

RÉSUME THÉORIQUE - FILIÈRE INFRASTRUCTURE DIGITALE

M206 – Gouverner les données dans le Cloud

30 heures

SOMMAIRE



1. **Préparer les données pour le Cloud**
   - Identifier les niveaux des données
   - Assurer la fiabilité des données
   - Vérifier la conformité réglementaire
2. **Cartographier les données sur le Cloud**
   - Inventorier les données
   - Cartographier les données
3. **Établir des stratégies de transferts des données**
   - Etablir des stratégies d'entrée
   - Etablir des stratégies de sortie

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

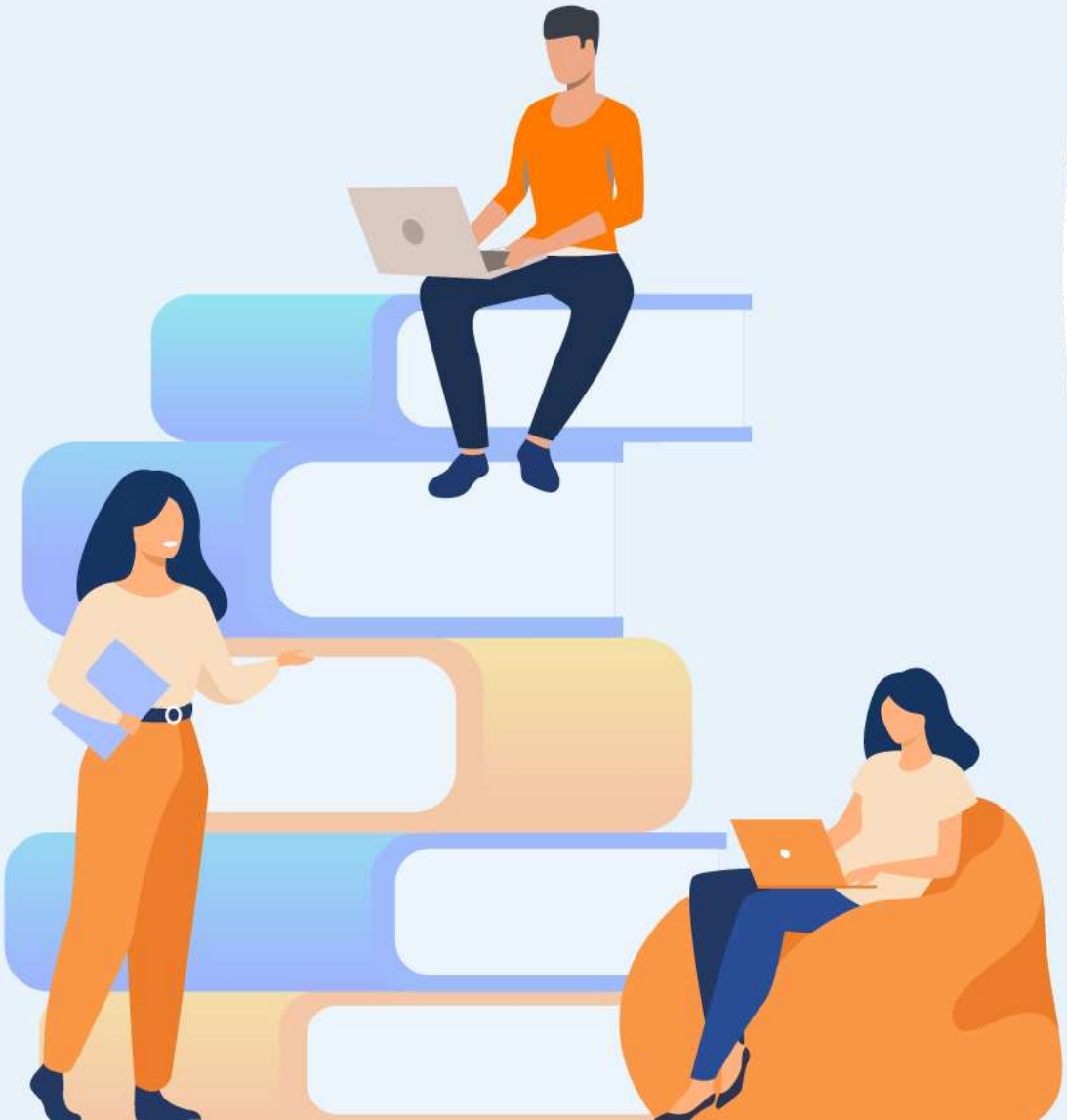


5

DES RESSOURCES EN LIGNES

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

Copyright - Tout droit réservé - OFPPT



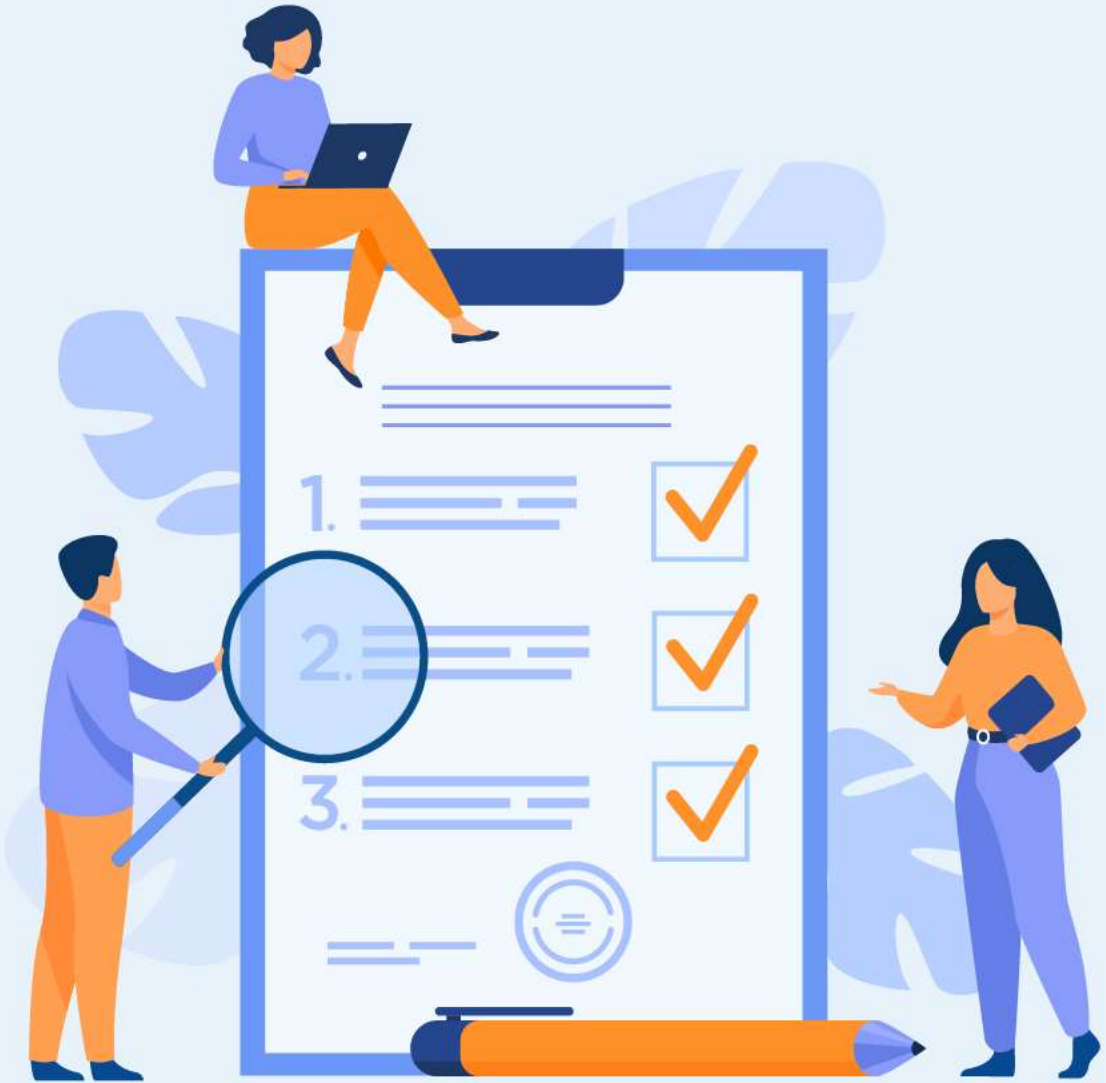
PARTIE 1

Préparer les données pour le Cloud

Dans ce module, vous allez :

- Identifier les niveaux des données
- Vous assurer de la fiabilité des données
- Vérifier la conformité réglementaire

9 heures



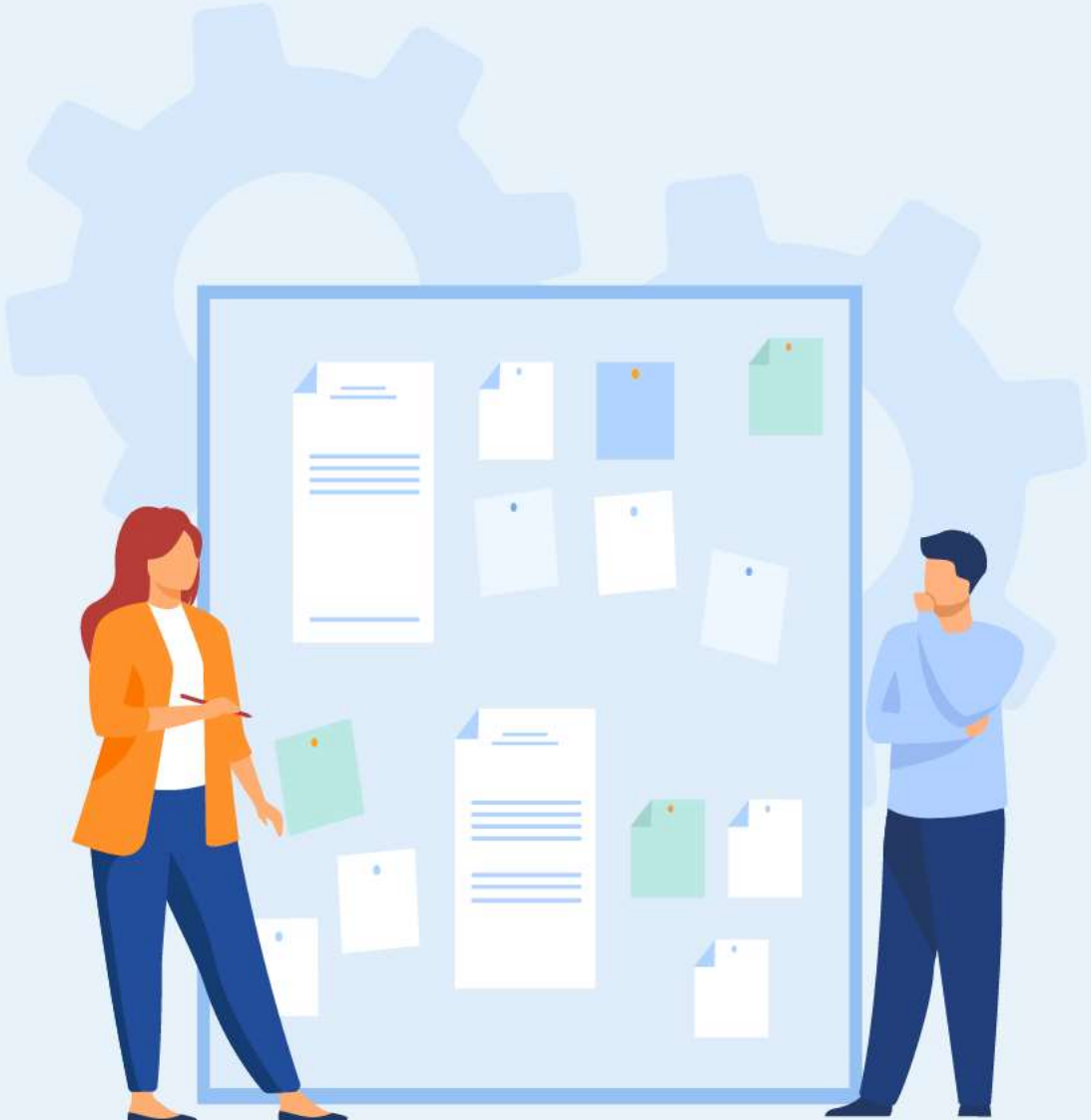
CHAPITRE 1

Identifier les niveaux des données

Ce que vous allez apprendre dans ce chapitre :

