP/SSH	Bastion utilise un client web basé sur HTML5 qui est automatiquement diffusé sur votre appareil local. Votre session RDP/SSH utilise TLS sur le port 443. Le trafic peut ainsi traverser les pare-feux de façon plus sécurisée.
Aucune adresse IP publique n'est nécessaire sur la machine virtuelle.	Bastion ouvre la connexion RDP/SSH à votre machine virtuelle en utilisant l'adresse IP privée sur votre machine virtuelle. Vous n'avez pas besoin d'une adresse IP publique sur votre machine virtuelle.
Aucune contrainte liée à la gestion des groupes de sécurité réseau	Vous n'avez pas besoin d'appliquer des groupes de sécurité réseau sur le sous-réseau Bastion. Comme le Bastion se connecte à vos machines virtuelles par le biais d'une adresse IP privée, vous pouvez configurer vos groupes de sécurité réseau pour autoriser RDP/SSH depuis Bastion uniquement. Vous n'avez plus à gérer les groupes de sécurité réseau à chaque fois que vous devez vous connecter de manière sécurisée à vos machines virtuelles.
Vous n'avez pas besoin de gérer un hôte Bastion distinct sur une machine virtuelle	Bastion est un service PaaS de plateforme entièrement géré par le fournisseur Cloud, renforcé en interne pour vous fournir une connectivité RDP/SSH sécurisée.
Protection contre l'analyse des ports	Vos machines virtuelles sont protégées contre l'analyse des ports par des utilisateurs malveillants, car vous n'avez pas besoin de les exposer à internet.
Renforcement de la sécurité à un seul endroit	Bastion résidant en périmètre de votre réseau virtuel, vous n'avez pas à vous soucier du durcissement de la sécurité de chacune des machines virtuelles de votre réseau virtuel.
Protection contre les exploits zero-day	Les fournisseurs Cloud protègent contre les attaques jour-zéro en assurant une sécurité durcie permanente et à jour pour le service Bastion.

Source Microsoft

Mise en place du service Bastion sur Azure

Nous allons procéder à la création du service Bastion à partir de la machine virtuelle disponible au niveau du Portail Azure. Ledit service sera déployé à l'aide des paramètres par défaut selon le réseau virtuel sur lequel se trouve la VM. Par la suite vous vous connecterez à votre machine virtuelle à l'aide de la connectivité RDP/SSH et l'adresse IP privée de la VM, ainsi l'adresse IP publique de la machine peut être supprimée ce qui permettra de renforcer le niveau de sécurité.

Prérequis :

Un compte Azure avec un abonnement actif.

Une machine virtuelle dans un réseau virtuel.

Lorsque vous déployez Bastion à l'aide des valeurs par défaut, les valeurs sont extraites du réseau virtuel dans lequel se trouve votre machine virtuelle. Cette machine virtuelle ne fait pas partie du déploiement Bastion proprement dit, mais vous vous y connecterez plus tard dans l'exercice.

- Si vous n'avez pas encore de machine virtuelle dans un réseau virtuel, créez-en une.
- Si vous disposez déjà d'un réseau virtuel, veillez à ce qu'il soit sélectionné sous l'onglet Réseau lors de la création de votre machine virtuelle.
- Si vous ne disposez pas d'un réseau virtuel, vous pouvez en créer un en même temps que votre machine virtuelle.

Droits sur la machine virtuelle nécessaires :

- Droit de lecteur sur la machine virtuelle.
- Droit de lecteur sur la carte réseau avec adresse IP privée de la machine virtuelle.

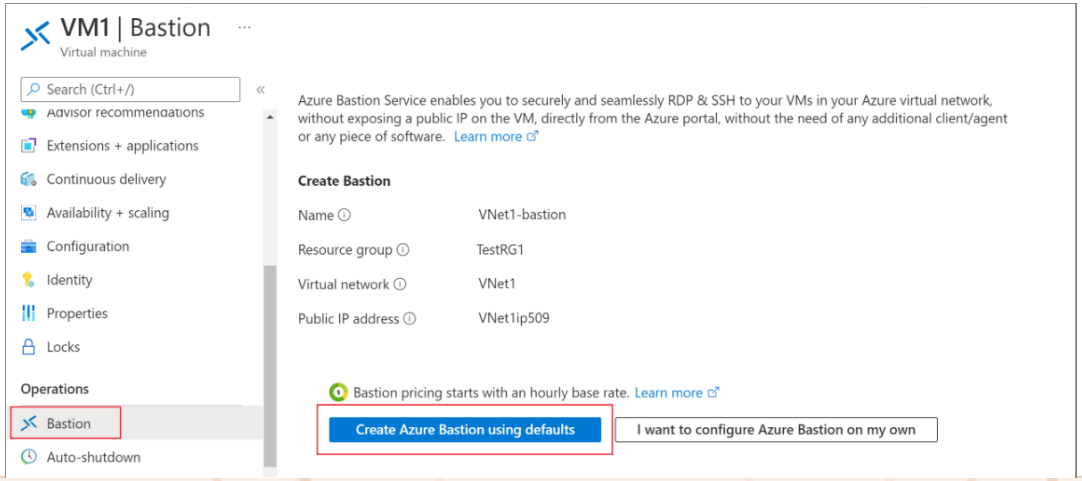
Ports d'entrée à ouvrir pour la machine virtuelle requis :

- Port RDP (3389) pour les machines virtuelles Windows.
- Port SSH (22) pour les machines virtuelles Linux.

Déployer Bastion sur Azure

Lorsque vous créez Azure Bastion à l'aide de paramètres par défaut, les paramètres sont configurés pour vous. Vous ne pouvez pas modifier ou spécifier des valeurs supplémentaires pour un déploiement par défaut.

1. Connectez-vous au portail Azure.
2. Sur le portail, accédez à la machine virtuelle à laquelle vous souhaitez vous connecter. Les valeurs du réseau virtuel dans lequel réside cette machine virtuelle seront utilisées pour créer le déploiement de Bastion.
3. Sur la page d'accueil de votre machine virtuelle, dans la section **Opérations** du menu de gauche, sélectionnez **Bastion**. Lorsque la page **Bastion** s'ouvre, elle vérifie si vous avez suffisamment d'espace d'adressage disponible pour créer AzureBastionSubnet. Si ce n'est pas le cas, les paramètres vous permettent d'ajouter davantage d'espace d'adressage à votre réseau virtuel pour répondre à cette exigence.
4. Sur la page **Bastion**, vous pouvez afficher certaines des valeurs qui seront utilisées lors de la création de l'hôte Bastion pour votre réseau virtuel. Sélectionnez **Créer Azure Bastion à l'aide de valeurs par défaut** pour déployer bastion à l'aide des paramètres par défaut.



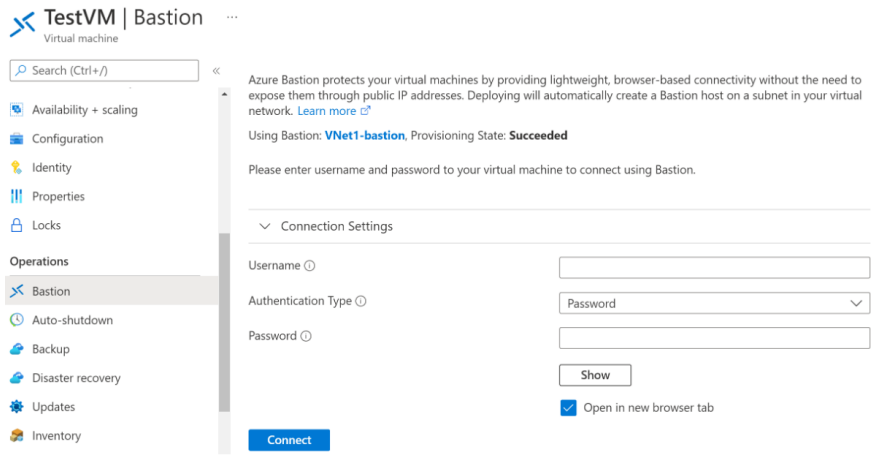
PARTIE 2

PARTIE 2

Se connecter à une machine virtuelle via Bastion

Une fois le déploiement de Bastion terminé, l'écran passe à la page **Connexion**.

1. Entrez vos informations d'authentification relatives à la VM, puis sélectionnez **Connect**.



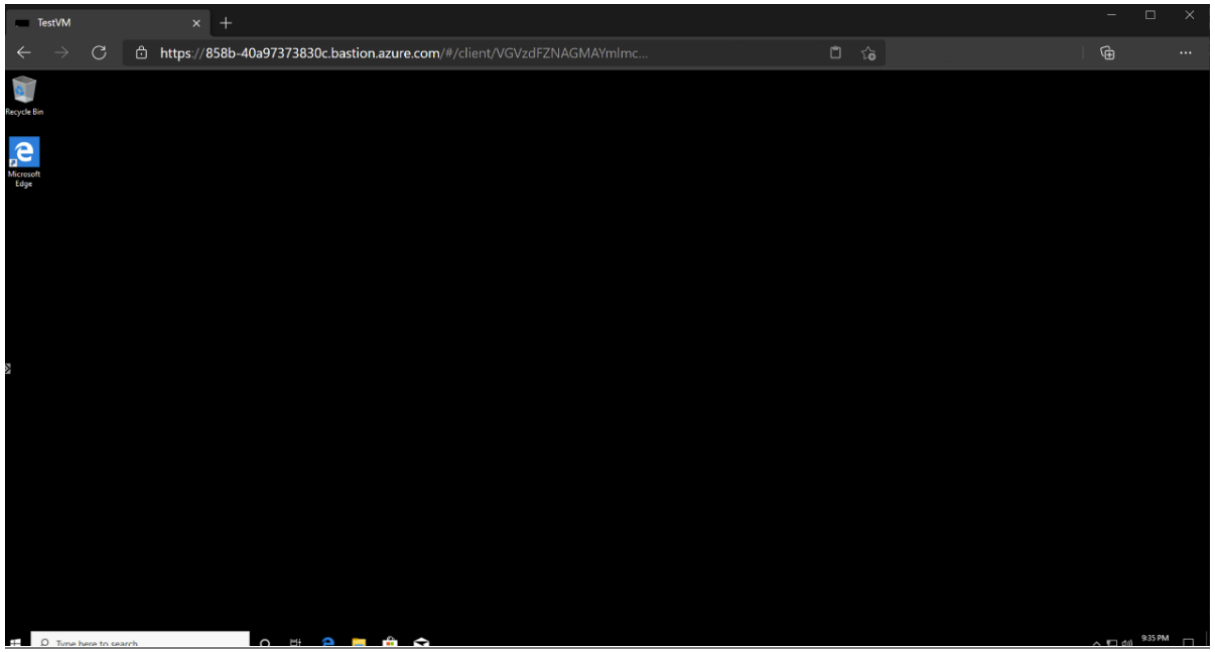
2. La connexion à cette machine virtuelle avec Bastion s'ouvrira directement dans le portail Azure (en HTML5) via le port 443 et le service Bastion.
   Sélectionnez Autoriser quand vous êtes invité à entrer des autorisations sur le Presse-papiers. Cela vous permet d'utiliser les flèches du Presse-papiers à distance sur la gauche de l'écran.

Se connecter à une machine virtuelle via Bastion

Lorsque vous vous connectez, le bureau de la machine virtuelle peut être différent de celui présenté dans la capture d'écran.

L'utilisation de touches de raccourcis lorsque vous êtes connecté à une machine virtuelle peut ne pas s'accompagner du même comportement que les touches de raccourcis sur un ordinateur local.

Par exemple, lorsque vous êtes connecté à une machine virtuelle Windows à partir d'un client Windows, CTRL+ALT+FIN est le raccourci clavier pour CTRL+ALT+SUPPR sur un ordinateur local. Pour effectuer cette opération depuis un Mac alors que vous êtes connecté à une machine virtuelle Windows, le raccourci clavier est Fn+CTRL+ALT+Retour arrière.

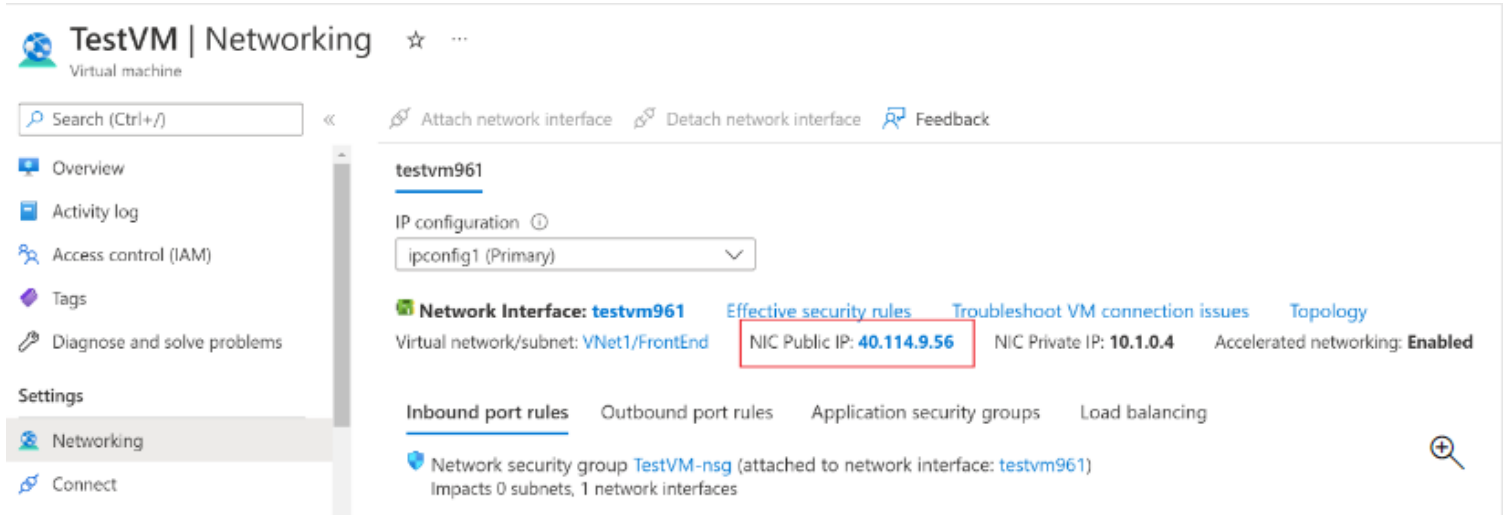


PARTIE 2

Supprimer une adresse IP publique de machine virtuelle

Quand vous vous connectez à une machine virtuelle à l'aide d'Azure Bastion, vous n'avez pas besoin d'une adresse IP publique pour votre machine virtuelle. Si vous n'utilisez pas l'adresse IP publique pour autre chose, vous pouvez la dissocier de votre VM. Pour dissocier une adresse IP publique de votre VM, procédez comme suit :

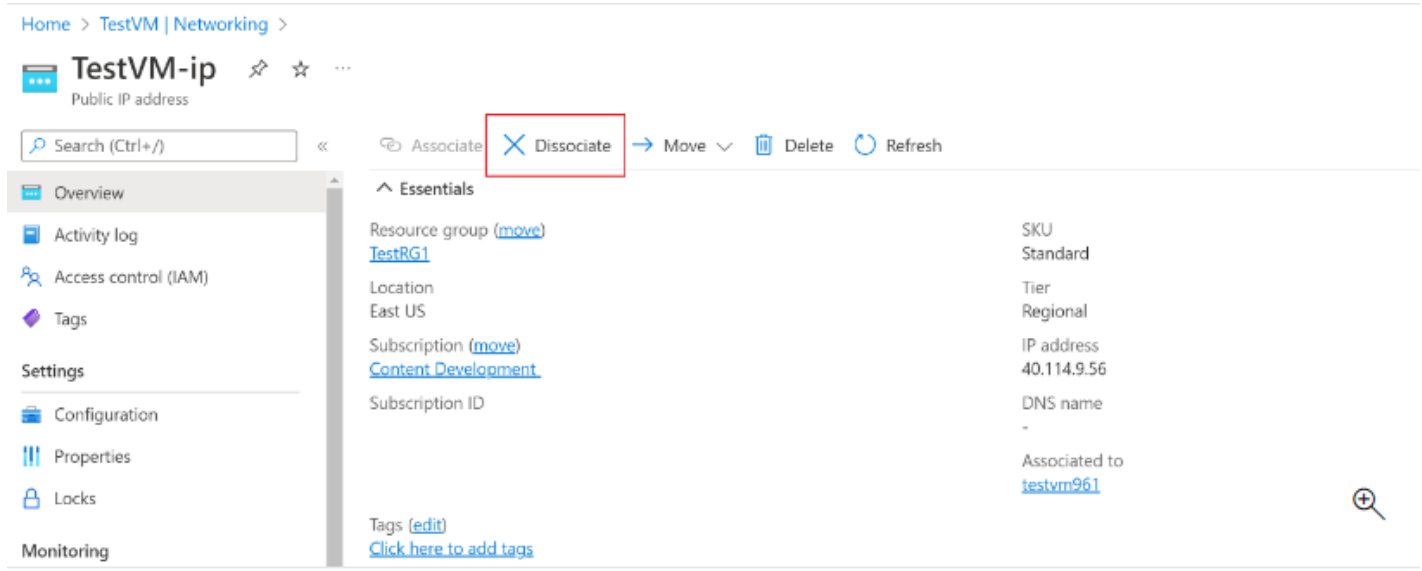
1. Accédez à votre machine virtuelle et sélectionnez **Réseau**. Cliquez sur l'**IP publique de la NIC** pour ouvrir la page de l'adresse IP publique.



PARTIE 2

Supprimer une adresse IP publique de machine virtuelle

2. Dans la page **d'adresse IP publique** , vous pouvez voir l'interface réseau de machine virtuelle répertoriée sous **Associée à** dans la partie inférieure droite de la page. Cliquez sur **Dissocier** en haut de la page.



2. Cliquez sur **Oui** pour dissocier l'adresse IP de l'interface réseau. Une fois l'adresse IP publique dissociée de l'interface réseau de la machine virtuelle, vous pouvez voir qu'elle n'est plus répertoriée sous **Associée à**.
3. Après avoir dissocié l'adresse IP, vous pouvez supprimer la ressource de l'adresse IP publique. Dans la page **Adresse IP publique** de la machine virtuelle, sélectionnez **Supprimer**.

CHAPITRE 2

Sécuriser le réseau

Ce que vous allez apprendre dans ce chapitre :

- Segmentation réseau
- Pare-feu
- Systèmes de détection des intrusions et de déni de service DDOS
- VPN

10 heures

CHAPITRE 2

Sécuriser le réseau

1. **Segmentation réseau**
2. Pare-feu
3. Systèmes de détection des intrusions et de déni de service DDOS
4. VPN

Définition de la segmentation réseau Azure

La segmentation réseau c'est la création des périmètres définis par logiciels dans l'empreinte réseau d'une entreprise à l'aide des différents services et fonctionnalités Azure. Lorsqu'une charge de travail, ou certaines parties d'une charge de travail, sont réparties sur plusieurs segments, on peut contrôler le trafic qui rentre et sort de ces segments en vue de sécuriser les chemins de communication. Si un segment est compromis, il sera alors plus facile de réduire l'impact de l'attaque et d'empêcher celle-ci de se répandre latéralement dans le reste de du réseau. Cette stratégie s'aligne sur le principe clé du modèle Confiance Zéro publié par Microsoft, qui vise à fournir une sécurité optimale pour l'entreprise.

Fonctionnalités de segmentation Azure

Lorsqu'on travaille dans Azure, on dispose de nombreuses options de segmentation.

Subscription	Virtual Network	Network Security Group	Application Security Group	Azure Firewall
Une isolation logique de l'environnement pour l'ensemble des ressources	**Un environnement isolé et hautement sécurisé pour exécuter les VMs et les applications**	**Renforcement et contrôle des règles de sécurité du trafic réseau qui autorisent ou empêchent le trafic entrant/sortant**	**Définir des politiques de sécurité du réseau jusqu'un niveau granulaire basée sur la charge du travail, et centralisées sur les applications**	**Renforcement et création des politiques de connectivité en utilisant les règles de filtrage du réseau par niveau**

PARTIE 2

Fonctionnalités de segmentation Azure (suite)

1- Abonnement: construction de haut niveau qui fournit une séparation des entités reposant sur une plateforme. Celle-ci est destinée à définir les limites entre les grandes organisations d'une entreprise. En outre, la communication entre les ressources de différents abonnements doit être explicitement provisionnée.

2- Réseau virtuel: créé au sein d'un abonnement dans des espaces d'adressage privés. Il fournit aux ressources une autonomie au niveau du réseau. Par défaut, aucun trafic n'est autorisé entre deux réseaux virtuels. Comme les abonnements, toute communication entre les réseaux virtuels doit être approvisionnée de manière explicite.

3- Groupes de sécurité réseau (NSG): mécanismes de contrôle d'accès permettant de contrôler le trafic entre les ressources au sein d'un réseau virtuel, et également avec les réseaux externes, comme internet, d'autres réseaux virtuels, etc. Les groupes de sécurité réseau permettent une stratégie de segmentation précise, grâce à la création de périmètres pour un sous-réseau, une machine virtuelle ou un groupe de machines virtuelles.

4- Groupes de sécurité d'application (ASG) : similaires aux groupes de sécurité réseau, mais référencés avec un contexte d'application. Cela permet de regrouper un ensemble de machines virtuelles sous une balise d'application et de définir des règles de trafic qui sont ensuite appliquées à chacune des machines virtuelles sous-jacentes.

5- Pare-feu Azure: pare-feu natif Cloud avec état fourni en tant que service, qui peut être déployé dans un réseau virtuel ou dans des déploiements de hubs Azure Virtual WAN pour le filtrage du trafic entre les ressources Cloud, internet et locales. On crée 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 à l'aide des contrôles des couches 3 à 7. On peut également filtrer le trafic vers internet en utilisant à la fois le pare-feu Azure et des tiers, en dirigeant tout ou partie du trafic via des fournisseurs de sécurité tiers pour le filtrage avancé et la protection des utilisateurs.

Modèles de segmentation

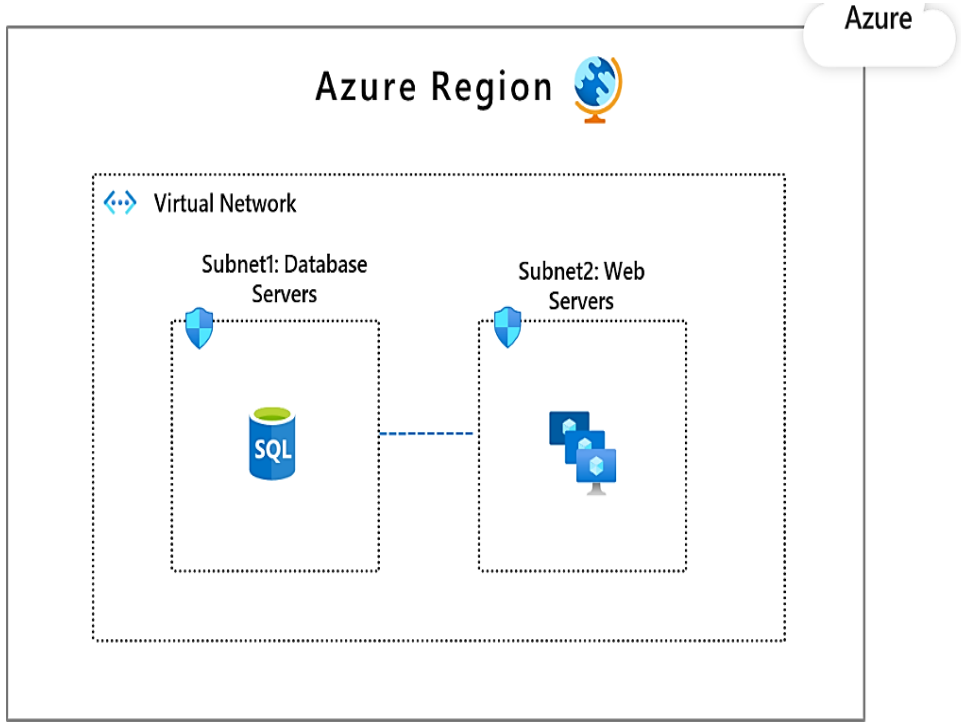
Dans cette partie on va présenter quelques modèles courants permettant de segmenter une charge de travail dans Azure. Chaque modèle fournit un type d'isolation et de connectivité différent. Une organisation doit choisir un modèle répondant à ses besoins :

Modèle 1 : Réseau virtuel unique

Tous les composants de la charge de travail se trouvent dans un même réseau virtuel. Ce modèle convient si on exerce dans une seule région, car un réseau virtuel ne peut pas s'étendre sur plusieurs régions.

Les méthodes courantes permettant de sécuriser des segments, comme des sous-réseaux ou des groupes d'applications, consistent à utiliser des groupes de sécurité réseau et des groupes de sécurité d'application. On peut également utiliser une appliance virtuelle réseau issue de la marketplace Azure ou du pare-feu Azure, afin d'appliquer et de sécuriser cette segmentation.

Dans l'image ci-après, Subnet1 comprend la charge de travail de la base de données. Subnet2 comprend les charges de travail web. On peut configurer des groupes de sécurité réseau qui autorisent Subnet1 à communiquer uniquement avec Subnet2, et Subnet2 à ne communiquer qu'avec internet.



Prenons l'exemple d'un cas d'usage impliquant plusieurs charges de travail placées dans des sous-réseaux distincts. On peut placer des contrôles qui permettront à une charge de travail de communiquer avec le back-end d'une autre charge de travail.

PARTIE 2

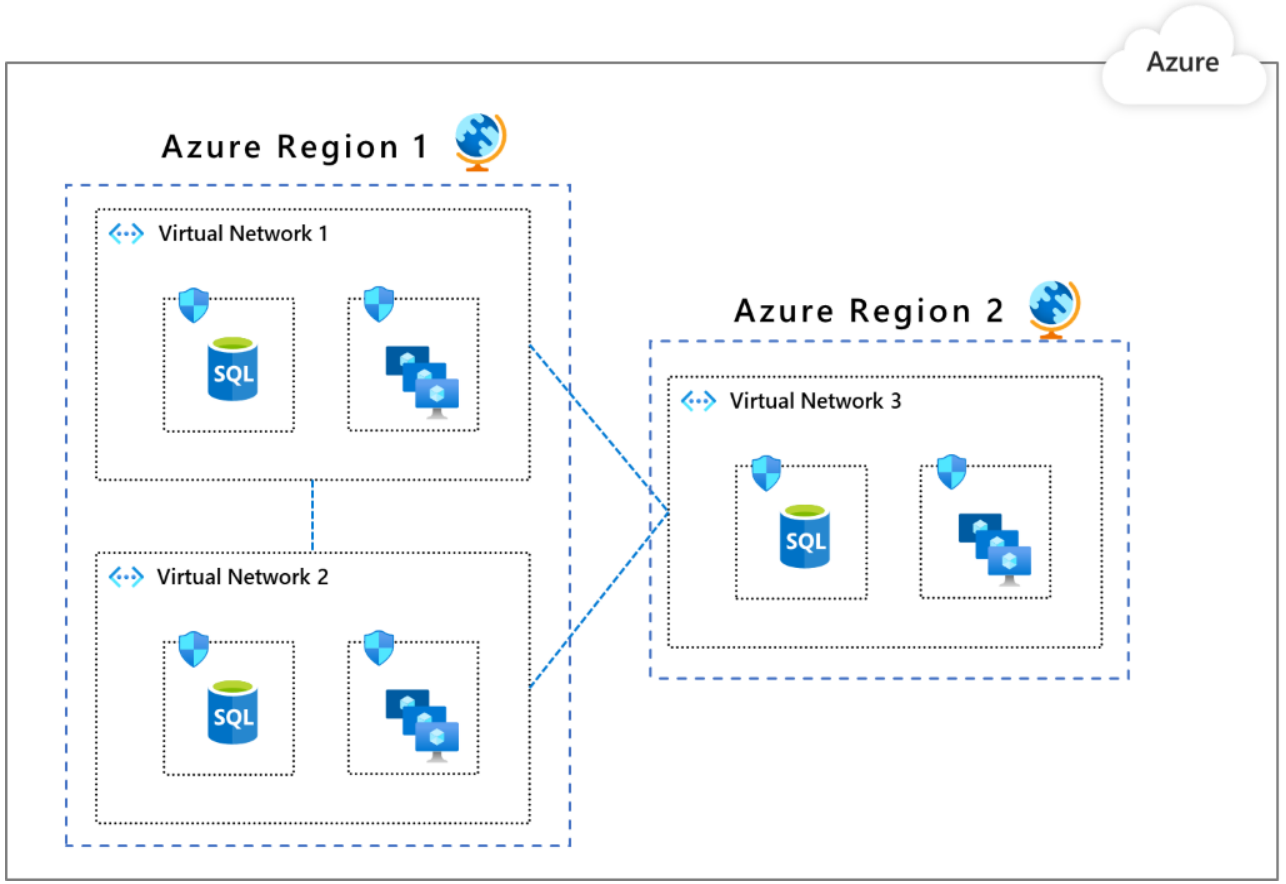
Modèles de segmentation (suite)

Modèle 2: Plusieurs réseaux virtuels qui communiquent par le biais d'un peering

Les ressources sont réparties ou répliquées sur plusieurs réseaux virtuels. Les réseaux virtuels peuvent communiquer par le biais d'un peering.

Ce modèle convient si on doit regrouper des applications dans des réseaux virtuels séparés, ou si on a besoin de plusieurs régions Azure.

L'un des avantages de ce modèle est la segmentation intégrée, car on doit appairer explicitement un réseau virtuel avec un autre. Le peering de réseaux virtuels n'est pas transitif. On peut effectuer une segmentation supplémentaire à l'intérieur d'un réseau virtuel en utilisant des groupes de sécurité réseau et des groupes de sécurité d'application, comme indiqué dans le modèle 1.



Modèles de segmentation (suite)

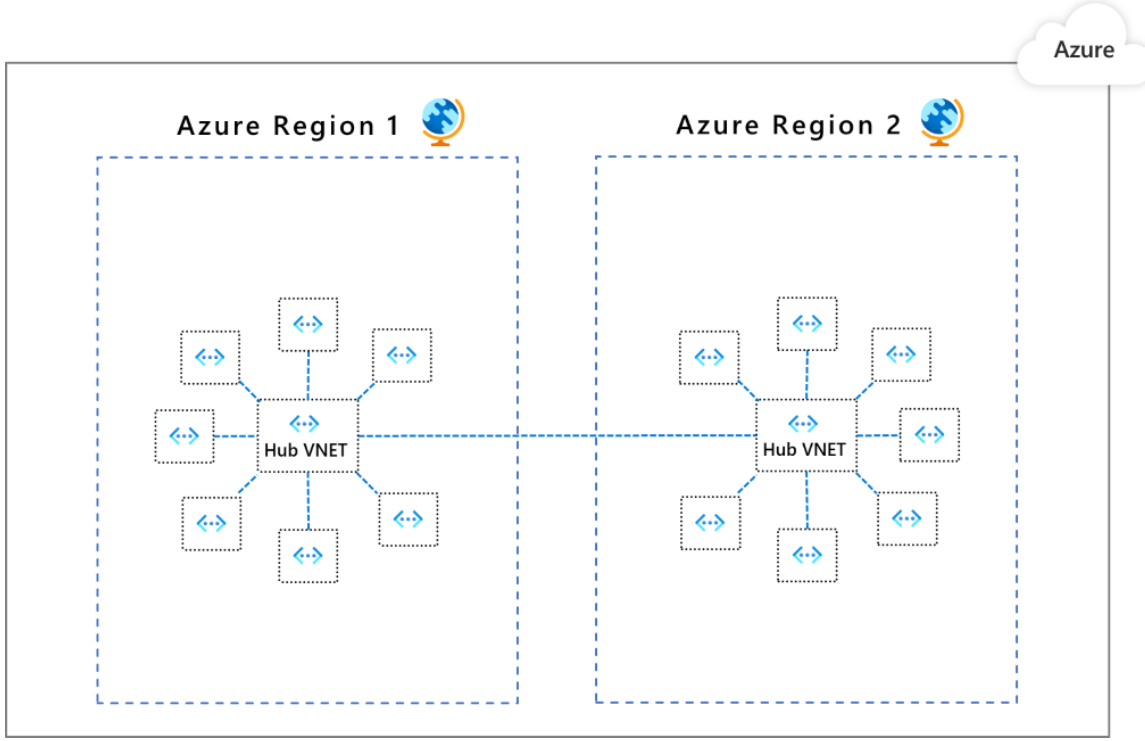
Modèle 3 : Plusieurs réseaux virtuels dans un modèle hub-and-spoke

Un réseau virtuel est désigné comme hub dans une région donnée pour tous les autres réseaux virtuels qui sont désignés comme des spokes dans cette même région. Le hub et ses spokes sont connectés par le biais d'un peering. Tout le trafic transite par le hub et peut servir de passerelle pour les hubs d'autres régions. Dans ce modèle, les contrôles de sécurité sont configurés au niveau des hubs afin de pouvoir segmenter et contrôler le trafic entre les autres réseaux virtuels de façon scalable.

L'un des avantages de ce modèle est que, lorsque la topologie de réseau d'une entreprise s'étend, les frais liés à la posture de sécurité n'augmentent pas (sauf lorsque cette entreprise effectue une extension vers de nouvelles régions).

L'option native recommandée est le pare-feu Azure. Cette option fonctionne à la fois sur les réseaux virtuels et sur les abonnements et a pour but de régir les flux de trafic à l'aide des contrôles des couches 3 à 7. On peut définir les règles de communication et les appliquer de manière cohérente. Voici quelques exemples :

- Le réseau virtuel 1 ne peut pas communiquer avec le réseau virtuel 2, mais il peut communiquer avec le réseau virtuel 3.
- Le réseau virtuel 1 ne peut pas accéder à l'internet public, sauf à « *.github.com ».



PARTIE 2

Comparaison entre les 3 modèles de segmentation réseau Azure

Considérations	Modèle 1	Modèle 2	Modèle 3
Connectivité/Routage : comment chacun des segments communique avec les autres	Le routage système fournit une connectivité par défaut à n'importe quelle charge de travail d'un sous-réseau.	Identique au modèle 1.	Aucune connectivité par défaut entre les réseaux spokes. Pour permettre la connectivité, le hub doit comprendre un routeur de couche 3, comme le pare-feu Azure.
Filtrage du trafic au niveau du réseau	Le trafic est autorisé par défaut. On utilise des groupes de sécurité réseau et des groupes de sécurité d'application pour filtrer le trafic.	Identique au modèle 1.	Le trafic entre les réseaux virtuels spokes est refusé par défaut. Ouvrir les chemins sélectionnés pour autoriser le trafic via la configuration du pare-feu Azure.
Journalisation centralisée	Journaux des groupes de sécurité réseau et des groupes de sécurité d'application pour le réseau virtuel.	Agréger les journaux des groupes de sécurité réseau et des groupes de sécurité d'application de tous les réseaux virtuels.	Le pare-feu Azure journalise tout le trafic accepté ou refusé qui est envoyé au hub. Afficher les journaux dans Azure Monitor.
Points de terminaison publics ouverts involontaires	DevOps peut ouvrir accidentellement un point de terminaison public par le biais de règles NSG/ASG incorrectes.	Identique au modèle 1.	Un point de terminaison public ouvert accidentellement dans un spoke ne permettra pas l'accès, car le paquet de retour sera supprimé via un pare-feu avec état (routage asymétrique).
Protection au niveau de l'application	Les groupes de sécurité réseau et les groupes de sécurité d'application fournissent uniquement la prise en charge de la couche réseau.	Identique au modèle 1.	Le pare-feu Azure prend en charge le filtrage de nom de domaine complet pour HTTP/S et MSSQL pour le trafic sortant et entre les réseaux virtuels.

CHAPITRE 2

Sécuriser le réseau

1. Segmentation réseau
2. **Pare-feu**
3. Systèmes de détection des intrusions et de déni de service DDOS
4. VPN

Définition générale d'un pare-feu

Un pare-feu est une fonctionnalité de sécurité réseau qui se situe entre un réseau approuvé et un réseau non approuvé, comme Internet. Le travail du pare-feu consiste à analyser tout le trafic réseau entrant et sortant. Sur la base de cette analyse, le pare-feu autorise le trafic à passer ou refuse. Dans l'idéal, le pare-feu autorise tout le trafic légitime tout en refusant le trafic malveillant, comme les programmes malveillants et les tentatives d'intrusion.

Par défaut, la plupart des pare-feu refusent tout le trafic entrant et sortant. Lorsqu'un pare-feu analyse le trafic réseau, il vérifie que certaines conditions sont remplies avant d'autoriser le trafic à passer. Ces conditions peuvent être une adresse IP, un nom de domaine complet, un port réseau, un protocole réseau ou n'importe quelle combinaison.

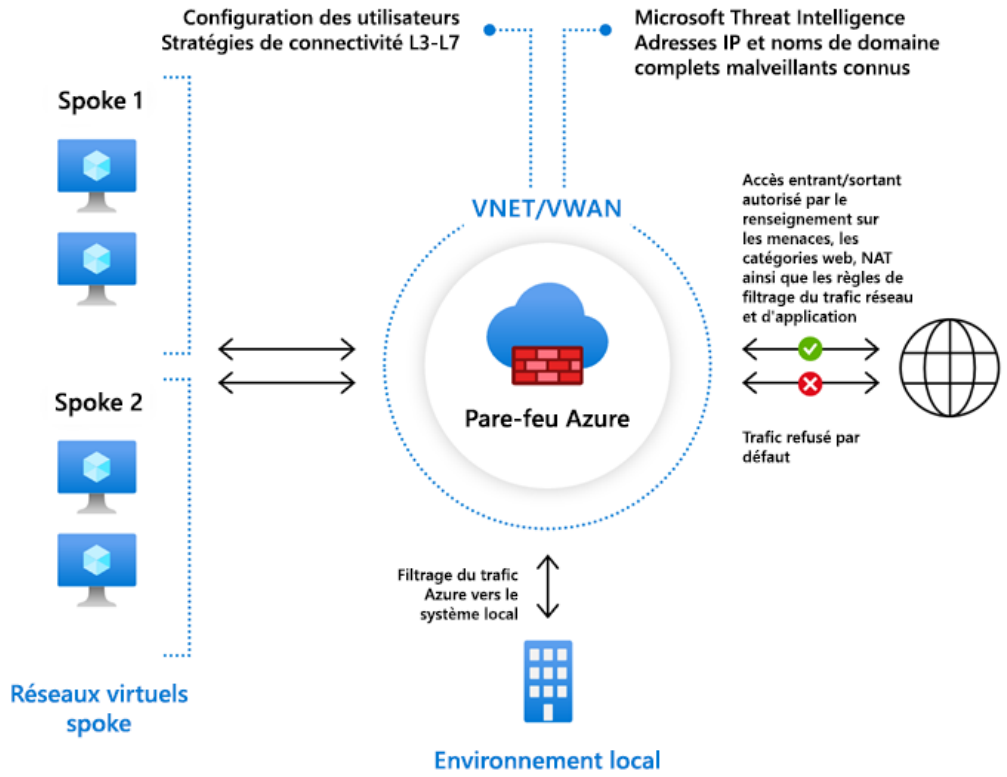
Ensemble, ces conditions définissent une règle de pare-feu. Un pare-feu peut avoir une seule règle, mais la plupart des pare-feux sont configurés avec de nombreuses règles. Seul le trafic réseau qui répond aux conditions des règles du pare-feu est autorisé à passer.

Certains pare-feux sont basés sur le matériel et résident dans des appareils qui sont conçus pour faire office de pare-feu. D'autres sont des logiciels qui s'exécutent sur des appareils informatiques à usage général.

Définition du pare-feu Azure

Le pare-feu Azure est un service de pare-feu basé sur le Cloud. Dans la plupart des configurations, le Pare-feu Azure est provisionné dans un réseau virtuel Hub. Le trafic vers, et depuis, les réseaux virtuels Spoke et le réseau local traverse le pare-feu avec le réseau Hub.

Tout le trafic vers et depuis internet est refusé par défaut. Le trafic est autorisé uniquement s'il passe divers tests, tels que les règles de pare-feu configurées.



PARTIE 2

Types de pare-feu Azure

Le Pare-feu Azure est proposé en deux références SKU : **Standard** et **Premium**.

- **Pare-feu Azure standard:**

Le Pare-feu Azure standard fournit un filtrage L3-L7 et des flux de renseignement sur les menaces directement à partir de la Cybersécurité Microsoft. Le filtrage basé sur le renseignement sur les menaces peut émettre des alertes et refuser le trafic provenant, ou à destination, d'adresses IP et de domaines malveillants connus, qui sont mis à jour en temps réel pour offrir une protection contre les attaques nouvelles et émergentes.

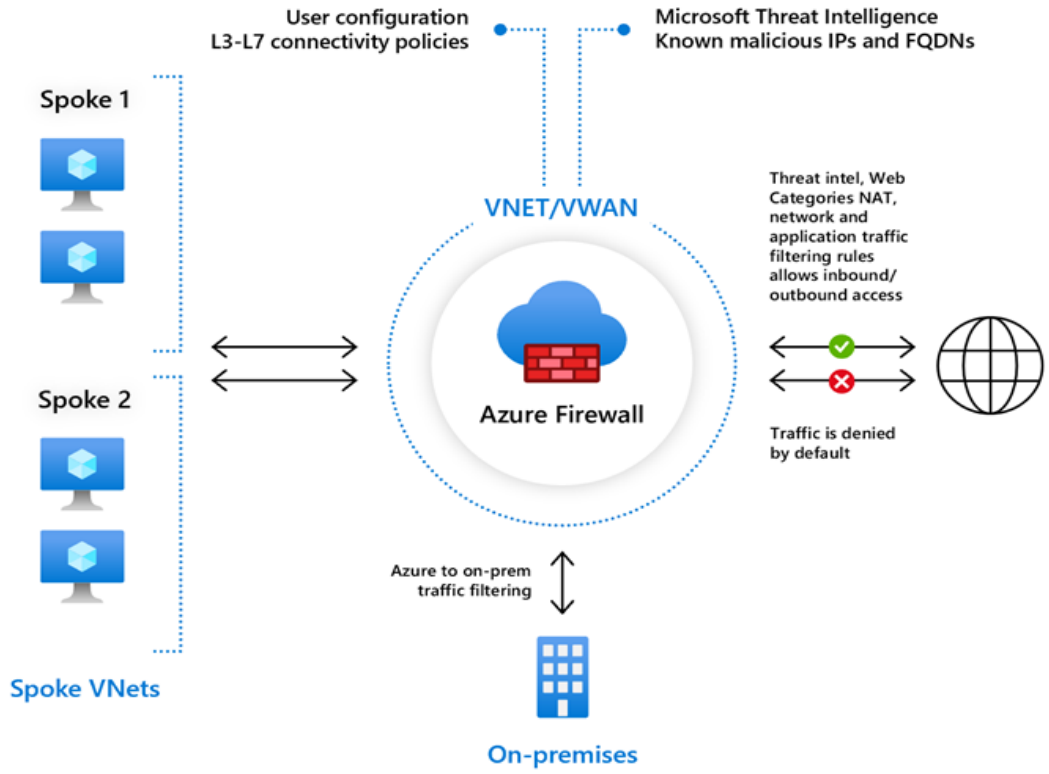
Le pare-feu Azure standard inclut les fonctionnalités suivantes :

- **Haute disponibilité intégrée:**

Comme la haute disponibilité est intégrée, aucun équilibreur de charge supplémentaire n'est nécessaire, et rien n'est à configurer.

- **Zones de disponibilité:**

Le pare-feu Azure peut être configuré pendant le déploiement pour couvrir plusieurs zones de disponibilité afin de fournir une disponibilité supérieure.



PARTIE 2

Pare-feu Azure standard

Avec les zones de disponibilité Azure, la disponibilité s'élève à 99,99 % du temps total. Un contrat de niveau de service de 99,99 % est offert quand deux zones de disponibilité ou plus sont sélectionnées.

On peut également associer le pare-feu Azure à une zone spécifique uniquement pour des raisons de proximité, en utilisant le contrat de niveau de service standard garantissant un taux de disponibilité de 99,95 %.

Il n'existe aucun coût supplémentaire pour un pare-feu déployé dans plusieurs zones de disponibilité. Par contre, il existe des coûts supplémentaires pour les transferts de données entrants et sortants associés aux zones de disponibilité Azure.

Les zones de disponibilité du pare-feu Azure sont disponibles dans les régions prenant en charge les zones de disponibilité.

- **Extensibilité du Cloud sans limites :**

On peut effectuer un scale-out au niveau du service pare-feu Azure en fonction des ses besoins pour prendre en charge des flux de trafic réseau changeants. On n'a donc pas besoin de budgéter son trafic de pointe.

- **Règles de filtrage des noms de domaine complets de l'application :**

On peut limiter le trafic HTTP/S sortant ou le trafic SQL Azure vers une liste spécifiée de noms de domaine complets (FQDN), y compris des caractères génériques. Cette fonctionnalité ne nécessite pas d'arrêt TLS.

Pare-feu Azure standard

- **Règles de filtrage du trafic réseau:**

On peut créer de façon centralisée des règles de filtrage réseau, autoriser ou refuser par protocole, port et adresse IP source et de destination. Le service pare-feu Azure étant entièrement avec état, il peut distinguer les paquets légitimes pour différents types de connexions. Les règles sont appliquées et consignées entre plusieurs abonnements et réseaux virtuels.

Le Pare-feu Azure prend en charge le filtrage avec état des protocoles réseau de couche 3 et de couche 4. Les protocoles IP de couche 3 peuvent être filtrés en sélectionnant n'importe quel protocole dans la règle réseau et en sélectionnant le caractère générique * pour le port.

- **Balises FQDN:**

Les balises FQDN aident à autoriser le trafic réseau du service Azure connu via le pare-feu. Par exemple, supposons que l'on souhaite autoriser le trafic réseau Windows Update via le pare-feu. On crée une règle d'application et on inclut la balise Windows Update. Le trafic réseau provenant de Windows Update peut désormais passer par le pare-feu.

- **Balises de service:**

Une balise de service représente un groupe de préfixes d'adresses IP qui permet de simplifier la création de règles de sécurité. On ne peut pas créer sa propre balise de service, ni spécifier les adresses IP incluses dans une balise. Microsoft gère les préfixes d'adresse englobés par la balise de service et met à jour automatiquement la balise de service quand les adresses changent.

Pare-feu Azure standard

- **Informations sur les menaces :**

Le filtrage basé sur Threat Intelligence peut être activé pour le pare-feu, afin de donner l'alerte et rejeter le trafic depuis ou vers des adresses IP et des domaines malveillants connus. Ces adresses IP et domaines proviennent du flux Microsoft Threat Intelligence.

- **Proxy DNS :**

Si le proxy DNS est activé, le pare-feu Azure peut traiter les requêtes DNS d'un ou plusieurs réseaux virtuels et les transférer vers le serveur DNS de son choix. Cette fonctionnalité essentielle est nécessaire pour disposer d'un filtrage de FQDN fiable dans les règles de réseau. On peut activer le proxy DNS dans les paramètres du pare-feu Azure et de la stratégie de pare-feu.

- **Système DNS personnalisé :**

Le système DNS personnalisé permet de configurer le pare-feu Azure pour qu'il utilise le serveur DNS d'une entreprise, tout en veillant à ce que les dépendances sortantes du pare-feu soient toujours résolues avec Azure DNS. On peut configurer un serveur DNS individuel ou plusieurs serveurs dans les paramètres DNS du pare-feu Azure et de la stratégie de pare-feu.

Le pare-feu Azure peut également résoudre les noms à l'aide du DNS privé Azure. Le réseau virtuel sur lequel réside le pare-feu Azure doit être lié à la zone privée Azure.

Pare-feu Azure standard

- **FQDN dans les règles de réseau :**

On peut utiliser des noms de domaine complets (FQDN) dans les règles de réseau basées sur la résolution DNS dans le pare-feu Azure et la stratégie de pare-feu.

Les FQDN spécifiés dans les regroupements de règles sont traduits en adresses IP en fonction des paramètres DNS du pare-feu. Cette fonctionnalité permet de filtrer le trafic sortant en utilisant des FQDN avec n'importe quel protocole TCP/UDP (y compris NTP, SSH, RDP, etc.). Étant donné que cette fonctionnalité est basée sur la résolution DNS, il est fortement recommandé d'activer le proxy DNS pour garantir la cohérence de la résolution de noms avec des machines virtuelles protégées et le pare-feu.

- **Déploiement sans adresse IP publique en mode tunneling forcé :**

Le service pare-feu Azure requiert une adresse IP publique à des fins opérationnelles. Bien qu'ils soient sécurisés, certains déploiements préfèrent ne pas exposer une adresse IP publique directement à internet.

Dans ce cas, on peut déployer le pare-feu Azure en mode tunneling forcé. Cette configuration crée une carte réseau de gestion qui est utilisée par le pare-feu Azure pour ses opérations. Le réseau Tenant Datapath peut être configuré sans adresse IP publique, et le trafic internet peut être transféré en mode tunneling forcé vers un autre pare-feu ou être complètement bloqué.

Le mode de tunneling forcé ne peut pas être configuré au moment de l'exécution. On peut soit redéployer le pare-feu, soit utiliser la fonctionnalité d'arrêt et de démarrage pour reconfigurer un pare-feu Azure existant en mode tunneling forcé. Les pare-feux déployés dans les hubs sécurisés sont toujours déployés en mode de tunneling forcé.

Pare-feu Azure standard

- **Prise en charge du mode SNAT sortant :**

Toutes les adresses IP du trafic réseau virtuel sortant sont traduites en adresse IP publique du pare-feu Azure (Source Network Address Translation). On peut identifier et autoriser le trafic entre le réseau virtuel de l'entreprise et des destinations internet distantes.

Si l'entreprise utilise une plage d'adresses IP publiques pour les réseaux privés, le pare-feu Azure traduit l'adresse réseau source du trafic en une des adresses IP privées du pare-feu dans AzureFirewallSubnet. On peut configurer le pare-feu Azure pour qu'il n'effectue pas une telle traduction.

- **Prise en charge du trafic DNAT entrant :**

Le trafic internet entrant vers l'adresse IP publique du pare-feu de l'entreprise est traduit (Destination Network Address Translation ou DNAT) et filtré selon les adresses IP privées sur les réseaux virtuels de l'entreprise.

- **Journalisation d'Azure Monitor :**

Tous les événements sont intégrés à Azure Monitor, ce qui permet d'archiver les journaux d'activité dans un compte de stockage, de transmettre en continu des événements au hub d'événements ou de les envoyer à des journaux d'activité Azure Monitor.

Pare-feu Azure standard

- **Adresses IP publiques multiples :**

On peut associer plusieurs adresses IP publiques (jusqu'à 250) au pare-feu d'une organisation.

Cela donne accès aux scénarios suivants :

- **DNAT** : on peut traduire plusieurs instances de ports standards vers des serveurs principaux. Par exemple, si on a deux adresses IP publiques, on peut traduire le port TCP 3389 (RDP) pour ces deux adresses IP.
- **SNAT** : des ports supplémentaires sont disponibles pour les connexions SNAT sortantes, réduisant ainsi le risque de pénurie de ports SNAT. À ce stade, le pare-feu Azure sélectionne aléatoirement l'adresse IP publique source à utiliser pour une connexion. Si le réseau est doté d'un filtrage en aval, on doit autoriser toutes les adresses IP publiques associées au pare-feu. Envisagez d'utiliser un préfixe d'adresse IP publique pour simplifier cette configuration.

- **Tunneling forcé :**

On peut configurer le pare-feu Azure pour router tout le trafic internet vers un tronçon suivant désigné au lieu d'accéder directement à internet. Par exemple, on peut disposer d'un pare-feu de périphérie local ou d'une autre appliance virtuelle réseau (NVA) pour traiter le trafic réseau avant qu'il ne soit dirigé vers internet.

- **Certifications :**

Le service pare-feu Azure est conforme aux normes PCI (Payment Card Industry), SOC (Service Organization Controls), ISO (Organisation Internationale de Normalisation) et ICSA Labs.

Pare-feu Azure standard

- **Catégories web :**

Les catégories web permettent aux administrateurs d'autoriser ou de refuser aux utilisateurs l'accès aux catégories de sites web telles que les sites web de jeux d'argent, les sites web de réseaux sociaux, etc. Les catégories web sont incluses dans le pare-feu Azure Standard, mais elles sont plus précises dans le pare-feu Azure Premium. Contrairement à la fonctionnalité de catégories web de la référence SKU Standard, qui correspond à la catégorie basée sur un nom de domaine complet, la référence SKU Premium correspond à la catégorie en fonction de l'URL complète pour le trafic HTTP et HTTPS.

Par exemple, si le pare-feu Azure intercepte une demande HTTPS pour www.google.com/news, la catégorisation suivante est attendue :

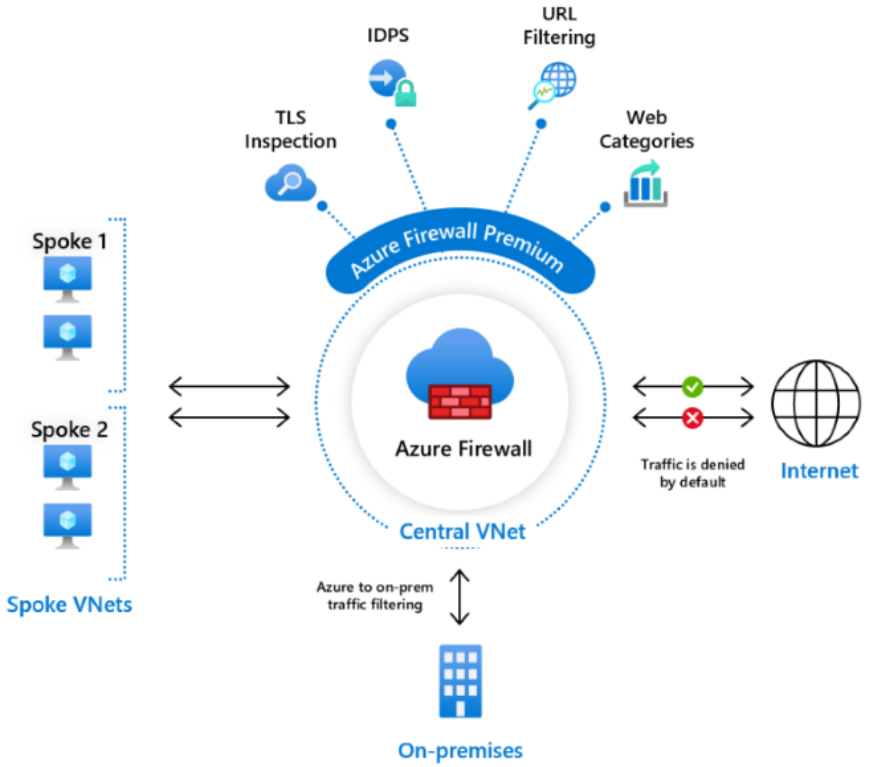
- Pare-feu Standard : seule la partie du nom de domaine complet étant examinée, www.google.com est classé en tant que Moteur de recherche.
- Pare-feu Premium : l'URL complète étant examinée, www.google.com/news est classée en tant qu'Actualités.

Les catégories sont organisées en fonction de leur gravité sous **Responsabilité**, **Bande passante élevée**, **Utilisation métier**, **Perte de productivité**, **Navigation générale** et **Sans catégorie**.

Types de pare-feu Azure

- **Pare-feu Azure premium:**

Le pare-feu Azure Premium propose des fonctionnalités avancées incluant un système IDPS basé sur les signatures pour permettre une détection rapide des attaques en recherchant des modèles spécifiques. Ces modèles peuvent inclure des séquences d'octets dans le trafic réseau ou des séquences d'instructions malveillantes connues utilisées par un programme malveillant. Il existe plus de 58 000 signatures dans plus de 50 catégories, qui sont mises à jour en temps réel pour offrir une protection contre les codes malveillants nouveaux et émergents exploitant une faille de sécurité. Les catégories de codes malveillants exploitant une faille de sécurité incluent les programmes malveillants, le hameçonnage, le minage de monnaie et les chevaux de Troie.



PARTIE 2

Pare-feu Azure premium

Le pare-feu Azure Premium inclut les fonctionnalités suivantes :

- **Inspection TLS** :

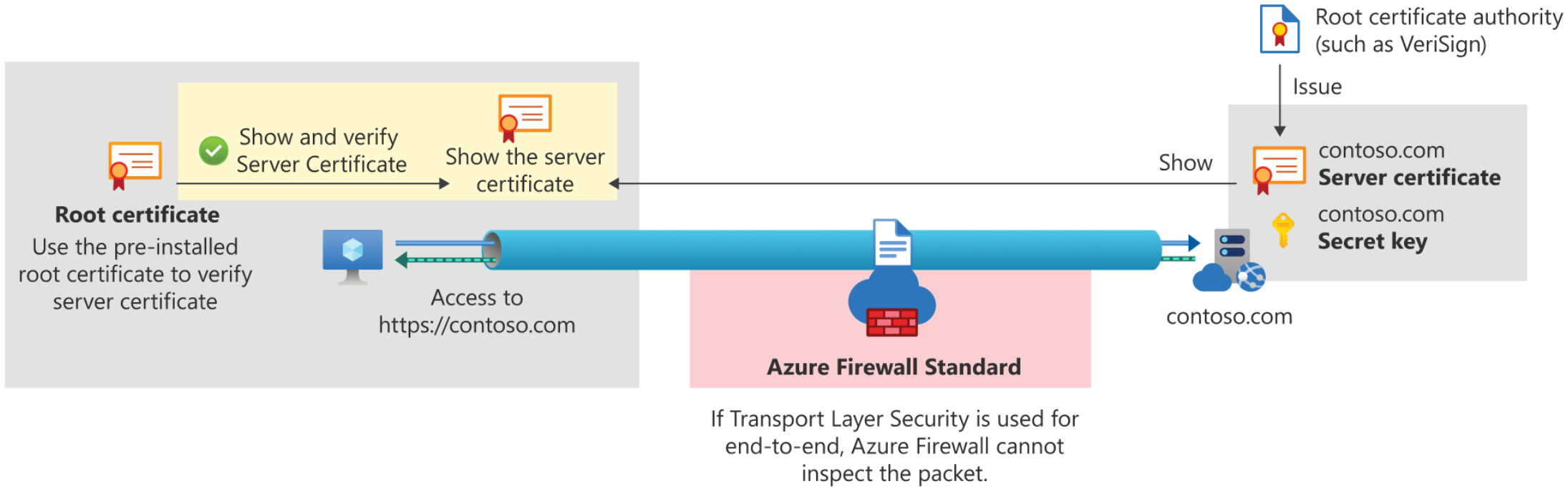
Le protocole TLS (Transport Layer Security) fournit principalement un chiffrement pour la confidentialité, l'intégrité et l'authenticité en utilisant des certificats entre deux applications de communication ou plus. Il s'exécute dans la couche application et est largement utilisé pour chiffrer le protocole HTTP.

Le trafic chiffré a un risque de sécurité possible, et peut masquer une activité utilisateur illégale et un trafic malveillant. Le pare-feu Azure sans inspection TLS (comme indiqué dans le diagramme suivant) n'a aucune visibilité sur les données qui circulent dans le tunnel TLS chiffré et ne peut donc pas fournir une couverture de protection complète.

Le second diagramme montre comment le pare-feu Azure Premium met fin aux connexions TLS et les inspecte pour détecter, alerter et atténuer les activités malveillantes dans HTTPS. Le pare-feu crée en fait deux connexions TLS dédiées : une avec le serveur web (contoso.com) et une autre avec le client. À l'aide du certificat d'autorité de certification fourni par le client, il génère un certificat à la volée qui remplace le certificat de serveur web et le partage avec le client pour établir la connexion TLS entre le pare-feu et le client.

Pare-feu Azure premium

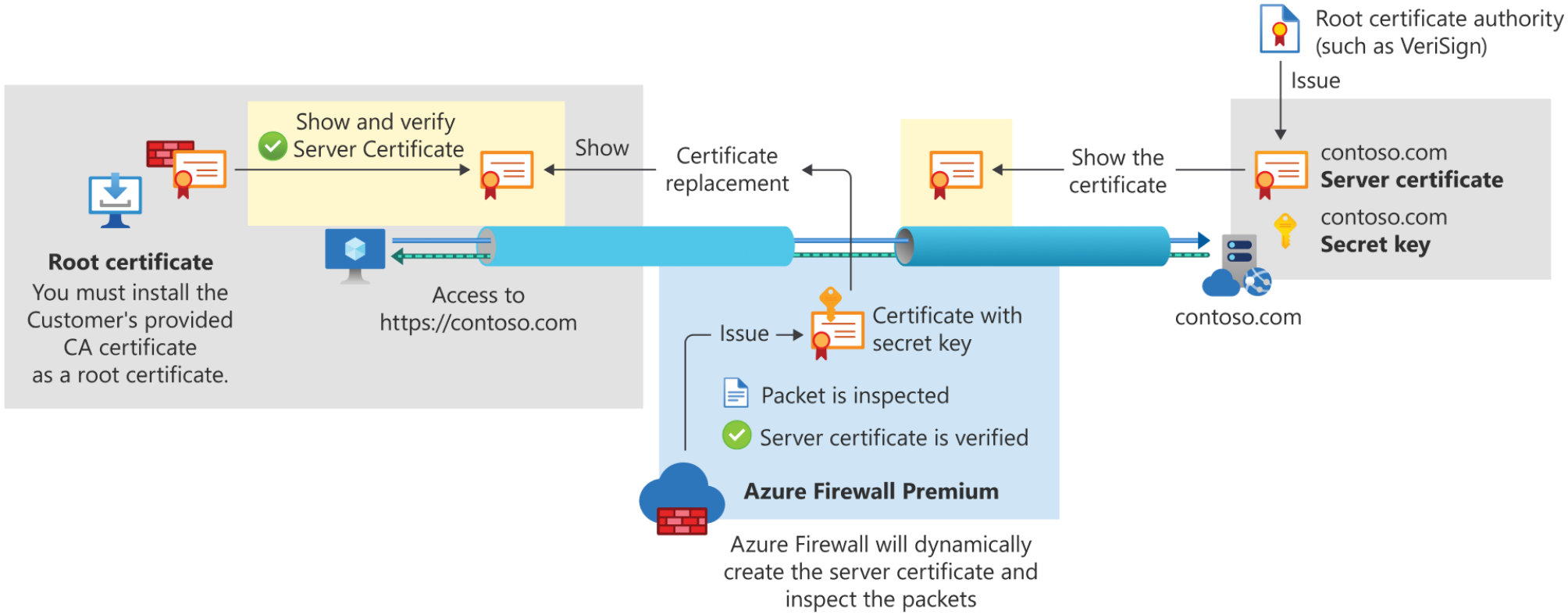
Pare-feu Azure sans inspection TLS :



PARTIE 2

Pare-feu Azure premium

Pare-feu Azure avec inspection TLS :



PARTIE 2

Pare-feu Azure premium

Les cas d'usage suivants sont pris en charge avec le pare-feu Azure :

- Inspection TLS du trafic sortant :

Pour se protéger contre le trafic malveillant envoyé depuis un client interne hébergé dans Azure vers internet.

- Inspection TLS du trafic Est-Ouest (comprend le trafic qui part depuis/vers un réseau local) :

Pour protéger des charges de travail Azure contre le trafic malveillant potentiel envoyé à partir d'Azure.

- Inspection TLS du trafic entrant :

Pour protéger les serveurs internes ou les applications hébergées dans Azure contre les demandes malveillantes provenant d'internet ou d'un réseau externe. Application Gateway fournit un chiffrement de bout en bout.

Pare-feu Azure premium

- **IDPS:**

Un système IDPS (Intrusion Detection and Prevention System) permet de surveiller les activités malveillantes, de consigner des informations sur ces activités, de les signaler, voire de les bloquer.

Le système IDPS permet de détecter les attaques dans tous les ports et protocoles pour le trafic non chiffré. Cela étant, lorsque le trafic HTTPS doit être inspecté, le pare-feu Azure peut utiliser sa fonction d'inspection TLS pour déchiffrer le trafic et mieux détecter les activités malveillantes.

La liste de contournement IDPS permet de ne pas filtrer le trafic vers les adresses IP, les plages et les sous-réseaux spécifiés dans cette liste.

- **Un filtrage des URL:**

Le filtrage d'URL étend la fonctionnalité de filtrage de nom de domaine complet du pare-feu Azure pour prendre en compte une URL entière. Par exemple, www.contoso.com/a/c plutôt que www.contoso.com.

Le filtrage d'URL peut être appliqué au trafic HTTP et HTTPS. Lorsque le trafic HTTPS est inspecté, le pare-feu Azure Premium peut utiliser sa fonctionnalité d'inspection TLS pour déchiffrer le trafic et extraire l'URL cible afin de vérifier si l'accès est autorisé. L'inspection TLS nécessite un consentement au niveau de la règle d'application. Après activation, on peut utiliser des URL pour le filtrage avec HTTPS.

Pare-feu Azure premium

- **Catégories web:**

Les catégories web permettent aux administrateurs d'autoriser ou de refuser aux utilisateurs l'accès aux catégories de sites web telles que les sites web de jeux d'argent, les sites web de réseaux sociaux, etc. Les catégories web sont incluses dans le pare-feu Azure Standard, mais elles sont plus précises dans le Pare-feu Azure Premium. Contrairement à la fonctionnalité de catégories web de la référence SKU Standard, qui correspond à la catégorie basée sur un nom de domaine complet, la référence SKU Premium correspond à la catégorie en fonction de l'URL complète pour le trafic HTTP et HTTPS.

Par exemple, si le Pare-feu Azure intercepte une demande HTTPS pour www.google.com/news, la catégorisation suivante est attendue :

- Pare-feu Standard : seule la partie du nom de domaine complet étant examinée, www.google.com est classé en tant que Moteur de recherche.
- Pare-feu Premium : l'URL complète étant examinée, www.google.com/news est classée en tant qu'Actualités.

Les catégories sont organisées en fonction de leur gravité sous **Responsabilité**, **Bande passante élevée**, **Utilisation métier**, **Perte de productivité**, **Navigation générale** et **Sans catégorie**.

Comment le pare-feu Azure protège un réseau virtuel Azure

Pour comprendre comment le pare-feu Azure protège le réseau virtuel, Il faut savoir qu'il existe deux caractéristiques clés dans tout déploiement de pare-feu Azure :

- L'instance de pare-feu a une adresse IP publique à laquelle tout le trafic entrant est envoyé.
- L'instance de pare-feu a une adresse IP privée à laquelle tout le trafic sortant est envoyé.

Ce qui signifie que tout le trafic, entrant et sortant, passe par le pare-feu. Par défaut, le pare-feu refuse l'accès à tout.

Votre tâche consiste à configurer le pare-feu avec les conditions sous lesquelles le trafic est autorisé via le pare-feu. Chaque condition est appelée une règle et chaque règle applique un ou plusieurs contrôles sur les données. Seul le trafic qui passe avec succès chaque contrôle de chaque règle du pare-feu est autorisé à traverser.

La façon dont le pare-feu Azure gère le trafic réseau dépend de l'origine du trafic :

- Pour le trafic entrant autorisé, le pare-feu Azure utilise DNAT pour traduire l'adresse IP publique du pare-feu en adresse IP privée de la ressource de destination appropriée dans le réseau virtuel.
- Pour le trafic sortant autorisé, le Pare-feu Azure utilise SNAT pour traduire l'adresse IP source en adresse IP publique du pare-feu.

Types de règles du pare-feu Azure

Le tableau suivant décrit les trois types de règles qu'on peut créer pour un pare-feu Azure:

Type de règle	Description
NAT	Traduire et filtrer le trafic internet entrant en fonction de l'adresse IP publique du pare-feu et d'un numéro de port spécifié. Par exemple, pour activer une connexion bureau à distance à une machine virtuelle, on peut utiliser une règle NAT pour traduire l'adresse IP publique du pare-feu et le port 3389 en adresse IP privée de la machine virtuelle.
Application	Filtrer le trafic en fonction d'un FQDN. Par exemple, on peut utiliser une règle d'application pour autoriser le trafic sortant à accéder à une instance Azure SQL Database avec le FQDN server10.database.windows.net.
Réseau	Filtrer le trafic en fonction d'un ou plusieurs des trois paramètres réseau suivants : adresse IP, port et protocole. Par exemple, on peut utiliser une règle de réseau pour autoriser le trafic sortant à accéder à un serveur DNS particulier à une adresse IP spécifique avec le port 53.

Options de déploiement du pare-feu Azure

Le pare-feu Azure offre de nombreuses fonctionnalités conçues pour faciliter la création et la gestion des règles. Le tableau suivant récapitule ces fonctionnalités.

Fonctionnalité	Description
FQDN	Nom de domaine d'un hôte ou d'une ou plusieurs adresses IP. L'ajout d'un FQDN à une règle d'application autorise l'accès à ce domaine. Lorsqu'on utilise un FQDN dans une règle d'application, on peut utiliser des caractères génériques comme *.google.com.
Étiquette de FQDN	Groupe de FQDN Microsoft très connus. L'ajout d'une étiquette de FQDN à une règle d'application autorise l'accès sortant aux FQDN de l'étiquette. Il existe des étiquettes de FQDN pour Windows Update, Azure Virtual Desktop, les diagnostics Windows, la Sauvegarde Azure et plus encore. Les étiquettes de FQDN sont gérées par Microsoft et ne peuvent pas être modifiées ou créées.
Étiquette de service	Groupe de préfixes d'adresses IP associés à un service Azure spécifique. L'ajout d'une étiquette de service à une règle de réseau autorise l'accès au service représenté par l'étiquette. Il existe des étiquettes de service pour des dizaines de services Azure, notamment Sauvegarde Azure, Azure Cosmos DB, Logic Apps et plus encore. Les étiquettes de service sont gérées par Microsoft et ne peuvent pas être modifiées ou créées.
Groupes IP	Groupe d'adresses IP, par exemple 10.2.0.0/16 ou 10.1.0.0-10.1.0.31. On peut utiliser un groupe d'adresses IP comme adresse source dans une règle NAT ou d'application, ou comme adresse source ou de destination dans une règle de réseau.
Système DNS personnalisé	Serveur DNS personnalisé qui résout les noms de domaine en adresses IP. Si on utilise un serveur DNS personnalisé plutôt qu'Azure DNS, on doit également configurer le pare-feu Azure en tant que proxy DNS.
Proxy DNS	On peut configurer le pare-feu Azure pour qu'il fasse office de proxy DNS, ce qui signifie que toutes les demandes DNS clientes passent par le pare-feu avant d'aller au serveur DNS.

Azure Firewall Manager

Azure Firewall Manager offre un point central pour configurer et gérer plusieurs instances du pare-feu Azure. Azure Firewall Manager permet de créer une ou plusieurs stratégies de pare-feu et de les appliquer rapidement à plusieurs pare-feux.

→ **stratégie de pare-feu :**

La configuration d'un seul pare-feu Azure peut être compliquée. Par exemple, le pare-feu peut être configuré avec plusieurs regroupements de règles. Une collection est une combinaison de tout ou partie des éléments suivants :

- Au moins une règle de traduction d'adresses réseau (NAT)
- Une ou plusieurs règles de réseau
- Une ou plusieurs règles d'application

Lorsqu'on inclut d'autres paramètres de pare-feu, tels que des règles DNS et de renseignement sur les menaces personnalisées, la configuration d'un seul pare-feu peut devenir une charge. À cette charge, s'ajoutent deux scénarios de sécurité réseau courants :

- les architectures réseau de l'entreprise demandent plusieurs pare-feux.
- On veut que chaque pare-feu implémente un niveau de base de règles de sécurité qui s'applique à tout le monde, ainsi que des règles spéciales pour des groupes spécifiés comme les développeurs, les utilisateurs de bases de données et le service marketing.

Azure Firewall Manager

Pour simplifier la gestion de ces scénarios de pare-feu similaires, on peut implémenter des stratégies de pare-feu. Une stratégie de pare-feu est une ressource Azure qui contient un ou plusieurs regroupements de règles NAT, réseau et d'application, des paramètres DNS personnalisés, des paramètres de renseignement sur les menaces, etc.

Ici, le point clé est qu'Azure offre une ressource appelée stratégie de pare-feu. Une stratégie de pare-feu qu'on crée est une instance de cette ressource. En tant que ressource distincte, on peut rapidement appliquer la stratégie à plusieurs pare-feu avec Azure Firewall Manager. On peut créer une stratégie comme stratégie de base, puis avoir des stratégies plus spécialisées qui héritent des règles de la stratégie de base.

Azure Firewall Manager

→ **Fonctionnalités clés d'Azure Firewall Manager :**

Le tableau suivant liste les fonctionnalités clés d'Azure Firewall Manager.

Fonctionnalité	Description
Gestion centralisée	Gérer toutes les configurations de pare-feu de l'ensemble du réseau.
Gérer plusieurs pare-feux	Déployer, configurer et surveiller tous les pare-feux qu'on veut à partir d'une seule interface.
Prise en charge de plusieurs architectures réseau	Protège à la fois les réseaux virtuels Azure standards et les hubs Azure Virtual WAN.
Routage du trafic automatisé	Le trafic réseau est automatiquement routé vers le pare-feu (si utilisé avec le hub Azure Virtual WAN uniquement).
Stratégies hiérarchiques	Permet de créer des stratégies de pare-feu parent et enfant. Une stratégie parent contient les règles et les paramètres qu'on souhaite appliquer globalement, tandis qu'une stratégie enfant hérite de toutes les règles et de tous les paramètres de son parent.
Prise en charge des fournisseurs de sécurité tiers	Permet d'intégrer des solutions de sécurité en tant que service (SECaaS) tiers pour protéger la connexion internet du réseau.

CHAPITRE 2

Sécuriser le réseau

1. Segmentation réseau
2. Pare-feu
3. **Systèmes de détection des intrusions et de déni de service DDOS**
4. VPN

Systèmes de détection et de prévention des intrusions

Un système IDPS (Intrusion Detection and Prevention System) permet de surveiller les activités malveillantes, de consigner des informations sur ces activités, de les signaler, voire de les bloquer.

Le pare-feu Azure (Premium) propose un système IDPS basé sur les signatures pour permettre une détection rapide des attaques en recherchant des modèles spécifiques, tels que des séquences d'octets dans le trafic réseau ou des séquences d'instructions malveillantes connues utilisées par un programme malveillant.

Les signatures IDPS sont applicables au trafic de niveau application et de niveau réseau (couches 3-7) et sont entièrement managées et mises à jour en permanence. Les IDPS peuvent être appliqués au trafic entrant, au trafic spoke-to-spoke (est-ouest) et au trafic sortant. Spoke-to-spoke (Est-Ouest) comprend le trafic qui part depuis/vers un réseau local. On peut configurer les plages d'adresses IP privées IDPS à l'aide de la fonctionnalité en préversion de plages d'adresses IP privées.

On peut également déployer un système de détection d'intrusion/prévention des intrusions tiers (IDS/IPS) à partir de la marketplace Azure avec des fonctionnalités d'inspection de charge utile. Ou bien utiliser une solution EDR (host-based IDS/IPS), ou une solution de détection et de réponse de point de terminaison basée sur l'hôte (EDR) conjointement avec, ou au lieu d'IDS/IPS basés sur le réseau.

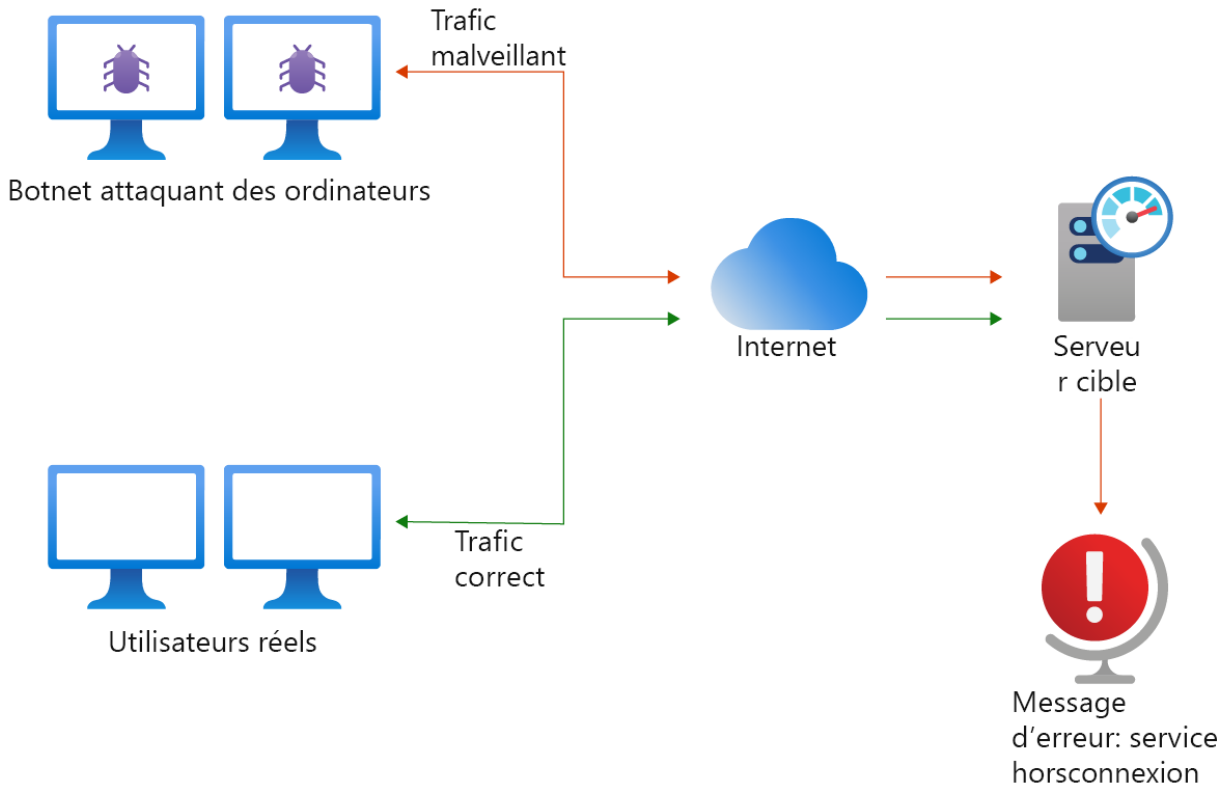
Systèmes de détection des dénis de service DDOS

- **Présentation du DDOS:**

Les attaques par déni de service distribué (DDoS) représentent certains des problèmes de disponibilité et de sécurité majeurs auxquels sont confrontés les clients qui déplacent leurs applications vers le Cloud. Une attaque DDoS tente d'épuiser les ressources d'une application afin de la rendre indisponible aux utilisateurs légitimes. Les attaques DDoS peuvent être ciblées sur n'importe quel point de terminaison qui est publiquement accessible via internet.

Dans une attaque DDoS, un pirate sature intentionnellement le système, comme un serveur, un site web ou une autre ressource réseau, avec un trafic factice. Les ordinateurs sont connectés à un réseau de commande et de contrôle coordonné, appelé botnet. Un tiers malveillant contrôle le botnet pour lancer l'attaque DDoS. En surchargeant les fonctionnalités du service, l'activité déclenche un déni de service pour les utilisateurs légitimes. Les attaques DDoS peuvent cibler n'importe quel point de terminaison publiquement accessible via Internet.

L'image ci-après illustre une attaque DDoS type à partir d'un botnet.



PARTIE 2

Quelques attaques DDOS

- Attaques volumétriques. Ces attaques utilisent plusieurs systèmes infectés pour submerger la couche réseau avec une grande quantité de trafic apparemment légitime. Tous les systèmes compromis font généralement partie d'un botnet criminel. Les types d'attaques volumétriques sont les suivantes :
    - Saturations d'UDP. L'attaquant envoie des paquets UDP, généralement volumineux, vers une seule destination ou à des ports aléatoires. Les systèmes attaquants peuvent facilement usurper leur adresse IP, car le protocole UDP est sans connexion.
    - Saturations d'amplification. Un serveur DNS est submergé de requêtes apparemment légitimes pour le service. L'objectif de l'attaquant est de saturer le service DNS en épuisant la capacité de la bande passante.
    - Saturations d'autres paquets falsifiés. Envoi d'importants volumes de trafic erroné à une ressource.
- Attaques de protocole. Ces attaques ciblent la couche 3 ou la couche 4 du modèle OSI. Ils exploitent une faiblesse dans le protocole TCP. Un exemple d'attaque DDoS basée sur un protocole est la saturation TCP SYN, qui exploite une partie de l'établissement d'une liaison triple. L'attaquant envoie une succession de requêtes TCP SYN, en ignorant la réponse SYN + ACK. Cette attaque est dirigée vers une cible et a pour objectif de surcharger la cible et de la rendre inactive.
- Attaques de la couche Ressource (application). Les attaques de ressources ciblent la couche « supérieure » dans le modèle OSI pour interrompre la transmission des données entre les hôtes. Ces attaques de couche 7 incluent l'exploitation du protocole HTTP, les attaques par injection de code SQL, les scripts inter-sites et d'autres attaques d'application.

Mécanismes Azure pour la protection contre un DDOS

- **DDoS Protection Basic:**

Azure fournit une protection contre les attaques DDoS. La protection DDoS ne stocke pas les données clients. Sans coût supplémentaire, Azure DDoS Protection Basic protège chaque service Azure qui utilise des adresses IPv4 et IPv6 publiques. Ce service de protection DDoS permet de protéger tous les services Azure, y compris les services PaaS (Platform as a service) tels que Azure DNS. DDoS Protection Basic ne nécessite aucun changement de la part de l'utilisateur au niveau de la configuration ou de l'application.

La protection DDoS De base offre :

- Une analyse active du trafic et une détection permanente. La protection DDOS de base analyse les modèles de trafic d'applications toute la journée, tous les jours, en recherchant des indicateurs d'attaques DDoS.
- Atténuation automatique des attaques. Une fois l'attaque détectée, elle est atténuée.
- Le contrat de niveau de service (SLA) de la protection DDoS de base, qui se base sur la région Azure avec le support « meilleur effort ».

Mécanismes Azure pour la protection contre DDOS

- **DDoS Protection Standard:**

DDoS Protection Standard offre des fonctionnalités améliorées d'atténuation DDoS pour la défense contre les attaques DDoS. Cette solution s'adapte automatiquement pour protéger des ressources Azure spécifiques dans un réseau virtuel.

La liste suivante décrit les fonctionnalités et les avantages de la protection DDoS Standard :

- Elle fournit un profilage du trafic intelligent.

- Elle offre une intégration native dans le portail Azure pour son installation et son déploiement. Ce niveau d'intégration permet à DDoS Standard d'identifier les ressources Azure et leurs configurations.

- Lorsque DDoS Standard est activée pour un réseau virtuel, toutes les ressources sur ce réseau sont automatiquement protégées. Aucune procédure administrative supplémentaire n'est nécessaire.

- Les ressources réseau d'une entreprise sont sous l'analyse constante du trafic pour les indications d'une attaque DDoS. Une fois détectée, DDoS Standard intervient et atténue automatiquement l'attaque.

Mécanismes Azure pour la protection contre DDOS

- Il permet de sécuriser les couches 3 et 4 au niveau de la couche réseau et de fournir une protection de l'application (couche 7) avec Azure Web Application Firewall, inclus dans Azure Gateway. Étant donné qu'Azure Gateway et Web Application Firewall sont accessibles sur internet, la protection DDoS Standard protège leurs interfaces réseau. Il s'agit d'un exemple de protection multicouche ou de défense en profondeur.

- Il fournit des rapports d'analyse d'attaques détaillés au cours de l'attaque à intervalles de cinq minutes, et un rapport après action pour obtenir un résumé complet de l'événement lorsque l'attaque se termine.

- Il inclut la prise en charge de l'intégration des journaux d'atténuation à Microsoft Defender pour le Cloud, Microsoft Sentinel ou un système SIEM (Security Information and Event Management) hors connexion pour un monitoring en quasi-temps réel durant une attaque.

- Azure Monitor collecte la télémétrie d'analyse de la protection DDoS Standard pour l'accès aux mesures de synthèse des attaques.

CHAPITRE 2

Sécuriser le réseau

1. Segmentation réseau
2. Pare-feu
3. Systèmes de détection des intrusions et de déni de service DDOS
4. **VPN**

Définitions

- **Passerelle de réseau virtuel :**

Une passerelle de réseau virtuel est composée de deux machines virtuelles ou plus qui sont automatiquement configurées et déployées sur un sous-réseau spécifique que l'on crée, appelé sous-réseau de la passerelle. Les machines virtuelles de passerelle contiennent des tables de routage et exécutent des services de passerelle spécifiques. On ne peut pas configurer directement les machines virtuelles qui font partie de la passerelle de réseau virtuel, même si les paramètres qu'on sélectionne lors de la configuration de la passerelle ont un impact sur les machines virtuelles de passerelle créées.

- **VPN :**

Un réseau privé virtuel (VPN) fournit une connexion chiffrée sécurisée sur un autre réseau. Les réseaux VPN sont généralement déployés pour connecter plusieurs réseaux privés approuvés via un réseau non approuvé comme Internet. Le trafic est chiffré lorsqu'il se déplace sur le réseau non approuvé pour empêcher un tiers d'espionner la communication réseau.

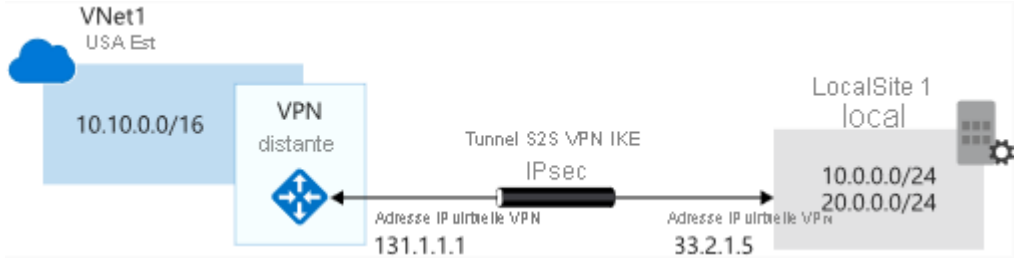
- **Passerelle VPN :**

Une passerelle VPN est un type spécifique de passerelle de réseau virtuel. Chaque réseau virtuel ne peut posséder qu'une seule passerelle VPN. Toutefois, on peut créer plusieurs connexions à la même passerelle VPN. Lorsqu'on crée plusieurs connexions à la même passerelle VPN, tous les tunnels VPN partagent la bande passante de passerelle disponible.

Définitions

- **Passerelle VPN Azure:**

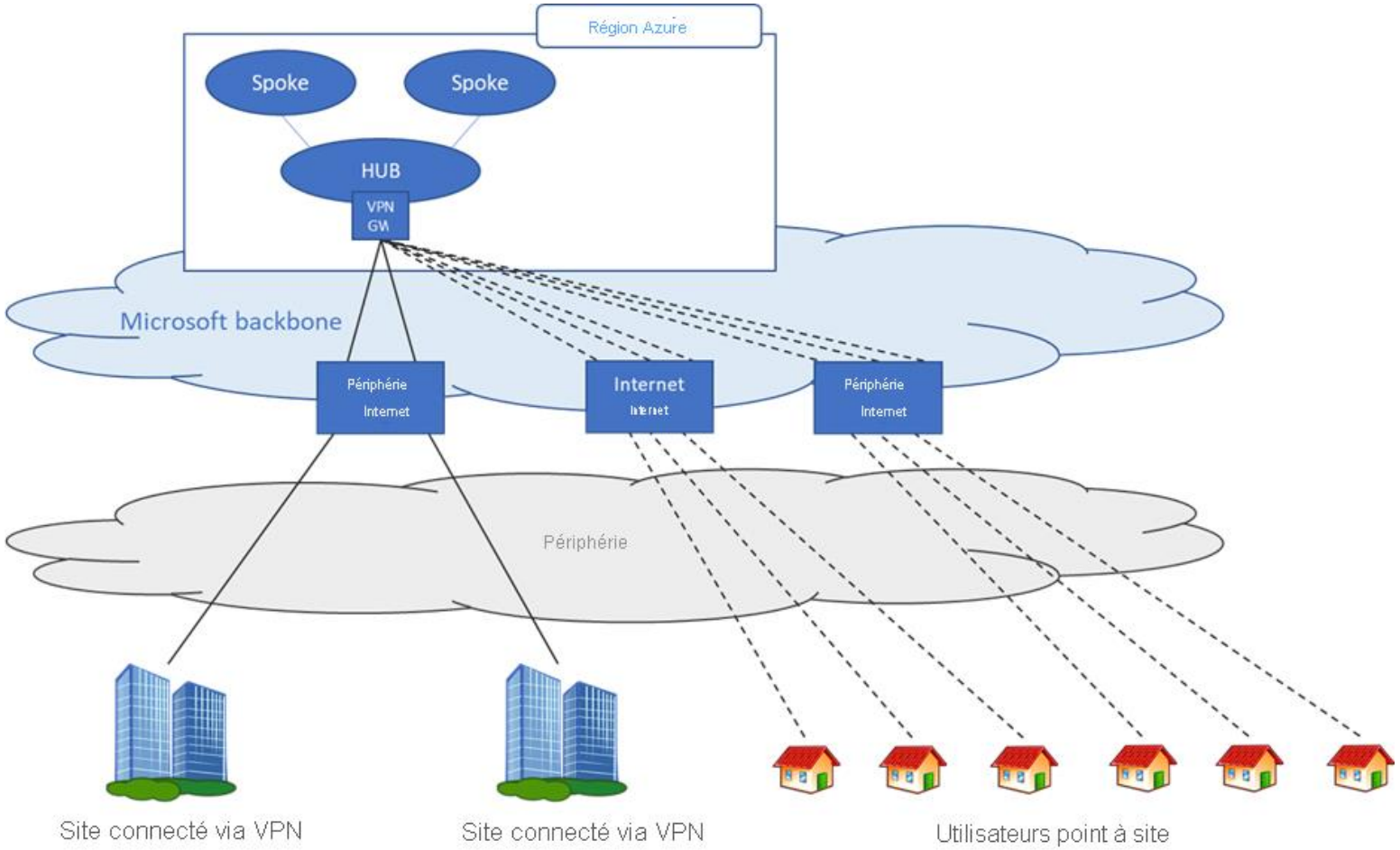
Une passerelle VPN Azure est un type spécifique de passerelle de réseau virtuel qui est utilisé pour envoyer et recevoir le trafic chiffré entre un réseau virtuel Azure et un emplacement local sur l'internet public. Les passerelles VPN Azure peuvent également être utilisées pour connecter des réseaux virtuels Azure distincts à l'aide d'un tunnel chiffré sur le réseau principal de Microsoft.