- Découvrir l'impact de la donnée sur l’activité
- Comprendre la classification des données : Publiques, Internes, Confidentielles
- Appréhender le format des données : Structurées, Semi-structurées, Non structurée

9 heures



CHAPITRE 1

Identifier les niveaux des données

1. **Découvrir l'impact des données sur l’activité**
2. Comprendre la classification des données : Publiques, Internes, Confidentielles
3. Appréhender le format des données : Structurées, Semi-structurées, Non structurée

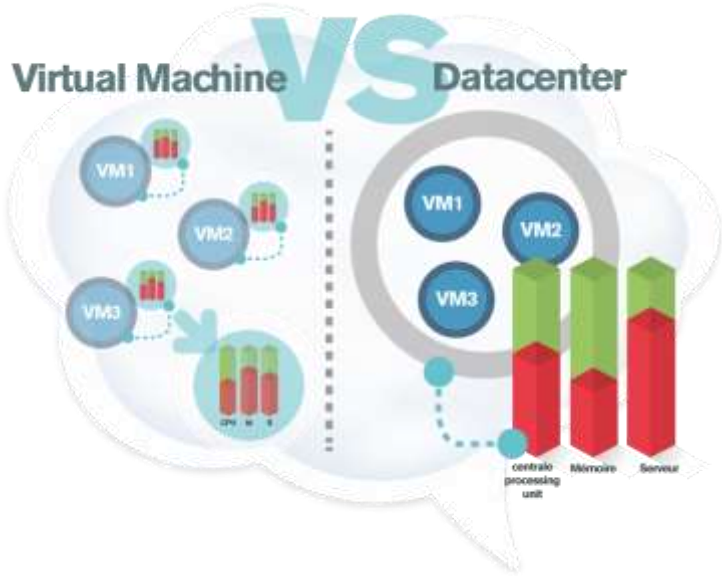
Préparer une stratégie informatique d'entreprise pour le Cloud

Les données sont le moteur de l'entreprise et leurs formats sont aussi divers que variés, allant des bases de données relationnelles constituées à partir de règles strictes jusqu'à votre dernier post sur Facebook. Quel que soit leur format, toutes ces données peuvent être classées en deux catégories : les données structurées et les données non structurées.

La gouvernance Cloud est le fruit d'un travail d'adoption sur le long terme, car une transformation durable nécessite un effort de moyen long terme. Vous avez peu de chances d'obtenir des résultats satisfaisants si vous essayez de fournir une gouvernance Cloud complète, avant de prendre en charge les modifications-clés de la stratégie d'entreprise ou si vous optez pour une méthode rapide et agressive. Nous recommandons donc d'opter pour une approche incrémentielle.

Ce qui est différent dans notre Framework d'adoption du Cloud, c'est le cycle d'achat et sa capacité à réaliser une transformation authentique. Comme il n'existe pas d'obligation à mobiliser des dépenses d'investissement importantes, les ingénieurs peuvent débuter par une expérimentation, puis la généraliser. Dans la plupart des cultures d'entreprise, le fait de faire tomber cette barrière financière à l'adoption peut aboutir à des boucles de rétroaction plus courtes, une croissance naturelle et une exécution incrémentielle.

Le passage au Cloud implique de changer la gouvernance. Dans beaucoup d'organisations, la transformation de la stratégie d'entreprise permet d'améliorer la gouvernance et d'augmenter les taux de conformité. Ces optimisations sont possibles grâce aux changements incrémentiels de stratégie et à l'application automatique de ces derniers. Pour ce faire, vous disposez de capacités nouvellement définies, que vous pouvez configurer avec votre fournisseur de services Cloud.



PARTIE 1

Copyright - Tout droit réservé - OFPPT

01- Identifier les niveaux des données

Découvrir l'impact des données sur l'activité

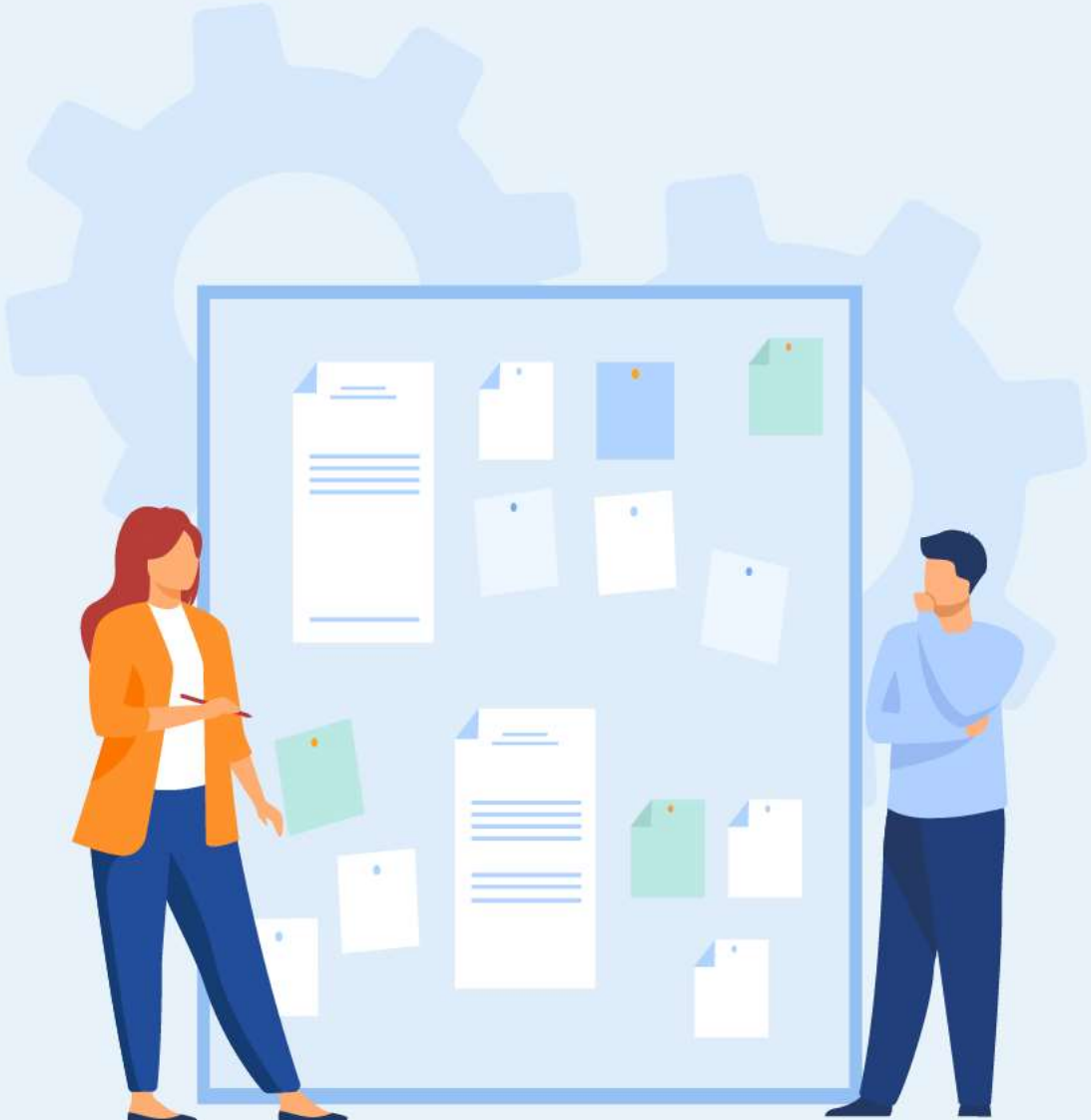
Définition de la stratégie d'entreprise pour faire évoluer la gouvernance Cloud

Dans la gouvernance traditionnelle et incrémentielle, la stratégie d'entreprise crée la définition pratique de la gouvernance. La plupart des actions de gouvernance informatique cherchent à implémenter la technologie afin de superviser, appliquer, exécuter et automatiser ces stratégies d'entreprise. La gouvernance Cloud s'appuie sur des concepts similaires.



PARTIE 1

Copyright - Tout droit réservé - OFPPT



CHAPITRE 1

Identifier les niveaux des données

1. Découvrir l'impact des données sur l’activité
2. **Comprendre la classification des données : Publiques, Internes, Confidentielles**
3. Appréhender le format des données : Structurées, Semi-structurées, Non structurée

01- Identifier les niveaux des données

Comprendre la classification des données : Publiques, Internes, Confidentielles

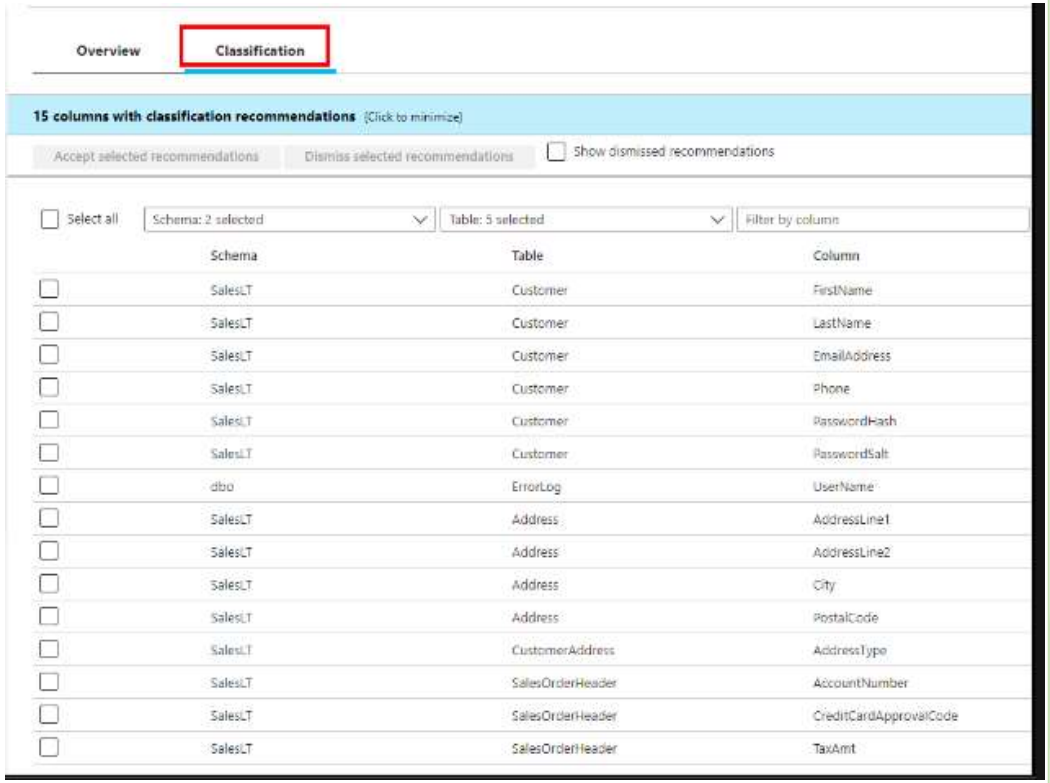
Qu'est-ce que la classification des données ?

La classification des données vous permet de déterminer et d'affecter la valeur aux données de votre organisation et constitue un point de départ commun pour la gouvernance. Le processus de classification des données classe les données en fonction de leur sensibilité et de leur impact commercial afin d'identifier les risques. Une fois les données classées, vous pouvez les gérer de manière à protéger les données sensibles ou importantes contre le vol ou la perte.

Comprendre les risques liés aux données, puis les gérer

Avant d'atténuer un risque, il convient de le comprendre. En cas de responsabilité face à une violation des données, cette compréhension passe par la classification des données. Le processus de classification des données consiste à associer une caractéristique de métadonnées à chaque ressource du patrimoine numérique afin d'identifier le type de données associé à cette ressource.

Toutes les ressources identifiées comme des candidates potentielles à la migration ou au déploiement vers le Cloud doivent être associées à des métadonnées qui permettent d'enregistrer la classification des données, l'importance dans l'entreprise et le responsable de facturation. Ces trois points de classification peuvent se révéler très utiles à la compréhension et l'atténuation des risques.



PARTIE 1

Copyright - Tout droit réservé - OFPPT

01- Identifier les niveaux des données

Comprendre la classification des données : Publiques, Internes, Confidentielles

Niveaux de classification des données

En vous posant ces questions, vous pouvez vous constituer une idée de comment classer vos données.

La data classification peut généralement être divisée en quatre catégories :

Données publiques

Ces données sont accessibles au public, soit localement, soit sur Internet.

Les données publiques nécessitent peu de sécurité, et leur divulgation n'entraînerait pas de violation de la conformité.