La passerelle VPN Azure prend en charge les connexions de point à site et de site à site :

- Connexion VPN de point à site. Une connexion VPN de point à site peut être utilisée pour connecter un seul ordinateur à un réseau virtuel Azure. Une connexion P2S est établie en étant démarrée à partir de l'ordinateur client. Ce type de connexion VPN est couramment utilisé par les télétravailleurs avec des ordinateurs portables.
- Connexion VPN de site à site. Une connexion VPN de site à site permet de connecter un réseau à un autre réseau avec un trafic entre les deux réseaux qui passe via un tunnel VPN chiffré. Ce type de connexion VPN est couramment utilisé pour connecter des sites locaux à Azure ou des réseaux virtuels Azure entre eux.

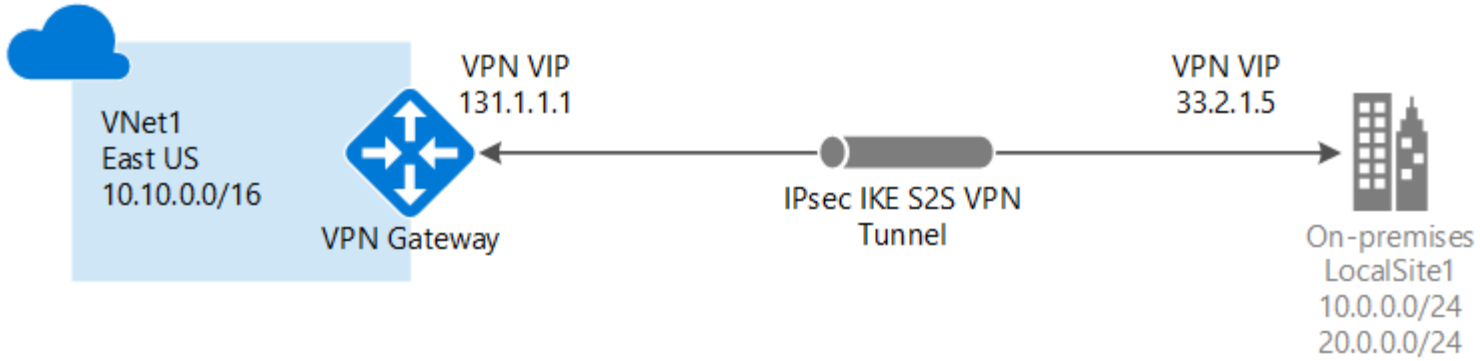
VPN Azure



Conception de la passerelle VPN

- **VPN de site à site :**

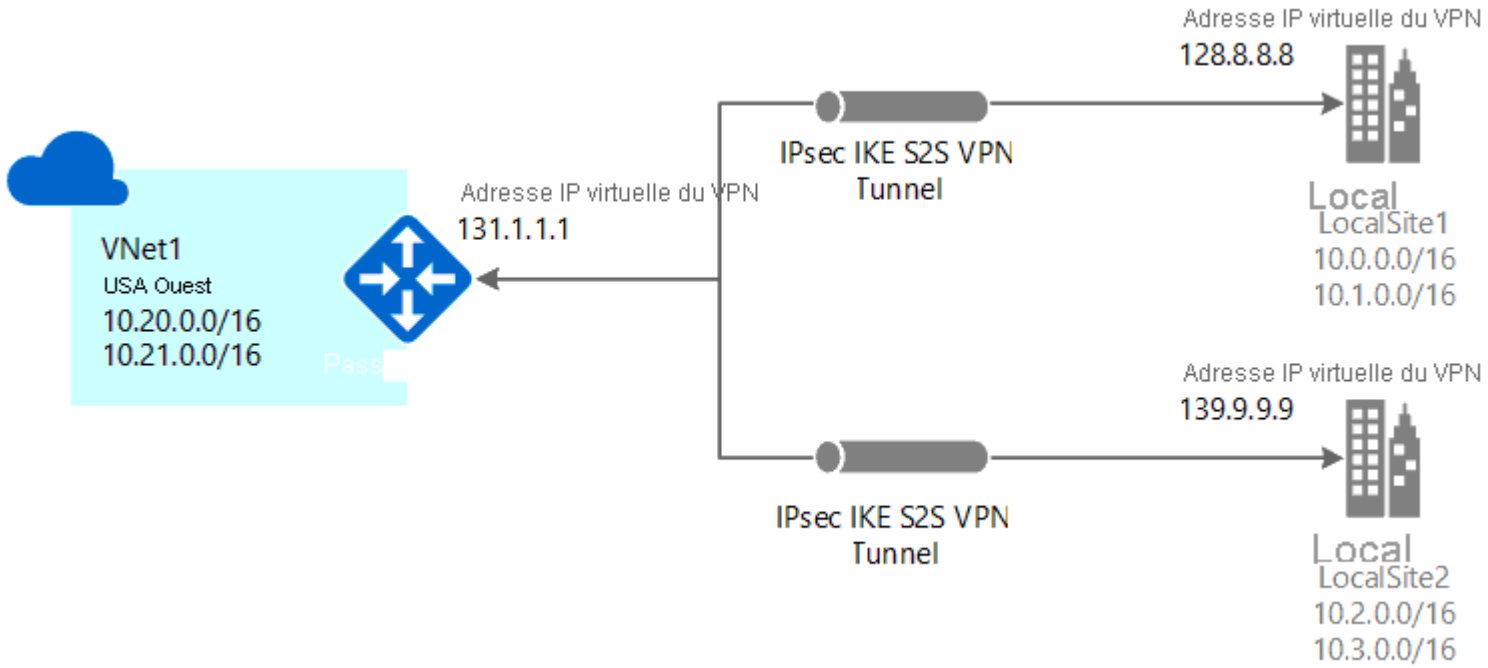
Une connexion par passerelle VPN site à site (S2S) est une connexion via un tunnel VPN IPsec/IKE (IKEv1 ou IKEv2). Les connexions S2S peuvent être utilisées pour les configurations hybrides et entre différents locaux. Une connexion site à site nécessite un appareil VPN local auquel est assignée une adresse IP publique.



La passerelle VPN peut être configurée en mode actif/en attente à l'aide d'une adresse IP publique ou en mode actif/actif à l'aide de deux adresses IP publiques. En mode actif/de secours, un tunnel IPsec est actif et l'autre est en veille. Dans cette configuration, le trafic transite par le tunnel actif et, si un problème se produit avec ce tunnel, le trafic bascule vers le tunnel de secours. La configuration d'une passerelle VPN en mode actif/actif est recommandée. C'est une configuration dans laquelle les deux tunnels IPsec sont simultanément actifs, les données transitant par les deux tunnels en même temps. L'un des avantages supplémentaires du mode actif/actif est que les clients bénéficient de débits plus élevés.

Conception de la passerelle VPN

On peut créer plusieurs connexions VPN à partir de la passerelle de réseau virtuel, généralement en se connectant à plusieurs sites locaux. Lorsqu'on travaille avec plusieurs connexions, on doit utiliser un type de VPN basé sur l'itinéraire (l'équivalent d'une passerelle dynamique pour les réseaux virtuels classiques). Chaque réseau virtuel ne pouvant disposer que d'une seule passerelle de réseau virtuel, toutes les connexions passant par la passerelle partagent la bande passante disponible. Pour ce type de connexion, on fait parfois référence à une connexion « multisite ».



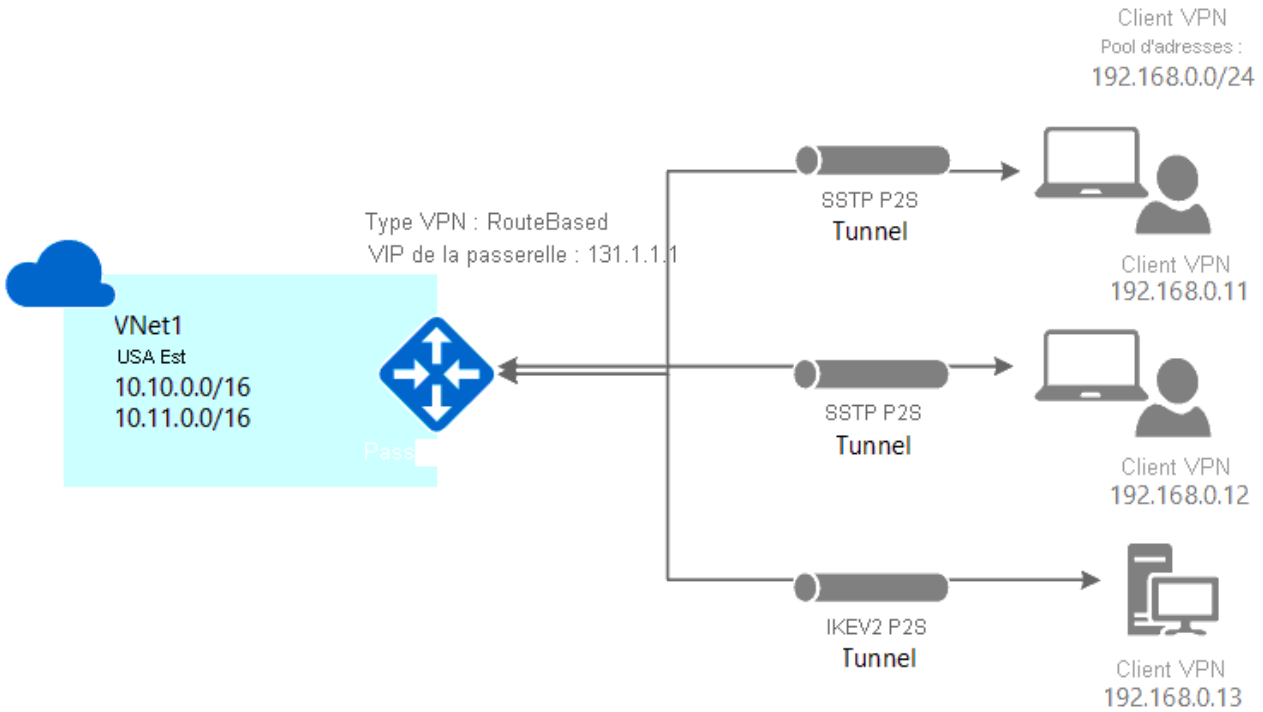
PARTIE 2

Conception de la passerelle VPN

- **VPN de point à site :**

Une connexion par passerelle VPN point à site (P2S) permet de créer une connexion sécurisée au réseau virtuel à partir d'un ordinateur de client individuel. Une connexion P2S est établie en étant démarrée à partir de l'ordinateur client. Cette solution est utile pour les télétravailleurs souhaitant se connecter à un réseau virtuel à partir d'un emplacement distant, comme depuis leur domicile ou pendant une conférence. De même, l'utilisation d'un VPN P2S est une solution utile qui constitue une alternative au VPN Site à Site (S2S) lorsqu'un nombre restreint de clients doit se connecter à un réseau virtuel.

Contrairement aux connexions S2S, les connexions P2S ne nécessitent pas d'adresse IP publique locale, ni de périphérique VPN. Les connexions P2S peuvent être utilisées avec des connexions S2S via la même passerelle VPN, dans la mesure où toutes les exigences de configuration des deux types de connexions sont compatibles.



PARTIE 2

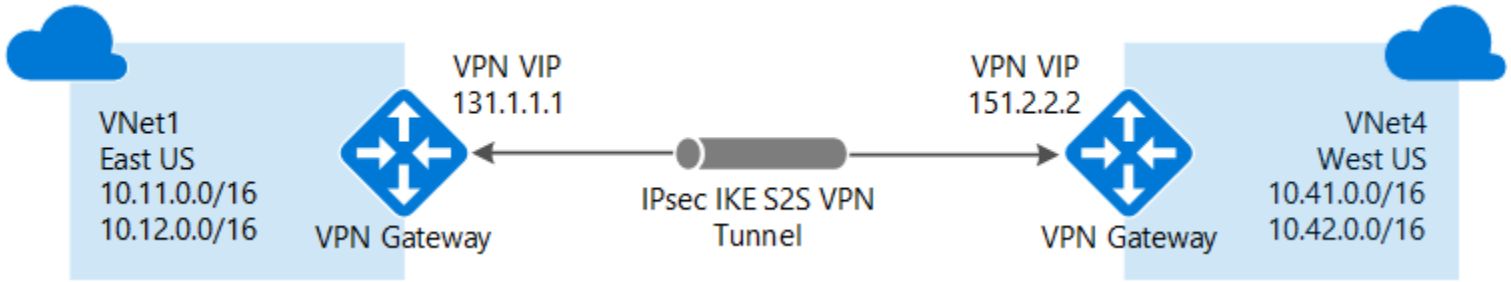
Conception de la passerelle VPN

- **Connexions de réseau virtuel à réseau virtuel (tunnel VPN IPsec/IKE) :**

La connexion entre deux réseaux virtuels est semblable à la connexion d'un réseau virtuel à un emplacement de site local. Les deux types de connectivités font appel à une passerelle VPN pour offrir un tunnel sécurisé utilisant Ipsec/IKE. On peut même combiner une communication de réseau virtuel à réseau virtuel avec des configurations de connexion multi-sites. On établit ainsi des topologies réseau qui combinent une connectivité entre différents locaux et une connectivité entre différents réseaux virtuels.

Les réseaux virtuels qu'on connecte peuvent être situés :

- dans la même région ou dans des régions différentes
- dans le même abonnement ou dans des abonnements différents
- dans le même modèle de déploiement ou dans des modèles de déploiement différents

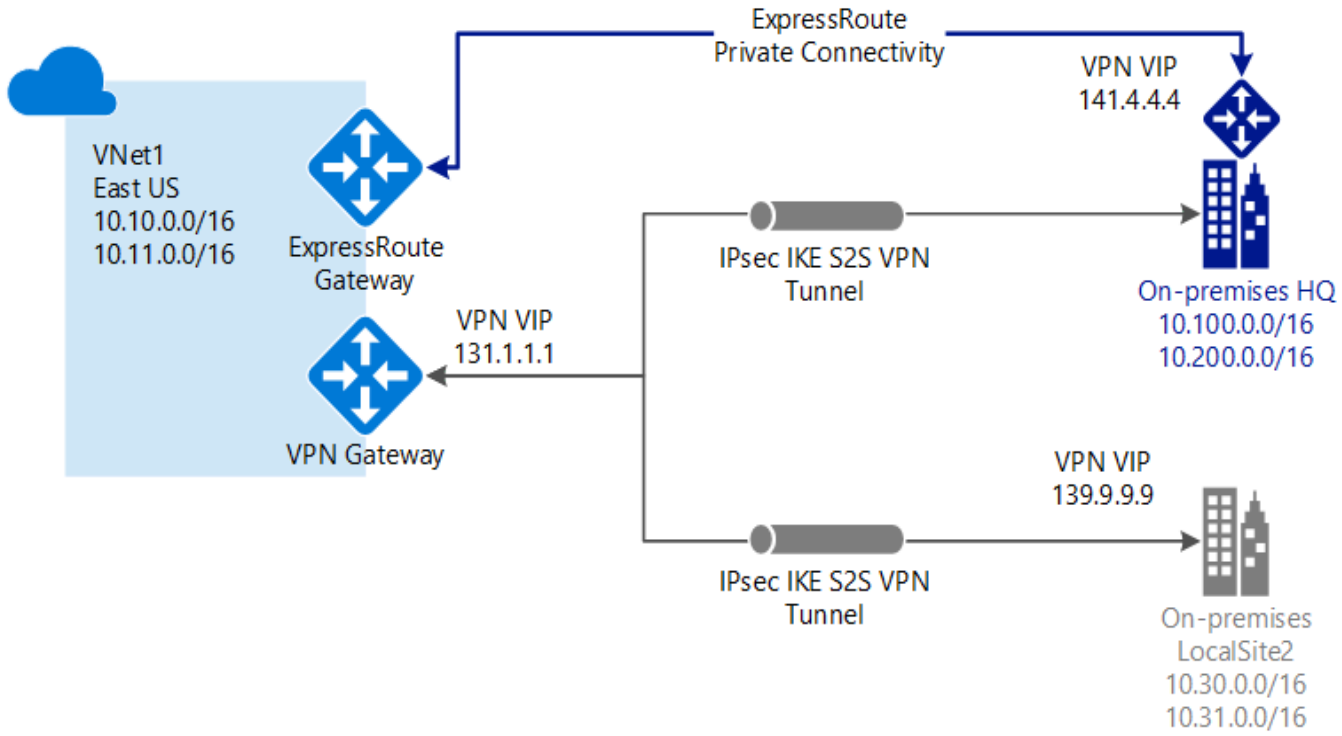


Conception de la passerelle VPN

- **Coexistence de connexions ExpressRoute et de site à site :**

ExpressRoute est une connexion directe et privée à partir d'un réseau étendu (et non pas sur l'Internet public) vers les services Microsoft, y compris Azure. Le trafic VPN de site à site transite via l'Internet public tout en étant chiffré. La possibilité de configurer des connexions VPN de site à site et ExpressRoute pour le même réseau virtuel présente plusieurs avantages.

On peut configurer un VPN de site à site comme un chemin d'accès de basculement sécurisé pour ExpressRoute, ou utiliser des VPN de site à site pour se connecter à des sites qui ne font pas partie du réseau, mais qui sont connectés via ExpressRoute. Il faut noter que cette configuration nécessite deux passerelles de réseau virtuel pour un même réseau virtuel, une de type « VPN », et l'autre de type « ExpressRoute ».



PARTIE 2

CHAPITRE 3

Gérer les identités

Ce que vous allez apprendre dans ce chapitre :

- Système centralisé d'identité et d'authentification
- Authentification unique (SSO)
- Authentification renforcée (MFA)
- Accès aux ressources en fonction des conditions

8 heures

CHAPITRE 3

Gérer les identités

1. **Système centralisé d’identité et d’authentification**
2. Authentification unique (SSO)
3. Authentification renforcée (MFA)
4. Accès aux ressources en fonction des conditions

Azure AD: Système centralisé d'identité et d'authentification

- Une identité est une chose qui peut être authentifiée. Une identité peut être un utilisateur avec un nom d'utilisateur et un mot de passe. Les identités incluent également des applications ou autres serveurs qui peuvent nécessiter l'authentification via des clés secrètes ou des certificats.

- Dans l'architecture informatique, l'identité constitue la base d'un pourcentage important des garanties de sécurité. Si l'infrastructure informatique héritée s'appuie largement sur l'utilisation des pare-feux et des solutions de sécurité réseau aux points de sortie internet pour se protéger des menaces extérieures, ces contrôles sont moins efficaces dans les architectures Cloud dotés de services partagés accessibles via des réseaux de fournisseurs Cloud ou internet.

- L'utilisation des solutions d'identité informatique, telle que Azure AD, offre des fonctionnalités de sécurité supplémentaires à la différence des services d'identité hérités, car elles peuvent donner des informations sur les menaces en provenance des demandes d'accès des différents clients.

- L'authentification est un processus qui accorde ou refuse l'accès à un système en vérifiant l'identité de l'accesseur. Utiliser un service d'identité managée pour toutes les ressources de permet de simplifier la gestion globale (comme des stratégies de mot de passe) et de limiter le risque de négligences ou d'erreurs humaines. Azure Active Directory (Azure AD) est le service incontournable pour la gestion des identités et des accès pour Azure.

- L'autorisation est un processus qui accorde ou refuse l'accès à un système en vérifiant si l'accesseur dispose des autorisations nécessaires pour effectuer l'action demandée. L'accesseur dans ce contexte est la charge de travail (application Cloud) ou l'utilisateur de la charge de travail. L'action peut être d'ordre opérationnel ou liée à la gestion des ressources. Il existe deux approches principales d'autorisation : basée sur les rôles et basée sur les ressources. Les deux peuvent être configurées avec Azure AD.

Azure AD: Système centralisé d'identité et d'authentification

Azure Active Directory ou Azure AD est un service de gestion des identités utilisateurs externalisé sur le Cloud public Microsoft Azure. Azure AD regroupe tout un ensemble de services et fonctionnalités permettant de gérer les identités des utilisateurs d'une entreprise ou de ses partenaires et de gérer les accès aux applications professionnelles.

Azure AD est un service supplémentaire plus puissant qu'un Active Directory local car il permet de mettre en place plus simplement et à moindre coût des fonctionnalités de sécurisation et monitoring plus avancées.

Grâce à Azure AD on pourra ainsi : assurer la gestion des identités, mettre en place l'authentification multi-facteur, gérer plus facilement les mots de passe utilisateurs, contrôler les accès automatiquement, surveiller les utilisations d'applications critiques, etc. Tant de services à portée de main qui permettront d'être plus efficace dans les processus informatiques. Azure AD s'intègre également à :

- Office365
- Dynamics CRM en ligne
- De nombreuses applications SaaS tierces

Pour les applications orientées consommateurs, Azure Active Directory B2C permet aux utilisateurs de s'authentifier avec leurs comptes sociaux existants, tels que :

- Facebook
- Google
- LinkedIn

Fonctionnement Azure AD

Azure AD est un service basé sur le Cloud pour la gestion des identités et des accès (IAM). Il s'agit d'un magasin d'authentification en ligne sécurisé pour les profils d'utilisateurs individuels et les groupes de profils d'utilisateurs, et il appartient à la catégorie Identité en tant que service (IDaaS).

Azure AD est destiné à gérer l'accès aux applications et serveurs basés sur le Cloud qui utilisent des protocoles d'authentification modernes tels que SAML 2.0, OpenID Connect, OAuth 2.0 et WS-Federation.

Azure AD gère l'accès via des comptes d'utilisateurs, qui portent un nom d'utilisateur et un mot de passe. Les utilisateurs peuvent être organisés en différents groupes, auxquels peuvent être accordés différents privilèges d'accès pour des applications individuelles. Des identités peuvent également être créées pour les applications Cloud, qui peuvent provenir de Microsoft ou d'un logiciel tiers en tant que service (SaaS), afin d'accorder l'accès aux utilisateurs.

Azure AD utilise SSO pour connecter les utilisateurs aux applications SaaS. Cela permet à chaque utilisateur d'accéder à la suite complète d'applications pour lesquelles il est autorisé, sans avoir à se connecter à plusieurs reprises à chaque fois.

Azure AD crée des jetons d'accès qui sont stockés localement sur les appareils des employés ; ces jetons peuvent être créés avec des dates d'expiration. Pour les ressources professionnelles importantes, Azure AD peut exiger une authentification multifacteur (MFA).

Windows AD vs Azure AD

Azure AD ne doit pas être confondu avec Windows Active Directory, un autre service Microsoft portant un nom similaire. Active Directory se compose de plusieurs services qui s'exécutent sur Windows Server, et qui gèrent l'accès des utilisateurs aux ressources en réseau, telles que les imprimantes. Bien qu'Azure AD et Windows AD gèrent tous deux les comptes d'utilisateurs, ils utilisent des protocoles d'authentification et des bases de code complètement différents. Par conséquent, Azure AD n'est pas simplement le pendant Cloud de Windows AD.

Les principales différences incluent les éléments suivants :

- Contrairement à Windows AD, Azure AD est conçu pour les services web. Azure AD prend en charge les services qui utilisent les API REST (Representational State Transfer) pour les applications Cloud en ligne telles qu'Office 365.
- Azure AD utilise des protocoles différents de Windows AD. Azure AD utilise des protocoles tels que SAML et OAuth.2.0. Il ne prend pas en charge NTLM, Kerberos ou LDAP (Lightweight Directory Access Protocol).
- Azure AD utilise Azure Policy, par opposition à la stratégie de groupe dans Windows AD.
- Azure AD n'utilise pas d'unités d'organisation (unités organisationnelles) ni de forêts . Il a une structure de répertoire plate.
- Azure AD Join, qui relie les PC (ordinateurs personnels), ne peut être utilisé qu'avec Windows 10.

Fonctionnalités et licences Azure AD

Azure AD est disponible en quatre niveaux de licence différents : gratuit (le plus bas), applications Office 365, Premium P1 et Premium P2 (le plus élevé).

Le niveau de licence gratuit a une limite de 500 000 objets pour les objets d'annuaire. Il contient toutes les fonctionnalités inter-entreprises de gestion des identités et des accès. Il n'inclut pas IAM pour Office 365, les fonctionnalités premiums, les identités hybrides, l'accès conditionnel, la protection des identités, la gouvernance des identités ou la gestion avancée des accès de groupe. Selon Microsoft, les fonctionnalités incluses dans le niveau gratuit sont :

- Authentification unique illimitée
- Approvisionnement des utilisateurs
- Authentification fédérée (services de fédération Active Directory ou fournisseur d'identité tiers)
- Gestion des utilisateurs et des groupes
- Enregistrement de l'appareil
- Authentification Cloud (Authentification Pass-Through, Synchronisation Password Hash, Seamless SSO)
- Synchronisation Azure AD Connect, qui étend les répertoires locaux d'une organisation à Azure AD
- Changement de mot de passe en libre-service

Fonctionnalités et licences Azure AD

- Azure AD Join (SSO de bureau et récupération BitLocker administrateur)
- Mot de passe de protection
- Authentification multifacteur
- Rapports de base pour la sécurité et l'utilisation
- Fonctionnalités Azure AD pour les utilisateurs invités

Le deuxième niveau le plus bas des services Azure AD est accessible aux abonnés aux applications Office 365. Il est accessible aux abonnés des niveaux E1, E3, E5, F1 et F3. Ce niveau n'a pas de limite d'objets d'annuaire. Il inclut toutes les fonctionnalités offertes dans le niveau gratuit, ainsi que la gestion des identités et des accès pour les applications Office 365, telles que :

- Marque d'entreprise personnalisée des panneaux d'accès et des pages de connexion/déconnexion
- Accord de niveau de service (SLA)
- Réinitialisation de mot de passe en libre-service pour les utilisateurs du Cloud
- Synchronisation bidirectionnelle des objets d'appareil entre Azure AD et les annuaires locaux

Fonctionnalités et licences Azure AD

Le niveau Premium P1 accorde le deuxième niveau d'accès le plus élevé à Azure AD. L'accès Premium P1 coûte 6 $ par mois et par utilisateur. Il inclut toutes les fonctionnalités d'Azure AD, à l'exception de la protection et de la gouvernance des identités. Les fonctionnalités spécifiques de Premium P1 incluent tout ce qui est proposé dans le niveau Office 365, plus :

- Protection par mot de passe premium, réinitialisation du mot de passe en libre-service avec réécriture sur site
- Gestion avancée des accès de groupe
- Azure AD Join avec l'inscription automatique à la gestion des appareils mobiles (MDM), la personnalisation de la politique d'administration locale, la récupération BitLocker en libre-service, l'itinérance de l'état de l'entreprise
- Rapports de sécurité et d'utilisation avancés
- Identités hybrides
- Accès conditionnel

Le niveau Premium P2 coûte 9 $ par mois, par utilisateur et comprend la suite complète de fonctionnalités Azure AD. Il comprend tout ce qui est proposé dans P1, ainsi que des fonctionnalités de protection et de gouvernance des identités.

CHAPITRE 3

Gérer les identités

1. Système centralisé d’identité et d’authentification
2. **Authentification unique (SSO)**
3. Authentification renforcée (MFA)
4. Accès aux ressources en fonction des conditions

Authentification unique (SSO)

- **Définition:**

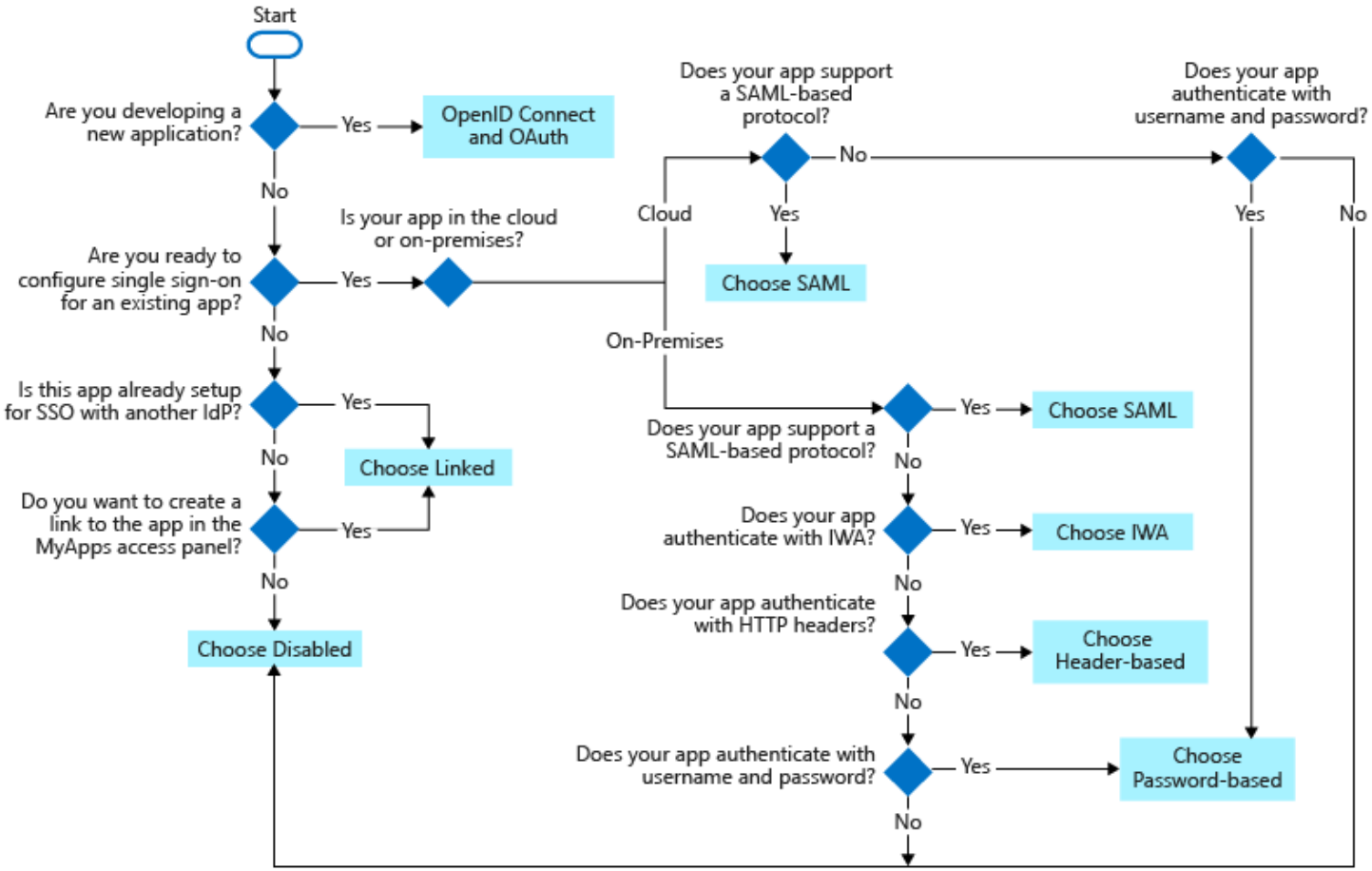
L'authentification unique est une méthode d'authentification qui permet aux utilisateurs de se connecter avec un ensemble d'informations d'identification à plusieurs systèmes logiciels indépendants. Avec l'authentification unique, un utilisateur n'a pas besoin de se connecter à chaque application dont il se sert. Avec l'authentification unique, les utilisateurs peuvent accéder à toutes les applications dont ils ont besoin sans avoir à s'authentifier avec d'autres informations d'identification.

- **Options d'authentification unique sur Azure:**

Le choix d'une méthode d'authentification unique dépend de la façon dont l'application est configurée pour l'authentification. Les applications Cloud peuvent utiliser des options basées sur la fédération comme OpenID Connect, OAuth et SAML. L'application peut également utiliser une authentification unique basée sur mot de passe, une authentification unique basée sur un lien, ou l'authentification unique peut avoir été désactivée.

Cet organigramme permet de décider quelle méthode d'authentification unique est la plus adaptée à la situation d'une entreprise:

Authentification unique (SSO)



PARTIE 2

Authentification unique (SSO)

- **Options d'authentification unique sur Azure:**

→ **Fédération:**

Avec l'authentification unique fédérée, Azure AD authentifie l'utilisateur dans l'application en se servant de son compte Azure AD. Cette méthode est prise en charge pour les applications SAML 2.0, WS-Federation ou OpenID Connect. L'authentification unique fédérée est le mode d'authentification unique le plus riche. Utilisez l'authentification unique fédérée avec Azure AD quand une application la prend en charge, au lieu d'une authentification unique basée sur mot de passe et les services de fédération Active Directory (AD FS).

Dans certains cas, l'option SSO n'est pas présente pour une application d'entreprise. Si l'application a été inscrite en utilisant « Inscriptions d'applications » dans le portail, la fonctionnalité d'authentification unique est configurée pour utiliser OpenID Connect et OAuth par défaut. Dans ce cas, l'option d'authentification unique n'apparaît pas dans le volet de navigation sous « Applications d'entreprise ».

.

Authentification unique (SSO)

L'authentification unique n'est pas disponible lorsqu'une application est hébergée chez un autre locataire. L'authentification unique n'est pas non plus disponible si le compte n'a pas les autorisations nécessaires (administrateur général, administrateur d'application Cloud, administrateur d'application ou propriétaire du principal de service). Les autorisations peuvent également être à l'origine d'un scénario dans lequel on peut ouvrir l'authentification unique, mais on ne pourra pas l'enregistrer.

→ Mot de passe :

Avec l'authentification par mot de passe, les utilisateurs se connectent à l'application avec un nom d'utilisateur et un mot de passe la première fois qu'ils y accèdent. Après la première authentification, Azure AD fournit le nom d'utilisateur et le mot de passe à l'application. L'authentification unique par mot de passe permet de sécuriser le stockage et la lecture des mots de passe des applications avec une extension de navigateur web ou une application mobile. Cette option utilise le processus de connexion existant fourni par l'application, permet à l'administrateur de gérer les mots de passe et n'a pas besoin que l'utilisateur connaisse le mot de passe.

→ Liée :

L'authentification liée peut fournir une expérience utilisateur homogène lorsqu'on migre des applications sur un certain laps de temps. Si on migre des applications vers Azure AD, on peut utiliser l'authentification unique basée sur des liens pour publier rapidement des liens vers toutes les applications que l'on veut migrer. Les utilisateurs peuvent trouver tous les liens dans les portails « Mes applications » ou Microsoft 365.

Une fois qu'un utilisateur s'est authentifié avec une application liée, un compte doit être créé avant que l'utilisateur obtienne l'accès par authentification unique. Le provisionnement de ce compte peut se produire automatiquement, ou manuellement par un administrateur. On ne peut pas appliquer de stratégies d'accès conditionnel ou d'authentification multifacteur à une application liée, car une application liée ne fournit pas de fonctionnalités d'authentification unique via Azure AD. Quand on configure une application liée, on ajoute juste un lien qui apparaît pour lancer l'application.

Authentification unique (SSO)

→ **Désactivée :**

Lorsque l'authentification unique est désactivée, elle n'est pas disponible pour l'application. Quand l'authentification unique est désactivée, les utilisateurs peuvent avoir besoin de s'authentifier deux fois. Les utilisateurs s'authentifient d'abord auprès d'Azure AD, puis ils se connectent à l'application.

Il faut désactiver l'authentification unique quand :

- On n'est pas prêt à intégrer cette application à l'authentification unique Azure AD
- On teste d'autres aspects de l'application
- Une application locale ne demande pas aux utilisateurs de s'authentifier, mais on le veut. Si l'authentification unique est désactivée, l'utilisateur doit s'authentifier.

CHAPITRE 3

Gérer les identités

1. Système centralisé d’identité et d’authentification
2. Authentification unique (SSO)
3. **Authentification renforcée (MFA)**
4. Accès aux ressources en fonction des conditions

Authentification renforcée (MFA)

L'authentification multifacteur est un processus où les utilisateurs sont invités pendant le processus de connexion à suivre une forme d'identification supplémentaire, comme un code sur leur téléphone portable ou un scan de leur empreinte digitale.

L'utilisation d'un mot de passe unique ne protège pas complètement des attaques. Si le mot de passe est faible ou s'il a été exposé ailleurs, un attaquant peut l'utiliser pour accéder au compte utilisateur. Quand on exige une deuxième forme d'authentification, la sécurité est renforcée parce que ce facteur supplémentaire n'est pas un élément qu'un attaquant peut facilement obtenir ou dupliquer.

- **Authentification renforcée Azure AD:**

L'authentification multifacteur Azure AD impose au minimum deux des méthodes d'authentification suivantes :

- Un élément qu'on connait, généralement un mot de passe.
- Un élément qu'on possède, tel qu'un appareil de confiance qui n'est pas facilement dupliqué, comme un téléphone ou une clé matérielle.
- Un élément biométrique identifiant la personne, tel qu'une empreinte digitale ou un scan du visage.

Authentification renforcée (MFA)

Les utilisateurs peuvent s'inscrire à la réinitialisation de mot de passe en libre-service et à l'authentification multifacteur Azure AD en une seule étape pour simplifier l'expérience d'intégration. Les administrateurs peuvent définir les formes d'authentification secondaire qui peuvent être utilisées. L'authentification multifacteur Azure AD peut également être nécessaire quand les utilisateurs effectuent une réinitialisation de mot de passe en libre-service pour sécuriser davantage ce processus.

→ **Protection par mot de passe :**

Par défaut, Azure AD bloque les mots de passe faibles tels que Motdepasse1. Une liste globale de mots de passe interdits est automatiquement mise à jour et appliquée, qui comprend des mots de passe faibles connus. Si l'utilisateur Azure AD tente de définir son mot de passe sur l'un de ces mots de passe faibles, il reçoit une notification lui demandant de choisir un mot de passe plus sécurisé.

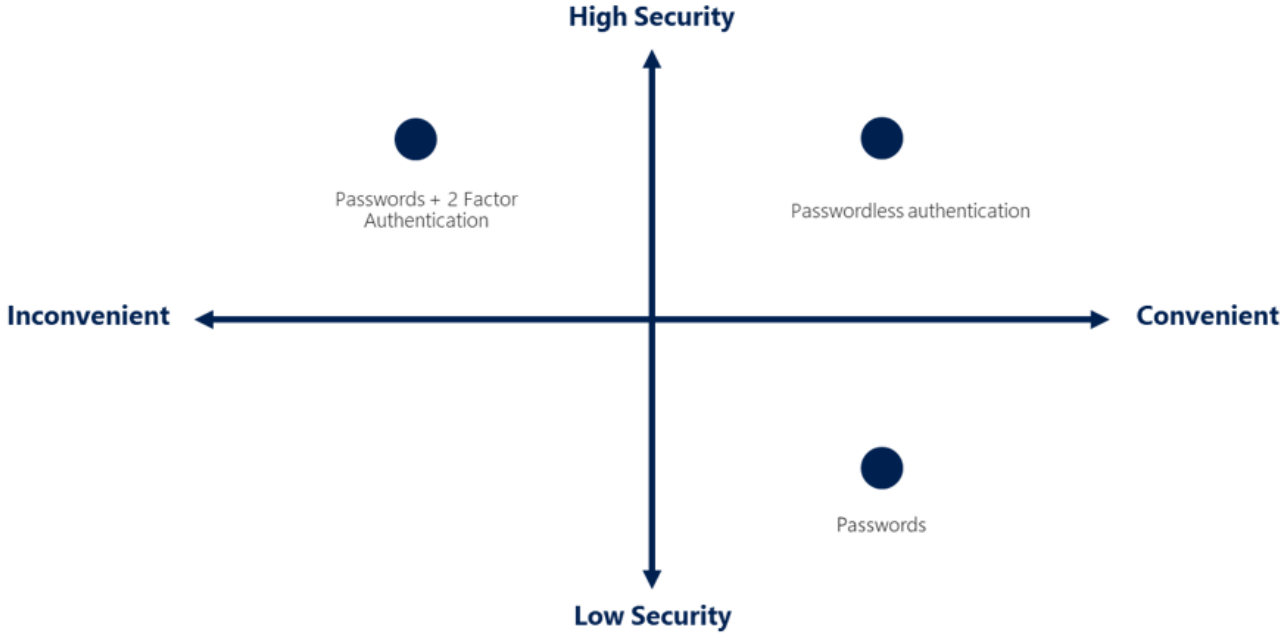
Pour renforcer la sécurité, on peut définir des stratégies de protection par mot de passe personnalisées. Ces stratégies peuvent utiliser des filtres pour bloquer toute variante d'un mot de passe contenant un nom comme Contoso ou un lieu comme Londres, par exemple.

Pour la sécurité hybride, on peut intégrer la protection par mot de passe Azure AD à un environnement Active Directory local. Un composant installé dans l'environnement local reçoit la liste globale de mots de passe interdits et les stratégies de protection par mot de passe personnalisées d'Azure AD, et les contrôleurs de domaine les utilisent pour traiter les événements de changement de mot de passe. Cette approche hybride permet de s'assurer que, peu importe où et comment l'utilisateur change ses informations d'identification, on applique l'utilisation de mots de passe forts.

Authentification renforcée (MFA)

→ **Authentification sans mot de passe :**

L'objectif final de nombreux environnements est de supprimer l'utilisation de mots de passe dans le cadre des événements de connexion. Les fonctionnalités telles que la protection par mot de passe Azure ou l'authentification multifacteur Azure AD permettent d'améliorer la sécurité, mais un nom d'utilisateur et un mot de passe restent une forme d'authentification faible qui peut être exposée ou faire l'objet d'une attaque par force brute.



Authentification renforcée (MFA)

Quand on se connecte avec une méthode sans mot de passe, les informations d'identification sont fournies au moyen de méthodes telles que la biométrie avec Windows Hello Entreprise ou une clé de sécurité FIDO2. Ces méthodes d'authentification ne peuvent pas être facilement dupliquées par un attaquant.

Azure AD permet d'effectuer une authentification en mode natif à l'aide de méthodes non basées sur un mot de passe afin de simplifier l'expérience de connexion des utilisateurs et de réduire le risque d'attaques.

Méthodes de vérification disponibles sur Azure MFA

Lorsque les utilisateurs se connectent à une application ou à un service et reçoivent une invite MFA, ils peuvent choisir l'une des formes enregistrées de vérification supplémentaire. Les utilisateurs peuvent accéder à « Mon profil » pour modifier ou ajouter des méthodes de vérification.