Données internes

Les mémos, la propriété intellectuelle et les messages électroniques sont quelques exemples de données qui doivent être réservés aux employés internes.

Données confidentielles

La différence entre les données internes et les données confidentielles est que les données confidentielles nécessitent une autorisation pour y accéder.

Vous pouvez attribuer cette autorisation à des employés spécifiques ou à des fournisseurs tiers autorisés.

PARTIE 1

Copyright - Tout droit réservé - OFPPT

01- Identifier les niveaux des données

Comprendre la classification des données : Publiques, Internes, Confidentielles

Classifications utilisées par Microsoft

La liste ci-dessous répertorie les classifications utilisées par Microsoft. En fonction de votre secteur d'activité ou de vos exigences de sécurité existantes, il se peut que des normes de classifications des données existent déjà au sein de votre organisation. Si ce n'est pas le cas, nous vous invitons à utiliser cet exemple de classification. Il vous permettra de mieux comprendre votre patrimoine numérique et votre profil de risque.

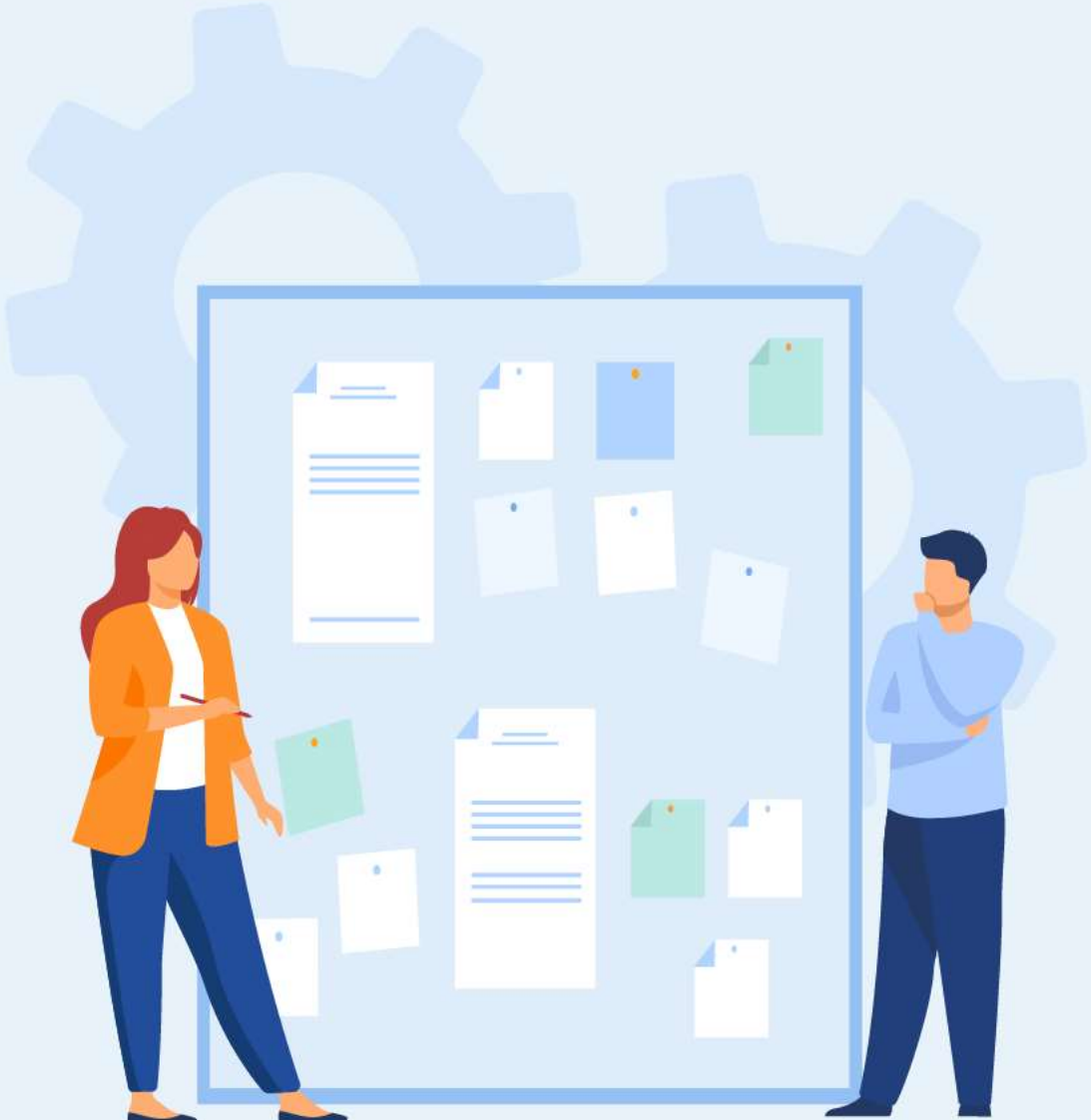
- **Non professionnelles :** Données concernant votre vie personnelle qui n'appartiennent pas à Microsoft.
- **Publiques :** Données d'entreprise qui sont mises à disposition librement et destinées à être utilisées publiquement.
- **Généralités :** Données d'entreprise non destinées au public.
- **Confidentielles :** Données d'entreprise susceptibles de nuire à Microsoft si elles sont partagées.
- **Hautement confidentielles :** Données d'entreprise susceptibles de porter un préjudice important à Microsoft si elles sont partagées

Balisage de classification des données dans Azure

Les balises de ressource sont une bonne approche suggérée pour le stockage des métadonnées. Vous pouvez utiliser ces balises pour appliquer des informations de classification aux ressources déployées. Bien que le marquage des ressources Cloud par classification ne remplace pas le processus formel de classification des données, il s'agit d'un outil précieux pour la gestion des ressources et l'application de la stratégie.

PARTIE 1

Copyright - Tout droit réservé - OFPPT



CHAPITRE 1

Identifier les niveaux des données

1. Découvrir l'impact des donnée sur l’activité
2. Comprendre la classification des données : Publiques, Internes, Confidentielles
3. **Appréhender le format des données : Structurées, Semi-structurées, Non structurée**

Les aspects fondamentaux pour définir le format des données

Les données structurées se différencient des données non structurées via le qui, quoi, quand, où et comment des données :

- Qui utilisera les données ?
- Quel type de données collectez-vous ?
- Quand faut-il préparer les données, avant leur stockage ou après leur traitement ?
- Où les données seront-elles stockées ?
- Comment les données seront-elles stockées ?

Ces cinq questions soulignent les aspects fondamentaux qui permettent aux utilisateurs de comprendre en quoi les données diffèrent les unes des autres.



Copyright - Tout droit réservé - OFPPT

Qu'est-ce qu'une donnée structurée ?

Une donnée structurée est une donnée qui a été prédéfinie et formatée selon une structure précise avant d'être placée dans un data Warehouse, un processus désigné par « schema-on-write », ou schéma à l'écriture. La base de données relationnelle est le meilleur exemple de données structurées : les données ont été formatées dans des champs précisément définis, comme le numéro de carte de crédit ou l'adresse, pour être facilement interrogées avec SQL.

Avantages des données structurées : elles présentent trois avantages clés repris ci-après :

1. **Un traitement facile par les algorithmes de Machine Learning** : le principal avantage des données structurées est leur facilité de traitement par le Machine Learning. La nature précise et organisée des données structurées permet de manipuler et interroger ces dernières facilement.
2. **Un traitement facile par les utilisateurs professionnels** : un autre avantage des données structurées est qu'elles peuvent être traitées par un utilisateur professionnel type qui connaît le sujet auxquelles elles se rapportent. Une connaissance approfondie des différents types de données ou des relations de ces données n'est pas nécessaire. Les données sont accessibles en libre-service par l'utilisateur professionnel.
3. **Davantage d'outils accessibles** : les données structurées ont également l'avantage d'être traitées depuis bien plus longtemps car elles étaient traditionnellement la seule option. Davantage d'outils ont donc été essayés et testés pour le traitement et l'analyse de données structurées. Les responsables des données peuvent choisir parmi davantage de produits lorsqu'ils utilisent des données structurées.

Copyright - Tout droit réservé - OFPPT

Qu'est-ce qu'une donnée structurée ?

Les inconvénients des données structurées

Les inconvénients des données structurées reposent principalement sur un manque de flexibilité. Voici quelques inconvénients potentiels à utiliser des données structurées :

- **Un but prédéfini en limite l'utilisation** : même si définir des données via un schéma à l'écriture est un gros avantage pour les données structurées, il est vrai qu'une donnée avec une structure prédéfinie ne peut être traitée que pour la finalité à laquelle elle est destinée. Cela limite sa flexibilité et ses cas d'usage.
- **Des options de stockage limitées :** les données structurées sont généralement stockées dans des data Warehouse. Les data Warehouse sont des systèmes de stockage de données ayant des schémas rigides. Toute modification des exigences entraîne la mise à jour de toutes ces données structurées pour les adapter aux nouveaux besoins. Cela génère des dépenses massives en termes de ressources et de temps. Une partie des coûts peut être réduite grâce au data Warehouse Cloud car il offre une plus grande évolutivité et supprime les frais de maintenance liés aux logiciels et machines on-premise.

Exemples de données structurées

Les données structurées font partie de nos vies depuis longtemps. Les systèmes de contrôle des stocks et les distributeurs automatiques en dépendent. Les données structurées peuvent être générées par l'homme ou par une machine.

Les statistiques de blog et les données relatives aux ventes, comme les codes-barres et les quantités, sont des exemples-types de données structurées générées par des machines. Et quiconque traite des données connaît les feuilles de calcul : un exemple classique de données structurées générées par l'homme.

Copyright - Tout droit réservé - OFPPT

Qu'est-ce qu'une donnée non structurée ?

Une donnée non structurée est une donnée stockée dans son format d'origine et non traitée avant son utilisation, un processus désigné par « schema-on-read », ou schéma à la lecture. Elle se présente sous une multitude de formats de fichiers, comme des e-mails, des posts sur les réseaux sociaux, des présentations, des chats, des données de capteurs IoT et des images satellites.

Avantages des données non structurée : tout comme les données structurées ont des avantages et des inconvénients, les données non structurées présentent également des forces et des faiblesses en fonction des besoins spécifiques de l'entreprise. Parmi ses avantages, on peut citer :

- **La liberté du format natif** : les données non structurées étant stockées dans leur format d'origine, elles ne sont définies qu'en cas de besoin. Cela permet un plus grand nombre de cas d'utilisation car la finalité des données est adaptable. Les experts en données peuvent donc préparer et analyser uniquement les données dont ils ont besoin. Le format natif permet aussi d'avoir une plus grande variété de formats de fichiers dans la base de données, car les données peuvent y être stockées quel que soit leur format. L'entreprise peut donc exploiter davantage de données.
- **Un taux d'accumulation plus rapide :** un autre avantage des données non structurées est le taux d'accumulation des données. Les données ne devant pas être prédéfinies, elles peuvent ainsi être collectées rapidement et facilement.
- **Un stockage dans un data lake :** les données non structurées sont souvent stockées dans des data lakes Cloud, qui offrent un espace de stockage massif. Les data lakes Cloud permettent aussi de facturer le stockage en fonction de son utilisation, ce qui réduit les coûts et simplifie l'évolutivité.

Copyright - Tout droit réservé - OFPPT

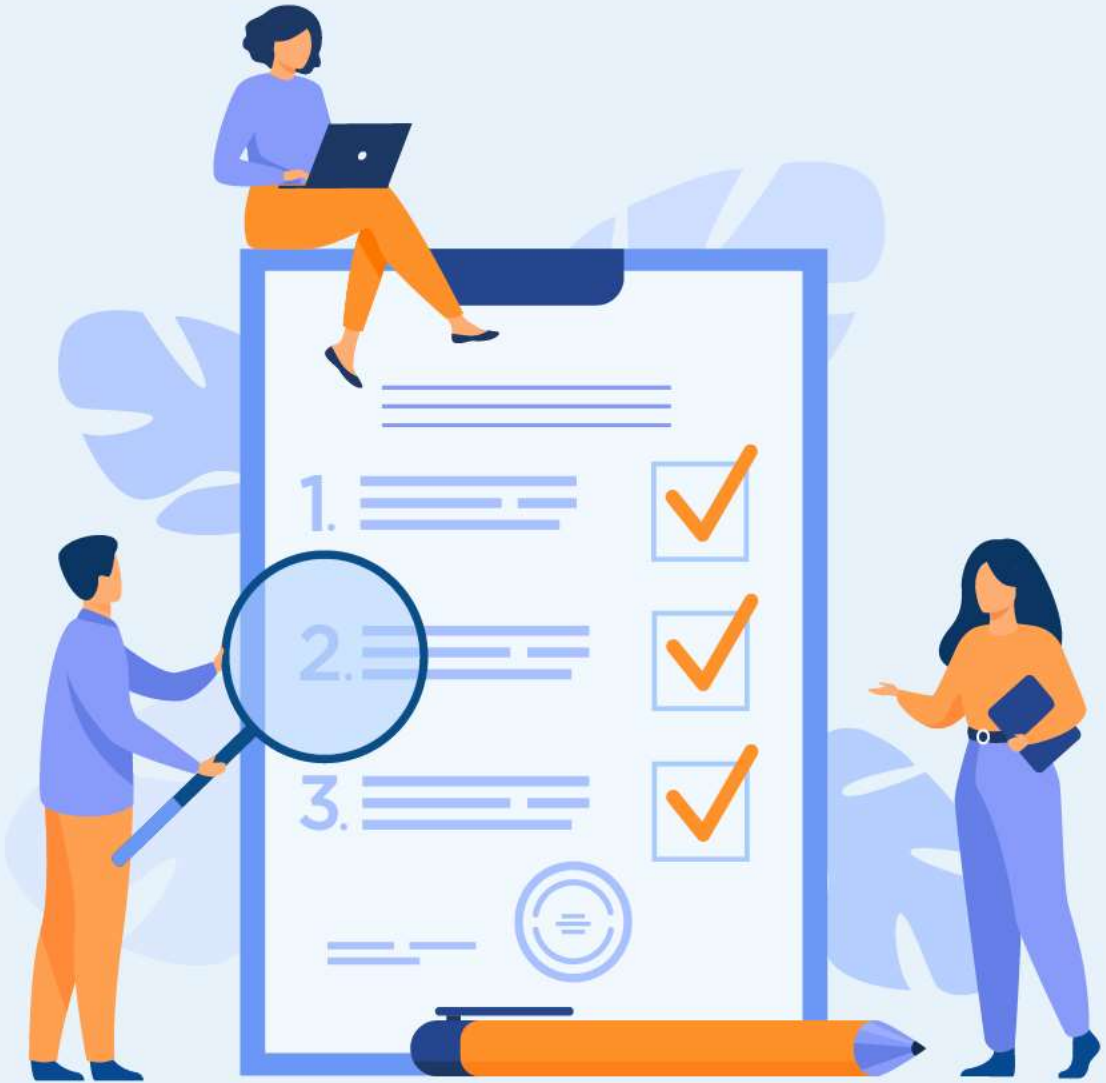
Qu'est-ce qu'une donnée non structurée ?

Les inconvénients des données non structurées

L'utilisation de données non structurées présente aussi des inconvénients. Elles nécessitent une expertise spécifique et des outils spéciaux pour en exploiter pleinement le potentiel.

- **Expertise en data science :** le principal inconvénient des données non structurées est que leur préparation et leur analyse nécessitent une expertise en data science. Un utilisateur professionnel standard ne peut pas utiliser des données non structurées telles quelles, en raison de leur nature non définie/non formatée. L'utilisation de données non structurées nécessite une connaissance du sujet ou du domaine des données, mais aussi de la façon de connecter ces dernières pour qu'elles soient exploitables.
- **Outils spéciaux** : en plus de l'expertise requise, les données non structurées nécessitent des outils spéciaux pour les manipuler. Les outils de données standards ont été conçus pour des données structurées, ce qui laisse un choix limité au responsable des données. Quand aux outils destinés aux données non structurées, certains n'en sont encore qu'à leurs balbutiements.

Copyright - Tout droit réservé - OFPPT



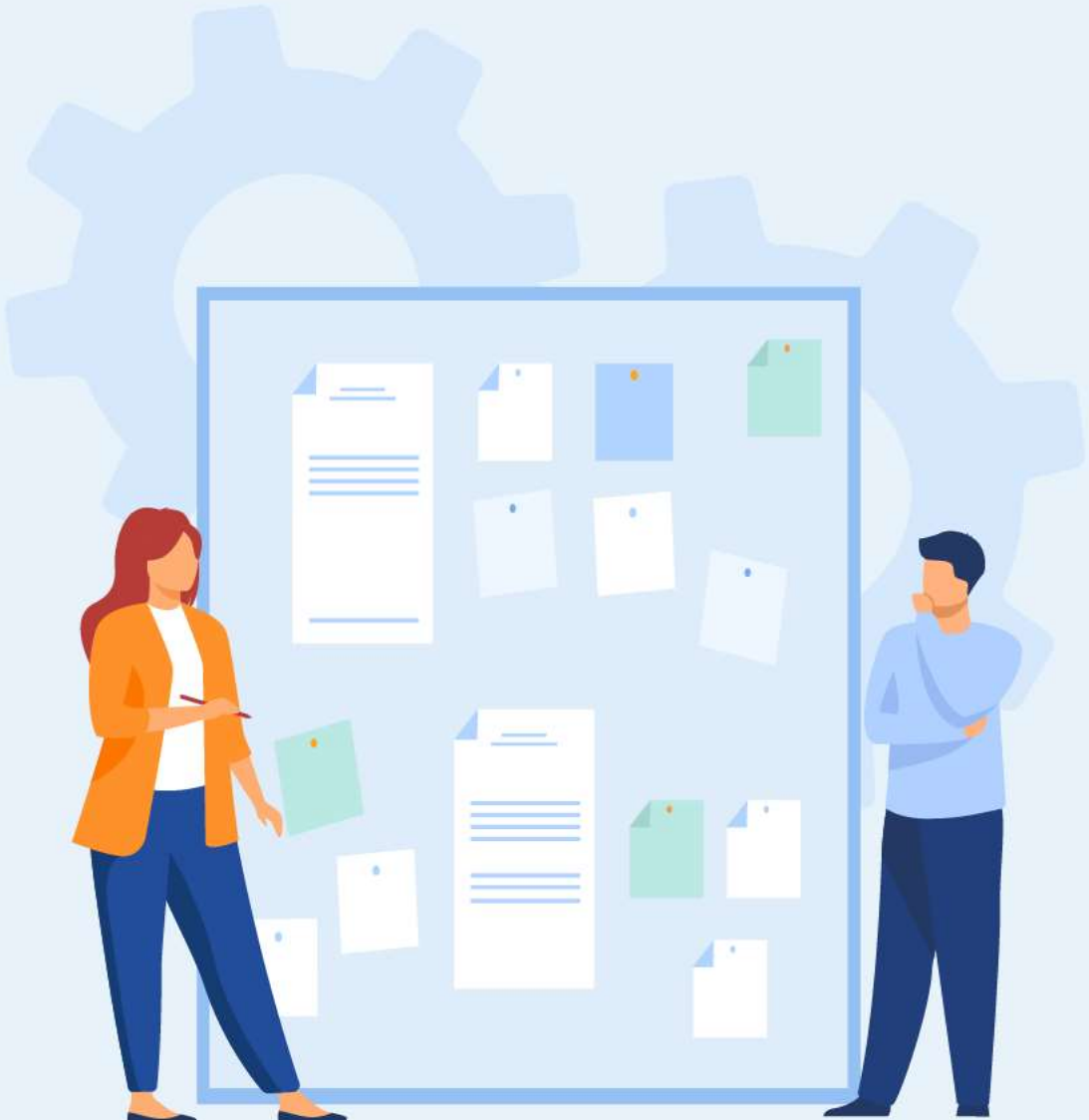
CHAPITRE 2

Assurer la fiabilité des données

Ce que vous allez apprendre dans ce chapitre :

- Sécuriser les données par la confidentialité
- Sécuriser les données par l’intégrité
- Sécuriser les données par la disponibilité

3 heures



CHAPITRE 2

Assurer la fiabilité des données

1. **Sécuriser des données par la confidentialité**
2. Sécuriser des données par l’intégrité
3. Sécuriser des données par la disponibilité

Sécurité de bout en bout dans Azure (Confidentialité)

La confidentialité vise à empêcher tout accès non autorisé à des informations sensibles. De tels accès peuvent être intentionnels, par exemple un intrus pénétrant dans le réseau et lisant des informations, ou non intentionnels, du fait de la négligence ou de l'incompétence des personnes qui manipulent les informations. Les deux principaux moyens de garantir la confidentialité sont le chiffrement et le contrôle d'accès.

Avec Azure, vous êtes le propriétaire des données que vous fournissez pour le stockage et l'hébergement dans les services Azure. Microsoft ne partage pas vos données avec ses services pris en charge par annonceur, et ne les exploite pas non plus à des fins marketing ou publicitaires.

Nous traitons vos données uniquement avec votre accord et, lorsque nous obtenons votre accord, nous utilisons vos données pour fournir uniquement les services que vous avez choisis. Ces accords s'appliquent également aux sous-traitants que auquel Microsoft recourt et autorise pour effectuer des tâches pouvant nécessiter l'accès à vos données : ces derniers peuvent uniquement réaliser les fonctions pour lesquelles Microsoft les a engagés et sont liés par les mêmes engagements de confidentialité contractuelle que Microsoft à votre égard.

Si vous quittez le service Azure ou si votre abonnement expire, Microsoft suit des normes strictes pour supprimer vos données de ses systèmes.

Des pratiques opérationnelles et des technologies spécifiques sont mises en œuvre pour garantir la sécurité, la conformité et la confidentialité de vos données au sein des services Microsoft :

1. Vous contrôlez vos données.
2. Nous sommes transparents concernant l'emplacement où vos données sont stockées et la manière dont elles sont utilisées.
3. Nous sécurisons vos données au repos et en transit.
4. Nous protégeons vos données.

Copyright - Tout droit réservé - OFPPT

Sécurité de bout en bout dans Azure (Confidentialité)

Chiffrement

Le chiffrement permet aux organisations de protéger les informations contre les divulgations accidentelles et les tentatives d'attaques internes et externes. L'efficacité d'un système de chiffrement à empêcher tout déchiffrement non autorisé en fait sa force. Un système de chiffrement fort est difficile à pirater. La force s'exprime également sous forme de facteur travail, c'est-à-dire une estimation du temps et des efforts nécessaires pour casser un système.

Algorithmes symétriques

Les algorithmes symétriques exigent de la part de l'expéditeur et du destinataire d'un message chiffré qu'ils aient la même clé et les mêmes algorithmes de traitement. Les algorithmes symétriques génèrent une clé symétrique (parfois appelée clé secrète ou clé privée) qui doit être protégée ; si la clé est perdue ou volée, la sécurité du système est compromise. Voici quelques-unes des normes courantes en matière d'algorithmes symétriques :

- **Data Encryption Standard (DES)**.
- **Triple-DES (3DES)**
- **Advanced Encryption Standard (AES)**
- **RC (Ron's Cipher ou Ron's Code)**.
- **Blowfish et Twofish**.
- **International Data Encryption Algorithm (IDEA)**.
- **Masques jetables**.

Copyright - Tout droit réservé - OFPPT

Sécurité de bout en bout dans Azure (Confidentialité)

Algorithmes asymétriques

Les algorithmes asymétriques utilisent deux clés : une clé publique et une clé privée. L'expéditeur utilise la clé publique pour chiffrer un message, et le destinataire utilise la clé privée pour le déchiffrer. La clé publique peut être effectivement publique ou être un secret entre les deux parties. La clé privée, elle, reste privée ; seul le propriétaire (le destinataire) la connaît. Si quelqu'un veut vous envoyer un message chiffré, il peut utiliser votre clé publique pour chiffrer le message et vous l'envoyer ensuite. Vous pouvez utiliser votre clé privée pour déchiffrer le message. Si les deux clés tombent entre les mains d'une tierce partie, le système de chiffrement ne protège pas la confidentialité du message. La force de ces systèmes est que la clé publique ne peut pas être utilisée pour déchiffrer un message. Si Bob envoie à Alice un message chiffré avec la clé publique d'Alice, il importe peu que tous les gens sur Terre possèdent la clé publique d'Alice, puisque cette clé ne peut pas déchiffrer le message. Voici quelques-unes des normes courantes en matière d'algorithmes asymétriques :

- **RSA**. Nommé d'après ses inventeurs, Ron **R**ivest, Adi **S**hamir et Leonard **A**dleman. L'algorithme RSA est un des premiers systèmes de chiffrement à clé publique qui se base sur de grands nombres entiers. Il est largement répandu et est devenu une norme de facto. RSA fonctionne à la fois avec le chiffrement et les signatures numériques. RSA est utilisé dans de nombreux environnements, y compris le protocole SSL (Secure Sockets Layer), il peut également être utilisé pour l'échange de clés.
- **Diffie-Hellman**. Whitfield **Diffie** et Martin **Hellman** sont considérés comme les inventeurs du concept de clé publique/clé privée. Leur algorithme Diffie-Hellman sert principalement à générer une clé secrète partagée sur les réseaux publics. Il ne sert pas à chiffrer ou déchiffrer les messages, mais simplement à créer une clé symétrique entre deux parties.
- **ECC (E**lliptic **C**urve **C**ryptography**)**. ECC offre des fonctionnalités similaires à celles de RSA, mais utilise des clés de taille inférieure pour obtenir un même niveau de sécurité. Les systèmes de chiffrement ECC reposent sur l'utilisation de points sur une courbe combinés avec un point à l'infini et sur la difficulté de résoudre des problèmes de logarithmes discrets.