Les autres formes de vérification suivantes peuvent être utilisées avec Azure AD Multi-Factor Authentication :

- Application Microsoft Authenticator
- Windows Hello Entreprise
- Clé de sécurité FIDO2
- Jeton matériel OATH (préversion)
- Jeton logiciel OATH
- sms
- Appel vocal

CHAPITRE 3

Gérer les identités

1. Système centralisé d’identité et d’authentification
2. Authentification unique (SSO)
3. Authentification renforcée (MFA)
4. **Accès aux ressources en fonction des conditions**

Accès aux ressources en fonction des conditions

Sur le Cloud Azure, ce système est appelé « accès en fonction du rôle Azure (Azure RBAC) ». Dans cette partie, nous allons découvrir quelles sont les caractéristiques de ce système.

- **Définitions :**

- **Principal de sécurité :**

Un principal de sécurité est un objet qui représente un utilisateur, un groupe, un principal de service ou une identité managée demandant l'accès à des ressources Azure. On peut attribuer un rôle à l'un de ces principaux de sécurité.

- **Définition de rôle :**

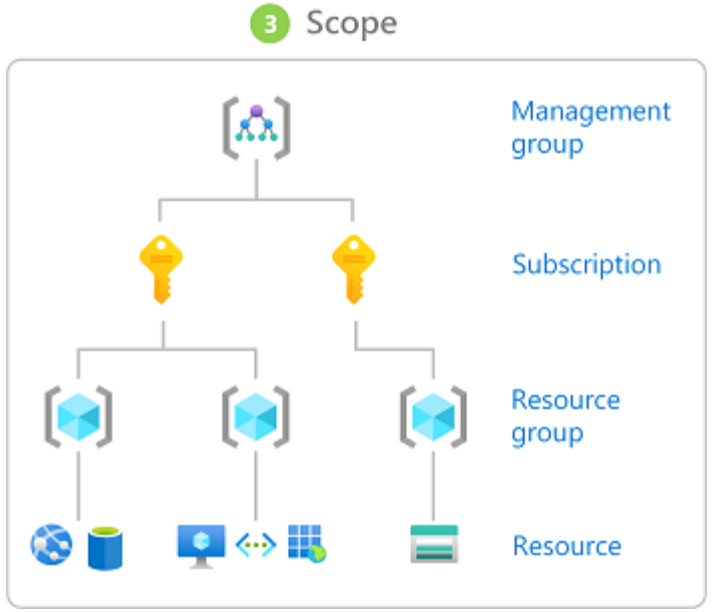
Une définition de rôle est une collection d'autorisations. Elle est généralement simplement appelée rôle. Une définition de rôle liste les actions qui peuvent être effectuées, comme lire, écrire et supprimer. Les rôles peuvent être de haut niveau, comme propriétaire, ou spécifiques, comme lecteur de machines virtuelles.

Accès aux ressources en fonction des conditions

- **Portée (étendue) :**

Le terme étendue fait référence à un ensemble de ressources avec un accès spécifique. Il permet d'attribuer le principal de sécurité approprié à un certain rôle. Limiter la portée signifie limiter la portée des ressources à risque si le principal de sécurité est compromis.

Azure RBAC permet de spécifier une étendue à quatre niveaux, notamment un niveau de groupe de gestion, un niveau d'abonnement, un niveau de groupe de ressources et un niveau de ressources. Azure structure les étendues dans une relation parent-enfant, chaque niveau de hiérarchie rendant l'étendue plus spécifique. Il permet d'attribuer des rôles à l'un des quatre niveaux. Cependant, notez que le niveau que l'on choisit détermine la façon dont le rôle est appliqué.



Azure permet également d'utiliser des groupes de gestion, un niveau de portée supérieur aux abonnements. Cependant, les groupes de gestion prennent en charge des hiérarchies complexes. Le schéma ci-après illustre un exemple de hiérarchie de groupes de gestion et d'abonnements.

Accès aux ressources en fonction des conditions

- **RBAC :**

Le contrôle d'accès basé sur les rôles (RBAC) est une méthode permettant de restreindre l'accès au réseau en fonction des rôles des utilisateurs individuels. RBAC permet aux employés d'accéder uniquement aux informations dont ils ont besoin pour faire leur travail. Les rôles des employés dans une organisation déterminent les privilèges accordés aux individus et empêchent les employés de niveau inférieur d'accéder à des informations sensibles ou d'effectuer des tâches de niveau supérieur.

Dans le modèle de données de contrôle d'accès basé sur les rôles, les rôles sont basés sur plusieurs facteurs, notamment les autorisations, les responsabilités et les compétences professionnelles. Ce modèle permet aux entreprises de spécifier si les individus sont des utilisateurs finaux, des administrateurs ou des utilisateurs experts. De plus, l'accès d'un utilisateur aux ressources informatiques peut être limité à certaines opérations, telles que la visualisation, la création ou la modification de fichiers.

Les restrictions d'accès au réseau sont particulièrement importantes pour les organisations comptant un grand nombre d'employés et pour les organisations qui autorisent l'accès à des tiers tels que des clients et des fournisseurs, qui peuvent être difficiles à surveiller. Les entreprises qui s'appuient sur RBAC peuvent mieux protéger leurs données et applications sensibles.

Accès aux ressources en fonction des conditions

- **Fonctionnement du RBAC :**

Avant d'implémenter leRBAC dans une entreprise, l'organisation doit définir les autorisations pour chaque rôle aussi précisément que possible. Cela inclut la définition précise des autorisations dans les domaines suivants :

- Autorisations de modifier les données (par exemple, lecture, écriture, accès complet)
- Autorisation d'accéder aux applications de l'entreprise
- Autorisations dans une application

La première étape pour tirer le meilleur parti du RBAC consiste à modéliser les rôles et les autorisations. Cela comprend l'attribution de toutes les responsabilités des employés à des rôles spécifiques qui déterminent les privilèges appropriés. L'organisation peut alors attribuer des rôles en fonction des responsabilités des employés.

Le contrôle d'accès basé sur les rôles permet aux organisations d'attribuer un ou plusieurs rôles à chaque utilisateur ou d'attribuer des autorisations individuellement. L'objectif est de définir des autorisations permettant aux utilisateurs d'effectuer leurs tâches sans autres modifications.

Les organisations utilisent des systèmes de gestion des identités et des accès (IAM) pour mettre en œuvre et surveiller le RBAC. Un IAM prend principalement en charge les entreprises comptant un grand nombre d'employés en enregistrant, surveillant et mettant à jour toutes les identités et les autorisations. L'attribution d'une autorisation est appelée "provisioning" et la suppression d'une autorisation est appelée "deprovisioning". Ce type de système exige des organisations qu'elles établissent un ensemble de rôles unifié et normalisé.

Accès aux ressources en fonction des conditions

- **Rôle du RBAC :**

Dans le cadre du RBAC, les rôles sont une sémantique que les organisations peuvent utiliser pour créer leurs privilèges. Les rôles peuvent être définis par divers critères, tels que l'autorité, la responsabilité, le centre de coûts, l'unité commerciale, etc.

Un rôle est un ensemble de privilèges utilisateur. Les rôles sont différents des groupes traditionnels, qui sont des ensembles d'utilisateurs. Dans le contexte du RBAC, les autorisations ne sont pas directement associées aux identités mais plutôt aux rôles. Les rôles sont plus fiables que les groupes car ils sont organisés autour de la gestion des accès. Dans une organisation classique, les fonctionnalités et les activités changent moins fréquemment que les identités.

Accès aux ressources en fonction des conditions

- **Modèles de RBAC :**

Il existe trois types de contrôle d'accès dans la norme RBAC : de base, hiérarchique et restrictif.

→ RBAC de base:

Le modèle de base décrit les éléments clés d'un système de contrôle d'accès basé sur les rôles. Core RBAC peut servir de méthode de contrôle d'accès autonome, mais il constitue également la base des modèles hiérarchiques et de contraintes.

Tous les modèles de RBAC doivent respecter les règles suivantes :

- Attribution de rôle : un sujet ne peut exercer des privilèges que lorsqu'un rôle lui est attribué.
- Autorisation de rôle : le système doit autoriser le rôle actif d'un sujet.
- Autorisation d'autorisation : un sujet ne peut appliquer que les autorisations accordées au rôle actif du sujet.

→ RBAC hiérarchique:

Le RBAC hiérarchique s'appuie sur le modèle de RBAC de base et introduit une hiérarchie des rôles. Une hiérarchie de rôles est un moyen de structurer les rôles pour refléter une structure organisationnelle complexe et permettre le partage et l'héritage des autorisations entre les rôles. Un exemple simple de RBAC hiérarchique est une série de rôles, dans laquelle chaque rôle hérite des autorisations du précédent et ajoute d'autres autorisations :

Accès aux ressources en fonction des conditions

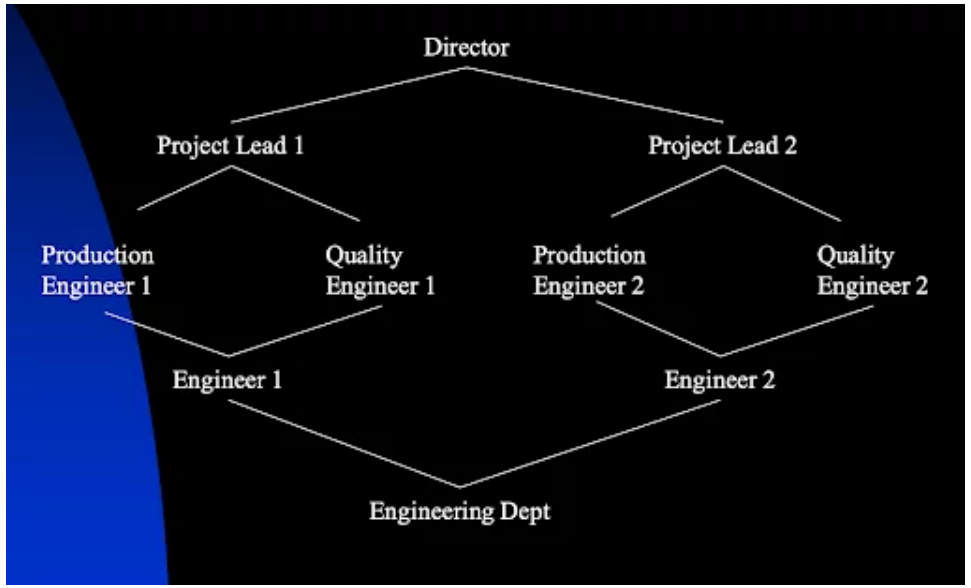
- Utilisateur invité – autorisations limitées
- Utilisateur régulier - mêmes autorisations que l'utilisateur invité et plus
- Utilisateur avec pouvoir - mêmes autorisations que l'utilisateur régulier et plus
- Administrateur - mêmes autorisations qu'un utilisateur avec pouvoir et plus

Ceci est utile car toute autorisation ajoutée à l'utilisateur invité, par exemple, sera automatiquement ajoutée à tous les rôles.

Le RBAC hiérarchique prend en charge plusieurs types de hiérarchies :

- **Arborescence** - hiérarchie ascendante dans laquelle les éléments au bas de l'arborescence accordent des autorisations aux éléments supérieurs. Par exemple, en bas se trouve un rôle de service avec des autorisations générales, qui accorde des autorisations à plusieurs employés.
- **Arborescence inversée** - hiérarchie descendante dans laquelle les rôles seniors héritent de certaines de leurs autorisations pour les rôles juniors sous eux.
- **Treillis** - une combinaison de bas en haut et de haut en bas, où chaque rôle peut hériter des autorisations des nœuds en-dessous et au-dessus.

L'image ci-dessous illustre la hiérarchie.



Accès aux ressources en fonction des conditions

→ RBAC restreint:

Le RBAC contraint ajoute la séparation des tâches au modèle de base. Il existe deux types de séparation des tâches :

- Séparation statique des tâches (SSD) - aucun utilisateur ne peut avoir des rôles mutuellement exclusifs (tels que définis par l'organisation). SSD empêche, par exemple, une personne de faire des achats et d'approuver ces achats.
- Séparation dynamique des tâches (DSD) — les utilisateurs peuvent avoir des rôles conflictuels. Cependant, le même utilisateur ne peut pas remplir les deux rôles dans une même session. Cette contrainte aide à contrôler les menaces de sécurité internes, par exemple en appliquant une règle de deux personnes qui exige que deux utilisateurs différents approuvent une action.

Accès aux ressources en fonction des conditions

- **Azure RBAC:**

Azure RBAC est une implémentation réelle de RBAC qui aide les administrateurs à gérer l'accès aux ressources Azure et à définir exactement les actions qui peuvent y être effectuées. Azure RBAC est un système d'autorisation basé sur Azure Resource Manager (ARM).

Il existe trois éléments clés pour attribuer un rôle dans Azure.

- **Principal** : un utilisateur, un groupe, un principal de service ou une identité managée qui a demandé une ressource et a obtenu l'accès à la ressource.
- **Définition de rôle** : un ensemble d'autorisations sur diverses ressources Azure, associées au rôle attribué à un mandataire. Il définit les actions qu'un principal avec un certain rôle peut effectuer sur une ressource.
- **Étendue** : définit les ressources auxquelles le rôle donne accès et le niveau d'autorisation pour un ou plusieurs rôles.

Dans Azure, il est possible de définir des étendues directement au niveau du groupe de gestion, de l'abonnement, du groupe de ressources ou de la ressource individuelle. Les étendues ont une relation parent-enfant et la ressource enfant hérite des autorisations de la ressource parent.

Azure inclut plusieurs rôles intégrés basés sur les meilleures pratiques du secteur et les structures de ressources Azure. Azure offre également une compatibilité pour la création de rôles RBAC personnalisés en fonction des exigences d'une organisation.

Après avoir défini des rôles et cartographié des étendues à ces rôles, les administrateurs peuvent utiliser des attributions de rôle pour accorder l'accès à une étendue de rôle pour un ou plusieurs principaux de sécurité. Ils peuvent également annuler l'attribution des rôles si l'organisation doit supprimer l'accès. Les portées facilitent ainsi la gestion des permissions.

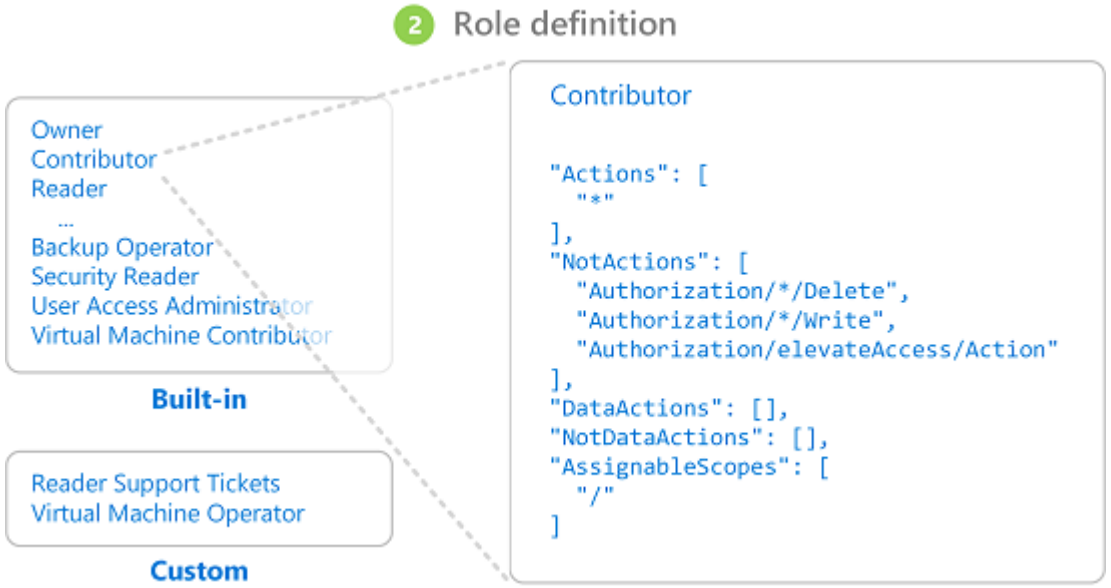
Accès aux ressources en fonction des conditions

- **Les rôles intégrés Azure :**

Le contrôle d'accès en fonction du rôle (RBAC) Azure a plusieurs rôles intégrés Azure qu'on peut affecter aux utilisateurs, groupes, principaux de service et identités managées. Les attributions de rôles permettent de contrôler l'accès aux ressources Azure.

Dans Azure RBAC, une définition de rôle est un ensemble d'autorisations (rôle).
Il définit les actions des utilisateurs, telles que l'écriture, la suppression et la lecture.
On peut définir des rôles de haut niveau, tels qu'un propriétaire, ou des rôles spécifiques, tels qu'un lecteur de machine virtuelle (VM).

Azure fournit divers rôles intégrés, notamment un rôle de contributeur de machine virtuelle qui permet aux utilisateurs de créer et de gérer des machines virtuelles.
Si les rôles intégrés ne répondent pas aux exigences d'une entreprise, on peut également définir des rôles personnalisés Azure. On peut utiliser des actions de données pour accorder l'accès aux données stockées dans un objet spécifique.



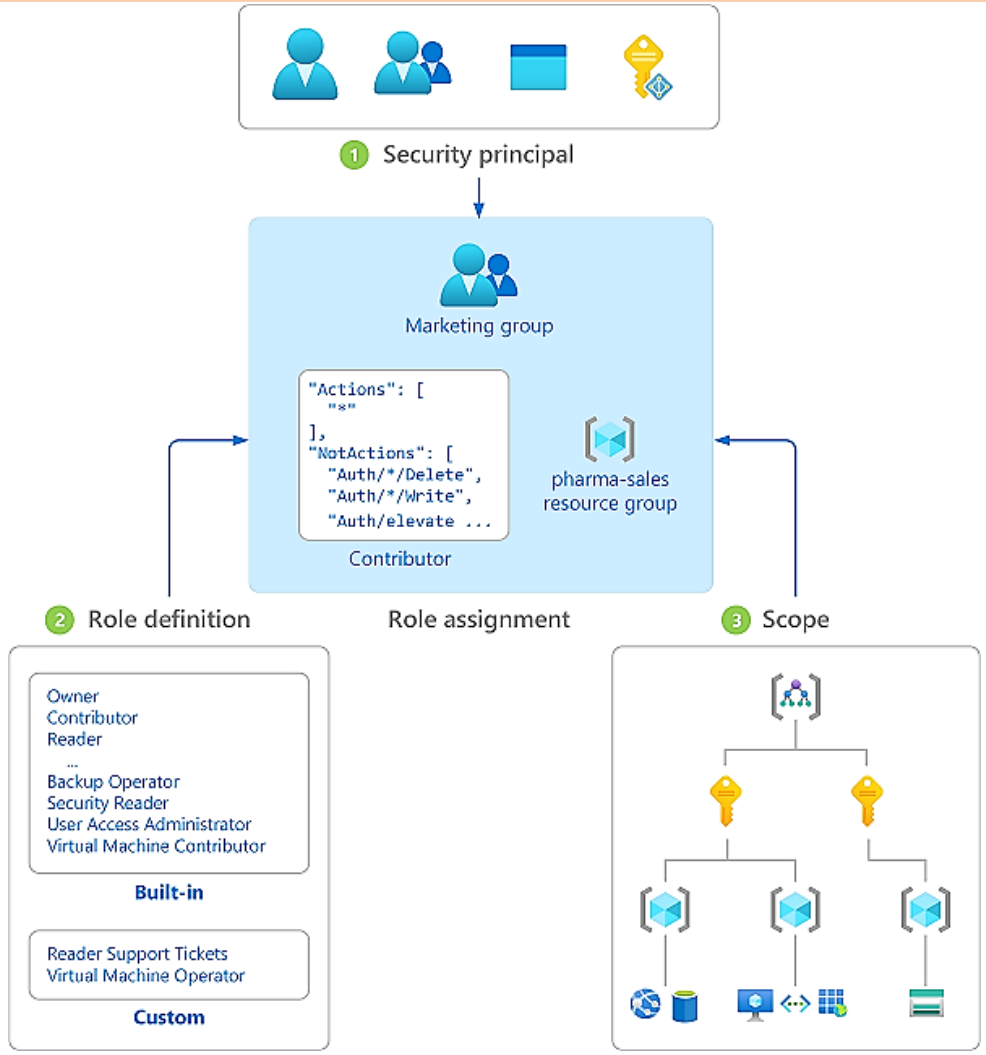
PARTIE 2

Accès aux ressources en fonction des conditions

- **Attributions des rôles:**

Les attributions de rôle permettent d'attacher des définitions de rôle à des utilisateurs, des groupes, des principaux de service ou des identités managées spécifiques dans une certaine
étendue. Lors de la création d'une attribution de rôle, on accorde un accès spécifique et la suppression de l'attribution révoque cet accès.

Voici un diagramme qui illustre un exemple d'attribution de rôle :



Cet exemple attribue un rôle de contributeur au groupe marketing, uniquement pour le groupe de ressources pharma-sales. Il permet à tous les utilisateurs du groupe marketing de créer ou de gérer des ressources Azure dans le groupe de ressources pharma-sales. Toutefois, il ne permet pas aux utilisateurs marketing d'accéder à des ressources externes au groupe de ressources pharma-sales.

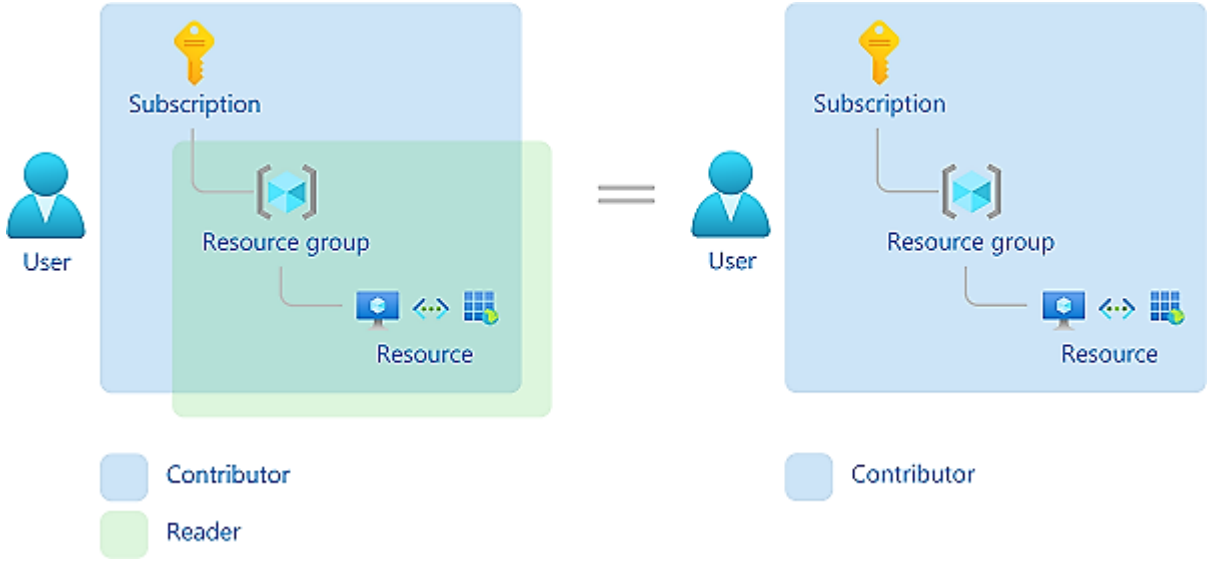
PARTIE 2

Accès aux ressources en fonction des conditions

- **Groupes Azure:**

Les attributions de rôles sont transitives pour les groupes, permettant aux utilisateurs d'obtenir des autorisations attribuées aux groupes. Si l'utilisateur A est membre du groupe B et que le groupe B est membre du groupe C avec sa propre attribution de rôle, l'utilisateur A obtient les autorisations dans l'attribution de rôle du groupe C.

Azure RBAC utilise un modèle additif pour éviter les problèmes lorsque les utilisateurs obtiennent plusieurs attributions de rôles qui se chevauchent. On peut voir un exemple de ce principe dans l'image ci-dessous. Un certain utilisateur se voit accorder un rôle de lecteur par un groupe de ressources et un rôle de contributeur au niveau de l'abonnement. La somme des autorisations de lecteur et de contributeur correspond au rôle de contributeur. L'attribution du rôle de lecteur n'a aucun impact.



PARTIE 2

Accès aux ressources en fonction des conditions

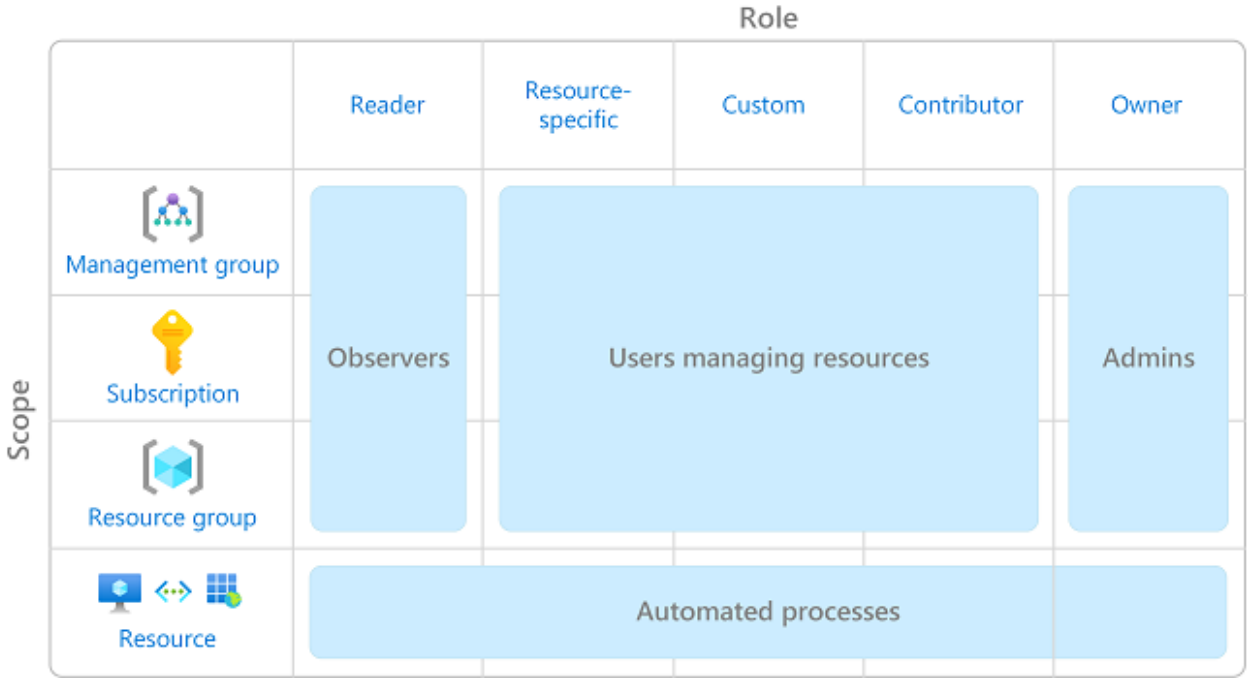
- **Bonnes pratiques Azure RBAC :**

→ Accorder uniquement l'accès dont les utilisateurs ont besoin:

Avec Azure RBAC, on peut créer une isolation entre différentes équipes, en accordant à chaque équipe uniquement l'accès dont elle a besoin pour faire le travail.

Au lieu d'accorder des autorisations illimitées à toutes les personnes disposant d'un abonnement ou d'une ressource Azure, on peut uniquement autoriser des actions spécifiques dans des étendues spécifiques. Il faut éviter d'attribuer des rôles larges, même s'ils semblent plus pratiques au premier abord. Lorsqu'on crée un rôle personnalisé, il vaut mieux inclure uniquement les autorisations dont les utilisateurs ont besoin. Cela garantit qu'il y a moins de risques si un compte principal est compromis.

Le diagramme suivant montre le modèle recommandé pour accorder des autorisations dans Azure RBAC.



Accès aux ressources en fonction des conditions

- **Bonnes pratiques Azure RBAC (suite) :**

→ Utiliser Azure AD Privileged Identity Management :

Pour protéger les comptes privilégiés contre les cyberattaques malveillantes, Azure Active Directory Privileged Identity Management (PIM) peut être utilisé pour réduire le temps d'émission de privilèges et améliorer la visibilité grâce à des rapports et des alertes. PIM aide à protéger les comptes privilégiés en fournissant un accès privilégié temporaire aux ressources Azure AD et Azure. L'accès est limité dans le temps, après quoi les privilèges sont automatiquement révoqués.

→ Attribuer des rôles à l'aide d'un ID de rôle unique au lieu du nom de rôle :

Les noms de rôle peuvent changer au fil du temps, mais l'ID de rôle reste toujours le même. Certains exemples courants de modification des noms de rôle sont lorsqu'on utilise son propre rôle personnalisé et que l'on décide de modifier le nom, ou lorsqu'on utilise un rôle d'aperçu dont le nom contient (Aperçu). Lorsque le rôle est libéré de l'aperçu, il est automatiquement renommé.

Pour garantir la cohérence dans le temps, il est conseillé de toujours affecter des utilisateurs à un ID de rôle lors de l'affectation de rôles à l'aide de scripts ou d'automatisations. De cette façon, les scripts ne se cassent pas si le nom change à l'avenir.

Accès aux ressources en fonction des conditions

- **Bonnes pratiques Azure RBAC (suite) :**

→ Attribuer des rôles aux groupes et limiter les propriétaires d'abonnements:

Pour faciliter la gestion des attributions de rôles, n'attribuez pas de rôles directement aux utilisateurs. Au lieu de cela, attribuez des rôles aux groupes. L'attribution de rôles à des groupes plutôt qu'à des utilisateurs réduit le nombre d'attributions de rôles. Il faut noter qu'Azure impose des restrictions sur le nombre total d'attributions de rôles autorisées par abonnement.

Microsoft recommande d'avoir un maximum de 3 propriétaires pour chaque abonnement Azure, afin de réduire la probabilité d'une violation par un initié compromis ou malveillant.

OFPPT
La Voie de l'Avenir

WEBFORCE
BE THE CHANGE

CHAPITRE 4

Protéger les données

Ce que vous allez apprendre dans ce chapitre :

- Chiffrement au repos et en transit
- Techniques de masquage des données
- Sauvegarde et récupération
- Anonymisation des données

12 heures

CHAPITRE 4

Protéger les données

1. **Chiffrement au repos et en transit**
2. Techniques de masquage des données
3. Sauvegarde et récupération
4. Anonymisation des données

Chiffrement des données au repos

- **Définition:**

Le chiffrement est le codage sécurisé des informations utilisées pour protéger la confidentialité des données. La conception du chiffrement au repos dans Azure utilise le chiffrement symétrique pour chiffrer et déchiffrer rapidement de grandes quantités de données selon un modèle conceptuel simple :

- Une clé de chiffrement symétrique est utilisée pour chiffrer les données au fil de leur stockage.
- La clé de chiffrement est utilisée pour déchiffrer ces données au fil de leur préparation à une utilisation en mémoire.
- Les données peuvent être partitionnées, et des clés différentes peuvent être utilisées pour chaque partition.
- Les clés doivent être stockées dans un emplacement sécurisé doté d'un contrôle d'accès basé sur l'identité et de stratégies d'audit. Les clés de chiffrement des données qui sont stockées en dehors des emplacements sécurisés sont chiffrées avec une clé de chiffrement principale conservée dans un emplacement sécurisé.

Dans la pratique, les scénarios de gestion et de contrôle des clés, ainsi que les garanties de scalabilité et de disponibilité, nécessitent des mécanismes supplémentaires. Les concepts et les composants du chiffrement des données au repos de Microsoft Azure sont décrits ci-dessous.

Les données au repos incluent des informations qui se trouvent dans un stockage persistant sur un support physique, sous n'importe quel format numérique. Il peut s'agir de fichiers sur un support magnétique ou optique, de données archivées et de sauvegardes de données. Microsoft Azure offre une variété de solutions de stockage de données en fonction des besoins, y compris le stockage sur fichier, disque, objet blob et table. Microsoft fournit également le chiffrement pour protéger Azure SQL Database, Azure Cosmos DB et Azure Data Lake.

Le chiffrement des données au repos est disponible pour les modèles de Cloud SaaS (Software-as-a-Service), PaaS (Platform-as-a-Service) et IaaS (Infrastructure-as-a-Service). Cet article résume et fournit des ressources pour aider à utiliser les options de chiffrement Azure.

Chiffrement des données au repos

- **Objectif du chiffrement au repos :**

Le chiffrement au repos offre une protection des données pour les données stockées (au repos). Les attaques contre les données au repos sont notamment des tentatives d'obtenir un accès physique au matériel sur lequel les données sont stockées puis de compromettre les données qui y sont contenues. Dans une telle attaque, le disque dur d'un serveur peut avoir fait l'objet d'une mauvaise manipulation lors de la maintenance, permettant à un attaquant de retirer le disque dur. Plus tard, cet attaquant peut placer le disque dur dans un ordinateur qu'il contrôle pour tenter d'accéder aux données.

Le chiffrement au repos est conçu pour empêcher l'attaquant d'accéder aux données non chiffrées en garantissant que les données sont chiffrées quand elles sont sur le disque. Si un attaquant récupère un disque dur comprenant des données chiffrées, mais qu'il ne dispose pas des clés de chiffrement, il doit résoudre le chiffrement pour lire les données. Ce type d'attaque est beaucoup plus complexe et laborieux comparé aux attaques de données non chiffrées sur un disque dur. Pour cette raison, le chiffrement au repos est fortement recommandé et constitue une exigence de haute priorité pour de nombreuses organisations.

Le chiffrement au repos peut également être nécessaire pour les besoins de l'organisation en matière de gouvernance et de conformité des données. Les réglementations publiques et de l'industrie, comme HIPAA, PCI et FedRAMP définissent des protections spécifiques quant aux exigences de protection et de chiffrement des données. Le chiffrement au repos est une mesure obligatoire nécessaire à la conformité avec certaines de ces réglementations.

Chiffrement des données au repos

- **Objectif du chiffrement au repos (suite) :**

Non seulement le chiffrement au repos répond aux exigences de conformité et aux obligations réglementaires, mais il fournit une défense en profondeur. Microsoft Azure fournit une plateforme conforme destinée aux services, aux applications et aux données. Il fournit également une sécurité complète des équipements et des éléments physiques, un contrôle d'accès aux données et des fonctionnalités d'audit. Toutefois, il est important de mettre en œuvre des mesures de sécurité « superposées » supplémentaires en cas de défaillance de l'une des mesures de sécurité principales. Le chiffrement au repos propose une telle mesure de sécurité.

Microsoft s'engage à fournir des options de chiffrement au repos sur les services Cloud et à donner aux clients le contrôle des clés de chiffrement et la journalisation de l'utilisation des clés. En outre, Microsoft s'emploie à mettre en œuvre par défaut le chiffrement au repos de toutes les données des clients.

Chiffrement des données au repos

- **Modèles de chiffrement Azure :**

Azure prend en charge plusieurs modèles de chiffrement, notamment le chiffrement côté serveur à l'aide de clés gérées par le service, de clés gérées par le client dans Key Vault, ou de clés gérées par le client sur du matériel contrôlé par le client. Avec le chiffrement côté client, on peut gérer et stocker des clés localement ou dans un autre emplacement sûr.

→ Chiffrement côté client :

Le chiffrement côté client est effectué en dehors d'Azure. Il inclut :

- Les données chiffrées par une application qui s'exécute dans le centre de données du client ou par une application de service.
- Les données qui sont déjà chiffrées lorsqu'elles sont reçues par Azure.

Avec le chiffrement côté client, les fournisseurs de services Cloud n'ont pas accès aux clés de chiffrement et ne peuvent pas déchiffrer ces données. On conserve un contrôle total des clés.

→ Chiffrement côté serveur :

Les trois modèles de chiffrement côté serveur offrent différentes caractéristiques de gestion de clés, qu'on peut choisir en fonction des besoins :

Chiffrement des données au repos

- **Modèles de chiffrement Azure (suite) :**

→ Chiffrement côté serveur :

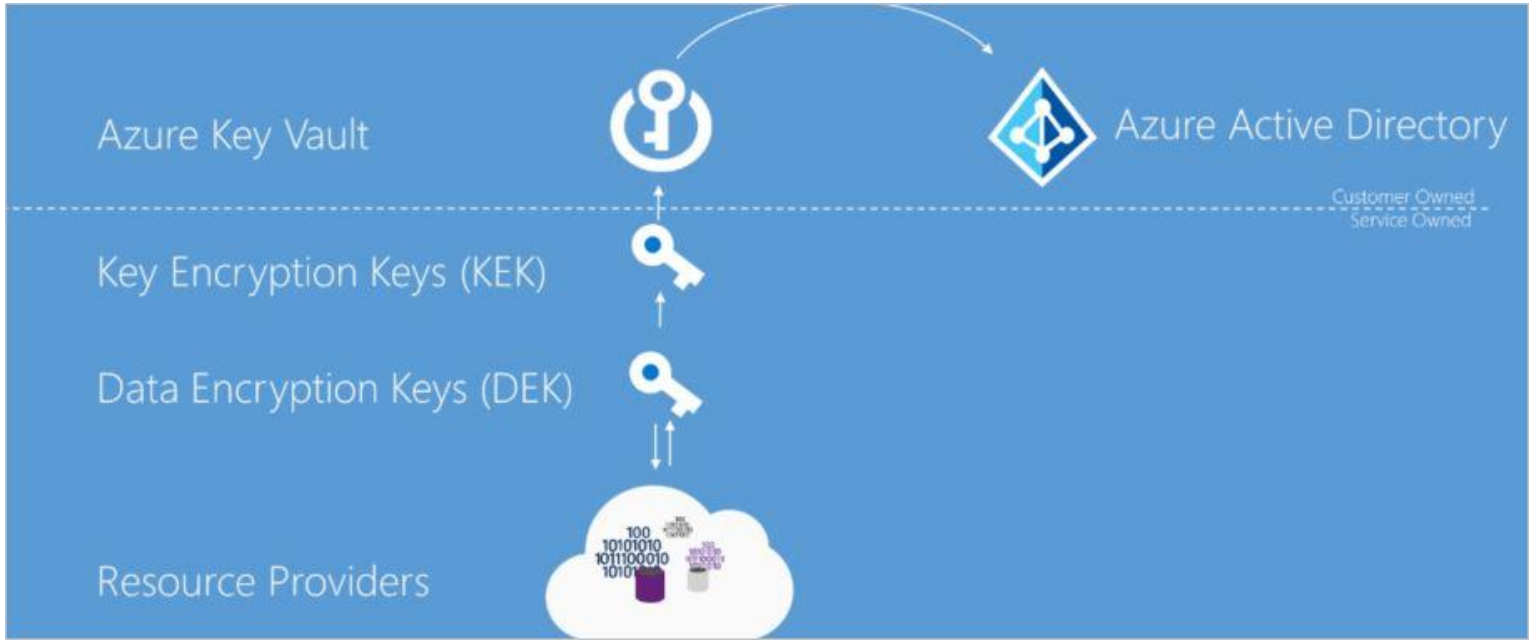
Les trois modèles de chiffrement côté serveur offrent différentes caractéristiques de gestion de clés, qu'on peut choisir en fonction des besoins :

- Clés gérées par le service : ce modèle fournit une combinaison de contrôles et de fonctionnalités avec une faible surcharge.
- Clés gérées par le client : ce modèle permet de contrôler les clés, avec notamment la prise en charge de BYOK (Bring Your Own Keys), ou d'en générer de nouvelles.
- Clés gérées par le service sur le matériel contrôlé par le client : ce modèle permet de gérer les clés dans le référentiel propriétaire, en dehors du contrôle de Microsoft. Cette caractéristique est appelée HYOK (Host Your Own Key). Toutefois, la configuration est complexe et la plupart des services Azure ne prennent pas en charge ce modèle.

Chiffrement des données au repos

- **Composants du chiffrement au repos d'Azure :**

Comme décrit dans les slides précédents, l'objectif du chiffrement au repos est que les données stockées sur disque soient chiffrées avec une clé de chiffrement secrète. Pour atteindre cet objectif de clés sécurisées, il est nécessaire de disposer d'un système permettant la création, le stockage, le contrôle d'accès et la gestion des clés de chiffrement. Bien que des détails puissent varier, les implémentations du chiffrement au repos des services Azure peuvent être décrites selon les termes illustrés dans le diagramme ci-dessous:



Chiffrement des données au repos

- **Composants du chiffrement au repos d'Azure (suite) :**

→ Azure Key Vault :

L'emplacement de stockage des clés de chiffrement et le contrôle d'accès à ces clés sont fondamentaux pour un modèle de chiffrement au repos. Les clés doivent être hautement sécurisées, mais gérables par des utilisateurs spécifiés et disponibles pour des services spécifiques. Pour les services Azure, Azure Key Vault est la solution de stockage des clés recommandée et offre une expérience de gestion commune entre les services. Les clés sont stockées et gérées dans des coffres de clés, et l'accès à un coffre de clés peut être donné à des utilisateurs ou à des services. Azure Key Vault prend en charge la création de clés par les clients ou l'importation de clés des clients pour les utiliser dans des scénarios où les clés de chiffrement sont gérées par ces clients.

→ Azure Active Directory :

Les autorisations d'utiliser les clés stockées dans Azure Key Vault, pour les gérer ou pour y accéder, pour les chiffrer et les déchiffrer dans le cadre du chiffrement au repos, peuvent être données à des comptes Azure Active Directory.

Chiffrement des données au repos

- **Composants du chiffrement au repos d'Azure (suite) :**

→ Chiffrement d'enveloppe avec une hiérarchie de clés :

Plusieurs clés de chiffrement sont utilisées dans une implémentation du chiffrement au repos. Le stockage d'une clé de chiffrement dans Azure Key Vault garantit l'accès sécurisé aux clés et la gestion centralisée des clés. Toutefois, l'accès local du service aux clés de chiffrement est plus efficace pour le chiffrement et le déchiffrement en bloc que d'interagir avec Key Vault pour chaque opération de données, ce qui permet un chiffrement renforcé et de meilleures performances. Limiter l'utilisation d'une seule clé de chiffrement réduit le risque que la clé soit compromise et le coût du re-chiffrement quand une clé doit être remplacée. Les modèles de chiffrement Azure au repos utilisent un chiffrement d'enveloppe où une clé de chiffrement à clé chiffre une clé de chiffrement de données. Ce modèle forme une hiérarchie de clés mieux adaptée pour répondre aux exigences en matière de performances et de sécurité :

- Clé de chiffrement de données (DEK) : clé AES256 symétrique utilisée pour chiffrer une partition ou un bloc de données, parfois simplement appelée clé de données. Une même ressource peut avoir plusieurs partitions et de nombreuses clés de chiffrement des données. Le chiffrement de chaque bloc de données avec une clé différente rend les attaques d'analyse du chiffrement plus difficiles. En gardant les clés de chiffrement locales pour le service, le chiffrement et le déchiffrement de données optimisent les performances.

- Clé de chiffrement à clé (KEK) : clé de chiffrement utilisée pour chiffrer les clés de chiffrement de données à l'aide d'un chiffrement d'enveloppe, également appelé encapsulation. L'utilisation d'une clé de chiffrement des clés ne quittant jamais le coffre de clés permet le chiffrement et le contrôle des clés de chiffrement des données elles-mêmes. L'entité qui a accès à la clé de chiffrement des clés peut être différente de l'entité qui a besoin de la clé de chiffrement des données. Une entité peut répartir l'accès à la clé de chiffrement des clés pour limiter l'accès de chaque clé de chiffrement des clés vers une partition spécifique. Étant donné que la KEK est requise pour déchiffrer les DEK, les clients peuvent effacer par chiffrement des DEK et des données en désactivant la KEK.

Chiffrement des données au repos

- **Chiffrement au repos dans les services Cloud Microsoft :**

Les services Microsoft Cloud sont utilisés dans les trois modèles de Cloud : IaaS, PaaS, SaaS. Voici des exemples de la façon dont ils s'adaptent sur chaque modèle :

- Services logiciel, appelés SaaS ou Software as a Service, qui ont des applications fournies par le Cloud, comme Microsoft 365.
- Services de plateforme dans lesquels les clients utilisent le Cloud pour des services tels que les fonctionnalités de stockage, d'analyse et de bus de service dans leurs applications.
- Services d'infrastructure, appelés IaaS ou Infrastructure as a Service, dans lesquels le client déploie des systèmes d'exploitation et des applications qui sont hébergés dans le Cloud, et tirant éventuellement parti d'autres services Cloud.

→ Chiffrement au repos pour les clients SaaS :

Les clients SaaS (Software as a Service) ont généralement le chiffrement au repos activé ou disponible dans chaque service. Microsoft 365 propose plusieurs options permettant aux clients de vérifier ou d'activer le chiffrement au repos.