Copyright - Tout droit réservé - OFPPT

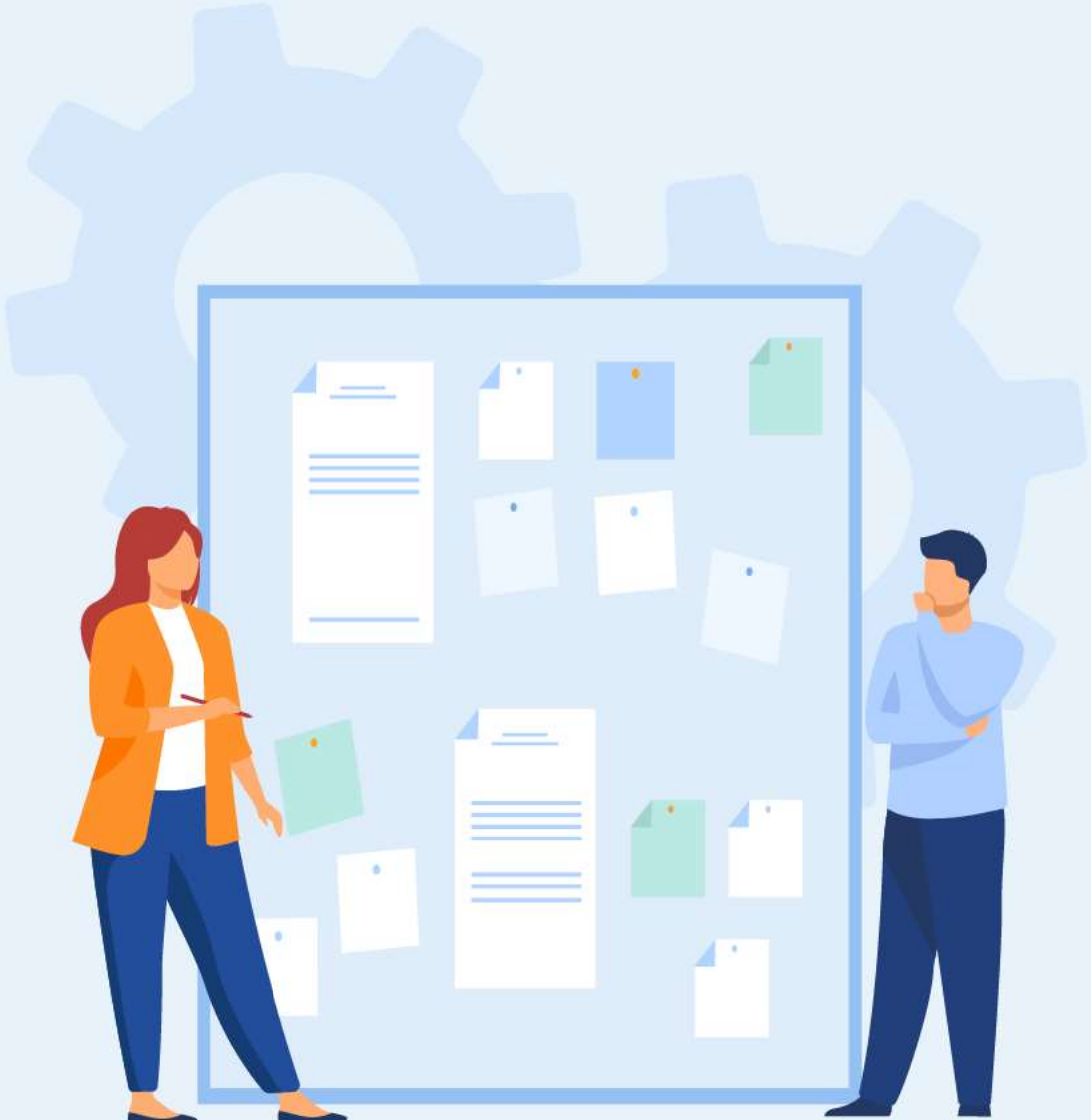
Sécurité de bout en bout dans Azure (Confidentialité)

Contrôle d'accès

Le chiffrement est un moyen de garantir la confidentialité, le contrôle d'accès en est un autre. Plusieurs approches du contrôle d'accès permettent d'assurer la confidentialité, chacune ayant ses propres forces et faiblesses :

- **Mandatory access control (MAC, Contrôle d'accès obligatoire)**. Dans un environnement MAC, toutes les capacités d'accès sont prédéfinies. Les utilisateurs ne peuvent pas partager d'informations, à moins que des administrateurs ne leur octroient ces droits. Les administrateurs doivent donc modifier ces droits en conséquence. Ce processus impose un modèle de sécurité rigide. Cependant, il est également considéré comme le modèle de cybersécurité le plus sûr.
- **Discretionary Access Control (DAC, Contrôle d'accès facultatif)**. Dans un modèle DAC, les utilisateurs peuvent partager des informations de manière dynamique avec d'autres utilisateurs. Cette méthode offre un environnement plus flexible, mais elle augmente le risque de divulgation non autorisée d'informations. Les administrateurs ont plus de mal à faire en sorte que seuls les utilisateurs appropriés puissent accéder aux données.
- **Role-Based Access Control (RBAC)**. Le contrôle d'accès basé sur les rôles instaure un contrôle d'accès basé sur la fonction ou la responsabilité des postes. Chaque employé a un ou plusieurs rôles qui lui permettent d'accéder à des informations spécifiques. Si une personne change de rôle, elle perd l'accès au rôle précédent. Les modèles RBAC offrent plus de flexibilité que le modèle MAC et moins que le modèle DAC. Ils présentent toutefois l'avantage de se fonder strictement sur la fonction du poste, et non sur les besoins individuels.
- **Rule-Based Access Control (RBAC)**. Le contrôle d'accès basé sur des règles utilise les paramètres des stratégies de sécurité préconfigurées pour prendre des décisions relatives à l'accès.
- **Attribute-based access control (ABAC)**. Le contrôle d'accès basé sur les attributs est une méthode relativement nouvelle de contrôle d'accès définie dans le document NIST 800-162, Attribute Based Control Definition and Considerations.

Copyright - Tout droit réservé - OFPPT



CHAPITRE 2

Assurer la fiabilité des données

1. Sécuriser des données par la confidentialité
2. **Sécuriser des données par l’intégrité**
3. Sécuriser des données par la disponibilité

Sécurité de bout en bout dans Azure (Intégrité)

L'intégrité comprend trois objectifs qui contribuent à la sécurité des données :

- Empêcher la modification des informations par des utilisateurs non autorisés
- Empêcher la modification non autorisée ou involontaire des informations par des utilisateurs autorisés
- Préserver une cohérence interne et externe :
    - **Cohérence interne** – Elle garantit que les données sont cohérentes sur le plan interne. Par exemple, dans une base de données organisationnelle, le nombre total d'éléments détenus par une organisation doit être égal à la somme de ces éléments mentionnés dans la base de données comme étant détenus par chaque élément de l'organisation.
    - **Cohérence externe** – Elle garantit que les données stockées dans la base de données sont cohérentes avec le monde réel. Par exemple, le nombre total d'articles en rayon doit correspondre au nombre total d'articles dans la base de données.

    Diverses méthodes de chiffrement peuvent contribuer à assurer l'intégrité en confirmant qu'un message n'a pas été modifié pendant sa transmission. Une modification peut rendre un message inintelligible ou, pire encore, inexact. Imaginez les graves conséquences que pourraient avoir des modifications non découvertes apportées à des dossiers médicaux ou à des prescriptions de médicaments. Si un message est altéré, le système de chiffrement doit comporter un mécanisme indiquant que le message a été corrompu ou modifié.

    Hachage

    L'intégrité peut également être vérifiée à l'aide d'un algorithme de hachage. Il s'agit en fait d'un hachage du message qui est généré et ajouté à la fin de celui-ci. Le destinataire calcule le hachage du message qu'il vient de recevoir et le compare au hachage reçu. Si quelque chose a été modifié au cours du transport, les deux hachages ne correspondent pas.

Copyright - Tout droit réservé - OFPPT

Sécurité de bout en bout dans Azure (Intégrité)

Algorithme de hachage

Les hachages utilisés pour stocker des données sont très différents des hachages de chiffrement. En matière de chiffrement, une fonction de hachage doit présenter trois caractéristiques :

- **Elle doit être à sens unique**. Une fois que vous avez haché quelque chose, vous ne pouvez pas le déhacher.
- **Une entrée de longueur variable produit une sortie de longueur fixe**. Que vous hachiez deux caractères ou deux millions, la taille du hachage reste la même.
- **L'algorithme ne doit présenter que peu ou pas de collision**s. Le hachage de deux entrées différentes ne donne pas le même résultat.

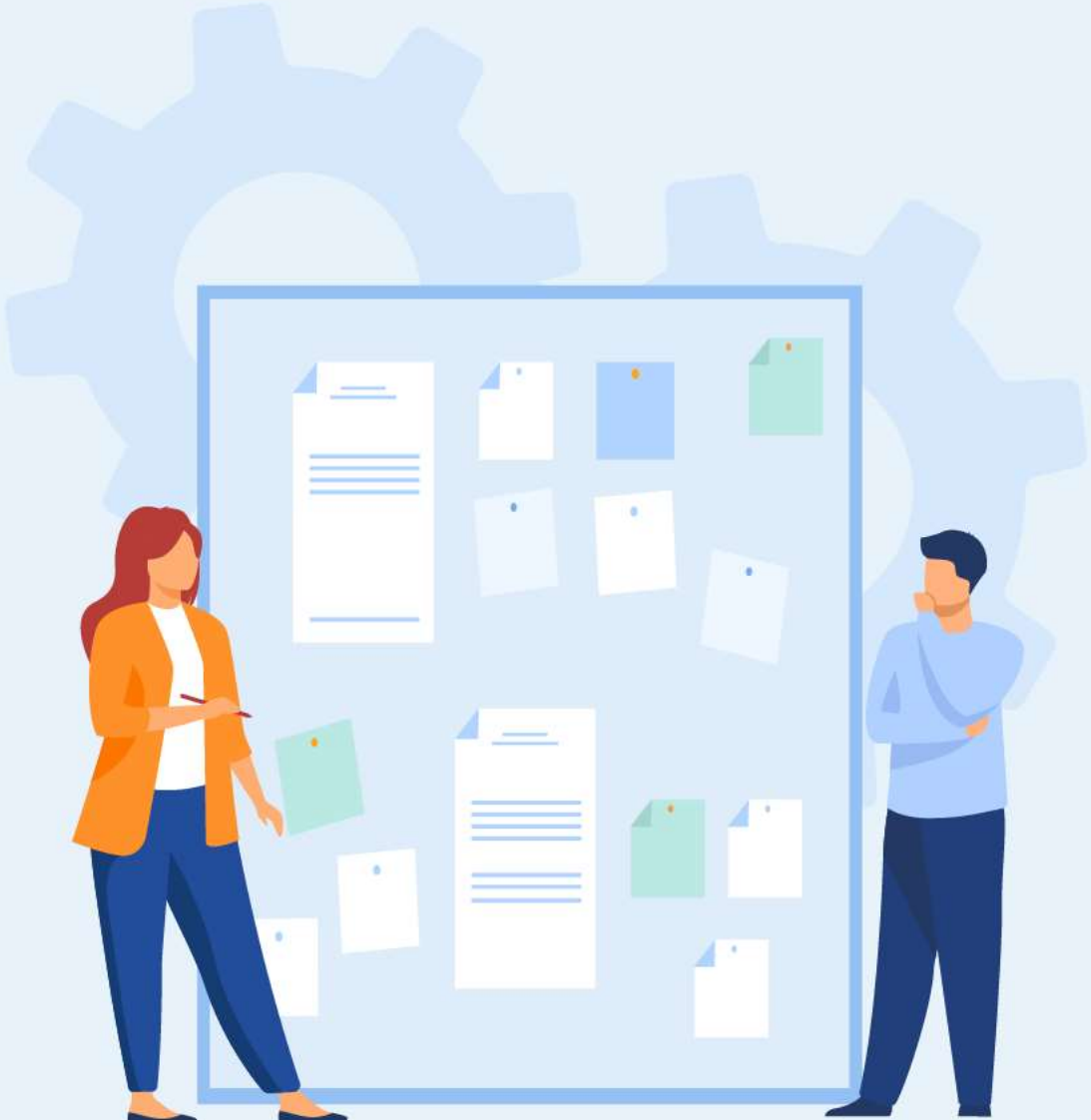
Voici les algorithmes de hachage et les concepts connexes que vous devez connaître :

- **Secure Hash Algorithm (SHA)**. Appelé Keccak au départ, SHA a été conçu par Guido Bertoni, Joan Daemen, Michaël Peeters et Gilles Van Assche. SHA-1 est un hachage unidirectionnel qui fournit une valeur de hachage de 160 bits pouvant être utilisée avec un protocole de chiffrement.

Référence

L'établissement d'une référence (référence de configuration, référence de systèmes, référence d'activité) est une stratégie importante pour une mise en réseau sécurisée. Il s'agit de trouver une référence que vous considérez comme sûre pour un système, un ordinateur, une application ou un service donné. Une sécurité absolue est certainement irréalisable ; l'objectif est une sécurité suffisante, en fonction des besoins de sécurité de votre organisation et de sa tolérance au risque. Toute modification peut être comparée à la référence pour voir si elle est suffisamment sûre. Une fois la référence définie, l'étape suivante consiste à surveiller le système pour s'assurer qu'il ne s'en écarte pas. Ce processus est défini comme une mesure d'intégrité.

Copyright - Tout droit réservé - OFPPT



CHAPITRE 2

Assurer la fiabilité des données

1. Sécuriser des données par la confidentialité
2. Sécuriser des données par l’intégrité
3. **Sécuriser des données par la disponibilité**

Sécurité de bout en bout dans Azure (Disponibilité)

La disponibilité garantit que les utilisateurs autorisés d'un système ont un accès rapide et ininterrompu aux informations contenues dans ce système, ainsi qu'au réseau. Voici les méthodes qui permettent cette disponibilité :

- **Répartition équitable**. Communément appelée équilibrage des charges, la répartition équitable permet de distribuer la charge (demandes de fichiers, acheminement des données, etc.) de manière à ce qu'aucun appareil ne soit trop sollicité.
- **Haute disponibilité**. La haute disponibilité se rapporte aux mesures utilisées pour maintenir opérationnels les services et les systèmes d'information pendant une panne. L'objectif de la haute disponibilité est souvent que les services clés soient disponibles 99,999 % du temps (disponibilité « cinq neufs »). Les stratégies de haute disponibilité comprennent la redondance et le basculement, qui sont abordés ci-dessous.
- **Redondance**. La redondance fait référence aux systèmes qui sont soit dupliqués, soit basculés vers d'autres systèmes en cas de dysfonctionnement. On appelle «basculement» le processus de reconstruction d'un système ou de passage à d'autres systèmes lorsqu'une défaillance est détectée. Dans le cas d'un serveur, lorsqu'une défaillance est détectée, le serveur bascule vers un serveur redondant. Cette stratégie permet de maintenir la continuité du service jusqu'à ce que le serveur principal soit restauré. Dans le cas d'un réseau, cela signifie qu'en cas de défaillance sur le chemin principal, le traitement passe à un autre chemin de réseau. Les systèmes de basculement peuvent être chers à mettre en œuvre. Dans un grand réseau d'entreprise ou un environnement d'e-commerce, un basculement peut nécessiter de transférer tous les traitements vers un site distant jusqu'à ce que l'installation principale redevienne opérationnelle. Le site principal et le site distant doivent synchroniser leurs données afin de garantir que les informations sont aussi à jour que possible.

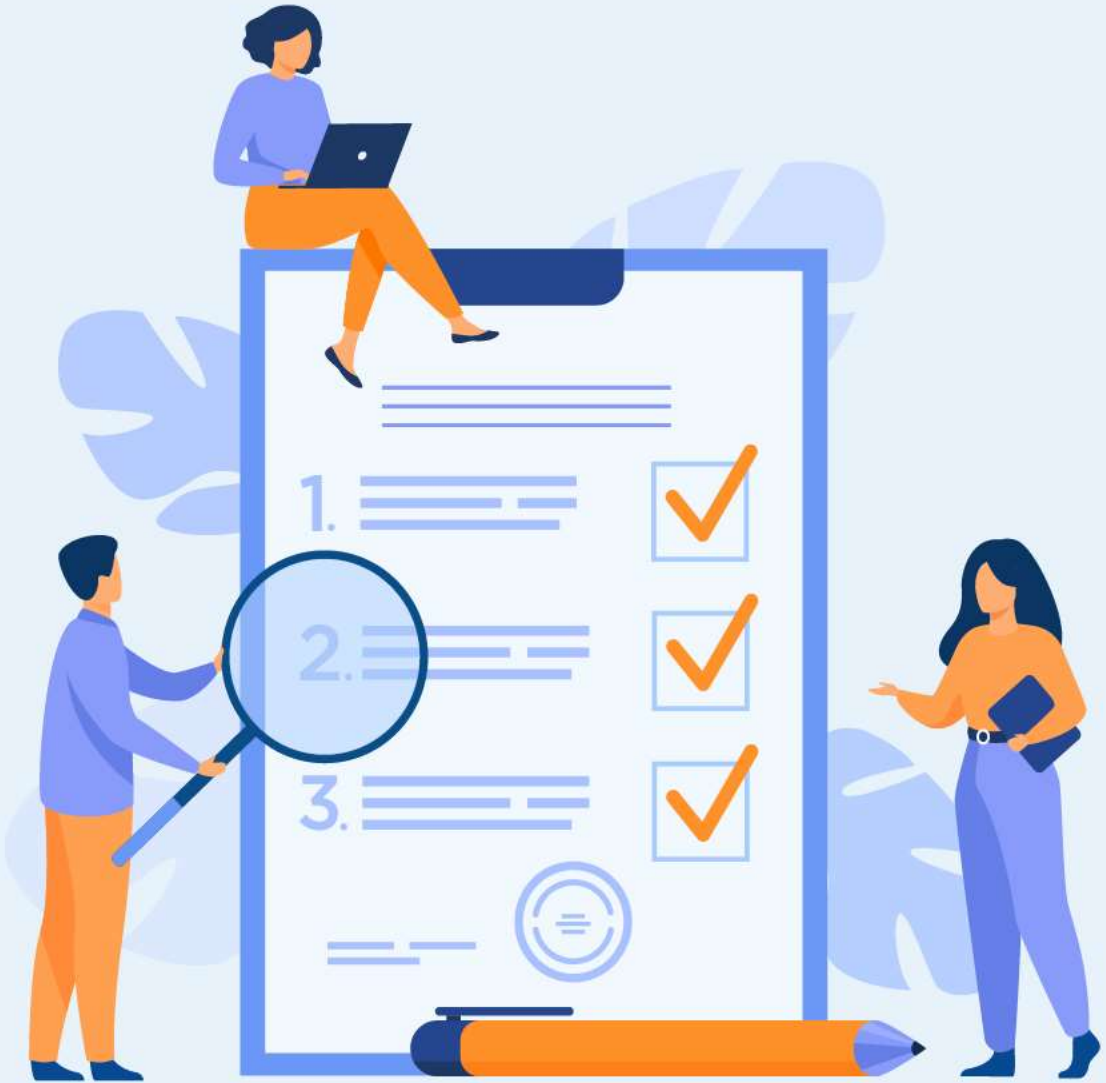
Tolérance aux pannes. La tolérance aux pannes est la capacité d'un système à rester opérationnel en cas de défaillance d'un composant. Les systèmes tolérants aux pannes peuvent continuer à fonctionner même si un composant critique, par exemple un lecteur de disque, tombe en panne. Cette capacité implique une sur-ingénierie des systèmes par ajout de composants et de sous-systèmes redondants visant à réduire les risques d'interruption. Par exemple, la tolérance aux pannes peut être intégrée à un serveur via l'ajout d'une seconde alimentation, d'un second processeur et d'autres composants clés. La plupart des fabricants (notamment HP, Sun et IBM) proposent des serveurs à tolérance aux pannes. Ces derniers sont généralement équipés de plusieurs processeurs qui basculent automatiquement en cas de dysfonctionnement.

Copyright - Tout droit réservé - OFPPT

Sécurité de bout en bout dans Azure (Disponibilité)

- **RAID (Redundant Array of Independent Disks)**. La technologie RAID utilise plusieurs disques pour assurer la tolérance aux pannes. Le RAID comporte plusieurs niveaux : RAID 0 (disques à bandes), RAID 1 (disques en miroir), RAID 3 ou 4 (disques à bandes avec parité dédiée), RAID 5 (disques à bandes avec parité distribuée), RAID 6 (disques à bandes avec double parité), RAID 1+0 (ou 10) et RAID 0+1.
- **Plan de reprise après sinistre**. Un plan de reprise après sinistre permet à une organisation de réagir efficacement lorsqu'une catastrophe se produit.
  Les catastrophes peuvent être des défaillances de systèmes, des pannes de réseaux, des défaillances d'infrastructures et des catastrophes naturelles comme les ouragans et les tremblements de terre. Un plan de reprise après sinistre définit les méthodes permettant de rétablir les services le plus rapidement possible et de protéger l'organisation contre des pertes inacceptables en cas de catastrophe.
  Dans une petite organisation, un plan de reprise après sinistre peut être relativement simple. Dans une organisation plus grande, il peut impliquer plusieurs sites, des plans stratégiques et des services entiers.
  Un plan de reprise après sinistre doit prendre en compte l'accès aux informations et leur stockage. Votre plan de sauvegarde des données sensibles fait partie intégrante de ce processus.

Copyright - Tout droit réservé - OFPPT



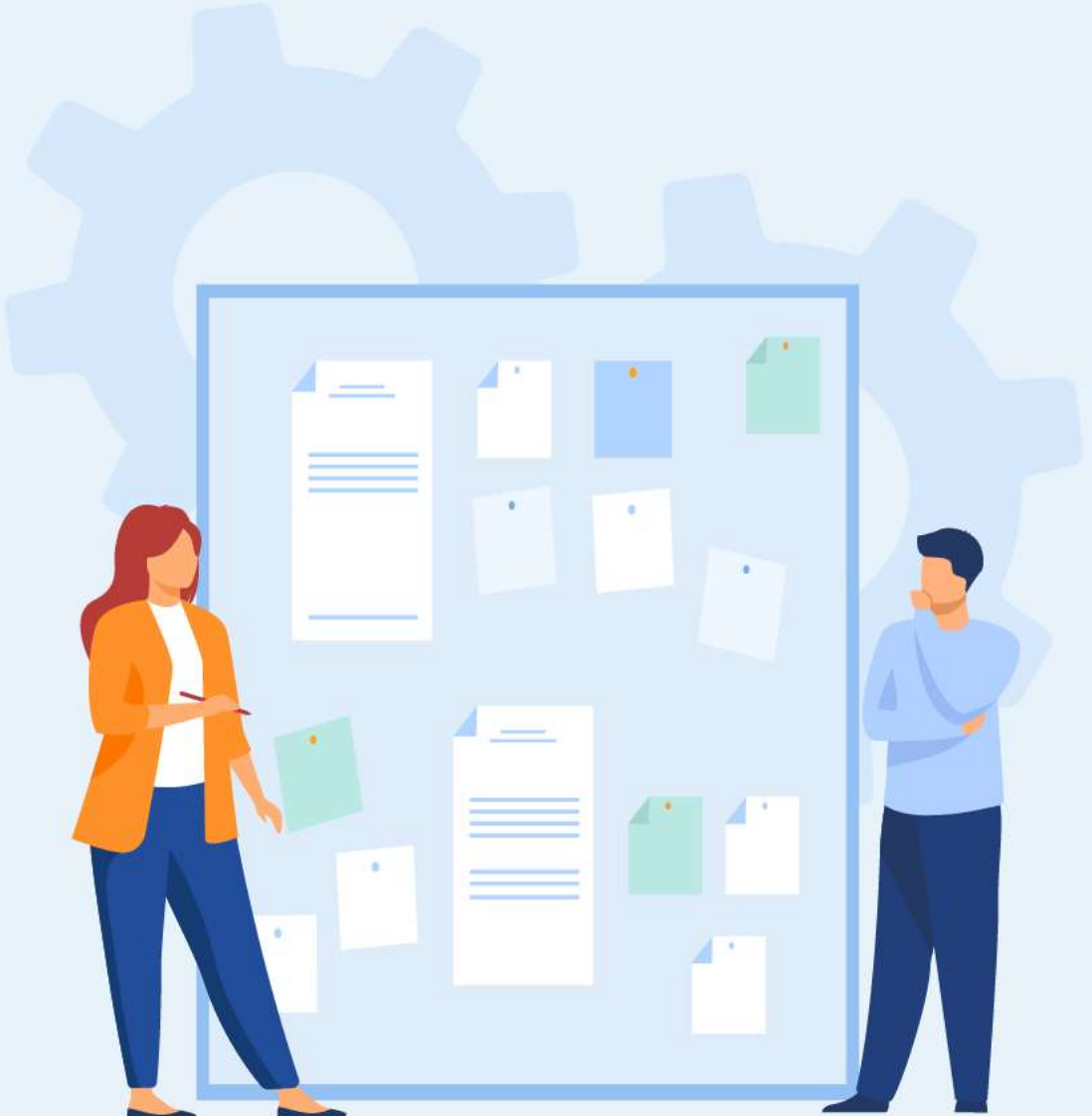
CHAPITRE 3

Vérifier la conformité réglementaire

Ce que vous allez apprendre dans ce chapitre :