→ Chiffrement au repos pour les clients PaaS :

Les données des clients PaaS (Platform as a Service) résident généralement dans un service de stockage tel que le Stockage Blob, mais peuvent également être mises en cache ou stockées dans l'environnement d'exécution des applications, par exemple, une machine virtuelle.

Chiffrement des données au repos

- **Chiffrement au repos dans les services Cloud Microsoft (suite) :**

→ Chiffrement au repos pour les clients IaaS :

Les clients IaaS (Infrastructure as a Service) peuvent utiliser différents services et applications. Les services IaaS peuvent activer le chiffrement au repos dans leurs machines virtuelles et leurs disques durs virtuels hébergés dans Azure en utilisant Azure Disk Encryption:

- Stockage chiffré :

Comme pour PaaS, les solutions IaaS peuvent tirer parti d'autres services Azure qui stockent les données chiffrées au repos. Dans ce cas, on peut activer la prise en charge du chiffrement au repos telle qu'elle est fournie par chaque service Azure utilisé.

- Calcul chiffré :

Tous les disques managés, instantanés et images sont chiffrés à l'aide de Storage Service Encryption au moyen d'une clé gérée par le service. Une solution plus complète de chiffrement au repos fait en sorte que les données ne soient jamais stockées sous une forme non chiffrée. Lors de leur traitement sur une machine virtuelle, les données peuvent être conservées dans le fichier d'échange Windows ou Linux, un vidage sur plantage ou le journal des applications. Pour garantir que ces données sont chiffrées au repos, les applications IaaS peuvent utiliser Azure Disk Encryption sur une machine virtuelle (Windows ou Linux) et sur un disque virtuel IaaS Azure.

- Chiffrement au repos personnalisé :

Il est recommandé que, dès que possible, les applications IaaS tirent parti des options d'Azure Disk Encryption et du chiffrement au repos fournis par les services Azure utilisés. Dans certains cas, comme en présence d'exigences de chiffrement irrégulières ou d'un stockage qui n'est pas basé sur Azure, le développeur d'une application IaaS peut être amené à implémenter lui-même le chiffrement au repos. Les développeurs de solutions IaaS peuvent mieux s'intégrer à la gestion d'Azure et répondre aux attentes des clients en tirant parti de certains composants Azure.

Chiffrement des données au repos

- **Prise en charge du modèle de chiffrement des fournisseurs de ressources Azure**

Les services Microsoft Azure prennent chacun en charge un ou plusieurs modèles de chiffrement au repos. Cependant, pour certains services, un ou plusieurs des modèles de chiffrement peuvent ne pas être applicables. Pour les services qui prennent en charge les scénarios de clé gérés par le client, ils peuvent prendre en charge uniquement un sous-ensemble des types de clés pris en charge par Azure Key Vault pour les clés de chiffrement à clé. En outre, les services peuvent prendre en charge ces scénarios et les types de clés selon des planifications différentes. Cette section décrit la prise en charge du chiffrement au repos au moment de la rédaction de ce document pour chacun des principaux services de stockage de données Azure.

→ Azure Disk Encryption :

Tout client utilisant les fonctionnalités IaaS d'Azure peut effectuer le chiffrement au repos pour ses machines virtuelles et ses disques IaaS via Azure Disk Encryption.

→ Stockage Azure :

Tous les services Stockage Azure (Stockage Blob, Stockage File d'attente, Stockage Table et Azure Files) prennent en charge le chiffrement au repos côté serveur ; certains services prennent également en charge les clés gérées par le client et le chiffrement côté client.

- Côté serveur : tous les services Stockage Azure permettent par défaut le chiffrement côté serveur avec des clés gérées par le service et une opération transparente pour l'application.
- Côté client : les objets blob, les tables et les files d'attente Azure prennent en charge le chiffrement côté client. Lors de l'utilisation du chiffrement côté client, les clients chiffrent les données et les chargent sous la forme d'un objet blob chiffré. La gestion des clés est effectuée par le client.

Chiffrement des données au repos

- **Prise en charge du modèle de chiffrement des fournisseurs de ressources Azure (suite)**

→ Azure SQL Database :

Azure SQL Database prend actuellement en charge le chiffrement au repos pour les scénarios de chiffrement côté service géré par Microsoft et côté client.

La prise en charge du chiffrement côté serveur est actuellement fournie par la fonctionnalité SQL nommée Transparent Data Encryption. Une fois qu'un client Azure SQL Database active Transparent Data Encryption, les clés sont créées et gérées automatiquement pour lui. Le chiffrement au repos peut être activé au niveau de la base de données et au niveau du serveur. À compter de juin 2017, Transparent Data Encryption (TDE) est activé par défaut sur les bases de données nouvellement créées. Azure SQL Database prend également en charge les clés RSA 2048 bits gérées par le client dans Azure Key Vault.

Le chiffrement côté client des données Azure SQL Database est pris en charge via la fonctionnalité Always Encrypted. Always Encrypted utilise une clé qui est créée et stockée par le client. Les clients peuvent stocker la clé principale dans un magasin de certificats Windows, dans Azure Key Vault ou dans un module de sécurité matériel local. Avec SQL Server Management Studio, les utilisateurs SQL choisissent quelle clé ils veulent utiliser pour quelle colonne.

Chiffrement des données en transit

- **Définition :**

Le terme chiffrement en transit est très clair. Il s'agit de protéger les données qui sont transférées d'un composant ou d'une couche à un autre composant ou une autre couche.

De nos jours, les systèmes distribués sont très courants et souvent les applications suivent une architecture de type micro-services . Ces micro-services s'envoient souvent des données les uns aux autres et, par conséquent, la protection des données en transit doit être connue de la plupart d'entre nous.

Ceci est réalisé en activant Transport Layer Security (TLS) . Pour les services basés sur HTTP, cela signifie utiliser le protocole HTTPS pour s'assurer que les données ne sont pas lisibles lorsqu'elles sont sur le fil.

- **Objectif du chiffrement des données en transit :**

La sécurité de la couche de transport garantit que personne ne peut écouter ou falsifier les messages lorsqu'ils sont en communication et en cours de transfert. Ainsi, non seulement il s'assure que les données sont sûres et protégées, mais il contribue également à maintenir l'intégrité des données.

- **Options du chiffrement des données en transit:**

La plupart des services Azure fournissent des paramètres de configuration pour activer TLS. Cette option est également activée par défaut et l'utilisateur peut la désactiver si, pour une raison quelconque, il n'en a pas besoin.

Chiffrement des données en transit

De plus, pour certains services comme les machines virtuelles RDP , on peut créer des VPN pour ajouter une autre couche de sécurité.

Il est également possible de créer des réseaux virtuels et d'en intégrer des services Azure au lieu de les exposer directement à internet. De cette façon, on peut configurer des règles de pare-feu et contrôler qui peut communiquer avec quel service.

On peut utiliser une passerelle VPN Azure pour envoyer du trafic chiffré entre le réseau virtuel et l'emplacement local via une connexion publique, ou pour envoyer du trafic entre des réseaux virtuels.

→ Chiffrement de la couche de liaison de données dans Azure :

Chaque fois que le trafic du client Azure s'effectue entre différents centres de données - en dehors des limites physiques non contrôlées par Microsoft (ou pour le compte de Microsoft) - une méthode de chiffrement de la couche de liaison de données utilisant les normes de sécurité MAC IEEE 802.1AE (également appelées MACsec) est appliquée de point à point sur le matériel réseau sous-jacent. Les paquets sont chiffrés et déchiffrés sur les appareils avant d'être envoyés, ce qui permet d'éviter les attaques physiques de l'intercepteur ou les attaques par snooping/écoutes téléphoniques.

Étant donné que cette technologie est intégrée au matériel réseau, elle fournit un chiffrement de débit de ligne sur le matériel réseau sans augmentation mesurable de la latence de la liaison. Ce chiffrement MACsec est activé par défaut pour tout le trafic Azure au sein d'une région ou entre des régions, et aucune intervention des clients n'est nécessaire pour l'activer.

Chiffrement des données en transit

→ Chiffrement TLS dans Azure :

Microsoft permet aux clients d'utiliser le protocole Transport Layer Security (TLS) pour protéger les données lorsqu'elles circulent entre les services Cloud et les clients. Les centres de données Microsoft négocient une connexion TLS avec les systèmes clients qui se connectent aux services Azure. TLS fournit une authentification forte, la confidentialité et l'intégrité des messages (activation de la détection de falsification et d'interception des messages), l'interopérabilité, la flexibilité des algorithmes, ainsi que la facilité de déploiement et d'utilisation.

Perfect Forward Secrecy (PFS) protège les connexions entre les systèmes clients des clients et les services Cloud de Microsoft par des clés uniques. Les connexions utilisent également les longueurs de clés de chiffrement RSA de 2 048 bits. Cette combinaison rend difficile pour une personne l'interception et l'accès aux données en transit.

→ Transactions de stockage Azure :

Si on interagit avec le stockage Azure via le portail Azure, toutes les transactions se produisent via HTTPS. L'API de stockage REST par le biais de HTTPS peut également être utilisée pour interagir avec le stockage Azure. On peut appliquer l'utilisation du protocole HTTPS quand on appelle les API REST pour accéder aux objets dans les comptes de stockage en activant le transfert sécurisé requis pour le compte de stockage.

Les signatures d'accès partagé (SAP), qui peuvent être utilisées pour déléguer l'accès aux objets de stockage Azure, incluent une option pour spécifier que seul le protocole HTTPS est autorisé quand on utilise des signatures d'accès partagé. Cette approche garantit que toute personne envoyant des liens avec des jetons SAP utilise le protocole approprié.

SMB 3.0, qui est utilisé pour accéder à Azure File Shares, prend en charge le chiffrement et est disponible dans Windows Server 2012 R2, Windows 8, Windows 8.1 et Windows 10. Cela rend possible l'accès entre les régions et même l'accès sur le bureau.

Le chiffrement côté client chiffre les données avant qu'elles soient envoyées à l'instance Stockage Azure de l'organisation, afin qu'elles soient chiffrées quand elles transitent sur le réseau.

Chiffrement des données en transit

→ Chiffrement SMB sur les réseaux virtuels Azure :

En utilisant SMB 3.0 sur des machines virtuelles qui exécutent Windows Server 2012 ou version ultérieure, on peut sécuriser les transferts de données en chiffrant les données en transit sur des réseaux virtuels Azure. Le chiffrement des données offre une protection contre la falsification et les attaques d'écoute. Les administrateurs peuvent activer le chiffrement SMB pour l'ensemble du serveur ou juste pour des partages spécifiques.

Par défaut, une fois le chiffrement SMB activé pour un partage ou un serveur, seuls les clients SMB 3.0 sont autorisés à accéder aux partages chiffrés.

→ Chiffrement en transit sur des machines virtuelles :

Les données en transit vers, à partir de et entre les machines virtuelles exécutant Windows peuvent être chiffrées de différentes manières, en fonction de la nature de la connexion.

- **Sessions RDP :**

  On peut se connecter et ouvrir une session sur une machine virtuelle à l'aide du protocole RDP (Remote Desktop Protocol) à partir d'un ordinateur client Windows ou d'un Mac avec un client RDP installé. Les données en transit sur le réseau dans les sessions RDP peuvent être protégées par le TLS.

  On peut également utiliser le Bureau à distance pour se connecter à une machine virtuelle Linux dans Azure.

- **Sécuriser l'accès aux machines virtuelles Linux avec SSH :**

  Pour la gestion à distance, on peut utiliser Secure Shell (SSH) afin de se connecter aux machines virtuelles Linux exécutées dans Azure. SSH est un protocole de connexion chiffré qui permet d'ouvrir des sessions en toute sécurité à travers des connexions non sécurisées. Il s'agit du protocole de connexion par défaut pour les machines virtuelles Linux hébergées dans Azure. En faisant appel à des clés SSH pour l'authentification, on élimine le besoin de mots de passe pour se connecter. SSH utilise une paire de clés publique/privée (chiffrement asymétrique) pour l'authentification.

Chiffrement des données en transit

→ Chiffrement VPN Azure :

On peut se connecter à Azure via un réseau privé virtuel qui crée un tunnel sécurisé pour protéger la confidentialité des données envoyées sur le réseau.

- **Passerelles VPN Azure :**

On peut utiliser la passerelle VPN Azure pour envoyer un trafic chiffré entre le réseau virtuel et l'emplacement local sur une connexion publique, ou pour envoyer un trafic entre des réseaux virtuels.

Les VPN de site à site utilisent IPsec pour le chiffrement du transport. Les passerelles VPN Azure utilisent un ensemble de propositions par défaut. On peut configurer des passerelles VPN Azure pour utiliser une stratégie IPsec/IKE personnalisée avec des algorithmes de chiffrement spécifiques et des avantages clés, plutôt que des ensembles de stratégies Azure par défaut.

- **VPN point à site :**

Les VPN point à site permettent à des ordinateurs clients d'accéder à un réseau virtuel Azure. Le protocole SSTP (Secure Socket Tunneling Protocol) est utilisé pour créer le tunnel VPN. Il peut traverser des pare-feux (le tunnel apparaît en tant que connexion HTTPS). On peut utiliser l'autorité de certification racine interne d'infrastructure à clé publique de l'entreprise pour la connectivité point à site.

On peut configurer une connexion VPN point à site à un réseau virtuel à l'aide du portail Azure avec l'authentification par certificat ou PowerShell.

- **VPN site à site :**

On peut utiliser une connexion de passerelle VPN de site à site pour connecter le réseau local à un réseau virtuel Azure par le biais d'un tunnel VPN IPsec/IKE (IKEv1 ou IKEv2). Ce type de connexion nécessite un périphérique VPN local disposant d'une adresse IP publique exposée en externe.

On peut configurer une connexion VPN de site à site à un réseau virtuel à l'aide du portail Azure, de PowerShell ou d'Azure CLI.

Chiffrement des données en transit

→ Chiffrement en transit dans Data Lake :

Les données en transit (ou données en mouvement) sont également toujours chiffrées dans Data Lake Store. Outre le chiffrement des données avant leur stockage sur un support permanent, les données sont également toujours sécurisées en transit à l'aide du protocole HTTPS. HTTPS est le seul protocole pris en charge pour les interfaces REST Data Lake Store.

→ Gestion des clés dans Key Vault :

Sans protection appropriée et la gestion des clés, le chiffrement est rendu inutilisable. Key Vault est la solution recommandée de Microsoft qui permet de gérer et de contrôler l'accès aux clés de chiffrement utilisées par les services Cloud. Les autorisations d'accès aux clés peuvent être attribuées aux services ou aux utilisateurs via des comptes Azure Active Directory.

Key Vault soulage les entreprises de la nécessité de configurer, de corriger et de tenir à jour des modules de sécurité matériels (HSM) et des logiciels de gestion de clés. Quand on utilise Key Vault, on conserve le contrôle. Microsoft ne voit jamais les clés des utilisateurs, et les applications n'y ont pas accès directement. On peut également importer ou générer des clés dans les modules HSM.

CHAPITRE 4

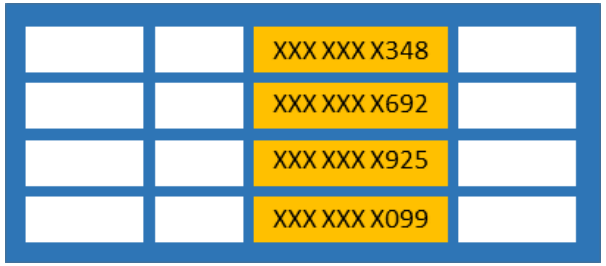
Protéger les données

1. Chiffrement au repos et en transit
2. **Techniques de masquage des données**
3. Sauvegarde et récupération
4. Anonymisation des données

Techniques de masquage des données

- **Masquage des données :**

Le masquage des données permet de cacher une partie des données sensibles à l'aide d'une fonction. Par exemple, lors d'un achat par carte de crédit, seuls les 4 derniers chiffres sont visibles. Le masquage des données d'un projet data permet de protéger les informations sensibles des consommateurs. Il convient de déterminer les champs à masquer pour éviter de partager des données confidentielles ou sensibles.



- **Masquage dynamique des données sur Azure :**

Le masquage dynamique des données (DDM) limite l'exposition des données sensibles en les masquant aux utilisateurs sans privilèges. Il peut être utilisé pour simplifier considérablement la conception et le codage de la sécurité dans une application.

Le masquage dynamique des données permet d'empêcher les accès non autorisés à des données sensibles. Pour cela, les clients peuvent spécifier la quantité de données sensibles à exposer avec un impact minimal sur la couche Application. Il peut être configuré sur les champs de la base de données désignés afin de masquer les données sensibles dans les jeux de résultats des requêtes. Avec la fonctionnalité DDM, les données figurant dans la base de données ne sont pas modifiées. La fonctionnalité DDM est facile à utiliser avec des applications existantes, car les règles de masquage sont appliquées dans les résultats de la requête. De nombreuses applications peuvent masquer des données sensibles sans modifier les requêtes existantes.

- Une stratégie de masquage des données centrale agit directement sur les champs sensibles de la base de données.
- Désigner les utilisateurs ou les rôles privilégiés qui ont accès aux données sensibles.
- Le masquage dynamique des données a des fonctions de masquage complet et partiel, ainsi qu'un masque aléatoire pour les données numériques.
- Des commandes Transact-SQL simples définissent et gèrent les masques.

Masquage dynamique des données sur Azure

Le masquage des données dynamique vise à limiter l'exposition des données sensibles, en empêchant les utilisateurs qui ne doivent pas pouvoir y accéder de les consulter. En revanche, le masquage des données dynamique n'a pas pour but d'empêcher des utilisateurs d'une base de données de se connecter directement à celle-ci ou d'exécuter des requêtes exhaustives ayant pour effet d'exposer des éléments de données sensibles. Le masquage des données dynamique est complémentaire à d'autres fonctionnalités de sécurité de SQL Server (audit, chiffrement, sécurité au niveau des lignes, etc.). Il est vivement recommandé de l'utiliser avec celles-ci pour mieux protéger les données sensibles contenues dans la base de données.

Le masquage des données dynamiques est disponible dans SQL Server 2016 (13.x) et Azure SQL Database. On le configure à l'aide de commandes Transact-SQL.

- **Définition d'un masque dynamique des données :**

Fonction	Description	Exemple
Default	Masquage complet en fonction des types de données des champs désignés. Pour les données de type chaîne (string), utiliser XXXX ou moins de X si la taille du champ est inférieure à 4 caractères (**char, nchar, varchar, nvarchar, text, ntext**). Pour les données de type numérique, utiliser une valeur zéro (**bigint, bit, decimal, int, money, numeric, smallint, smallmoney, tinyint, float, real**). Pour les données de type date et heure, utilisez 01.01.1900 00:00:00.0000000 (**date, datetime2, datetime, datetimeoffset, smalldatetime, time**). Pour les données de type binaire, utiliser un seul octet de valeur ASCII 0 (**binary, varbinary, image**).	Exemple de syntaxe de définition de colonne : Phone# varchar(12) MASKED WITH (FUNCTION = 'default()') NULL Exemple de syntaxe alter : ALTER COLUMN Gender ADD MASKED WITH (FUNCTION = 'default()')

Masquage dynamique des données sur Azure

- **Définition d'un masque dynamique des données (suite) :**

Fonction	Description	Exemple
E-mail	Méthode de masquage qui affiche la première lettre d'une adresse de messagerie et le suffixe de constante « .com », sous la forme d'une adresse de messagerie. aXXX@XXXX.com.	Exemple de syntaxe de définition : Email varchar(100) MASKED WITH (FUNCTION = 'email()') NULL Exemple de syntaxe alter : ALTER COLUMN Email ADD MASKED WITH (FUNCTION = 'email()')
Aléatoire	Fonction de masquage aléatoire à utiliser sur tout type de donnée numérique pour masquer la valeur d'origine à l'aide d'une valeur aléatoire dans une plage spécifiée.	Exemple de syntaxe de définition : Account_Number bigint MASKED WITH (FUNCTION = 'random([start range], [end range])') Exemple de syntaxe alter : ALTER COLUMN [Month] ADD MASKED WITH (FUNCTION = 'random(1, 12)')

Masquage dynamique des données sur Azure

- **Définition d'un masque dynamique des données (suite) :**

Fonction	Description	Exemple
Chaîne personnalisée	Méthode de masquage qui affiche la première et la dernière lettres, et ajoute une chaîne de remplissage personnalisée au milieu. prefix,[padding],suffix Remarque : Si la valeur d'origine est trop courte pour occuper la totalité du masque, une partie du préfixe ou du suffixe n'est pas exposée.	Exemple de syntaxe de définition : FirstName varchar(100) MASKED WITH (FUNCTION = 'partial(prefix,[padding],suffix)') NULL Exemple de syntaxe alter : ALTER COLUMN [Phone Number] ADD MASKED WITH (FUNCTION = 'partial(1,"XXXXXXX",0)') Autre exemple : ALTER COLUMN [Phone Number] ADD MASKED WITH (FUNCTION = 'partial(5,"XXXXXXX",0)')

Masquage dynamique des données sur Azure

- **Définition d'un masque dynamique des données (suite) :**

Fonction	Description	Exemple
Datetime	S'applique à : SQL Server 2022 Méthode de masquage pour la colonne définie avec le type de données **datetime, datetime2, date, time, datetimeoffset, smalldatetime**. Cela permet de masquer la partie **year => datetime("Y"), month=> datetime("M"), day=>datetime("D"), hour=>datetime("h"), minute=>datetime("m")** ou **seconds=>datetime("s")** du jour	Exemple de masquage de l'année pour la valeur datetime : ALTER COLUMN BirthDay ADD MASKED WITH (FUNCTION = 'datetime("Y")') Exemple de masquage du mois pour la valeur datetime : ALTER COLUMN BirthDay ADD MASKED WITH (FUNCTION = 'datetime("M")') Exemple de masquage des minutes pour la valeur datetime : ALTER COLUMN BirthDay ADD MASKED WITH (FUNCTION = 'datetime("m")')

PARTIE 2

Masquage dynamique des données sur Azure

- **Autorisations :**

Aucune autorisation spéciale n'est requise pour créer une table avec un masque de données dynamique. Les autorisations de schéma standard CREATE TABLE et ALTER suffisent.

Pour ajouter, remplacer ou supprimer le masque d'une colonne, on doit disposer des autorisations ALTER ANY MASK et ALTER sur la table. Il convient d'octroyer l'autorisation ALTER ANY MASK à un responsable sécurité.

Les utilisateurs disposant de l'autorisation SELECT sur une table peuvent afficher les données de celle-ci. Les colonnes définies comme masquées affichent alors les données masquées. Accorder l'autorisation UNMASK à un utilisateur pour lui permettre de récupérer les données non masquées de colonnes pour lesquelles un masquage est défini.

L'autorisation CONTROL sur la base de données inclut les autorisations ALTER ANY MASK et UNMASK .

Remarques

L'autorisation UNMASK n'influence pas la visibilité des métadonnées : l'octroi de l'autorisation UNMASK seule ne divulgue pas de métadonnées. L'autorisation UNMASK doit toujours être accompagnée d'une autorisation SELECT pour avoir un effet. Exemple : Si on octroie UNMASK sur l'étendue d'une base de données et SELECT sur une table individuelle, l'utilisateur peut uniquement voir les métadonnées de la table individuelle sur laquelle il dispose de l'autorisation SELECT.

Masquage dynamique des données sur Azure

- **Bonnes pratiques et cas d'usage courants :**

- La création d'un masque sur une colonne n'empêche pas les mises à jour de celle-ci. Par conséquent, si les utilisateurs reçoivent des données masquées quand ils interrogent une colonne masquée, ils peuvent mettre à jour les données s'ils disposent d'autorisations en écriture. Il convient néanmoins d'utiliser une stratégie de contrôle d'accès appropriée pour limiter les autorisations de mise à jour.

- L'utilisation de **SELECT INTO** ou de **INSERT INTO** pour copier les données d'une colonne masquée dans une autre table a pour effet de masquer les données dans la table cible.

- Un masquage dynamique des données est appliqué pendant l'exécution d'opérations d'importation et d'exportation dans SQL Server . Une base de données contenant des colonnes masquées produit un fichier de données exportées dont les données sont masquées (en supposant qu'elle est exportée par un utilisateur sans privilèges **UNMASK**), et la base de données importée contient des données masquées statiquement.

Masquage dynamique des données sur Azure

- **Limitations et restrictions :**

Il n'est pas possible de définir une règle de masquage pour les types de colonnes suivants :

- Colonnes chiffrées (Always Encrypted)
- FILESTREAM
- COLUMN_SET, ou colonne éparse faisant partie d'un jeu de colonnes.
- Un masque ne peut pas être configuré sur une colonne calculée, mais si la colonne calculée dépend d'une colonne MASK, alors la colonne calculée retournera des données masquées.
- Une colonne avec masquage de données ne peut pas être une clé pour un index FULLTEXT.
- Colonne d'une table externe PolyBase.

L'ajout d'un masque de données dynamique est implémenté comme un changement de schéma dans la table sous-jacente, et ne peut donc pas être effectué sur une colonne ayant des dépendances. Pour contourner cette restriction, on peut tout d'abord supprimer la dépendance, puis ajouter le masque de données dynamique et recréer la dépendance. Par exemple, si la dépendance est liée à un index qui dépend de cette colonne, on peut supprimer l'index, ajouter le masque, puis recréer l'index dépendant.

Masquage dynamique des données sur Azure

- **Limitations et restrictions (suite) :**

L'ajout d'un masque de données dynamique est implémenté comme un changement de schéma dans la table sous-jacente, et ne peut donc pas être effectué sur une colonne ayant des dépendances. Pour contourner cette restriction, on peut tout d'abord supprimer la dépendance, puis ajouter le masque de données dynamique et recréer la dépendance. Par exemple, si la dépendance est liée à un index qui dépend de cette colonne, on peut supprimer l'index, ajouter le masque, puis recréer l'index dépendant.

Chaque fois que l'on projette une expression faisant référence à une colonne pour laquelle une fonction de masquage de données est définie, l'expression est également masquée. Quelle que soit la fonction (par défaut, e-mail, aléatoire, chaîne personnalisée) utilisée pour masquer la colonne référencée, l'expression résultante sera toujours masquée avec la fonction par défaut.

Les requêtes entre bases de données couvrant deux bases de données Azure SQL Database différentes ou des bases de données hébergées sur différentes instances de SQL Server et impliquant une opération quelconque de comparaison ou de jointure sur des colonnes MASKED fournissent des résultats incorrects. Les résultats retournés par le serveur distant sont déjà sous forme MASKED et ne conviennent pas aux opérations de comparaison ou de jointure effectuées localement.

Masquage dynamique des données sur Azure

- **Exemples**

→ Création d'un masque dynamique des données :

L'exemple suivant crée une table avec trois types différents de masques dynamiques des données. L'exemple remplit la table, puis affiche le résultat.

```
-- schema to contain user tables
CREATE SCHEMA Data;
GO

-- table with masked columns
CREATE TABLE Data.Membership(
    MemberID        int IDENTITY(1,1) NOT NULL PRIMARY KEY CLUSTERED,
    FirstName        varchar(100) MASKED WITH (FUNCTION = 'partial(1, "xxxxx", 1)') NULL,
    LastName        varchar(100) NOT NULL,
    Phone            varchar(12) MASKED WITH (FUNCTION = 'default()') NULL,
    Email            varchar(100) MASKED WITH (FUNCTION = 'email()') NOT NULL,
    DiscountCode    smallint MASKED WITH (FUNCTION = 'random(1, 100)') NULL
    );

-- inserting sample data
INSERT INTO Data.Membership (FirstName, LastName, Phone, Email, DiscountCode)
VALUES
('Roberto', 'Tamburello', '555.123.4567', 'RTamburello@contoso.com', 10),
('Janice', 'Galvin', '555.123.4568', 'JGalvin@contoso.com.co', 5),
('Shakti', 'Menon', '555.123.4570', 'SMenon@contoso.net', 50),
('Zheng', 'Mu', '555.123.4569', 'ZMu@contoso.net', 40);
```

PARTIE 2

Masquage dynamique des données sur Azure

- **Exemples**

→ Création d'un masque dynamique des données :

Un nouvel utilisateur est créé et reçoit l'autorisation SELECT sur le schéma où réside la table. Les requêtes exécutées en tant que **MaskingTestUser** affichent les données masquées.

```
CREATE USER MaskingTestUser WITHOUT LOGIN;

GRANT SELECT ON SCHEMA::Data TO MaskingTestUser;

  -- impersonate for testing:
EXECUTE AS USER = 'MaskingTestUser';

SELECT * FROM Data.Membership;

REVERT;
```

Le résultat montre les masques en modifiant les données de

1 Roberto Tamburello 555.123.4567 RTamburello@contoso.com 10

en

1 Rxxxxxo Tamburello xxxx RXXX@XXXX.com 91

où le nombre dans DiscountCode est aléatoire pour chaque résultat de requête.

Masquage dynamique des données sur Azure

- **Exemples :**

→ Ajout ou modification d'un masque sur une colonne existante :

Utiliser l'instruction ALTER TABLE pour ajouter un masque à une colonne existante de la table ou pour modifier le masque appliqué à cette colonne.

L'exemple suivant ajoute une fonction de masquage à la colonne LastName :

```
ALTER TABLE Data.Membership
ALTER COLUMN LastName ADD MASKED WITH (FUNCTION = 'partial(2,"xxxx",0)');
```

L'exemple suivant modifie une fonction de masquage appliquée à la colonne LastName :

```
ALTER TABLE Data.Membership
ALTER COLUMN LastName varchar(100) MASKED WITH (FUNCTION = 'default()');
```

Masquage dynamique des données sur Azure

- **Exemples d'autorisations précises :**

1- Créer un schéma pour contenir des tables utilisateur :

```
CREATE SCHEMA Data;
GO
```

2- Créer une table avec des colonnes masquées :

```
CREATE TABLE Data.Membership (
  MemberID int IDENTITY(1,1) NOT NULL PRIMARY KEY CLUSTERED,
  FirstName varchar(100) MASKED WITH (FUNCTION = 'partial(1, "xxxxx", 1)') NULL,
  LastName varchar(100) NOT NULL,
  Phone varchar(12) MASKED WITH (FUNCTION = 'default()') NULL,
  Email varchar(100) MASKED WITH (FUNCTION = 'email()') NOT NULL,
  DiscountCode smallint MASKED WITH (FUNCTION = 'random(1, 100)') NULL,
  BirthDay datetime MASKED WITH (FUNCTION = 'default()') NULL
);
```

Masquage dynamique des données sur Azure

- **Exemples d'autorisations précises (suite) :**

3- Insérer les exemples de données :

```
INSERT INTO Data.Membership (FirstName, LastName, Phone, Email, DiscountCode, BirthDay)
VALUES
('Roberto', 'Tamburello', '555.123.4567', 'RTamburello@contoso.com', 10, '1985-01-25 03:25:05'),
('Janice', 'Galvin', '555.123.4568', 'JGalvin@contoso.com.co', 5,'1990-05-14 11:30:00'),
('Shakti', 'Menon', '555.123.4570', 'SMenon@contoso.net', 50,'2004-02-29 14:20:10'),
('Zheng', 'Mu', '555.123.4569', 'ZMu@contoso.net', 40,'1990-03-01 06:00:00');
```

4- Créer un schéma pour contenir des tables de service :

```
CREATE SCHEMA Service;
GO
```

Masquage dynamique des données sur Azure

- **Exemples d'autorisations précises (suite) :**

5- Créer une table de service avec des colonnes masquées :

```
CREATE TABLE Service.Feedback (
    MemberID int IDENTITY(1,1) NOT NULL PRIMARY KEY CLUSTERED,
    Feedback varchar(100) MASKED WITH (FUNCTION = 'default()') NULL,
    Rating int MASKED WITH (FUNCTION='default()'),
    Received_On datetime)
    );
```

6- Insérer les exemples de données :

```
INSERT INTO Service.Feedback(Feedback,Rating,Received_On)
VALUES
('Good',4,'2022-01-25 11:25:05'),
('Excellent', 5, '2021-12-22 08:10:07'),
('Average', 3, '2021-09-15 09:00:00');
```

Masquage dynamique des données sur Azure

- **Exemples d'autorisations précises (suite) :**

7- Créer différents utilisateurs dans la base de données :

```
CREATE USER ServiceAttendant WITHOUT LOGIN;
GO

CREATE USER ServiceLead WITHOUT LOGIN;
GO

CREATE USER ServiceManager WITHOUT LOGIN;
GO

CREATE USER ServiceHead WITHOUT LOGIN;
GO
```

8- Accorder des autorisations de lecture aux utilisateurs de la base de données :

```
ALTER ROLE db_datareader ADD MEMBER ServiceAttendant;

ALTER ROLE db_datareader ADD MEMBER ServiceLead;

ALTER ROLE db_datareader ADD MEMBER ServiceManager;

ALTER ROLE db_datareader ADD MEMBER ServiceHead;
```

Masquage dynamique des données sur Azure

- **Exemples d'autorisations précises (suite) :**

9- Accorder différentes autorisations UNMASK aux utilisateurs :

```
--Grant column level UNMASK permission to ServiceAttendant
GRANT UNMASK ON Data.Membership(FirstName) TO ServiceAttendant;

-- Grant table level UNMASK permission to ServiceLead
GRANT UNMASK ON Data.Membership TO ServiceLead;

-- Grant schema level UNMASK permission to ServiceManager
GRANT UNMASK ON SCHEMA::Data TO ServiceManager;
GRANT UNMASK ON SCHEMA::Service TO ServiceManager;

--Grant database level UNMASK permission to ServiceHead;
GRANT UNMASK TO ServiceHead;
```

10- Interroger les données dans le contexte de l'utilisateur **ServiceAttendant** :

```
EXECUTE AS USER='ServiceAttendant';
SELECT MemberID,FirstName,LastName,Phone,Email,BirthDay FROM Data.   Membership;
SELECT MemberID,Feedback,Rating FROM Service.Feedback;
REVERT;
```

Masquage dynamique des données sur Azure

- **Exemples d'autorisations précises (suite) :**

11- Interroger les données dans le contexte de l'utilisateur **ServiceLead** :

```
EXECUTE AS USER='ServiceManager';
SELECT MemberID,FirstName,LastName,Phone,Email FROM Data.Membership;
SELECT MemberID,Feedback,Rating FROM Service.Feedback;
REVERT;
```

12- Interroger les données dans le contexte de l'utilisateur **ServiceManager** :

```
EXECUTE AS USER='ServiceHead';
SELECT MemberID,FirstName,LastName,Phone,Email,BirthDay FROM Data.Membership;
SELECT MemberID,Feedback,Rating FROM Service.Feedback;
REVERT;
```

Masquage dynamique des données sur Azure

- **Exemples d'autorisations précises (suite):**

13- Interroger les données dans le contexte de l'utilisateur **ServiceHead** :

```
EXECUTE AS USER='ServiceHead';
SELECT MemberID,FirstName,LastName,Phone,Email,BirthDay FROM Data.Membership;
SELECT MemberID,Feedback,Rating FROM Service.Feedback;
REVERT;
```

14- Pour révoquer les autorisations UNMASK, utiliser les instructions T-SQL suivantes :

```
REVOKE UNMASK ON Data.Membership(FirstName) FROM ServiceAttendant;

REVOKE UNMASK ON Data.Membership FROM ServiceLead;

REVOKE UNMASK ON SCHEMA::Data FROM ServiceManager;

REVOKE UNMASK ON SCHEMA::Service FROM ServiceManager;

REVOKE UNMASK FROM ServiceHead;
```

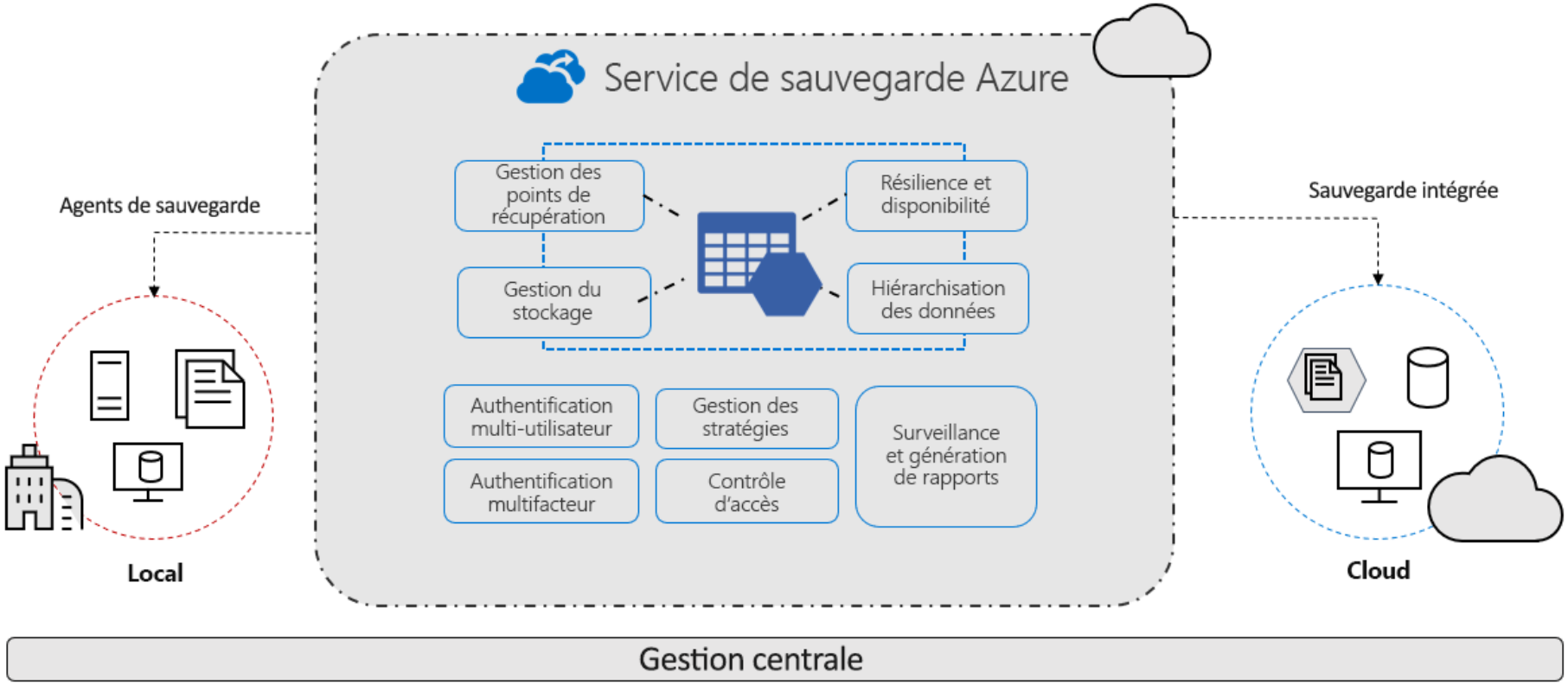
CHAPITRE 4

Protéger les données

1. Chiffrement au repos et en transit
2. Techniques de masquage des données
3. **Sauvegarde et récupération**
4. Anonymisation des données

Sauvegarde Azure

Le service de sauvegarde Azure fournit des solutions simples, sécurisées et rentables pour sauvegarder les données et les récupérer à partir du Cloud Microsoft Azure.



Sauvegarde Azure

- **Fonctionnement :**

On peut sauvegarder des machines et des données à l'aide de plusieurs méthodes :

- Sauvegarder des ordinateurs locaux :
    - On peut sauvegarder des machines Windows locales directement sur Azure à l'aide de l'agent Microsoft Azure Recovery Services (MARS) de Sauvegarde Azure. Les machines Linux ne sont pas prises en charge.
    - On peut sauvegarder des machines locales sur un serveur de sauvegarde (System Center Data Protection Manager [DPM] ou Serveur de sauvegarde Microsoft Azure [MABS]). On peut ensuite sauvegarder le serveur de sauvegarde dans un coffre Recovery Services dans Azure.
- Sauvegarder des machines virtuelles Azure :
    - On peut directement sauvegarder des machines virtuelles Azure. Le service Sauvegarde Azure installe une extension de sauvegarde de l'agent de machine virtuelle Azure qui s'exécute sur la machine virtuelle. Cette extension sauvegarde la totalité de la machine virtuelle.
    - On peut sauvegarder des fichiers et dossiers spécifiques sur la machine virtuelle Azure en exécutant l'agent MARS.
    - On peut sauvegarder des machines virtuelles Azure sur le Serveur Sauvegarde Microsoft Azure qui s'exécute dans Azure, puis sauvegarder ce serveur dans un coffre Recovery Services.

Sauvegarde Azure

- **Endroit de sauvegarde des données :**

Le service Sauvegarde Azure stocke les données sauvegardées dans des coffres Recovery Services et de sauvegarde. Un coffre est une entité de stockage en ligne dans Azure qui permet de conserver des données telles que des copies de sauvegarde, des points de récupération et des stratégies de sauvegarde.

Les coffres présentent les fonctionnalités suivantes :

- Les coffres facilitent l'organisation des données de sauvegarde, tout en réduisant le temps de gestion.
- On peut superviser les éléments sauvegardés dans un coffre, notamment les machines virtuelles Azure et les ordinateurs locaux.
- On peut gérer l'accès au coffre avec le contrôle d'accès en fonction du rôle Azure (Azure RBAC).
- On spécifie le mode de réplication des données dans le coffre pour la redondance :
    - Stockage localement redondant (LRS) : pour protéger les données contre les défaillances de rack de serveur et de lecteur, on peut utiliser le LRS. Le LRS réplique les données trois fois au sein d'un même centre de données dans la région primaire. Le stockage localement redondant offre une durabilité des objets d'au moins 99,999999999 % (11 « neuf ») sur une année donnée.
    - Stockage géo-redondant (GRS) : Pour se protéger contre des pannes régionales, on peut utiliser un stockage géo-redondant. Celui-ci réplique les données dans une région secondaire.
    - Stockage redondant interzone (ZRS) : réplique les données dans des zones de disponibilité, garantissant ainsi la résidence et la résilience des données dans la même région. Par défaut, les coffres Recovery Services utilisent un stockage géo-redondant.

Sauvegarde Azure

- **Endroit de sauvegarde des données (suite) :**

Les coffres Recovery Services offrent les fonctionnalités supplémentaires suivantes :

- Dans chaque abonnement Azure, on peut créer jusqu'à 500 coffres.

- **Agents de sauvegarde:**

Sauvegarde Azure fournit différents agents de sauvegarde, selon le type de machine sauvegardée :

Agent	Détails
Agent MARS	• S'exécute sur des serveurs Windows locaux pour sauvegarder des fichiers, des dossiers et l'état du système. • S'exécute sur des machines virtuelles Azure pour sauvegarder des fichiers, des dossiers et l'état du système. • S'exécute sur des serveurs DPM/MABS pour sauvegarder le disque de stockage DPM/MABS local sur Azure.
Extension de machine virtuelle Azure	• S'exécute sur des machines virtuelles Azure pour les sauvegarder dans un coffre.

Sauvegarde Azure

- **Types de sauvegarde :**

Le tableau suivant présente les différents types de sauvegardes et quand ils sont utilisés :

Type de sauvegarde	Détails	Utilisation
Complète	Une sauvegarde complète contient la source de données entière. Occupe davantage de bande passante réseau que les sauvegardes différentielles ou incrémentielles.	Utilisée pour la sauvegarde initiale.
Différentielle	Un sauvegarde différentielle stocke les blocs ayant changé depuis la sauvegarde complète initiale. Utilise une plus petite quantité de stockage et de réseau, et ne conserve pas de copies redondantes des données inchangées. Inefficace, car les blocs de données inchangés entre les sauvegardes successives sont transférés et stockés.	Non utilisée par Sauvegarde Azure.
Incrémentielle	Une sauvegarde incrémentielle stocke uniquement les blocs de données ayant changé depuis la sauvegarde précédente. Efficacité élevée du point de vue du stockage et du réseau. Avec une sauvegarde incrémentielle, il est inutile d'effectuer des sauvegardes complètes régulières.	Utilisée par DPM/MABS pour les sauvegardes sur disque, et utilisée dans toutes les sauvegardes vers Azure. Non utilisée pour la sauvegarde SQL Server.

Sauvegarde Azure

- **Types de sauvegarde SQL Server :**

Le tableau suivant présente les différents types de sauvegardes utilisées pour les bases de données SQL Server et la fréquence à laquelle elles sont utilisées :

Type de sauvegarde	Détails	Utilisation
Sauvegarde complète	Une sauvegarde complète de base de données sauvegarde l'intégralité de la base de données. Elle contient toutes les données d'une base de données spécifique ou d'un ensemble de fichiers ou de groupes de fichiers. Elle contient également suffisamment de journaux pour récupérer ces données.	On peut déclencher au plus une sauvegarde complète par jour. On peut choisir d'effectuer une sauvegarde complète à intervalle quotidien ou hebdomadaire.
Sauvegarde différentielle	Une sauvegarde différentielle est basée sur la sauvegarde de données complète précédente la plus récente. Elle capture uniquement les données qui ont changé depuis la sauvegarde complète.	On peut déclencher au plus une sauvegarde différentielle par jour. On ne peut pas configurer une sauvegarde complète et une sauvegarde différentielle le même jour.
Sauvegarde de fichier journal	Une sauvegarde de fichier journal permet d'effectuer une restauration ponctuelle à la seconde donnée.	Au plus, on peut configurer des sauvegardes du journal des transactions toutes les 15 minutes.

Sauvegarde Azure

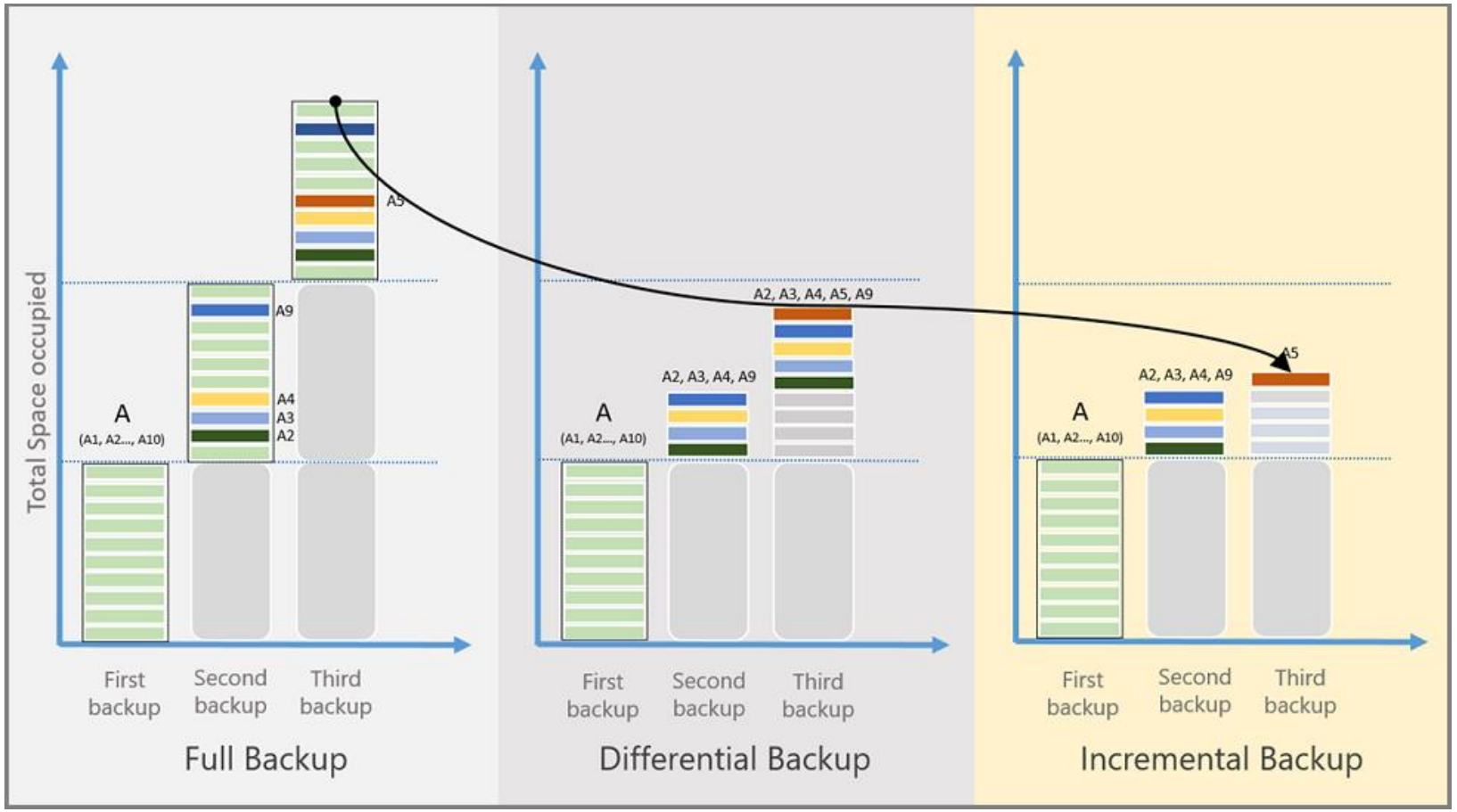
- **Comparaison des types de sauvegardes :**

La consommation du stockage, l'objectif de délai de récupération (RTO) et la consommation réseau varient pour chaque type de sauvegarde. L'illustration dans le slide suivant compare les types de sauvegarde :

- La source de données A est composée de 10 blocs de stockage A1-A10, qui sont sauvegardés mensuellement.
- Les blocs A2, A3, A4 et A9 ont changé lors du premier mois et le bloc A5 a changé lors du mois suivant.
- Pour les sauvegardes différentielles, le deuxième mois, les blocs A2, A3, A4 et A9 qui ont changé sont sauvegardés. Lors du troisième mois, ces mêmes blocs sont à nouveau sauvegardés, ainsi que le bloc A5 qui a changé. Les blocs modifiés continuent d'être sauvegardés jusqu'à la prochaine sauvegarde complète.
- Pour les sauvegardes incrémentielles, le deuxième mois, les blocs A2, A3, A4 et A9 sont marqués comme modifiés et transférés. Lors du troisième mois, seul le bloc A5 qui a changé est marqué et transféré.

Sauvegarde Azure

- **Comparaison des types de sauvegardes :**



Sauvegarde Azure

- **Fonctionnalités de sauvegarde :**

Le tableau suivant présente les différents types de sauvegardes utilisées pour les bases de données SQL Server et la fréquence à laquelle elles sont utilisées :

Fonctionnalité	Sauvegarde directe de fichiers et de dossiers (à l'aide de l'agent MARS)	Sauvegarde de machines virtuelles Azure	Ordinateurs ou applications avec DPM/MABS
Sauvegarder vers le coffre	Supporté	Supporté	Supporté
Sauvegarder sur disque DPM/MABS, puis sur Azure	Non supporté	Non supporté	Supporté
Compresser les données envoyées pour la sauvegarde	Supporté	Aucune compression n'est effectuée lors du transfert des données. Le stockage croît légèrement, mais la restauration est plus rapide.	Supporté
Exécuter une sauvegarde incrémentielle	Supporté	Supporté	Supporté
Sauvegarder les disques dédupliqués	Non supporté	Non supporté	Partiellement supporté. Uniquement pour les serveurs DPM/MABS déployés localement.

Sauvegarde Azure

- **Principes de base de la stratégie de sauvegarde :**
    - Une stratégie de sauvegarde est créée par coffre.
    - Une stratégie de sauvegarde peut être créée pour la sauvegarde des charges de travail suivantes : machines virtuelles Azure, SQL dans des machines virtuelles Azure, SAP HANA dans des machines virtuelles Azure et partages de fichiers Azure. La stratégie de sauvegarde des fichiers et des dossiers à l'aide de l'agent MARS est spécifiée dans la console MARS.
        - Partage de fichiers Azure
    - Une stratégie peut être attribuée à de nombreuses ressources. Une stratégie de sauvegarde de machine virtuelle Azure peut être utilisée pour protéger plusieurs machines virtuelles Azure.
    - Une stratégie est constituée de deux composants :
        - Planification : quand effectuer la sauvegarde.
        - Conservation : la durée de conservation de chaque sauvegarde.
    - La planification peut être définie comme « quotidienne » ou « hebdomadaire » avec un point de temps spécifique.
    - La rétention peut être définie pour les points de sauvegarde « quotidienne », « hebdomadaire », « mensuelle », « annuelle ».
        - « hebdomadaire » fait référence à une sauvegarde un certain jour de la semaine.
        - « mensuelle » fait référence à une sauvegarde un certain jour du mois.
        - « annuelle » fait référence à une sauvegarde un certain jour de l'année.

Sauvegarde Azure

- **Principes de base de la stratégie de sauvegarde (suite) :**
  - La rétention pour les points de sauvegarde « mensuelle » et « annuelle » est appelée rétention à long terme (LTR, Long Term Retention).
  - Lors de la création d'un coffre, une « DefaultPolicy » est également créée, qui peut être utilisée pour sauvegarder des ressources.
  - Toutes les modifications apportées à la période de rétention d'une stratégie de sauvegarde sont appliquées de manière rétroactive à tous les anciens points de récupération en plus des nouveaux.

Récupération Azure: Azure site Recovery

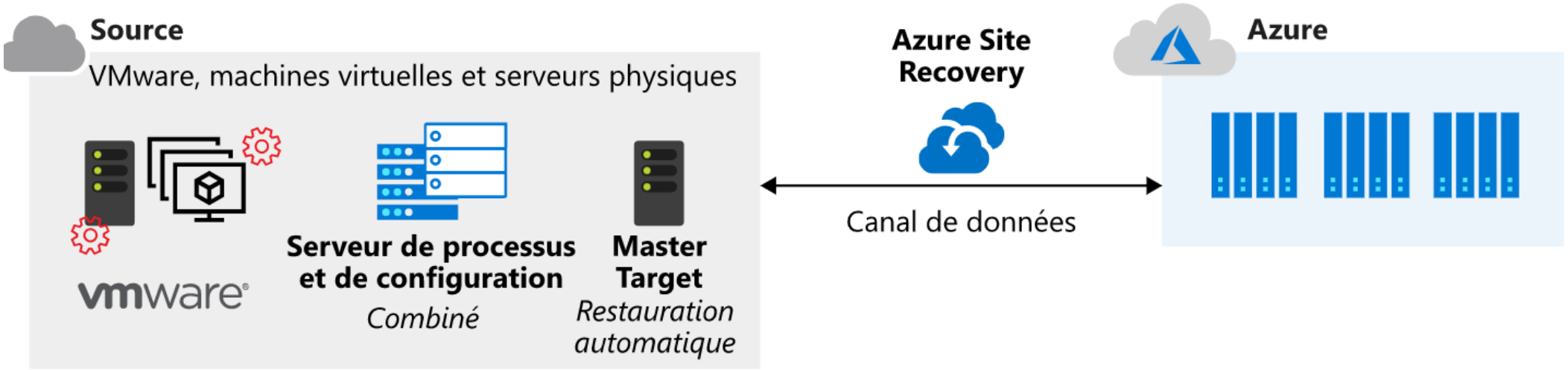
Azure Site Recovery peut contribuer à un plan BCDR, car il peut répliquer des charges de travail d'un site principal sur un site secondaire. Si un problème se produit dans le site principal, Site Recovery peut être appelé automatiquement pour répliquer les machines virtuelles protégées sur un autre emplacement. Le basculement peut se faire d'un emplacement local vers Azure ou d'une région Azure vers une autre.

Voici certaines des fonctionnalités remarquables d'Azure Site Recovery :

- Gestion centralisée : La réplication peut être configurée et gérée, et le basculement et la restauration automatique peuvent être appelés à partir du portail Azure.
- Réplication de machines virtuelles locales : Les machines virtuelles locales peuvent être répliquées si nécessaire vers Azure ou vers un centre de données local secondaire.
- Réplication de machines virtuelles Azure : Les machines virtuelles Azure peuvent être répliquées d'une région vers une autre.
- Cohérence des applications pendant le basculement : Avec les points de récupération et les instantanés de cohérence des applications, les machines virtuelles sont conservées dans un état cohérent à tout moment pendant la réplication.
- Basculement flexible : Les basculements peuvent être effectués à la demande en guise de test ou bien déclenchés lors d'un sinistre réel. On peut effectuer des tests pour simuler un scénario de reprise d'activité sans interruption du service actif de l'entreprise.
- Intégration réseau : Site Recovery peut prendre en charge la gestion du réseau pendant un scénario de réplication et de reprise d'activité. Les adresses IP réservées et les équilibreurs de charge sont inclus, afin que les machines virtuelles puissent fonctionner au nouvel emplacement.

Récupération Azure: Azure site Recovery

- **Configuration Azure Site Recovery :**



Serveur de processus - Utilisé pour la mise en cache, la compression et le chiffrement

Serveur de configuration - Utilisé pour la gestion centralisée

Master Target - Utilisé pour la restauration automatique uniquement

Service Mobilité
Capture toutes les écritures de données de la mémoire

PARTIE 2

Récupération Azure: Azure site Recovery

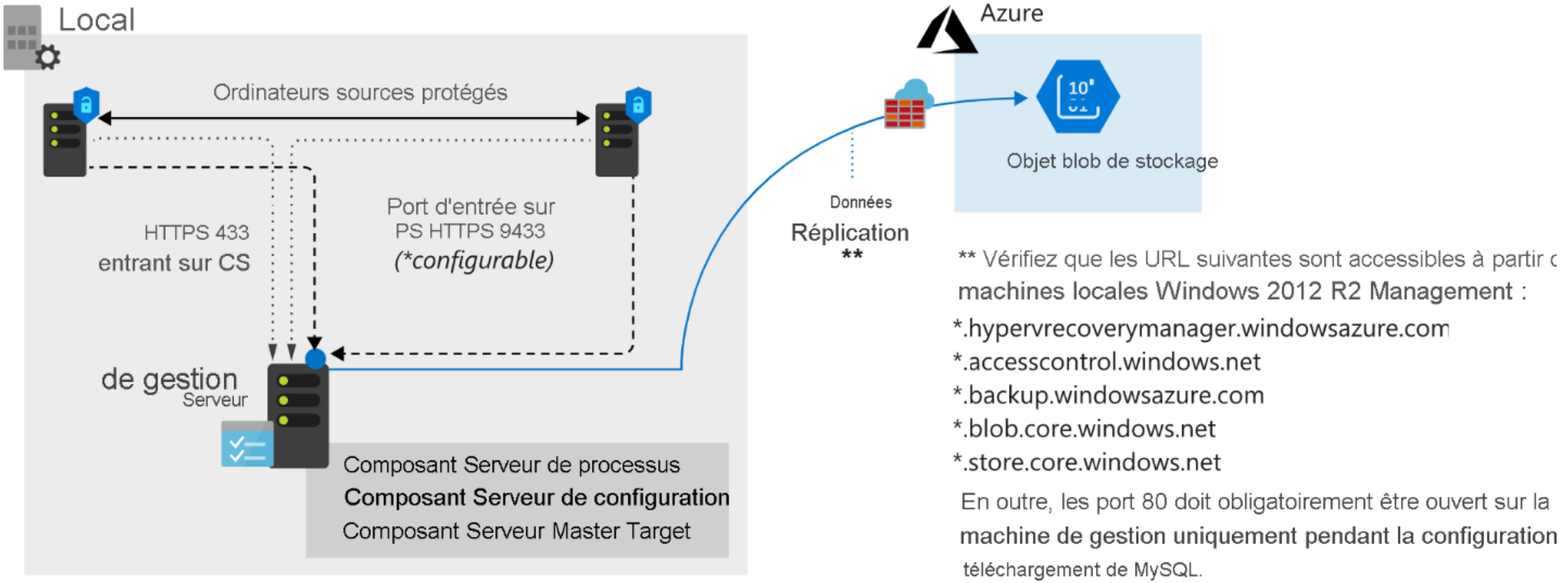
- **Configuration Azure Site Recovery :**

Plusieurs composants doivent être configurés pour activer Azure Site Recovery :

- **Réseau** : un réseau virtuel Azure valide est nécessaire pour les machines virtuelles répliquées à utiliser.
- **Coffre Recovery Services** : un coffre dans un abonnement Azure stocke les machines virtuelles migrées quand un basculement est effectué. Le coffre contient également la stratégie de réplication ainsi que les emplacements source et cible pour la réplication et le basculement.
- **Informations d'identification** : les informations d'identification qu'on utilise pour Azure doivent avoir les rôles Contributeur de machines virtuelles et Collaborateur Site Recovery pour pouvoir autoriser la modification tant de la machine virtuelle que le stockage auxquels Site Recovery est connecté.
- **Serveur de configuration** : un serveur VMware local remplit plusieurs rôles pendant le processus de basculement et de réplication. Il est obtenu à partir du portail Azure sous la forme d'une appliance de machine virtuelle ouverte (OVA) pour faciliter le déploiement. Le serveur de configuration comprend les composants suivants :
    - **Serveur de processus** : ce serveur joue le rôle de passerelle pour le trafic de réplication. Il met en cache, compresse et chiffre le trafic avant de l'envoyer via le WAN à Azure. Le serveur de processus installe également le service Mobilité sur toutes les machines physiques et virtuelles ciblées pour le basculement et la réplication.
    - **Serveur cible maître** : cette machine gère le processus de réplication lors d'une restauration automatique à partir d'Azure.

Récupération Azure: Azure site Recovery

- **Processus de réplication :**



PARTIE 2

Récupération Azure: Azure site Recovery

- **Processus de réplication :**

Une fois les tâches prérequises configurées, la réplication des machines peut commencer. Elles sont répliquées en fonction de la stratégie de réplication en place. Au cours des phases initiales de la première copie, les données du serveur sont répliquées sur Stockage Azure. Quand la réplication initiale se termine, une deuxième réplication se produit. Cette fois, les modifications d'ordre différentiel de la machine virtuelle sont répliquées sur Azure.

Récupération Azure: Azure site Recovery

- **Fonctionnalités de Azure site Recovery :**

Fonctionnalité	Description
Solution BCDR simple	Grâce à Site Recovery, on peut configurer et gérer la réplication, le basculement et la restauration automatique à partir d'un seul emplacement dans le portail Azure.
Réplication de machines virtuelles Azure	On peut configurer la récupération d'urgence de machines virtuelles Azure d'une région primaire vers une région secondaire.
Réplication de machines virtuelles VMware	On peut répliquer des machines virtuelles VMware sur Azure à l'aide de l'appliance de réplication Azure Site Recovery améliorée qui offre une meilleure sécurité et une meilleure résilience que le serveur de configuration.
Réplication de machines virtuelles locales	On peut répliquer des machines virtuelles et des serveurs physiques locaux sur Azure ou vers un centre de données local secondaire. La réplication sur Azure réduit le coût et la complexité qu'implique la maintenance d'un centre de données secondaire.
Réplication de charges de travail	Répliquer n'importe quelle charge de travail en cours d'exécution sur des machines virtuelles Azure, des machines virtuelles Hyper-V locales et VMware, et des serveurs physiques Windows/Linux pris en charge.
Résilience des données	Site Recovery orchestre la réplication sans intercepter les données d'une application. Lorsqu'on effectue une réplication vers Azure, les données sont stockées dans le stockage Azure, avec la résilience que cela implique. Lors du basculement, les machines virtuelles Azure sont créées à partir des données répliquées.

Récupération Azure: Azure site Recovery

- **Fonctionnalités de Azure site Recovery (suite) :**

Fonctionnalité	Description
Cibles RTO et RPO	Maintenir les objectifs de délai de récupération (RTO) et les objectifs de point de récupération (RPO) au sein des limites fixées par l'organisation. Site Recovery fournit une réplication continue pour les machines virtuelles Azure et VMware. Les machines virtuelles Hyper-V bénéficient d'une fréquence de réplication de 30 secondes seulement. On peut réduire davantage les RTO en les intégrant à Azure Traffic Manager.
Maintenir la cohérence des applications en cas de basculement	On peut effectuer une réplication à l'aide des points de récupération avec des captures instantanées cohérentes au niveau des applications. Ces captures récupèrent les données des disques, l'ensemble des données en mémoire et toutes les transactions en cours de traitement.
Tests sans interruption	On peut facilement exécuter la marche à suivre en cas de récupération d'urgence et ce, sans affecter une réplication en cours.
Basculements flexibles	On peut effectuer des basculements planifiés en cas d'interruptions prévues sans aucune perte de données. On peut également effectuer des basculements non planifiés avec une perte de données minimale (en fonction de la fréquence de réplication) en cas de sinistres inattendus. On peut effectuer en toute simplicité une restauration automatique vers un site principal dès qu'il est à nouveau disponible.
Plans de récupération personnalisés	À l'aide de plans de récupération, on peut personnaliser et séquencer le basculement et la récupération des applications multiniveaux s'exécutant sur plusieurs machines virtuelles. On regroupe des machines dans un plan de récupération et on peut ajouter éventuellement des scripts et des actions manuelles. Les plans de récupération peuvent être intégrés à des runbooks Azure Automation.

Récupération Azure: Azure site Recovery

- **Fonctionnalités de Azure site Recovery (suite) :**

Fonctionnalité	Description
Intégration BCDR	Site Recovery s'intègre à d'autres technologies BCDR. Par exemple, on peut utiliser Site Recovery pour protéger le serveur principal SQL Server de charges de travail d'entreprise, avec la prise en charge native de SQL Server Always On pour gérer le basculement des groupes de disponibilité.
Intégration Azure Automation	La bibliothèque Azure Automation diversifiée fournit des scripts spécifiques à l'application prêts pour la production, qui peuvent être téléchargés et intégrés au service Site Recovery.
Intégration réseau	Site Recovery est intégré à Azure pour la gestion du réseau d'applications. Par exemple, pour réserver des adresses IP, configurer des équilibreurs de charge et utiliser Azure Traffic Manager pour des basculements réseau efficaces.

Récupération Azure: Azure site Recovery

- **Scénarios de réplication :**

Avec Azure Site Recovery, on peut répliquer les éléments ci-dessous:

- Répliquer des machines virtuelles Azure d'une région Azure vers une autre.
- Répliquer des machines virtuelles VMware, des machines virtuelles Hyper-V, des serveurs physiques (Windows et Linux) et des machines virtuelles Azure Stack locales sur Azure.
- Répliquer des instances Windows AWS sur Azure.
- Répliquer des machines virtuelles VMware locales, des machines virtuelles Hyper-V gérées par System Center VMM et des serveurs physiques vers un site secondaire.

CHAPITRE 4

Protéger les données

1. Chiffrement au repos et en transit
2. Techniques de masquage des données
3. Sauvegarde et récupération
4. **Anonymisation des données**

Anonymisation des données

L'anonymisation ou la désidentification des données est un élément crucial de certains systèmes et une exigence fondamentale pour de nombreuses organisations. Les scénarios découverts par la possibilité de masquer, de hacher ou même de remplacer des entités PII par des entités simulées dans du texte et des images incluent le déplacement de données vers le Cloud ou vers des partenaires, la génération de données de test à partir de données réelles, le stockage de données pour le traitement AI/ML,…

Dans cette partie nous allons expliquer comment utiliser Azure et Presidio pour créer un processus ETL entièrement fonctionnel sur Azure qui déplace un ensemble de documents d'un emplacement à un autre tout en nettoyant, remplaçant, hachant ou chiffrant les entités PII du texte.

Avant de commencer dans le vif du sujet, présentant quelques définitions:

- **PII:**

Les informations personnelles identifiables, ou PII, de l'anglais Personal Identifiable Information, sont un ensemble de données qui peuvent être utilisées pour distinguer un individu spécifique.

Il s'agit de données sensibles qui peuvent être utilisées pour l'usurpation d'identité. Les PII peuvent être aussi simples que le nom, l'adresse et la date de naissance d'un utilisateur ou aussi sensibles que le nom complet, l'adresse, le numéro de sécurité sociale et les données financières.

En cas de violation de données, les PII sont une cible privilégiée pour les attaquants en raison de leur valeur élevée sur les marchés darknet.

Anonymisation des données

- **Presidio :**

Presidio est un service de protection des données et d'anonymisation des données PII sensible au contexte, enfichable et personnalisable pour le texte et les images. Presidio aide à garantir que les données sensibles sont correctement gérées et gouvernées. Il fournit des modules d'identification et d'anonymisation rapides pour les entités privées sous forme de texte tels que les numéros de carte de crédit, les noms, les emplacements, les numéros de sécurité sociale, les portefeuilles Bitcoin, les numéros de téléphone américains, les données financières, etc.

- **Anonymisation des données avec Presidio :**

Dans la suite de cette section, nous allons voir la manière d'intégrer Presidio à Azure Data Factory à l'aide du modèle intégré « Anonymisation des données avec Presidio »:

Le scénario couvert dans cette section prend un type générique d'ensemble de données d'entrée, un *Azure Storage blob container*, et utilise les services Azure pour déplacer cet ensemble vers un autre emplacement, où le contenu des fichiers a été anonymisé de toutes les entités PII.

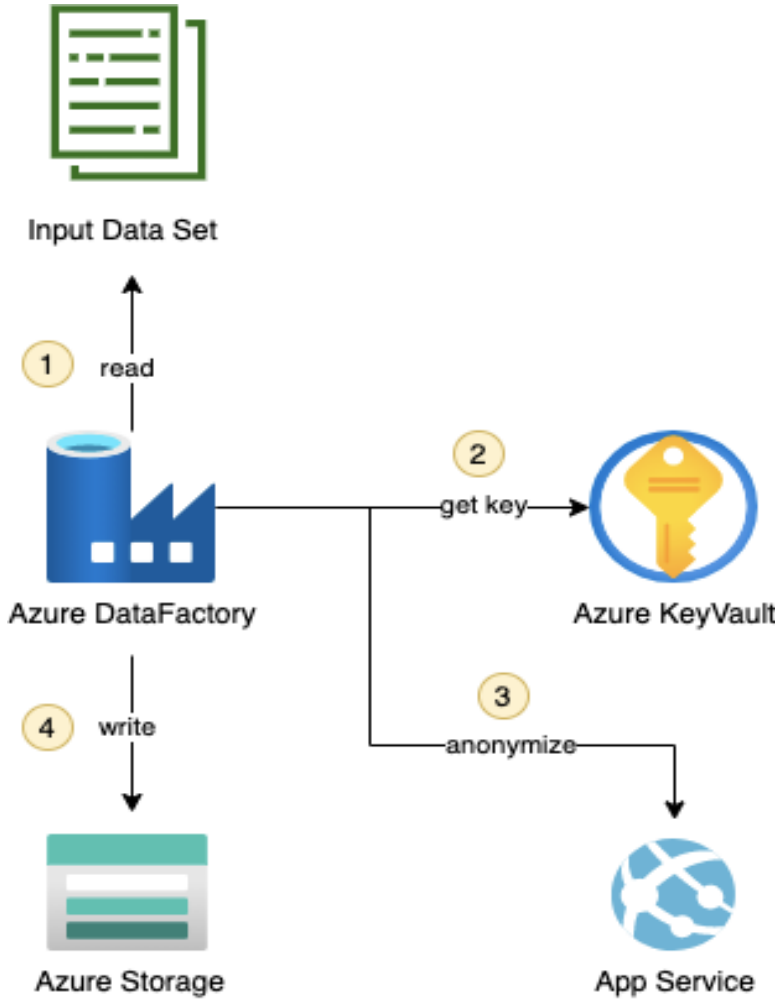
Anonymisation des données

Les services Azure utilisés sont :

- **Azure Data Factory** : un service ETL basé sur le Cloud qui va héberger le pipeline de transformation.·
- **Azure Storage** : fournit la couche de persistance ETL.·
- **Azure Key-Vault** : stockage des clés d'accès Azure Storage à utiliser dans l'ETL de manière sécurisée.
- **Azure App Service** : hébergement de Presidio en tant que point de terminaison HTTP REST.

Le diagramme ci-après affiche la relation entre les parties du système ETL où Presidio est utilisé comme point de terminaison HTTP:

1. Lire l'ensemble de données à partir de la source.
2. Obtenir une clé d'accès pour Azure Storage à partir d'Azure Key Vault.
3. Envoyer la valeur textuelle de chaque document de l'ensemble à anonymiser par Presidio.
4. Enregistrer le texte anonymisé dans un fichier texte nommé de manière aléatoire sur Azure Blob Storage.



PARTIE 2

Anonymisation des données

- L'entrée du pipeline d'anonymisation des données est un ensemble de documents contenant du texte PII, tel que :

```
Need to change billing data of my card 123-345-11123
```

- Un fichier de sortie des pipelines devrait ressembler à ceci :

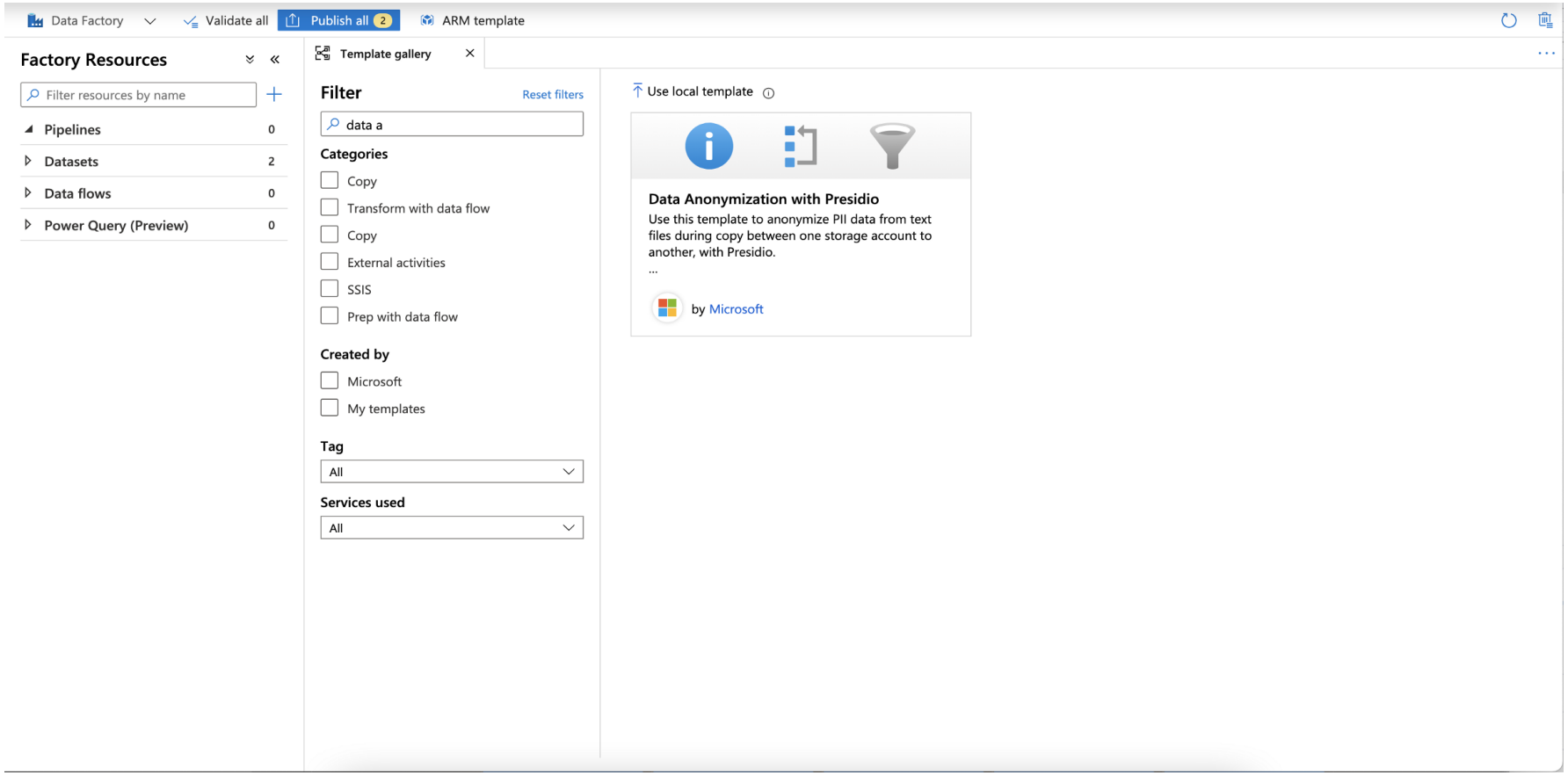
```
Need to change billing date of my card ANONYMIZED
```

- **Provisionnement des services Azure :**

Si on a déjà une instance Azure Data Factory, à partir de l'interface utilisateur Azure Data Factory, il faut accéder à la galerie de modèles et rechercher le modèle nommé « Anonymisation des données avec Presidio ». Il faut ensuite suivre les instructions à l'écran pour mettre en service l'infrastructure prérequise et connecter le conteneur d'entrée Azure Storage.

Anonymisation des données

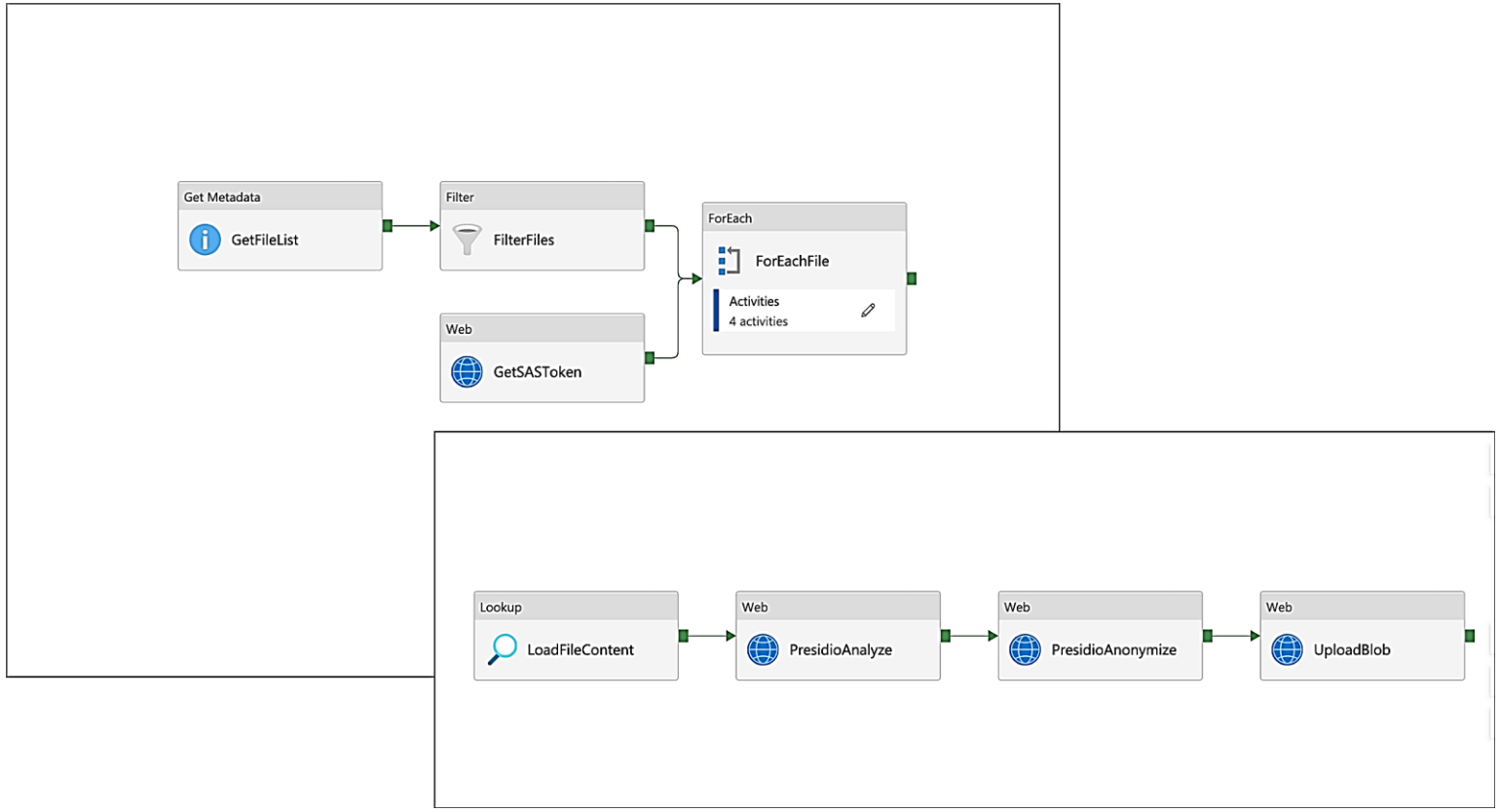
- **Provisionnement des services Azure (suite) :**



Anonymisation des données

- **Exécuter un exemple :**

À partir de l'interface utilisateur d'Azure Data Factory, ouvrir le pipeline nommé Anonymize.



PARTIE 2

Anonymisation des données

- **Exécuter un exemple (suite) :**

- **GetFileList** : obtient la liste des fichiers du conteneur source.
- **FilterFiles** : filtre le répertoire de la liste, seuls les fichiers seront traités.
- **ForEachFile** : une boucle For-Each incluant une clause d'exécution pour chaque document du tableau.
- **GetSASToken** : obtenir le jeton SAS d'Azure Key Vault. Sera utilisé plus tard pour écrire dans le conteneur blob.
- **LoadFileContent** : charge le contenu d'un fichier texte dans un jeu de données.
- **PresidioAnalyze** : envoie le texte au point de terminaison de l'analyseur Presidio.
- **PresidioAnonymize** : envoie la réponse de l'analyseur Presidio au point de terminaison de l'anonymiseur presidio.
- **UploadBlob** : enregistre la réponse anonymisée de Presidio dans un fichier texte sur le stockage Azure Blob cible.

Anonymisation des données

- **Exécuter un exemple (suite) :**

Appuyer sur le bouton de débogage et remplir les paramètres de pipeline suivants :

SourceStore_Location : nom du conteneur source.

DestinationStore_Name : nom du compte cible.

DestinationStore_Location : nom du conteneur cible. A une valeur par défaut d'un conteneur qui a été créé lors de l'approvisionnement du modèle ARM (presidio).

KeyVault_Name : nom Azure Key Vault.

Analyzer_Url : URL du service d'application de l'analyseur.

Anonymizer_Ur l: URL du service d'application d'anonymisation.

→ Au fur et à mesure que le pipeline s'exécute, on devra voir les fichiers en cours de création sur le conteneur d'objets blob cible, où les données sont anonymisées du contenu PII.

PARTIE 3

SUPERVISER LES RESSOURCES CLOUD

Dans ce module, vous allez :

- Utiliser les outils natifs du Cloud
- Utiliser un outil externe SIEM

5,5 heures

CHAPITRE 1

Utiliser les outils natifs du Cloud

Ce que vous allez apprendre dans ce chapitre :

- Connaitre la journalisation des opérations
- Comprendre l'audits de conformité
- Appréhender le respect des règles de sécurité
- Avoir une idée sur les mesures de sécurité

3,5 heures

CHAPITRE 1

Utiliser les outils natifs du Cloud

1. **Journalisation des opérations**
2. Audits de conformité
3. Respect des règles de sécurité
4. Mesures de sécurité

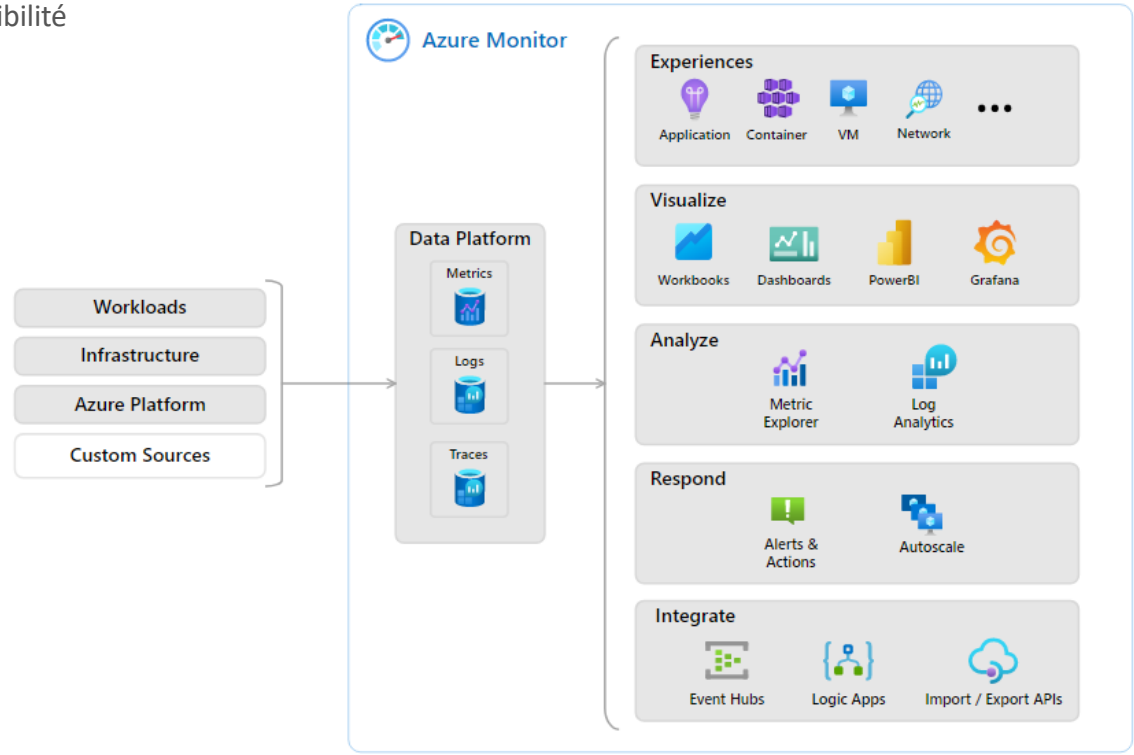
PARTIE 3

Journalisation des opérations via Azure Monitor

Les journaux des opérations fournissent des informations de diagnostic et d'audit détaillées pour les ressources et la plateforme dont elles dépendent. Bien qu'ils soient générés automatiquement, vous devez configurer certains journaux à transférer vers un ou plusieurs espaces de stockages à des fins de rétention. En effet, la durée de rétention des journaux des opérations est limitée dans le temps pour certains fournisseurs Cloud (Pour Azure 90 Jours).

Azure Monitor est une solution SaaS Cloud native qui vous aide à optimiser la disponibilité et les performances de vos applications et services. Il offre une solution complète pour collecter, analyser et exploiter des données de télémétrie de vos environnements Cloud et locaux.

Le diagramme suivant donne une vue d'ensemble d'Azure Monitor. Au centre du diagramme se trouvent les magasins de données pour les métriques et les journaux d'activité, qui sont les deux types fondamentaux d'utilisation des données par Azure Monitor. Sur la gauche se trouvent les sources de données de supervision qui remplissent ces magasins de données. Sur la droite figurent les différentes actions qu'Azure Monitor effectue avec ces données collectées. Il s'agit d'actions telles que l'analyse, la création d'alertes et le streaming vers des systèmes externes.



Source Microsoft

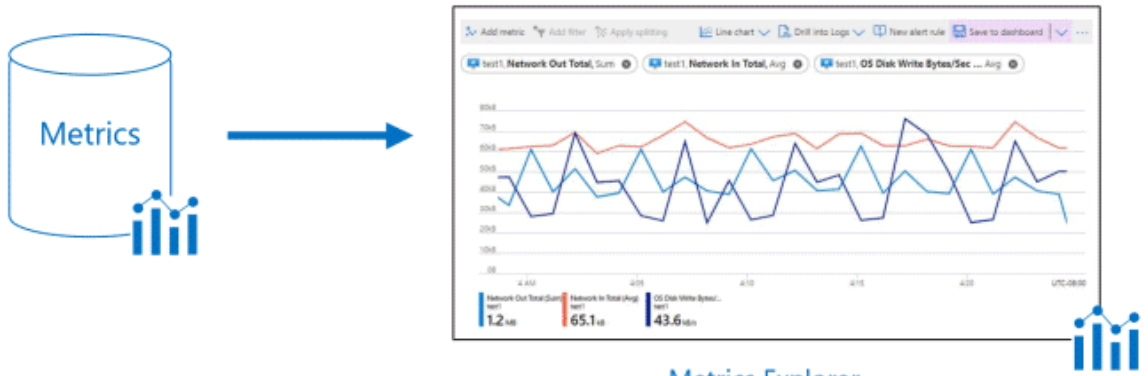
Plateforme de données Azure Monitor

Toutes les données collectées par Azure Monitor font partie d'un des deux types fondamentaux, les métriques et les journaux d'activité.

Les métriques sont des valeurs numériques décrivant un aspect d'un système à un moment précis dans le temps. Elles sont légères et capables de prendre en charge des scénarios en quasi-temps réel.