- Découvrir la conformité du fournisseur
- Découvrir les aspects législatifs et réglementaires

3 heures



CHAPITRE 3

Vérifier la conformité réglementaire

1. **Découvrir les offres pour la conformité du fournisseur**
2. Découvrir les aspects législatifs et réglementaires

Les offres pour la conformité du fournisseur

Pour aider les clients à répondre à leurs propres obligations en matière de conformité dans les industries et sur les marchés réglementés du monde entier, Azure gère le plus grand portefeuille de conformité du secteur en largeur (nombre total d'offres) et en profondeur (nombre de services B2C dans l'étendue d'évaluation). Les offres de conformité Azure sont regroupées en quatre segments :

- Global
- Gouvernement américain
- Secteur d'activité
- Zones géographiques

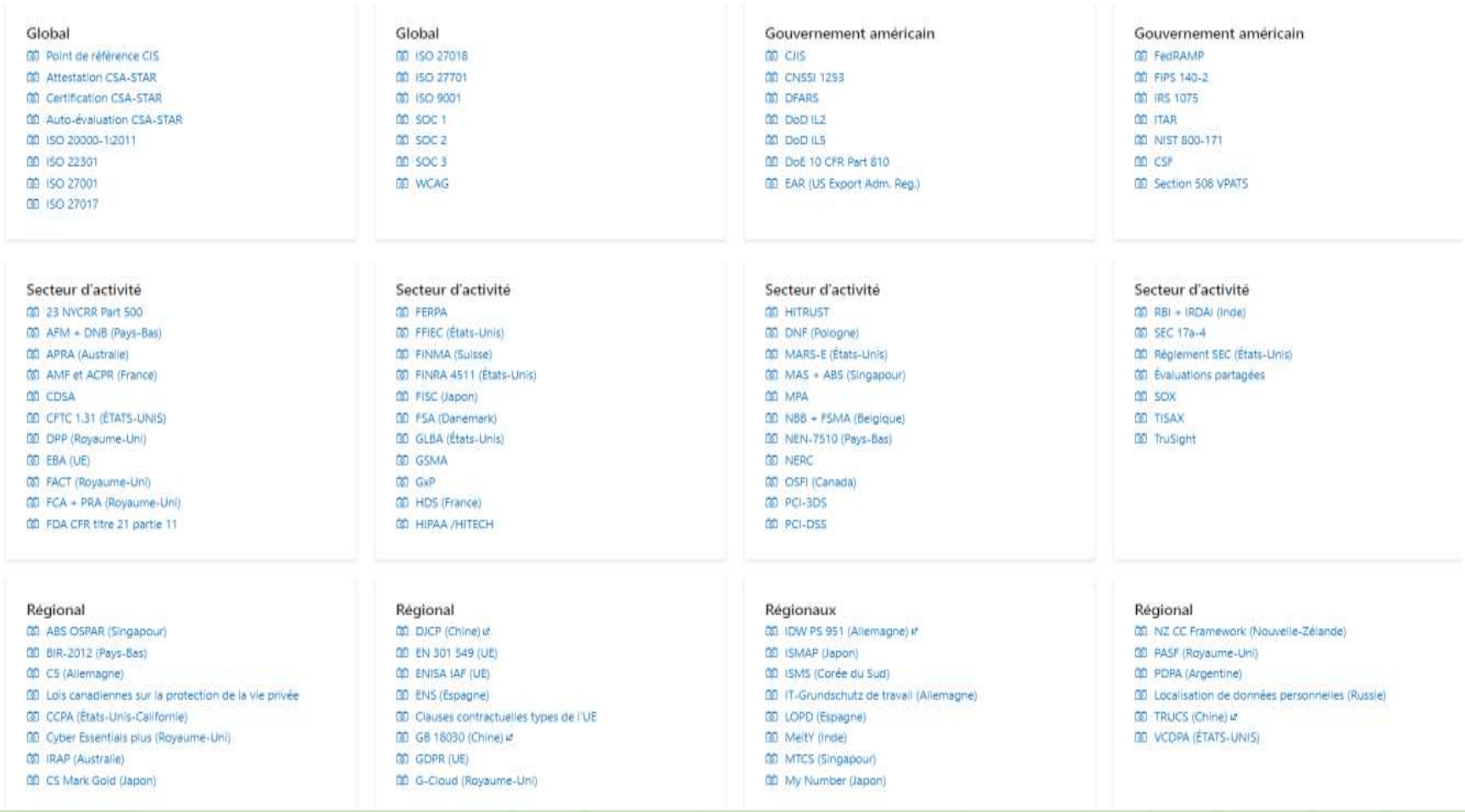
Les offres de conformité Azure sont basées sur divers types de garanties, notamment des certifications, attestations, validations, autorisations et évaluations officielles créées par des sociétés d'audit tierces indépendantes, ainsi que des modifications contractuelles, des auto-évaluations et des documents de conseils pour les clients créés par Microsoft. Chacune des descriptions d'offres de ce document fournit une instruction SCOPE à jour indiquant quels services Azure orientés client se trouvent dans le champ d'application de l'évaluation, ainsi que des liens vers des ressources téléchargeables permettant d'aider les clients à gérer leurs propres obligations en matière de conformité.

Copyright - Tout droit réservé - OFPPT

03- Vérifier la conformité réglementaire

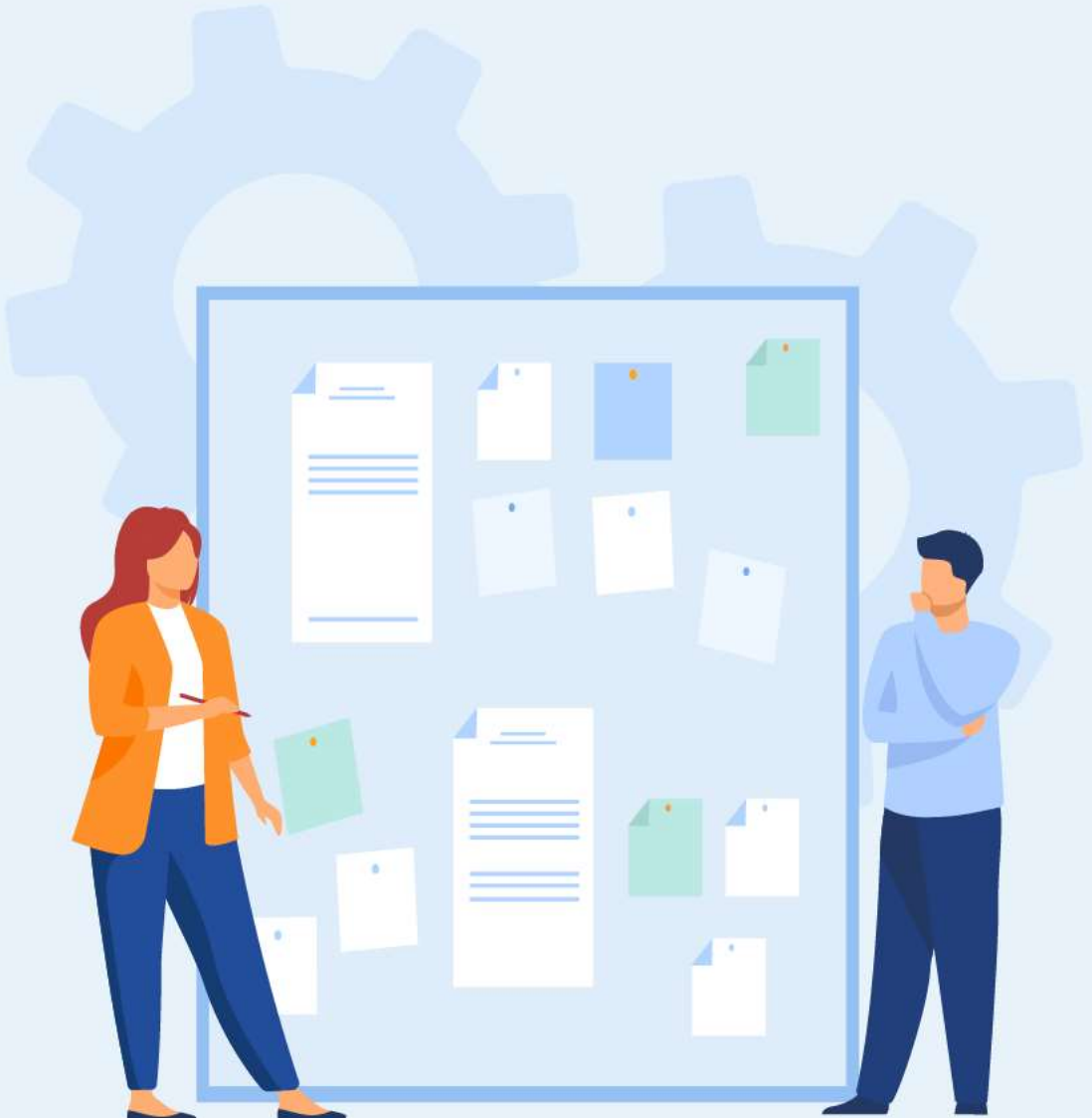
Découvrir les offres pour la conformité du fournisseur

Pour Azure, Dynamics 365, Microsoft 365 et Power Platform, et d'autres services peuvent vous aider pour se conformer avec les réglementations selon la localisation et selon le secteur d'activité.



PARTIE 1

Copyright - Tout droit réservé - OFPPT



CHAPITRE 3

Vérifier la conformité réglementaire

1. Découvrir les offres pour la conformité du fournisseur
2. **Découvrir les aspects législatifs et réglementaires**

À quelle législation vos données sont-elles soumises ?

En choisissant un hébergeur Web, vous choisissez également à quelle législation vos données seront soumises. Or trop souvent, cette réflexion sur le traitement des données n'est pas aussi aboutie qu'elle devrait l'être et la tentation est grande d'opter pour des solutions proposées par des grands acteurs du cloud étranger. Depuis plusieurs années, la notion de sécurité des données est primordiale. Il est donc crucial de bien choisir sa solution d'hébergement.

Si vous confiez vos données personnelles à un prestataire américain ou bien un prestataire européen avec un hébergement de vos données sur le territoire américain, vous pouvez directement vous retrouvez confrontés aux lois américaines.

Parmi les lois appliqués par les hébergeurs américains on trouve :

- Patriot Act
- Cloud Act

Parmi les lois appliqués par les hébergeurs européens on trouve :

- RGPD

Copyright - Tout droit réservé - OFPPT

Patriot Act

« Adopté au lendemain des attentats du 11 septembre 2001, le USA Patriot Act (pour Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) est un texte pivot central de la lutte des autorités fédérales américaines contre le terrorisme. Conçu à l'origine pour ne durer que quelques années, ce texte a été rendu permanent depuis 2005. Le Patriot Act permet aux agences fédérales américaines (le FBI, la CIA, la NSA, l'armée, le fisc…) d'obtenir des informations dans le cadre d'une enquête relative à des actes de terrorisme, au moyen d'injonctions destinées à rester secrètes compte tenu de la sensibilité du sujet. C'est d'ailleurs également le cas pour les demandes formulées sur ce sujet par les autorités françaises qui disposent d'un arsenal législatif en ce sens via notamment les dispositions du Code de la Sécurité Intérieure.