Les journaux d'activité contiennent différents types de données organisées en enregistrements, avec différents jeux de propriétés pour chaque type. Les données de télémétrie, comme les événements et les traces, sont stockées sous forme de journaux d'activité en plus des données de performances, afin qu'elles puissent être combinées pour une analyse.

Pour de nombreuses ressources Azure, vous verrez les données collectées par Azure Monitor directement sur la page Vue d'ensemble correspondante sur le portail Azure. Par exemple au niveau de toutes les machines virtuelles, vous pouvez accéder à plusieurs graphiques affichant les mesures de performances à travers l'onglet Metrics.

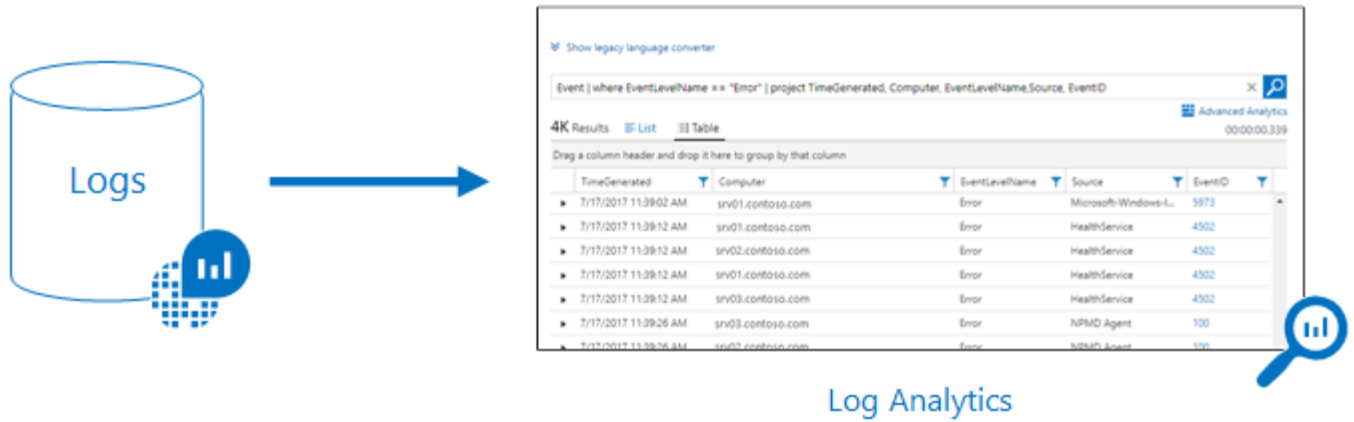


Source Microsoft

Plateforme de données Azure Monitor

Les données de journal collectées par Azure Monitor peuvent être analysées à l'aide de requêtes qui permettent de récupérer, consolider et analyser rapidement les données collectées. Vous pouvez créer et tester des requêtes à l'aide d'Azure Log Analytics dans le portail Azure. Vous pouvez ensuite analyser directement les données avec différents outils ou enregistrer les requêtes pour les utiliser avec des visualisations ou des règles d'alerte.

Azure Monitor utilise une version du langage de requête Kusto qui est adapté aux requêtes simples dans les journaux, mais comprend également des fonctionnalités avancées telles que les agrégations, les jointures et l'analytique intelligente.



Source Microsoft

Les données collectées par Azure Monitor

Azure Monitor peut collecter des données à partir de sources allant de votre application à n'importe quel système d'exploitation et services sur lesquels elle s'appuie, jusqu'à la plateforme elle-même. Azure Monitor collecte des données dans chacun des niveaux suivants :

- **Données de supervision de l'application** : données concernant les performances et les fonctionnalités du code que vous avez écrit, quelle que soit sa plateforme.
- **Données de surveillance du système d'exploitation invité** : données concernant le système d'exploitation sur lequel votre application est exécutée. Ce système d'exploitation peut s'exécuter dans Azure, un autre Cloud ou un système local.
- **Données de surveillance des ressources Azure** : données concernant le fonctionnement d'une ressource Azure.
- **Données de supervision de l'abonnement Azure** : données concernant le fonctionnement et la gestion d'un abonnement Azure, et données concernant l'intégrité et le fonctionnement d'Azure lui-même.
- **Données de surveillance de locataire Azure** : données concernant le fonctionnement des services Azure au niveau du locataire, tels qu'Azure Active Directory.
- **Données de modification des ressources Azure** : données sur les modifications apportées à vos ressources Azure et sur la façon de traiter et de trier les incidents et les problèmes.

Dès que vous créez un abonnement Azure et que vous commencez à ajouter des ressources, comme des machines virtuelles et des applications web, Azure Monitor commence à collecter des données. Les journaux d'activité enregistrent la création et la modification des ressources. Les métriques vous indiquent les performances de la ressource et les ressources qu'elle consomme.

Source Microsoft

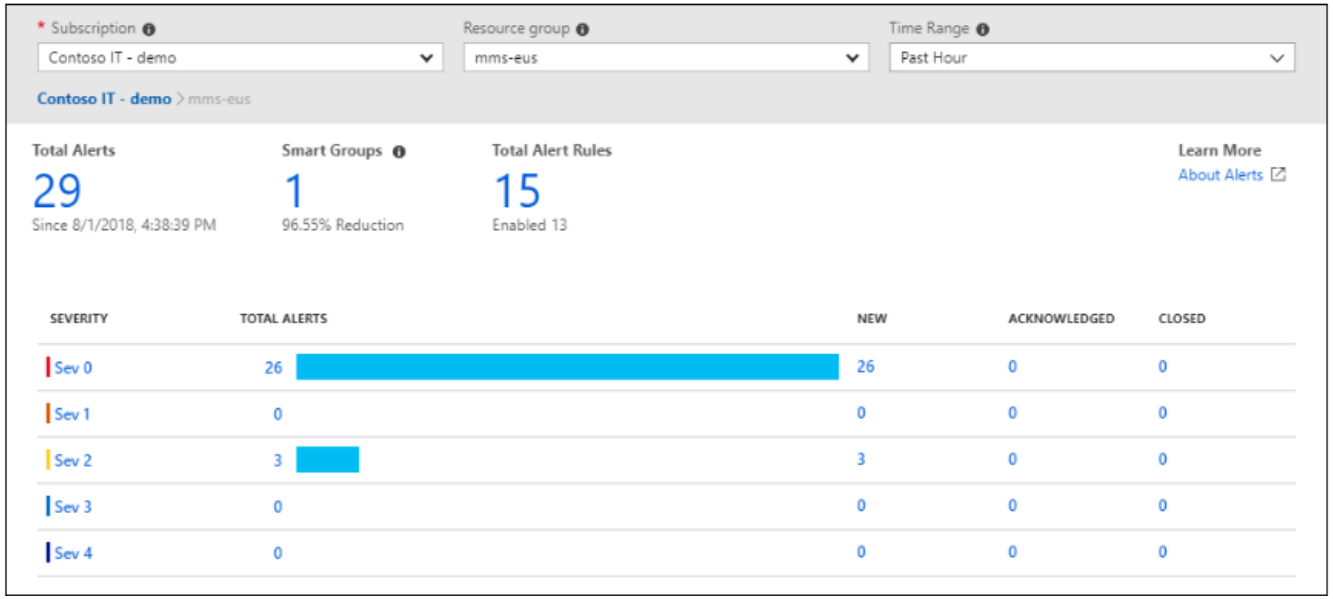
Les alertes dans Azure Monitor

Les alertes dans Azure Monitor vous avertissent de manière proactive en cas de condition critique, et sont susceptibles d'essayer de prendre des mesures correctives.

Les règles d'alerte basées sur les métriques fournissent des alertes en quasi-temps réel basées sur des valeurs numériques.

Les règles basées sur les journaux autorisent une logique complexe entre les données de plusieurs sources.

Les règles d'alerte dans Azure Monitor utilisent des groupes d'actions, qui contiennent des ensembles uniques de destinataires et d'actions qui peuvent être partagés entre plusieurs règles.



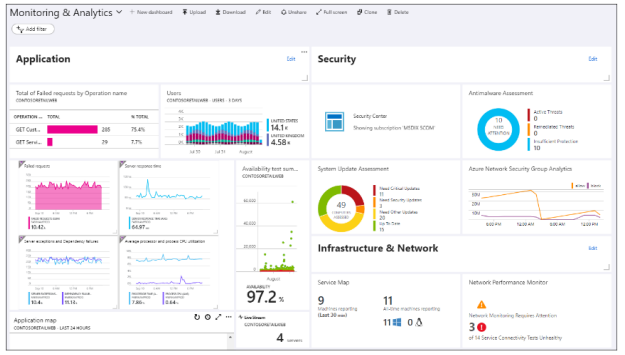
Source Microsoft

PARTIE 3

Visualisation des données dans Azure Monitor

Les visualisations, telles que les tables et les graphiques, sont des outils efficaces pour résumer les données de supervision et les proposer à différents publics.

Azure Monitor dispose de ses propres fonctionnalités pour visualiser les données de supervision et utilise d'autres services Azure pour les publier auprès de différentes audiences.



- **Tableaux de bord :** Vous permettent de combiner différentes sortes de données dans un même volet du portail Azure.

Si vous le souhaitez, vous pouvez partager le tableau de bord avec d'autres utilisateurs d'Azure.

Ajoutez la sortie de n'importe quelle requête de journal ou graphique de métriques à un tableau de bord Azure.

- **Power BI** est un service d'analytique métier qui fournit des visualisations interactives pour diverses sources de données. Il est idéal pour mettre des données à la disposition d'autres personnes internes ou externes à votre entreprise.

- **Workbooks** fourni un canevas flexible pour l'analyse des données et la création de rapports visuels enrichis dans le portail Azure. Cela vous permet d'exploiter plusieurs sources de données à travers l'écosystème Azure et de les combiner dans des expériences interactives unifiées.

Source Microsoft

CHAPITRE 1

Utiliser les outils natifs du Cloud

1. Journalisation des opérations
2. **Audits de conformité**
3. Respect des règles de sécurité
4. Mesures de sécurité

Microsoft Defender pour le Cloud Azure

Microsoft Defender pour le Cloud est une solution native Cloud de gestion de la posture de sécurité Cloud (CSPM) et une plateforme de protection de charge de travail (CWPP) pour toutes vos ressources Azure, locales et multiClouds (Amazon AWS et Google GCP). Defender pour le Cloud répond à trois besoins essentiels lorsque vous gérez la sécurité de vos ressources et charges de travail dans le Cloud et localement.

Defender pour le Cloud offre plusieurs fonctionnalités de sécurité renforcée qui permettent de protéger les entreprises contre les menaces et les attaques. On retrouve parmi les différentes fonctionnalités celle qui permet de **Veiller au respect de la conformité au moyen d'une série de normes**.

En effet, Defender pour le Cloud évalue continuellement votre environnement Cloud afin d'analyser les facteurs de risque en fonction des contrôles et des bonnes pratiques du **Benchmark de sécurité Azure***. Quand vous activez les fonctionnalités de sécurité renforcée, vous pouvez appliquer d'autres normes industrielles, normes réglementaires et points de référence en fonction des besoins de votre entreprise. **Le tableau de bord de conformité réglementaire** vous permet d'ajouter des normes et de veiller au respect de la conformité.

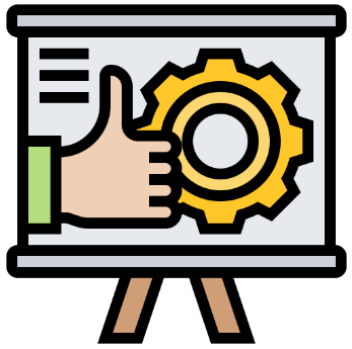
***Le benchmark de sécurité Azure** comprend un ensemble de recommandations de sécurité à fort impact qui peuvent aider l'entreprise à sécuriser les services qu'elles utilisent dans Azure.

Tableau de bord de conformité réglementaire (Microsoft Defender)

Le **tableau de bord de conformité réglementaire** de Microsoft Defender pour le Cloud simplifie le processus visant à respecter les exigences de conformité réglementaire. Defender pour le Cloud évalue continuellement votre environnement Cloud hybride afin d'analyser les facteurs de risque en fonction des contrôles et des bonnes pratiques du point de vue des normes appliquées à vos abonnements. Le tableau de bord reflète l'état de votre conformité à ces normes.

Quand vous activez Defender pour le Cloud dans un abonnement Azure, le Benchmark de sécurité Azure lui est automatiquement attribué. Ce benchmark, largement respecté et centré sur le Cloud, est basé sur les contrôles du CIS (Center for Internet Security) et du NIST (National Institute of Standards and Technology).

Le tableau de bord de conformité réglementaire montre l'état de toutes les évaluations au sein de votre environnement pour les normes et réglementations de votre choix. Si vous suivez les recommandations et réduisez les facteurs de risque de votre environnement, votre niveau de conformité s'améliore.



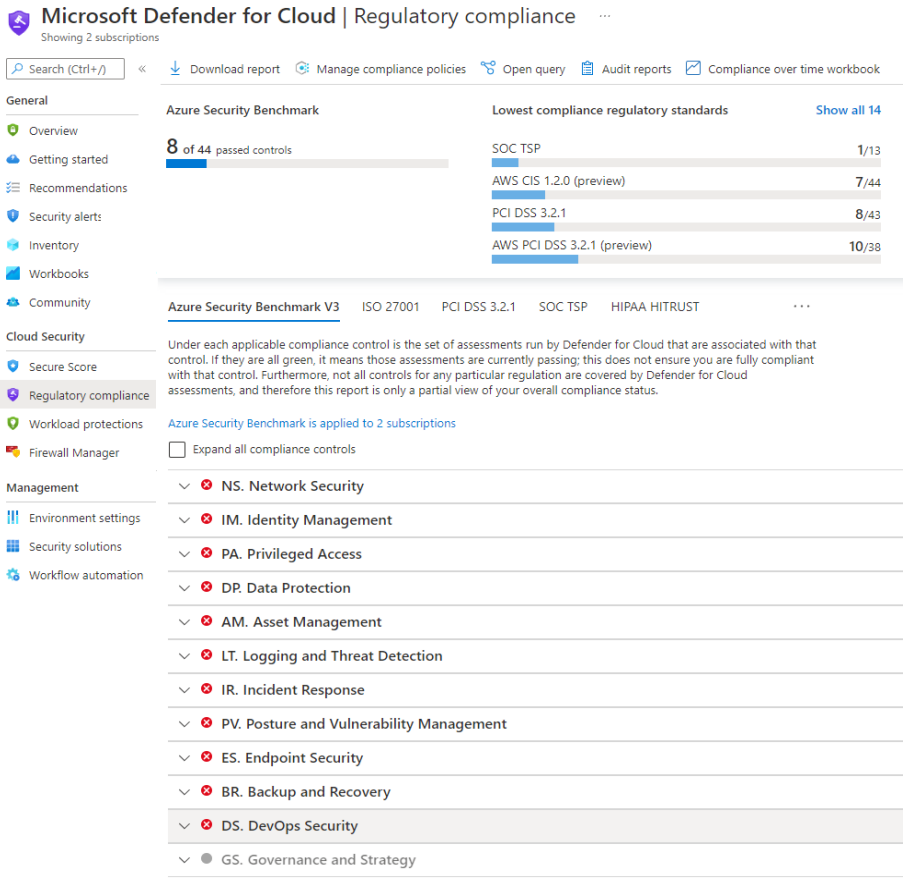
PARTIE 3

Évaluer votre conformité aux réglementations

Le tableau de bord de conformité réglementaire montre vos normes de conformité sélectionnées et toutes leurs exigences, celles prises en charge étant comparées aux évaluations de sécurité applicables. L'état de ces évaluations reflète votre conformité à la norme.

Utilisez le tableau de bord de conformité réglementaire pour vous aider à prendre conscience d'un manque de conformité aux normes et aux réglementations de votre choix. Cette vue ciblée vous permet également de superviser votre conformité au fil du temps dans les environnements Cloud et hybrides dynamiques.

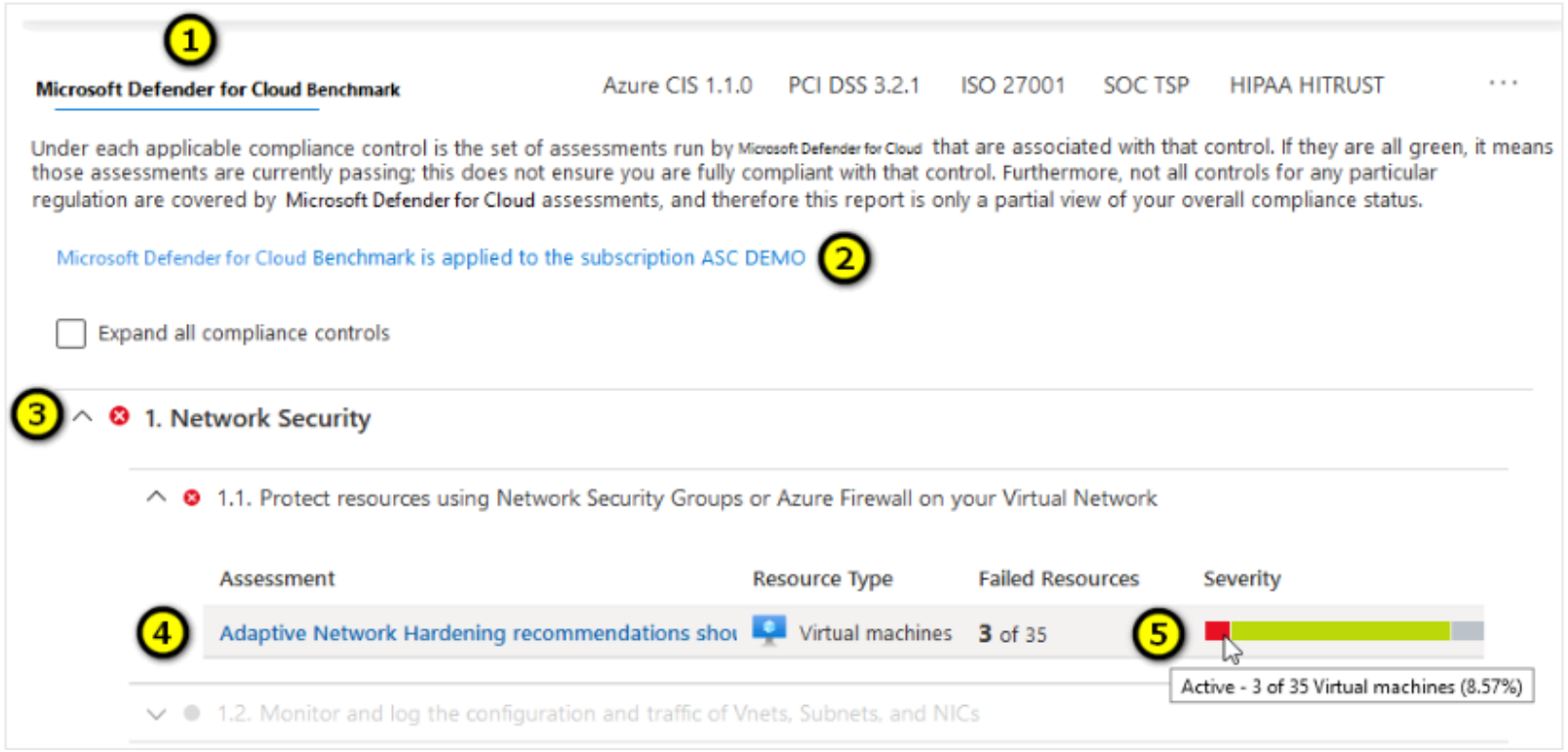
1. Dans le menu de Defender pour le Cloud, sélectionnez **Conformité réglementaire**.
Un tableau de bord apparaît en haut de l'écran avec une vue d'ensemble de votre état de conformité et l'ensemble des réglementations de conformité prises en charge.
Vous verrez votre score de conformité global et le nombre d'évaluations ayant réussi ou échoué pour chaque norme.



PARTIE 3

Évaluer votre conformité aux réglementations

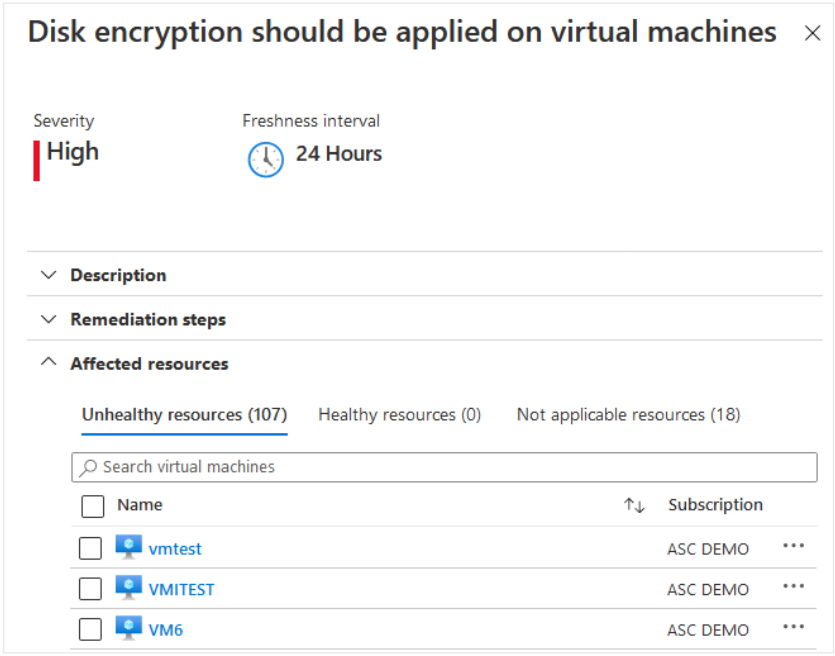
2. Sélectionnez un onglet correspondant à une norme de conformité qui vous intéresse (1). Vous verrez sur quels abonnements la norme est appliquée (2) et la liste de tous les contrôles relatifs à cette norme (3). Pour les contrôles applicables, vous pouvez voir les détails des évaluations ayant réussi ou échoué associées à ce contrôle (4) et le nombre de ressources affectées (5). Certains contrôles sont grisés. Ces contrôles ne sont associés à aucune évaluation Defender pour le Cloud. Vérifiez les conditions qui leur sont associées et évaluez-les dans votre environnement. Certaines d'entre elles peuvent être liées au processus et ne pas être d'ordre technique.



Améliorer votre niveau de conformité

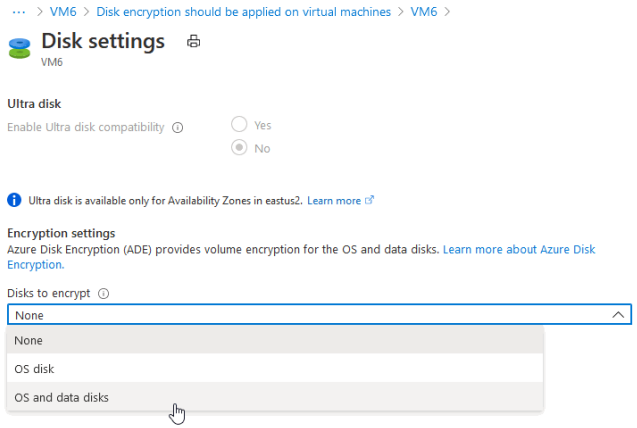
À l'aide des informations figurant dans le tableau de bord de conformité réglementaire, améliorez votre niveau de conformité en résolvant les recommandations directement dans le tableau de bord.

1. Sélectionnez l'une des évaluations ayant échoué dans le tableau de bord pour voir les détails de cette recommandation. Chaque recommandation comprend un ensemble d'étapes de correction pour résoudre le problème.
2. Sélectionnez une ressource particulière pour voir plus de détails et résoudre la recommandation associée à cette ressource.
   Par exemple, dans la **norme Azure CIS 1.1.0**, sélectionnez la recommandation **Le chiffrement de disque doit être appliqué sur les machines virtuelles**.



Améliorer votre niveau de conformité

3. Dans cet exemple, quand vous sélectionnez Entreprendre une action dans la page des détails de la recommandation, vous arrivez dans les pages relatives aux machines virtuelles Azure du portail Azure, où vous pouvez activer le chiffrement sous l'onglet Sécurité :



4. Quand vous aurez pris des mesures pour appliquer les recommandations, vous constaterez une amélioration de votre score de conformité dans le rapport du tableau de bord de conformité.

Remarque

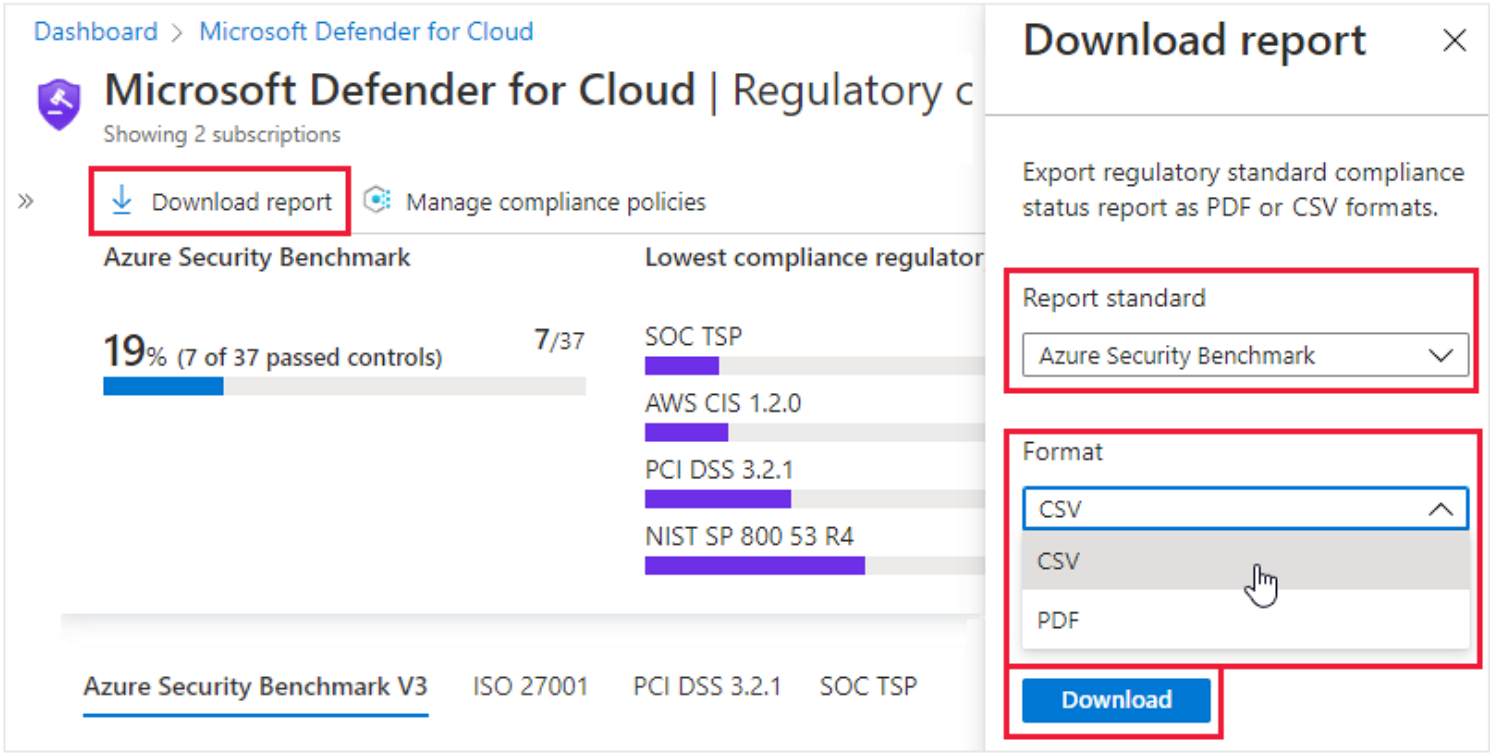
- Les évaluations s'exécutent toutes les 12 heures environ. L'impact sur vos données de conformité n'est donc visible qu'après l'exécution suivante de l'évaluation correspondante.

PARTIE 3

Générer des rapports d'état de conformité et des certificats

Pour générer un rapport PDF comportant un résumé de votre état de compatibilité actuel pour une norme particulière, sélectionnez **Télécharger un rapport**.

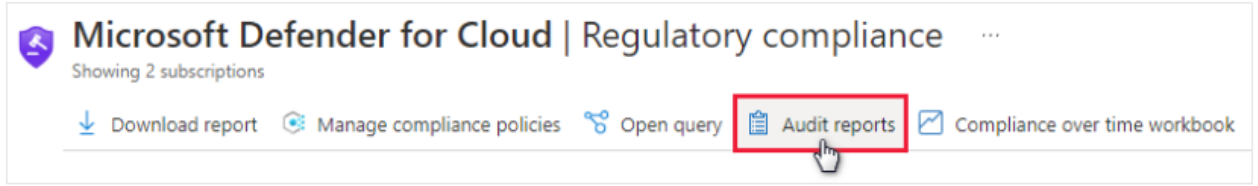
Le rapport fournit un résumé général de votre état de conformité pour la norme sélectionnée en fonction des données d'évaluation Defender pour le Cloud. Le rapport est organisé en fonction des contrôles de cette norme particulière. Le rapport peut être partagé avec les parties prenantes concernées et servir de preuve aux auditeurs internes et externes.



PARTIE 3

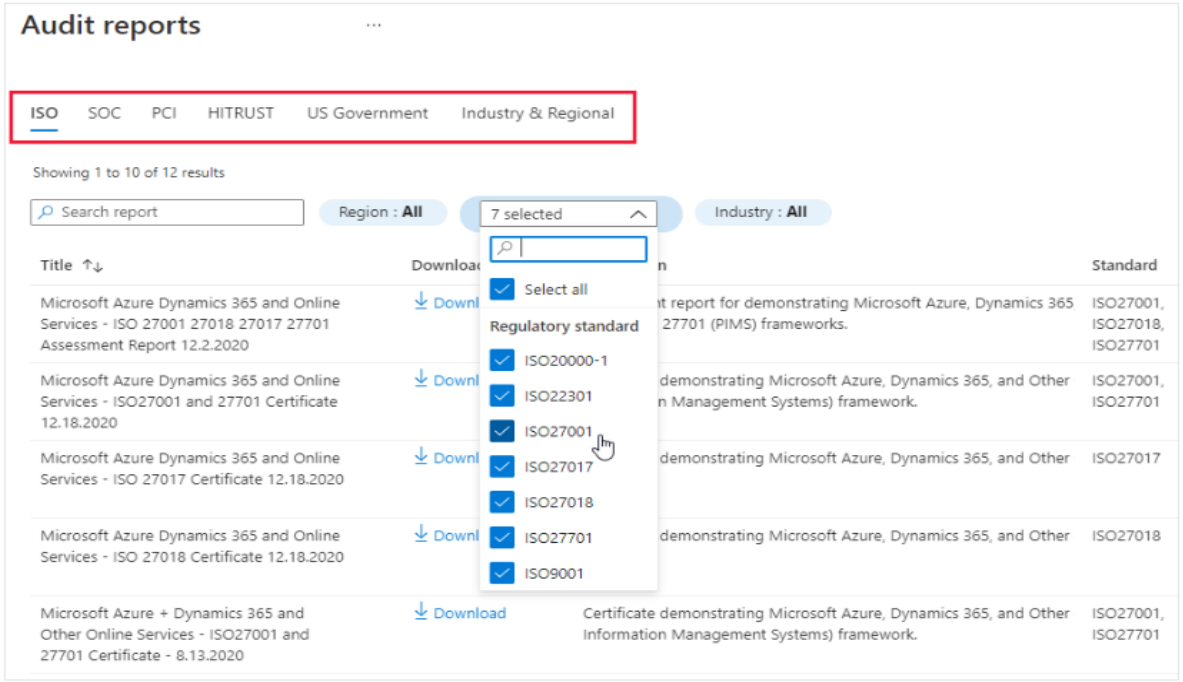
Télécharger les rapports de certification

Pour télécharger des **rapports de certification** Azure et Dynamics pour les normes appliquées à vos abonnements, utilisez l'option **Rapports d'audit**.



Sélectionnez l'onglet pour les types de rapports appropriés (PCI, SOC, ISO et autres) et utilisez des filtres pour rechercher les rapports spécifiques dont vous avez besoin :

Par exemple, à partir de l'onglet PCI, vous pouvez télécharger un fichier ZIP contenant un certificat signé numériquement, qui démontre la conformité de Microsoft Azure, Dynamics 365 et d'autres services en ligne au framework ISO22301,ainsi que la documentation nécessaire pour interpréter et présenter le certificat.



CHAPITRE 1

Utiliser les outils natifs du Cloud

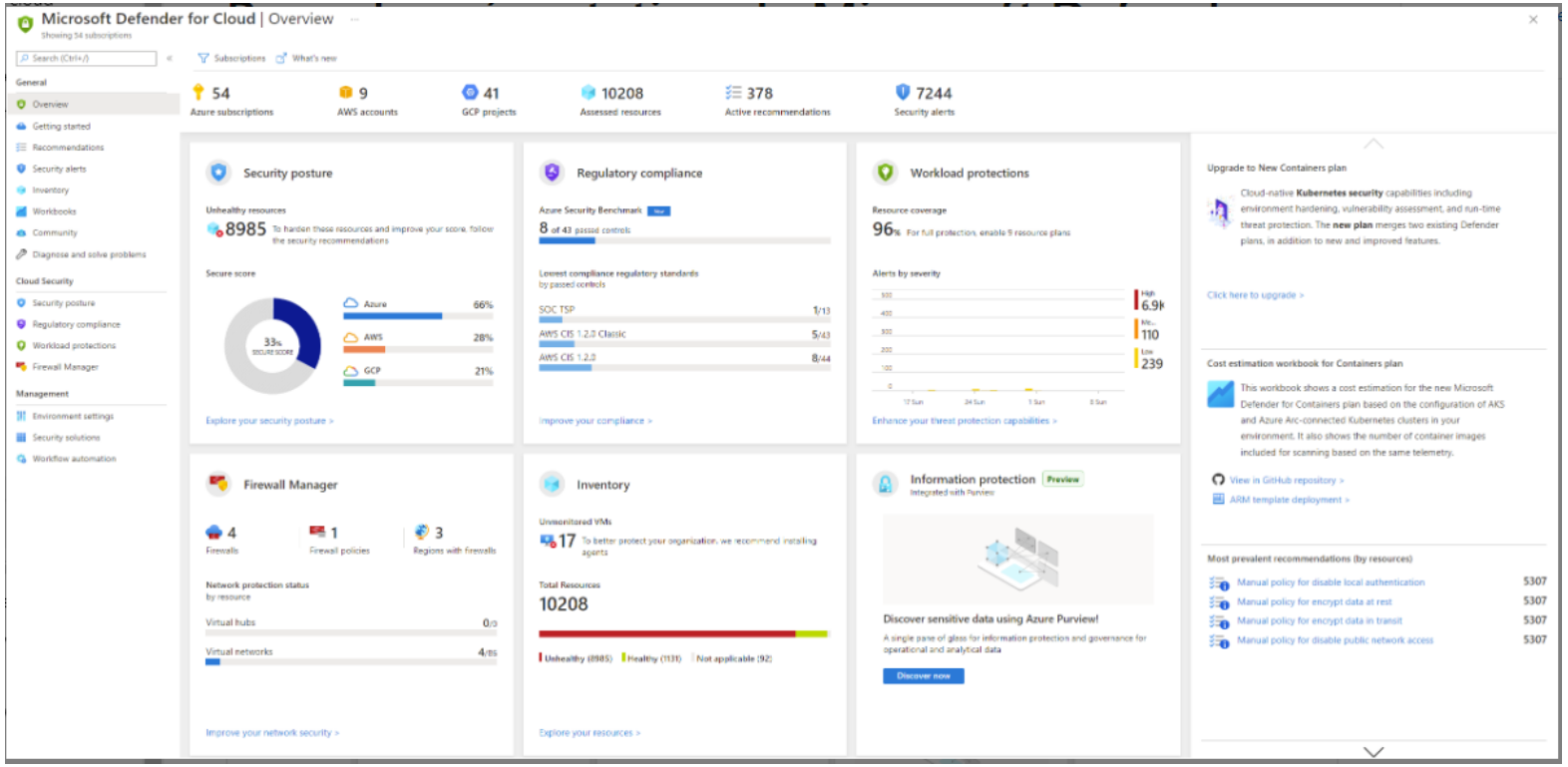
1. Journalisation des opérations
2. Audits de conformité
3. **Respect des règles de sécurité**
4. Mesures de sécurité

PARTIE 3

Microsoft Defender pour le Cloud Azure

Microsoft Defender pour le Cloud est une solution native Cloud qui offre à travers la page de vue d'ensemble un tableau de bord interactif qui fournit une vue unifiée de la posture de sécurité de vos charges de travail Cloud hybrides. En outre, elle affiche des alertes de sécurité, des informations de couverture, etc.

Vous pouvez sélectionner n'importe quel élément de la page pour obtenir des informations plus détaillées.



Source : Portail Azure

Microsoft Defender pour le Cloud Azure

Ainsi le Tableau de bord de Defender on retrouve plusieurs widgets, chacune lié à une fonctionnalité ou à un tableau de bord dédié et qui permettent d'évaluer le respect des règles de sécurité de l'abonné avec un niveau très détaillé.

Widgets	Syntaxe
Posture de sécurité	Defender pour le Cloud évalue continuellement vos ressources, vos abonnements et votre entreprise pour y rechercher d'éventuels problèmes de sécurité. Il agrège ensuite toutes ses découvertes sous la forme d'un score qui vous permet de déterminer d'un coup d'œil votre niveau de sécurité actuel : plus le score est élevé, plus le niveau de risque identifié est faible.
Protections de charge de travail	Il s'agit de la plateforme de protection de charge de travail Cloud (CWPP) intégrée à Defender pour le Cloud qui offre une protection avancée et intelligente de vos charges de travail exécutées sur Azure, sur des machines locales ou d'autres fournisseurs de Cloud. À chaque type de ressource correspond un plan Microsoft Defender. La mosaïque affiche la couverture de vos ressources connectées (pour les abonnements actuellement sélectionnés) et les alertes récentes, avec un code de couleur par gravité.
Conformité réglementaire	Defender pour le Cloud fournit des aperçus sur votre posture de conformité à partir d'évaluations continues de votre environnement Azure. Defender pour le Cloud analyse les facteurs de risque dans votre environnement conformément aux bonnes pratiques de sécurité. Ces évaluations sont comparées à des contrôles de conformité provenant d'un ensemble de normes prises en charge.

Microsoft Defender pour le Cloud Azure

Widgets	Syntaxe
Firewall Manager	Cette vignette indique l'état de vos hubs et réseaux à partir d'Azure Firewall Manager.
Inventaire	La page d'inventaire des ressources de Microsoft Defender pour le Cloud vous permet de voir dans une même page la posture de sécurité des ressources que vous avez connectées à Microsoft Defender pour le Cloud. Toutes les ressources avec des recommandations de sécurité non résolues sont affichées dans l'inventaire. Si vous avez activé l'intégration de Microsoft Defender pour point de terminaison et Microsoft Defender pour les serveurs, vous avez également accès à l'inventaire logiciel. La vignette de la page de présentation vous montre un aperçu du nombre total de ressources saines et non saines (pour les abonnements actuellement sélectionnés).
Protection des informations	Un graphique sur cette vignette montre les types de ressources analysés par Microsoft Purview qui contiennent des données sensibles, et qui ont des recommandations et des alertes non résolues. Suivez le lien d'analyse pour accéder aux comptes Azure Purview et configurer de nouvelles analyses, ou sélectionnez une autre partie de la vignette pour ouvrir l'inventaire des ressources et voir vos ressources en fonction de la classification de sensibilité de vos données Microsoft Purview.

CHAPITRE 1

Utiliser les outils natifs du Cloud

1. Journalisation des opérations
2. Audits de conformité
3. Respect des règles de sécurité
4. **Mesures de sécurité**

Créer des stratégies et des initiatives de sécurité

Pour vous aider à sécuriser vos systèmes et votre environnement, Microsoft Defender pour le Cloud génère des recommandations de sécurité. Ces recommandations sont basées sur les meilleures pratiques du secteur, qui sont incorporées à la stratégie de sécurité par défaut générique fournie à tous les clients. Elles peuvent également provenir des connaissances que Defender pour le Cloud a des normes et réglementations du secteur.

Avec cette fonctionnalité, vous pouvez ajouter vos propres initiatives personnalisées. Ces initiatives contiennent une ou plusieurs stratégies de sécurité. Chacune de ces stratégies entraîne une recommandation de sécurité pour améliorer votre position de sécurité.

Une stratégie de sécurité ?

Une définition Azure Policy, créée dans Azure Policy, est une règle relative à des conditions de sécurité spécifiques que vous souhaitez contrôler. Les définitions intégrées incluent des éléments tels que le contrôle du type de ressource qui peut être déployé ou le respect des balises sur toutes les ressources. Vous pouvez également créer vos propres définitions de stratégies personnalisées.

Une initiative de sécurité ?

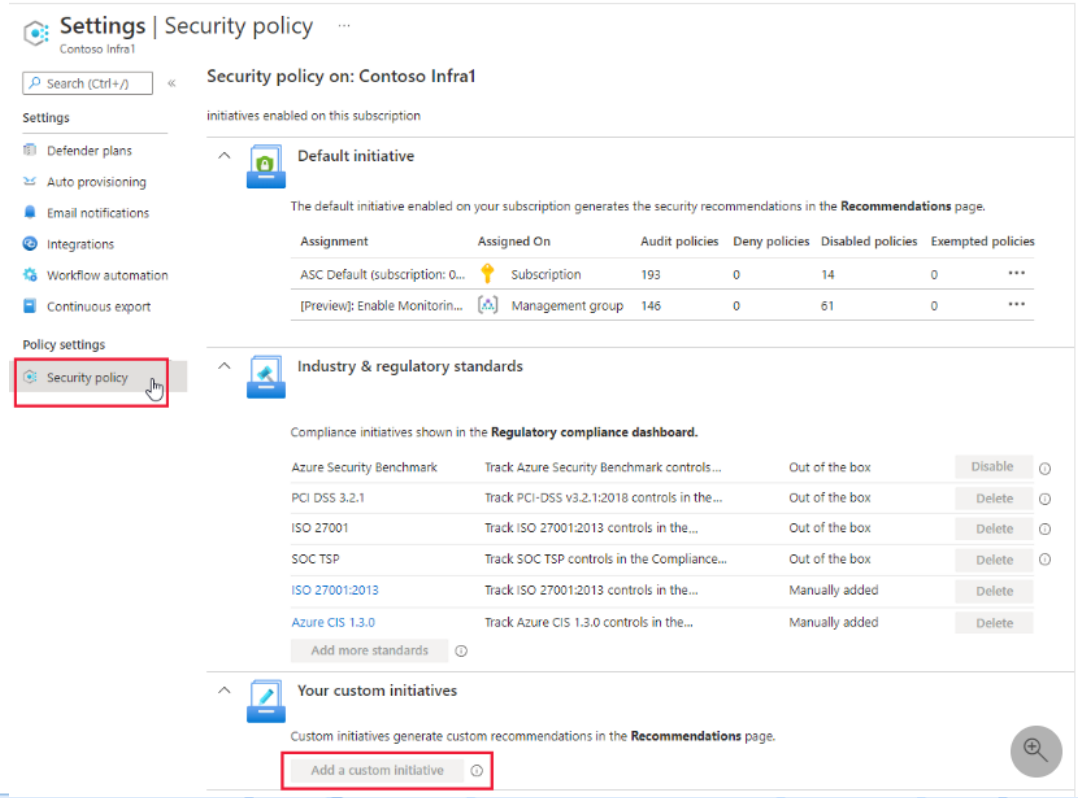
Une initiative de sécurité est une collection de définitions ou de règles Azure Policy regroupées pour atteindre un objectif spécifique. Les initiatives de sécurité simplifient la gestion de vos stratégies en regroupant un ensemble de stratégies de manière logique sous la forme d'un seul élément.

Une initiative de sécurité définit la configuration souhaitée de vos charges de travail, et vous permet de vous assurer que vous êtes en conformité avec les exigences de sécurité de votre entreprise ou des régulateurs.

PARTIE 3

Créer des stratégies et des initiatives de sécurité personnalisées

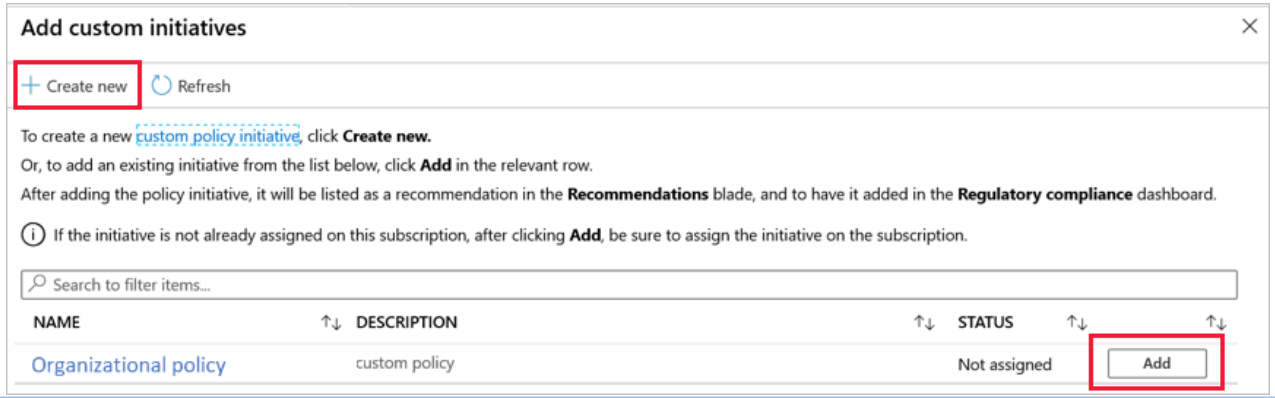
1. Dans le menu de Defender pour le Cloud, ouvrez **Paramètres de l'environnement**.
2. Sélectionnez l'abonnement ou le groupe d'administration pertinent auquel vous voulez ajouter une initiative personnalisée.
3. Ouvrez la page **Stratégie de sécurité**, puis dans la zone **Vos initiatives personnalisées**, sélectionnez **Ajouter une initiative personnalisée**.



Source : portail Azure

Créer des stratégies et des initiatives de sécurité personnalisées

4. Dans la page Ajouter des initiatives personnalisées, passez en revue la liste de stratégies personnalisées déjà créées dans votre entreprise.
    - Si vous en voyez une que vous souhaitez attribuer à votre abonnement, sélectionnez **Ajouter**.
    - Si aucune initiative dans la liste ne répond à vos besoins, créez une nouvelle initiative personnalisée :
        a) Sélectionnez **Créer nouveau**.
        b) Entrez l'emplacement et le nom de la définition.
        c) Choisissez les stratégies à inclure, puis sélectionnez **Ajouter**.
        d) Entrez les paramètres souhaités.
        e) Sélectionnez **Enregistrer**.
        f) Dans la page Ajouter des initiatives personnalisées, sélectionnez Actualiser. Votre nouvelle initiative sera disponible.
        g) Sélectionnez **Ajouter** et affectez-la à votre abonnement.



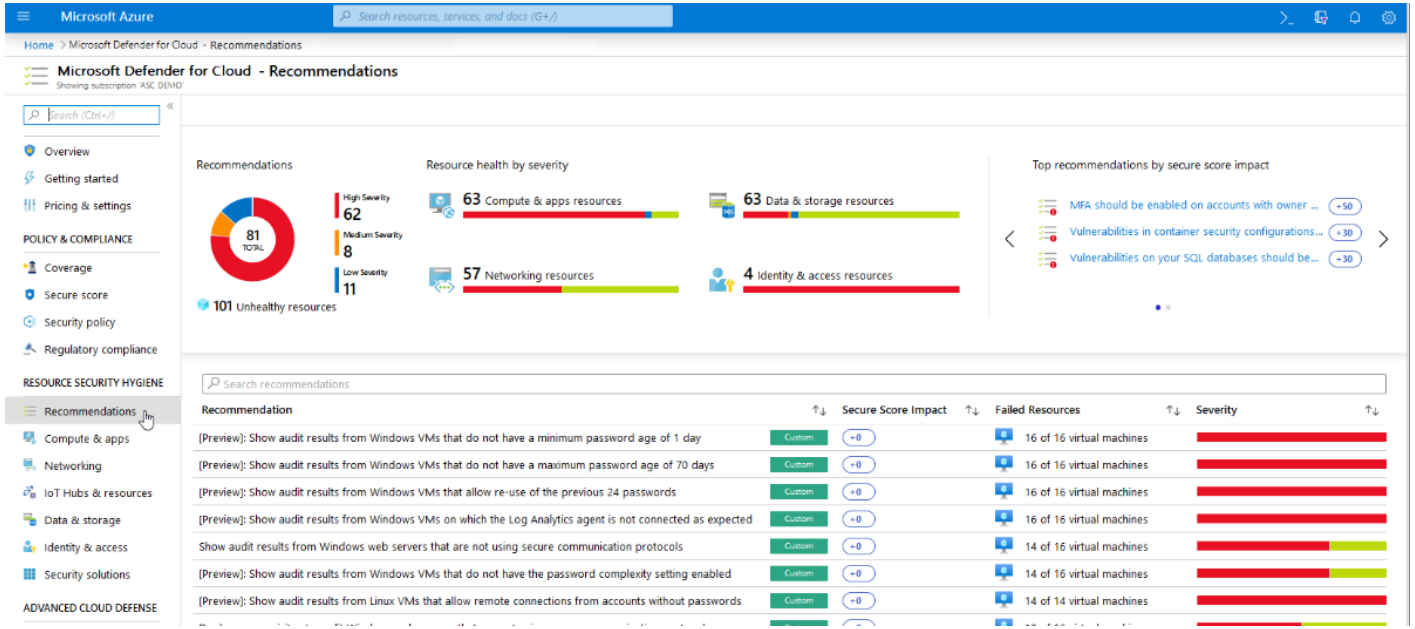
Créer des stratégies et des initiatives de sécurité personnalisées

Votre nouvelle initiative est appliquée et vous pouvez visualiser son impact de deux façons :

Dans le menu de Defender pour le Cloud, sélectionnez **Conformité réglementaire**. Le tableau de bord de conformité s'ouvre pour montrer votre nouvelle initiative personnalisée à côté des initiatives intégrées.

Vous commencerez ensuite à recevoir des recommandations si votre environnement ne suit pas les stratégies que vous avez définies.

5. Pour afficher les suggestions qui en résultent pour votre stratégie, sélectionnez **Suggestions** dans la barre latérale pour ouvrir la page des suggestions. Les recommandations apparaissent avec une étiquette « Personnalisée » et sont disponibles dans un délai d'une heure environ.



Source : Portail Azure

CHAPITRE 2

Utiliser les outils natifs du Cloud

Ce que vous allez apprendre dans ce chapitre :

- Connaitre l’interconnexion SIEM avec le Cloud
- Comprendre le principe de rapatriement des événements Cloud sur le SIEM
- Avoir une idée sur Tableau de bord de la sécurité sur Azure Sentinel

2 heures

CHAPITRE 2

Utiliser un outil externe SIEM

1. **Interconnexion SIEM avec le Cloud**
2. Rapatriement des événements Cloud sur le SIEM
3. Tableau de bord de la sécurité

Qu’est-ce qu’un système SIEM ?

Un système de gestion des informations et des événements de sécurité (**SIEM**) est une solution de sécurité qui permet aux entreprises de détecter les menaces avant qu’elles ne perturbent leurs activités.

Les solutions de gestion des informations et des événements de sécurité (**SIEM**) aident les entreprises à détecter, analyser et réagir aux menaces liées à la sécurité avant qu’elles ne nuisent à leur activité professionnelle.

Les technologies **SIEM** (que l’on prononce « sim ») combinent la gestion des informations de sécurité (**SIM**) et la gestion des événements de sécurité (**SEM**) au sein d’un même système de gestion de la sécurité. Un système **SIEM** collecte les données des journaux d’événements à partir de sources diverses, identifie les activités qui s’écartent de la norme grâce à une analyse en temps réel et applique les mesures appropriées.

En bref, une solution **SIEM** offre aux entreprises une visibilité sur l’activité de leur réseau pour leur permettre de réagir rapidement aux cyberattaques potentielles et de se conformer aux exigences de conformité.

Au cours de la dernière décennie, les technologies **SIEM** ont évolué : grâce à l’intelligence artificielle, la détection des menaces et la réponse aux incidents s’effectuent désormais plus intelligemment et plus rapidement.

PARTIE 3

Magic Quadrant SIEM – Gartner 2021

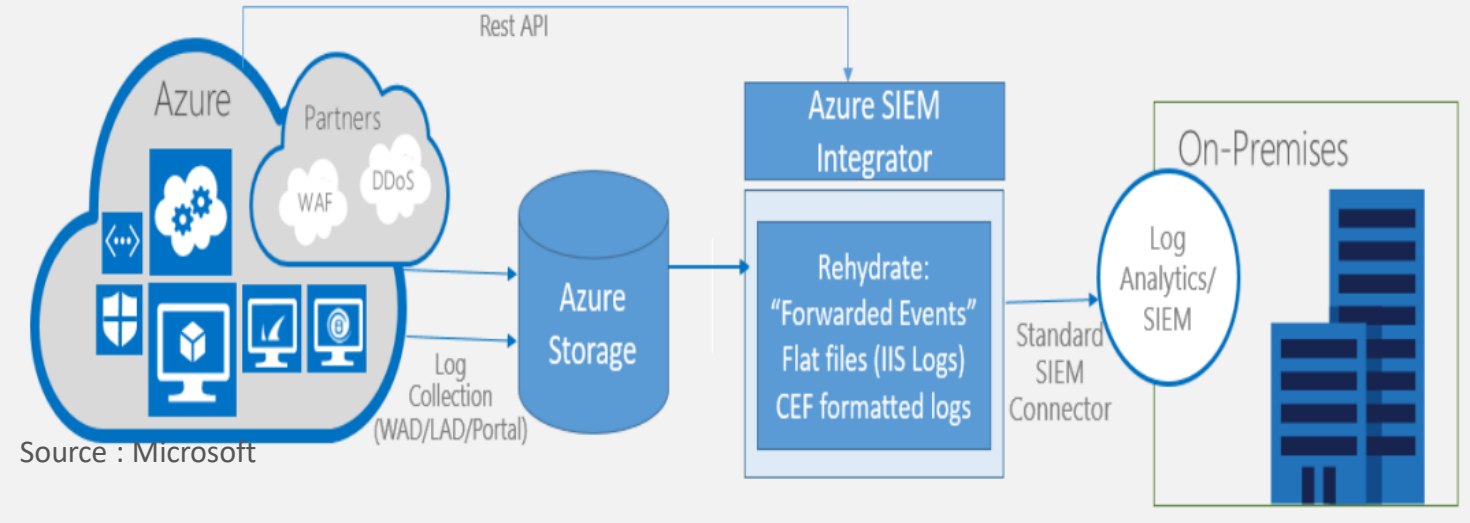
Figure 1: Magic Quadrant for Security Information and Event Management

Source: Gartner (June 2021)

Interconnexion SIEM avec le Cloud Azure

Microsoft Azure offre un ensemble d'outils (Azure SIEM Integrator) permettant l'interfaçage de la plateforme de journalisation avec les différents éditeurs SIEM du marché.

Ci-dessous, un schéma macro relatif à l'interconnexion des outils de journalisations avec une solution SIEM déployées on-premise :



Source : Microsoft

1. **Audit et collecte :** pour activer l'audit, vous pouvez soit le faire dans le portail Azure, soit avec l'API Azure et ligne de commande PowerShell. Une fois l'audit activé, la plupart des journaux sont stockés dans le compte de stockage du client. Vous pouvez configurer la durée de conservation. Certains services stockent les données de manière centralisée et exposent les données via l'API REST.
2. **Intégration SIEM :** l'intégrateur Azure SIEM est un composant côté client qui peut être configuré sur des VM dans un environnement sur site ou dans une machine virtuelle dans Azure. L'intégrateur SIEM collecte les données d'Azure et les réhydrate au fur et à mesure du besoin.

Interconnexion SIEM avec le Cloud Azure

Comme indiqué dans le schéma d'architecture, les ressources Azure et les solutions des partenaires produisent des audits et des journaux, qui sont soit stockés dans les comptes de stockage du client ou accessibles via l'API REST.

Intégrateur Azure SIEM qui est un composant côté client qui peut être installé sur une machine sur site ou sur des machines virtuelles dans Azure qui lit ces journaux et les convertit format standard (par exemple XML ou JSON) qui est ensuite transféré vers le SIEM sans que les fournisseurs SIEM n'aient besoin de déployer d'autres connecteurs.

Vous pouvez télécharger l'outil sur https://aka.ms/azlogdownload . Il est destiné à être installé sur une machine virtuelle avec un agent de connecteur SIEM standard (par exemple , Splunk Universal Forwarder , ArcSight Windows Event Collector agent ou Qradar wincollect). La VM est censée agir comme une passerelle de journalisation : elle collecte les journaux des comptes de stockage et les envoie au SIEM via un connecteur SIEM standard.

CHAPITRE 2

Utiliser un outil externe SIEM

1. Interconnexion SIEM avec le Cloud
2. **Rapatriement des événements Cloud sur le SIEM**
3. Tableau de bord de la sécurité

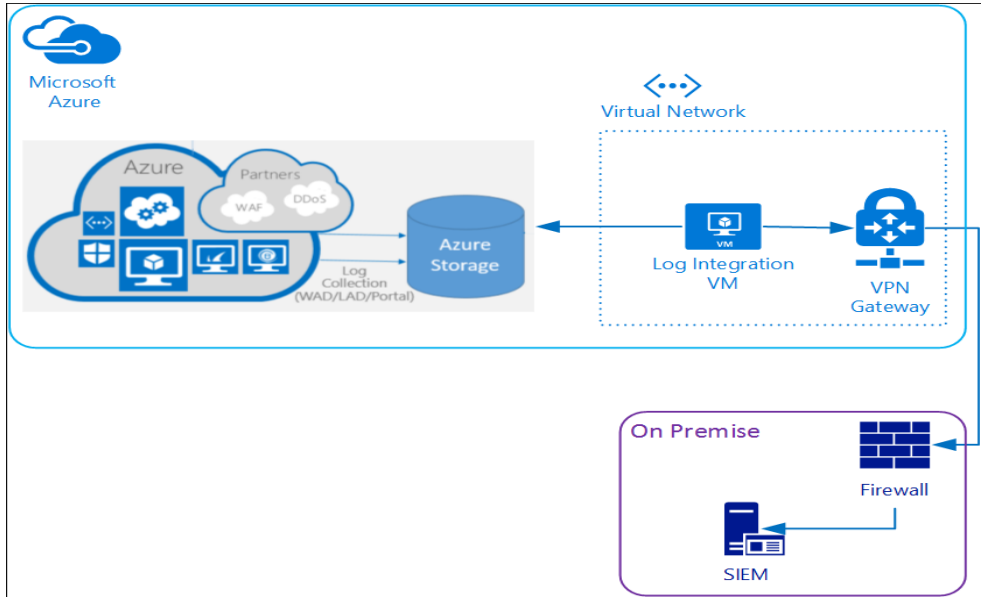
Architecture de rapatriement des événements Cloud sur le SIEM

Maintenant que nous avons examiné la solution générale, nous allons détailler où vont résider les différents composants.

En suivant le schéma de la section précédente de gauche à droite, les ressources Azure et le stockage Azure sont, bien sûr, dans Azure. La machine virtuelle exécutant l'intégration des journaux sera déployée sur Azure, alors que notre solution SIEM sera disponible sur site.

L'outil d'intégration de journaux sondera différentes parties du stockage Azure à intervalles réguliers. Pour de nombreuses ressources Azure avec des journaux détaillés, les besoins en bande passante du réseau peuvent être si exigeants que la connexion via Internet est trop lente ou peu fiable, auquel cas nous envisagerions de mettre en place une interconnexion site to site via une passerelle VPN Azure ou Azure Express Route.

Cette architecture hybride est la plus efficace sur le plan du réseau, car toutes les vérifications du stockage Azure se produiront dans Azure sans bande passante sur site. Seuls les journaux collectés expédiés sur site au SIEM nécessiteront de la bande passante.



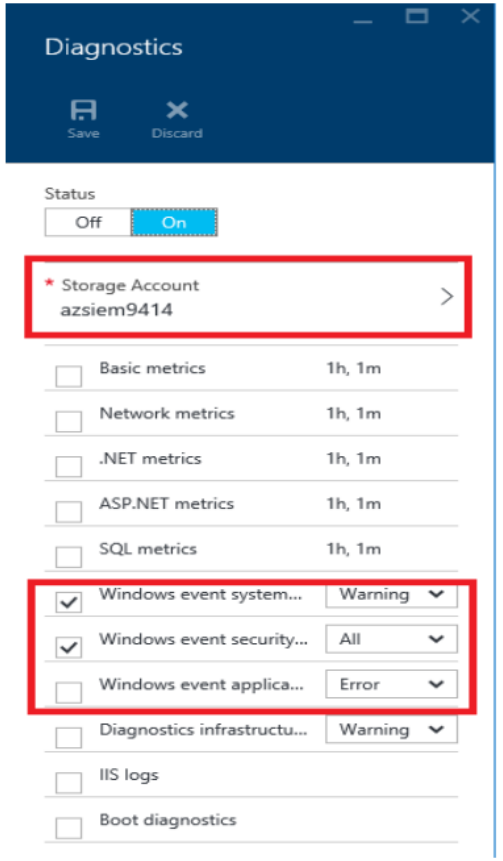
Source : Microsoft

Configuration pour le rapatriement des journaux d'événements Windows de la machine vers le SIEM

ÉTAPE 1 : ACTIVEZ LA COLLECTE DES JOURNAUX DANS LE PORTAIL AZURE

Pour une machine virtuelle Azure, vous pouvez activer la collecte de journaux à l'aide du portail Azure ou les lignes de commande PowerShell. Pour activer la collecte de journaux à partir du portail Azure :

1. Connectez-vous au portail Azure - https://portal.azure.com/
2. Cliquez sur Machines virtuelles dans la liste des services de gauche
3. Cliquez sur la machine virtuelle pour laquelle vous souhaitez activer collecte de journaux
4. Cliquez sur Diagnostics
5. Configurez les journaux que vous souhaitez collecter.
6. Sélectionnez également le compte de stockage où les données seront débarquées



PARTIE 3

Configuration pour le rapatriement des journaux d'événements Windows de la machine vers le SIEM

ÉTAPE 2 : CONFIGURER L'INTÉGRATEUR AZURE SIEM

Prérequis :

- Vous pouvez installer l'intégrateur SIEM sur une machine en local ou sur une machine virtuelle dans Azure (Windows OS)
- Cette machine doit avoir l'agent SIEM standard installé (par exemple, Splunk Universal Forwarder ou ArcSightagent Windows Event Collector ou Qradar wincollect) et pointant vers l'instance SIEM.
- Cette machine doit avoir accès à Internet pour se connecter au stockage Azure.

Installation :

Téléchargez le package à partir du lien http://aka.ms/azsiem et décompressez-le (placez-le dans un dossier autre qu'un répertoire à l'intérieur de n'importe quel profil utilisateur)

2. Ouvrez un invite de commande avec droit admin

3. Exécutez la commande : azsiem install accepteula

Configuration pour le rapatriement des journaux d'événements Windows de la machine vers le SIEM

4. Exécutez la commande : azsiem source add **<FriendlyNameForTheSource>** WAD **<Nom du compte de stockage> <StorageKey>**

Exemple : **azsiem source add maheshsiemtest WAD azsiem9414 FullKey**

En option, vous pouvez ajouter l'ID d'abonnement au nom convivial si vous souhaitez que l'ID d'abonnement s'affiche dans l'événement XML.

azsiem source add <FriendlyNameForTheSource.SubscriptionID> WAD <StorageNom du compte> <StorageKey>

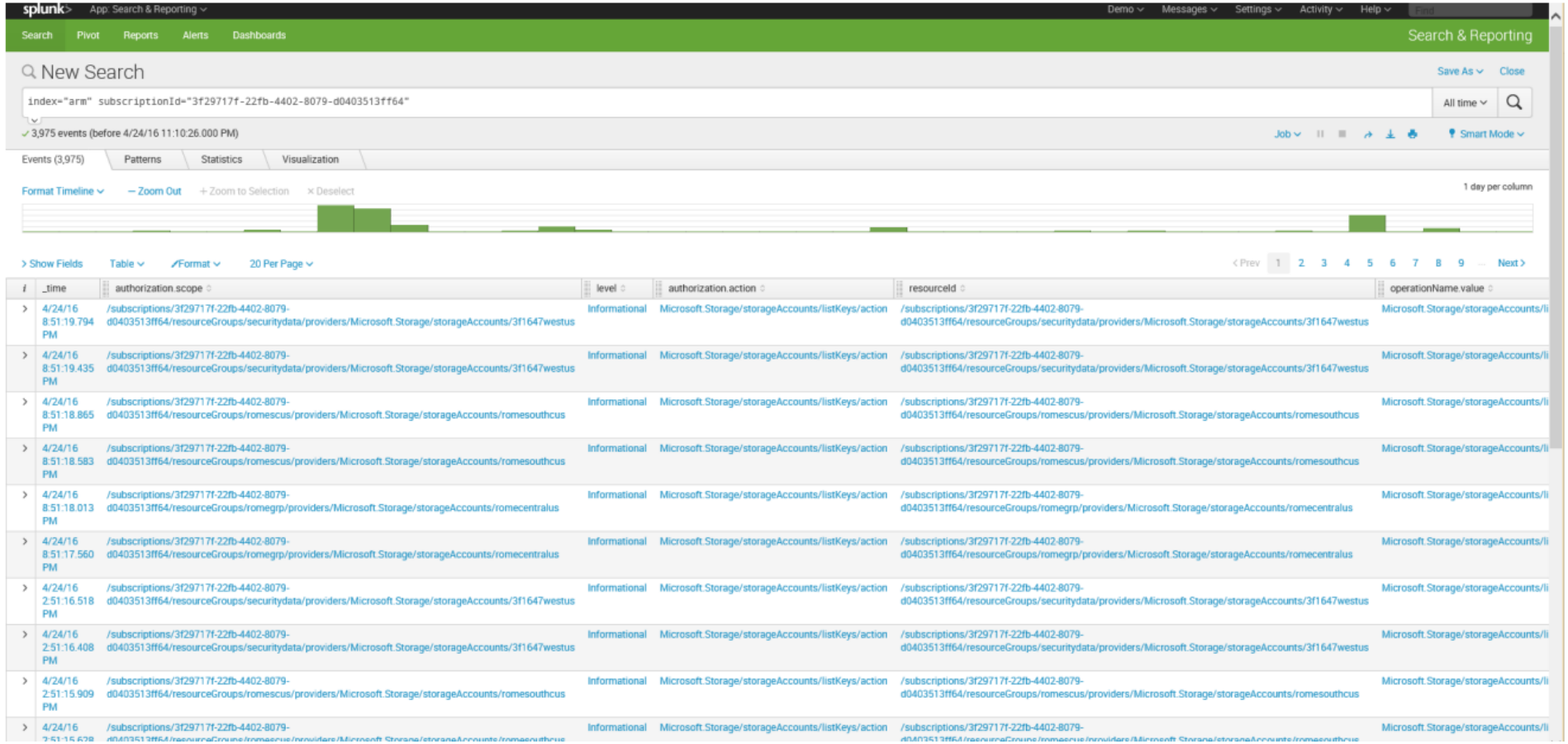
Remarque : Le nom et la clé du compte de stockage doivent correspondre au compte de stockage que vous avez sélectionné lors de la collecte des journaux à l'étape 1 ci-dessus.

5. Vous devriez maintenant commencer à voir les événements dans le dossier des événements transférés sur la même machine. Ouvrir l'Observateur d'événements → Journal des événements Windows → Événements transférés.

6. Assurez-vous que le connecteur SIEM standard (par exemple, Splunk Universal Forwarder ou ArcSight Windows Event SmartCollector ou Qradar wincollect) installé sur la machine est configuré pour sélectionner les événements du dossier des événements transférés et dirigez-les vers l'instance SIEM.

Interface de consultation des logs dans SPLUNK

L'interface principale de recherche Splunk, permet d'afficher les différents évènements reçus depuis Azure :



CHAPITRE 2

Utiliser un outil externe SIEM

1. Interconnexion SIEM avec le Cloud
2. Rapatriement des événements Cloud sur le SIEM
3. **Tableau de bord de la sécurité**

PARTIE 3

Microsoft Azure Sentinel pour le Cloud Azure

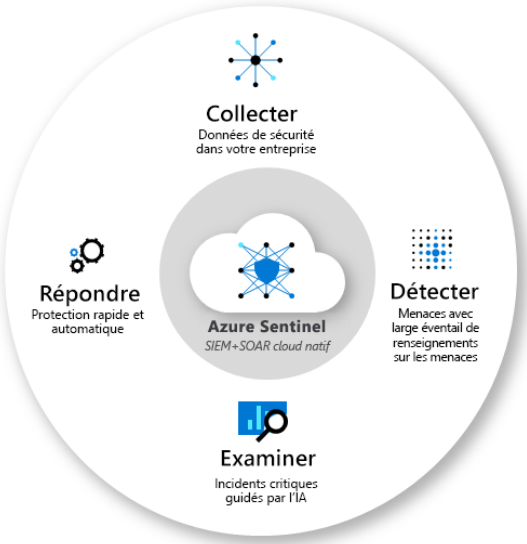
Microsoft Sentinel est une solution native Cloud évolutive qui fournit les fonctions suivantes :

- Informations et gestion des événements (SIEM)
- Orchestration, automatisation et réponse en matière de sécurité (SOAR)

Microsoft Sentinel fournit une analytique de sécurité intelligente et des renseignements sur les menaces à l'échelle de l'entreprise. Avec Microsoft Sentinel, vous disposez d'une solution unique pour la détection des attaques, la visibilité des menaces, la chasse proactive et la réponse aux menaces.

Microsoft Sentinel vous offre une vue d'ensemble de l'entreprise, ce qui réduit le stress lié aux attaques de plus en plus sophistiquées, aux volumes croissants d'alertes et aux longs délais de résolution.

- **Collectez des données à l'échelle du Cloud** sur l'ensemble des utilisateurs, appareils, applications et infrastructures, tant locaux que dans de multiples Cloud.
- **Détectez les menaces non détectées précédemment** et réduisez les faux positifs en vous appuyant sur l'analytique et les systèmes de renseignement incomparables sur les menaces fournis par Microsoft.
- **Investiguez les menaces à l'aide de l'intelligence artificielle** et recherchez les activités suspectes à grande échelle en profitant des années de travail que Microsoft a consacrées à la cybersécurité.
- **Répondez aux incidents rapidement** avec une orchestration et une automatisation intégrées des tâches courantes.



PARTIE 3

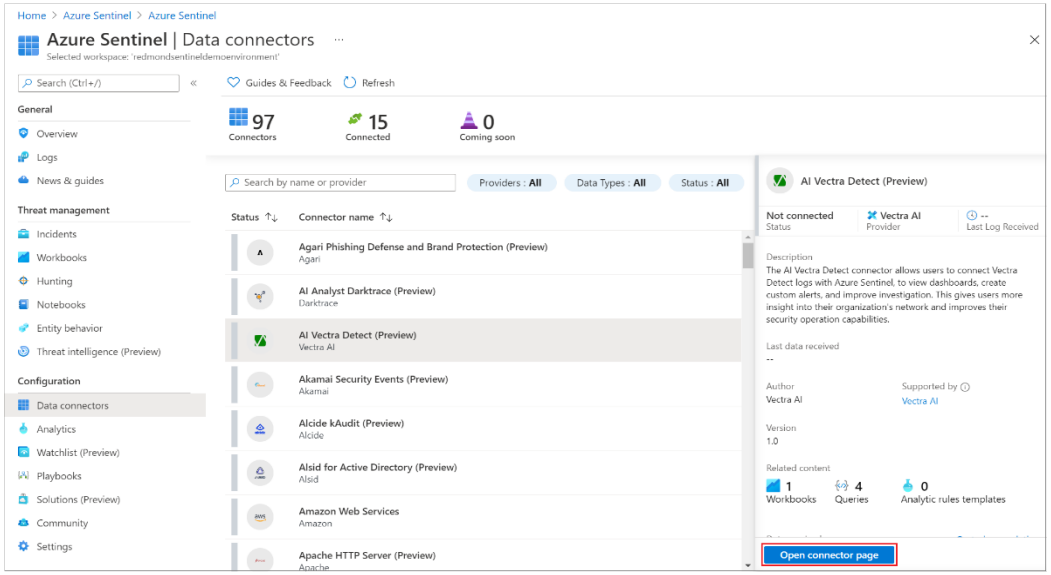
Collecter des données à l'aide de connecteurs de données

Pour intégrer Microsoft Sentinel, vous devez commencer par vous connecter à vos sources de données.

Microsoft Sentinel est fourni avec de nombreux connecteurs pour les solutions Microsoft, prêts à l'emploi et offrant une intégration en temps réel. Certains de ces connecteurs incluent les éléments suivants :

- Sources Microsoft telles que Microsoft 365 Defender, Microsoft Defender pour le Cloud, Office 365, Microsoft Defender pour IoT, etc.
- Sources de service Azure comme Azure Active Directory, Activité Azure, Stockage Azure, Azure Key Vault, Azure Kubernetes Service, etc.

Microsoft Sentinel a des connecteurs intégrés à des écosystèmes de sécurité et d'applications plus larges pour les solutions non-Microsoft. Vous pouvez également utiliser le format d'événement commun, Syslog ou une API REST pour connecter vos sources de données avec Microsoft Azure Sentinel.



Source : Portail Azure

PARTIE 3

Créer des Tdb interactifs à l'aide de Workbooks (Classeurs)

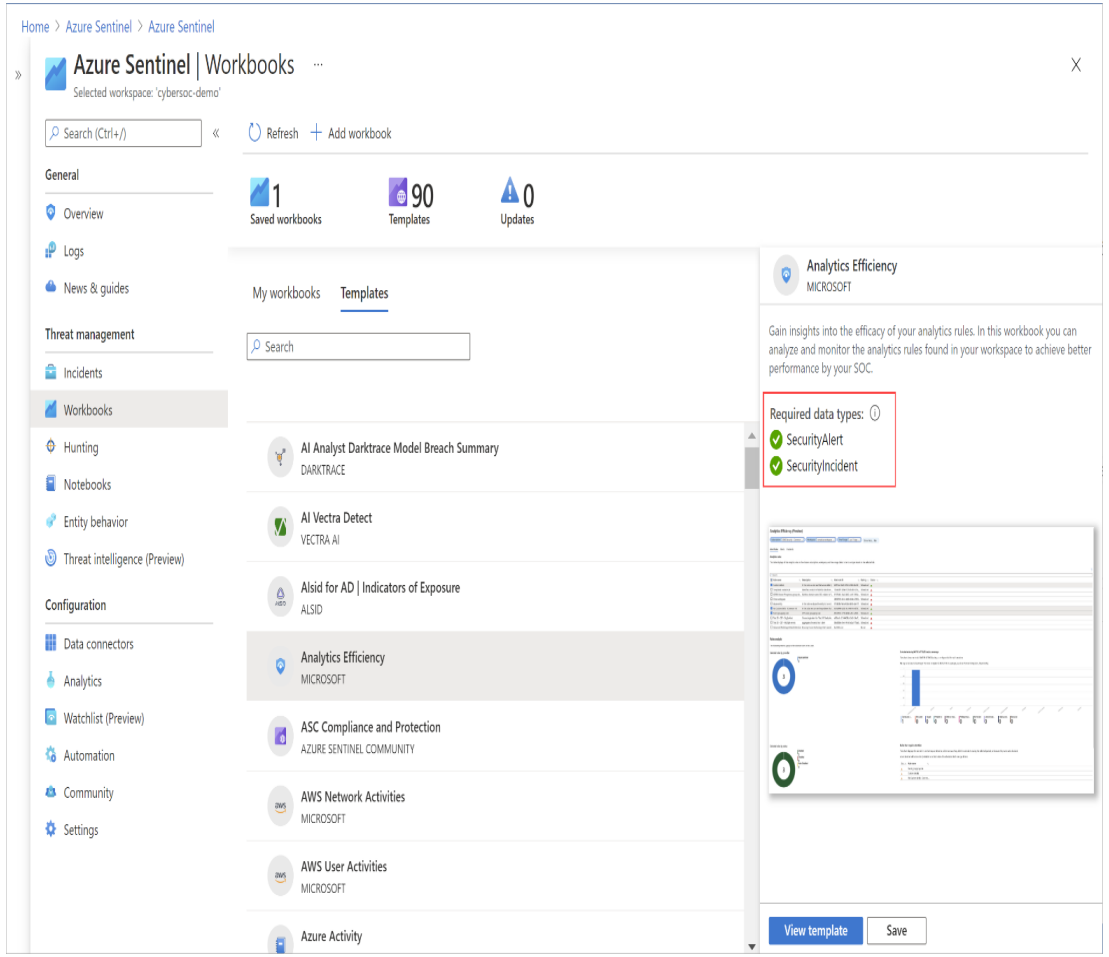
Après avoir opéré l'intégration à Microsoft Sentinel, surveillez vos données en utilisant l'intégration avec des classeurs Azure Monitor.

Les classeurs s'affichent différemment dans Microsoft Sentinel et dans Azure Monitor. Il peut cependant être utile de voir comment créer un classeur dans Azure Monitor. Microsoft Sentinel vous permet de créer des classeurs personnalisés à partir de vos données. Microsoft Sentinel est également fourni avec des modèles de classeurs intégrés qui vous permettent d'obtenir rapidement des aperçus sur vos données dès que vous vous connectez à une source de données.

Les classeurs sont destinés aux ingénieurs et analystes SOC de tous niveaux pour visualiser les données.

Les classeurs sont idéaux pour des vues générales de données Microsoft Sentinel et ne nécessitent aucune connaissance en codage.

Toutefois, vous ne pouvez pas intégrer des classeurs avec des données externes.

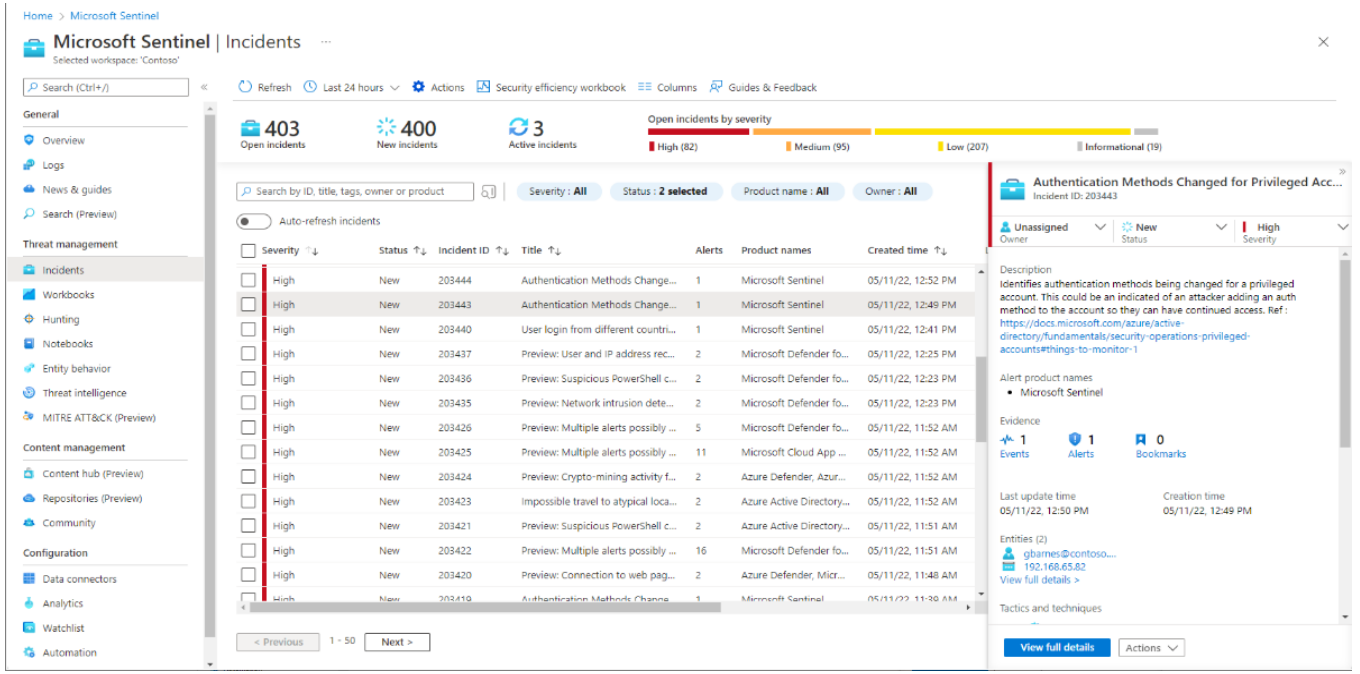


PARTIE 3

Corréler des alertes dans des incidents en utilisant des règles d'analyse

Pour vous aider à réduire le niveau de bruit et à réduire le nombre d'alertes que vous devez examiner, Microsoft Sentinel utilise l'analytique pour mettre en corrélation les alertes et les incidents.

Les incidents sont des groupes d'alertes liées qui, prises ensemble, indiquent une menace possible actionnable, que vous pouvez examiner et résoudre. Utilisez les règles de corrélation intégrées telles quelles ou utilisez-les comme point de départ pour créer vos propres règles. Microsoft Sentinel fournit également des règles d'apprentissage machine pour cartographier le comportement de votre réseau et rechercher les possibles anomalies sur vos ressources. Ces analyses connectent ensuite les informations en transformant les alertes basse fidélité sur différentes entités en incidents de sécurité potentiels de haute fidélité.

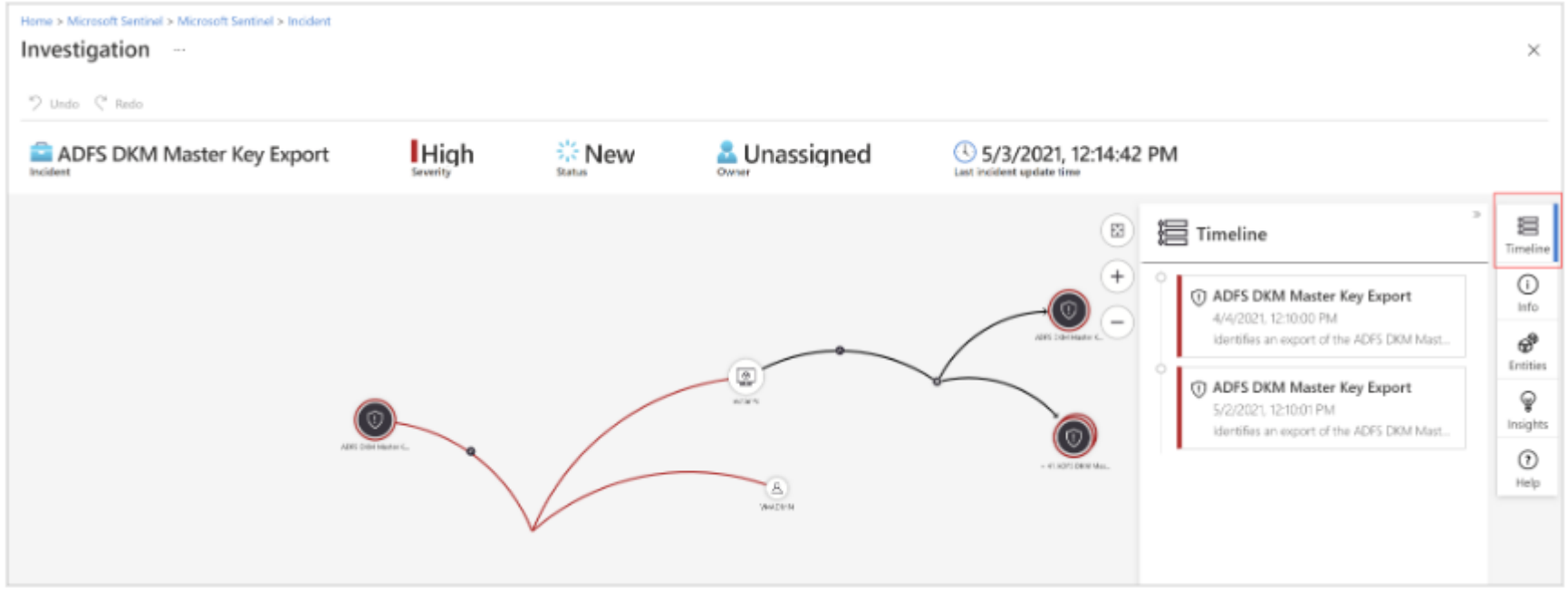


Source : Portail Azure

PARTIE 3

Examiner l'étendue et la cause racine de menaces de sécurité

Les outils d'investigation approfondie d'Azure Sentinel vous aident à comprendre l'étendue et à identifier la cause racine d'une menace de sécurité potentielle. Vous pouvez choisir une entité sur le graphique interactif pour poser des questions sur une entité spécifique et approfondir cette entité et ses connexions pour arriver à la cause racine de la menace.

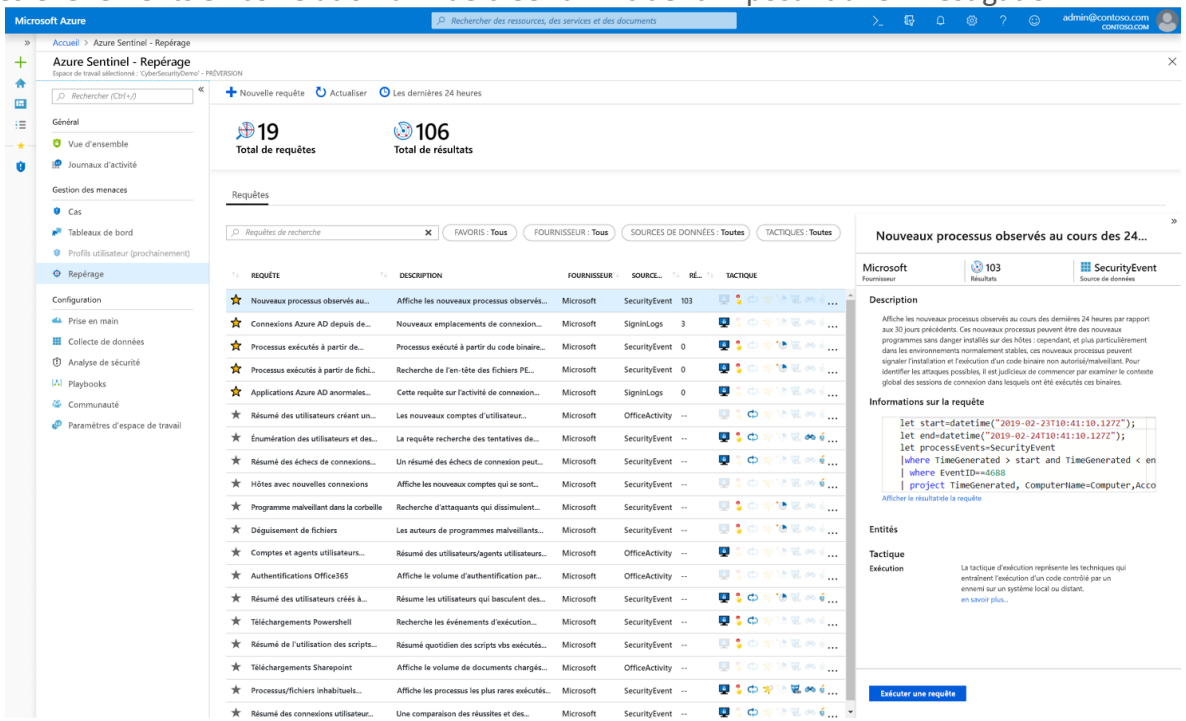


PARTIE 3

Repérer les menaces de sécurité à l'aide de requêtes intégrées

Utilisez les puissants outils de recherche et de requête de Microsoft Sentinel, basés sur l'infrastructure MITRE, et qui vous permettent de façon proactive de rechercher les menaces de sécurité sur toutes les sources de données de votre organisation avant même le déclenchement d'une alerte. Créez des règles de détection personnalisées en fonction de votre requête de chasse (repérage). Ensuite, exposez ces aperçus en tant qu'alertes à vos répondeurs d'incidents de sécurité.

Lors de la chasse, créez des signets pour revenir aux événements intéressants plus tard. Utilisez un signet pour partager un événement avec d'autres personnes. Ou bien, regroupez des événements avec d'autres événements en corrélation afin de créer un incident imposant une investigation.



Source : Portail Azure