Copyright - Tout droit réservé - OFPPT

Cloud Act

Certains ont présenté le Cloud Act comme l'application au Cloud du Patriot Act. Il s'agit d'une loi fédérale américaine datant de 2018 qui est avant tout une loi de procédure, qui ne vise pas spécifiquement les acteurs du Cloud (ici Cloud est entendu par Clarifying Lawful Overseas Use of Data Act). Critiquée par de nombreuses associations de défense de la vie privée, mais également des Parlementaires, cette Loi permet notamment aux autorités américaines de solliciter les données d'une personne *, après autorisation judiciaire auprès des fournisseurs de services relevant des lois des États-Unis.



Copyright - Tout droit réservé - OFPPT

RGPD



Copyright - Tout droit réservé - OFPPT

Cloud Act, Patriot Act, RGPD : à quelle législation vos données sont-elles soumises ?

- Que ce soit pour l'hébergement des données sur le territoire américain par un acteur américain, ou étranger, mais détenu par une société de droit américain, pas de doute, Patriot Act et Cloud Act s'appliquent pleinement. ET c'est le cas, même si les données concernent une société, une association, une collectivité d'un pays tiers.
- Idem, hébergement des données sur le territoire Américain par une structure de droit américain détenu par une société de droit européen : pas de doute, Patriot Act et Cloud Act s'appliquent pleinement. Même si les données concernent une société, une association, une collectivité d'un pays tiers.
- A contrario, pour l'hébergement des données en Europe par un acteur américain, ou étranger, mais détenu par une société de droit américain : c'est compliqué. Les autorités américaines vous diront que Patriot Act et Cloud Act s'appliquent, les autorités européennes vous diront que le RGPD prime, l'hébergeur étant placé quant à lui entre ces deux injonctions.
- Enfin, l'hébergement des données sur le territoire Européen par une structure de droit Européen, détenue par une société de droit européen : pas de doute, le RGPD prime. Tout manquement au RGPD est susceptible de déboucher sur une sanction allant jusqu'à 4% du chiffre d'affaires réalisé au niveau mondial.

Copyright - Tout droit réservé - OFPPT

Aspects Juridiques Microsoft Azure

Au niveau d'Azure, d'autres aspects juridiques sont aussi présentés. On trouve ainsi :

Déclaration de confidentialité

La Déclaration de Confidentialité Microsoft décrit les données à caractère personnel et explique leur mode de traitement par Microsoft, ainsi que les finalités du traitement. Votre Contrat de services applicable ou les Conditions supplémentaires d'avant-première peuvent spécifier des mesures de confidentialité moindres ou différentes pour certains services d'avant-première.

Data Protection

L'Addendum relatif à la Protection des Données des Services en Ligne (« DPA ») énonce vos obligations et celles de Microsoft en ce qui concerne le traitement et la sécurité des Données Client et des Données à Caractère Personnel relativement à Azure. La section Conditions de Confidentialité et de Sécurité des Services en Ligne du site Conditions des Produits énonce en outre des exclusions de la DPA ainsi que des engagements supplémentaires pour les Services en ligne de base. Le Microsoft Trust Center donne plus d'informations sur des sujets de sécurité, confidentialité et conformité pour les clients d'Azure et autres services en ligne de Microsoft. Le Service Trust Portal (STP) est une fonctionnalité complémentaire du Trust Center qui donne accès aux rapports d'audit, aux documents GDPR, aux guides de conformité et aux documents connexes qui fournissent des précisions sur la manière dont Microsoft contribue à protéger vos données.

Contrats de Niveau de Service

Les Contrats de Niveau de Service décrivent les engagements en termes de temps de disponibilité et de connectivité pour Azure.

Conditions Générales Supplémentaires des Versions d'Évaluation

Elles s'appliquent à votre utilisation des options Azure qui sont en version bêta, avant première ou autrement non encore mises à disposition de façon générale.

Copyright - Tout droit réservé - OFPPT

Aspects Juridiques Microsoft Azure

Conditions Microsoft Azure Marketplace

Les Conditions générales régissant votre utilisation de Microsoft Azure Marketplace sont définis dans les Conditions de Microsoft Azure Marketplace.

Conditions de Microsoft Azure Government

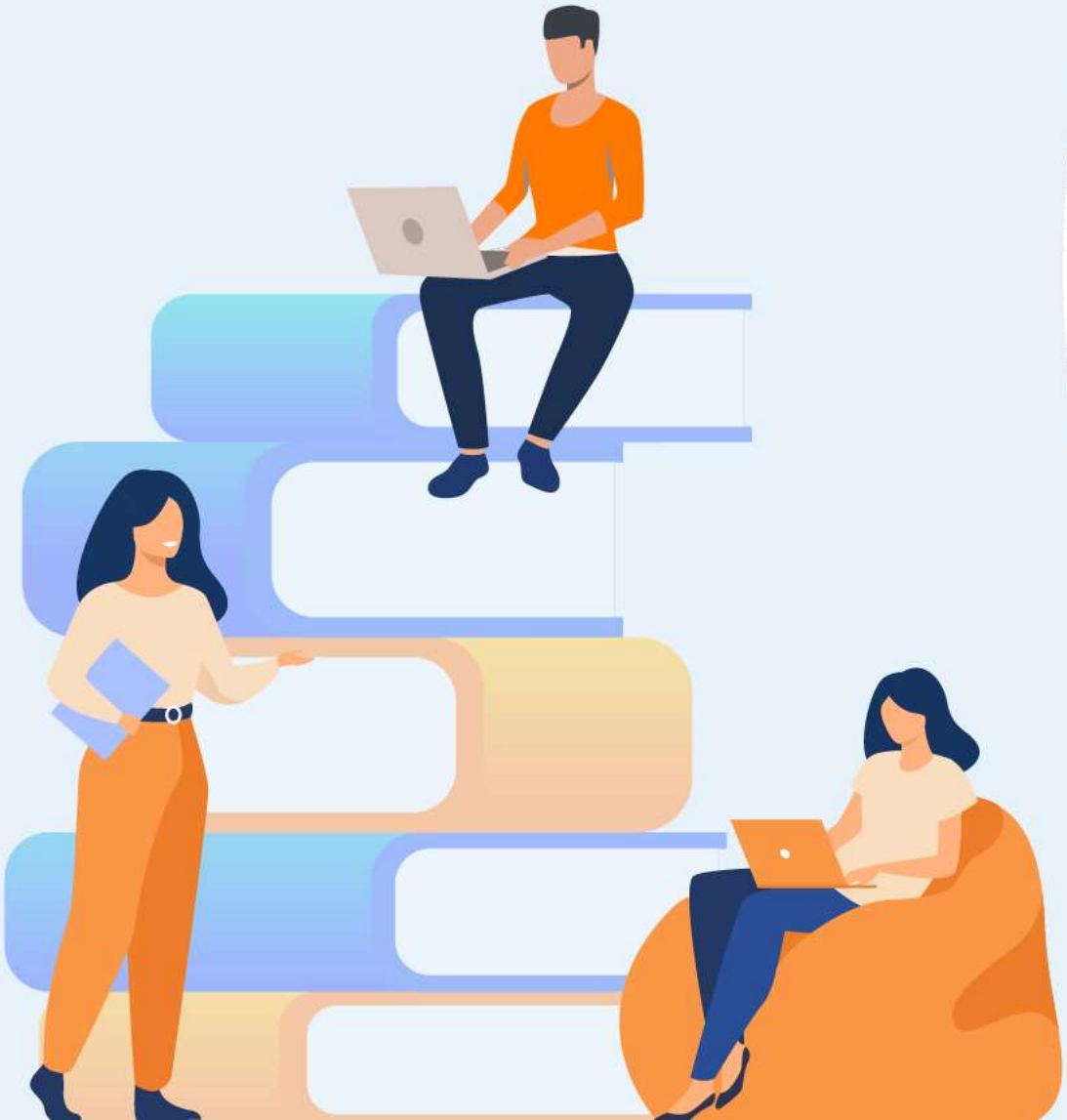
Les Termes et conditions régissant votre utilisation du Microsoft Azure Government Cloud sont définis dans l'Accord de souscription en ligne de Microsoft – US Government Cloud.

Conditions d'Utilisation du Site Web

Les Conditions d'utilisation de Microsoft s'appliquent à votre utilisation du site Internet d'Azure. Elles s'appliquent aussi aux services Azure limités que vous pouvez utiliser sans abonnement.

Cet aperçu des conditions générales régit l'achat et l'utilisation d'Azure. Les services, logiciels et contenus accessoires sont susceptibles d'être régis par des conditions supplémentaires ou différentes non recensées ci-dessus.

Copyright - Tout droit réservé - OFPPT



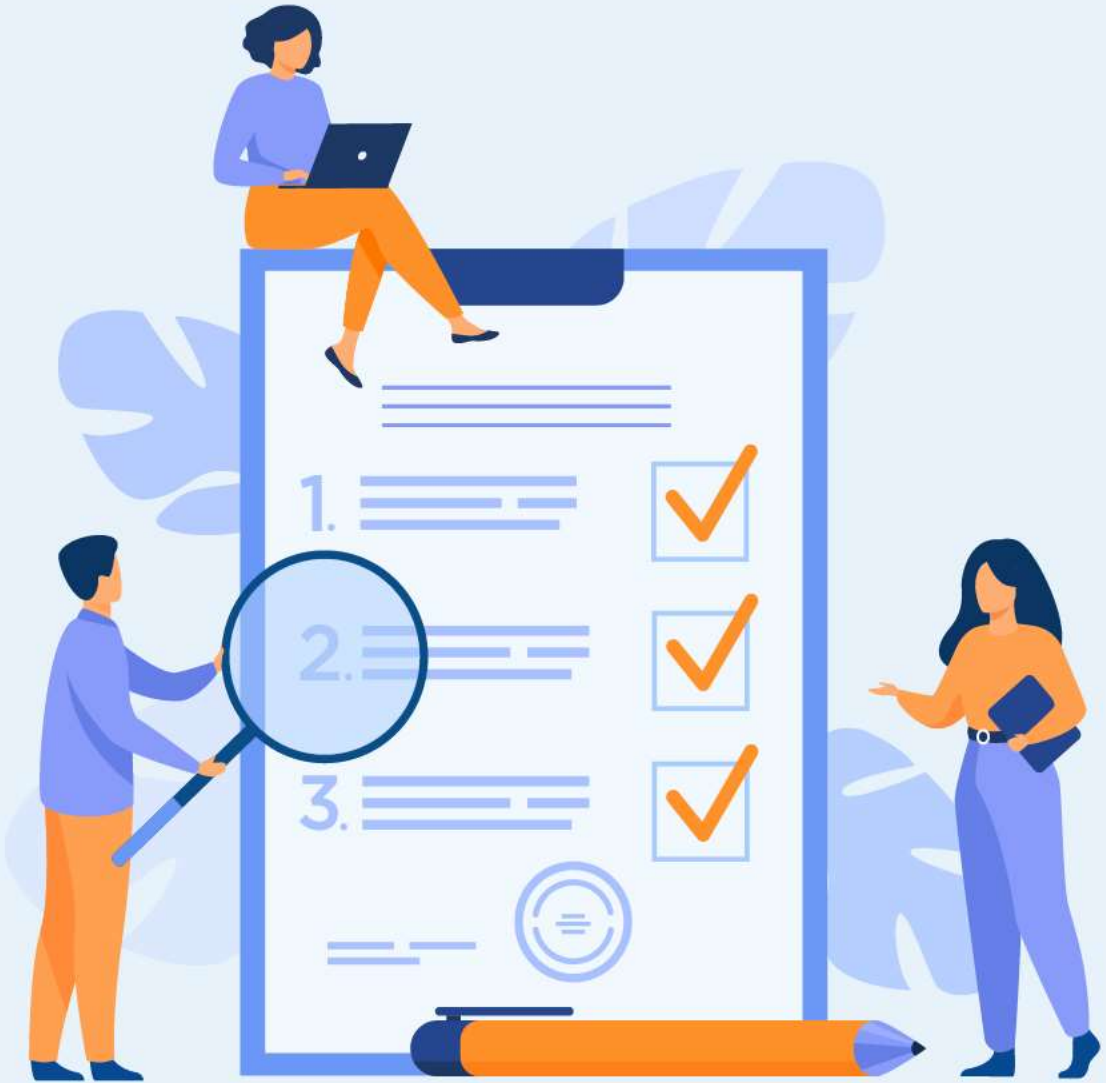
PARTIE 2

Cartographier les données sur le Cloud

Dans ce module, vous allez :

- Inventorier les données
- Cartographier les données

12 heures



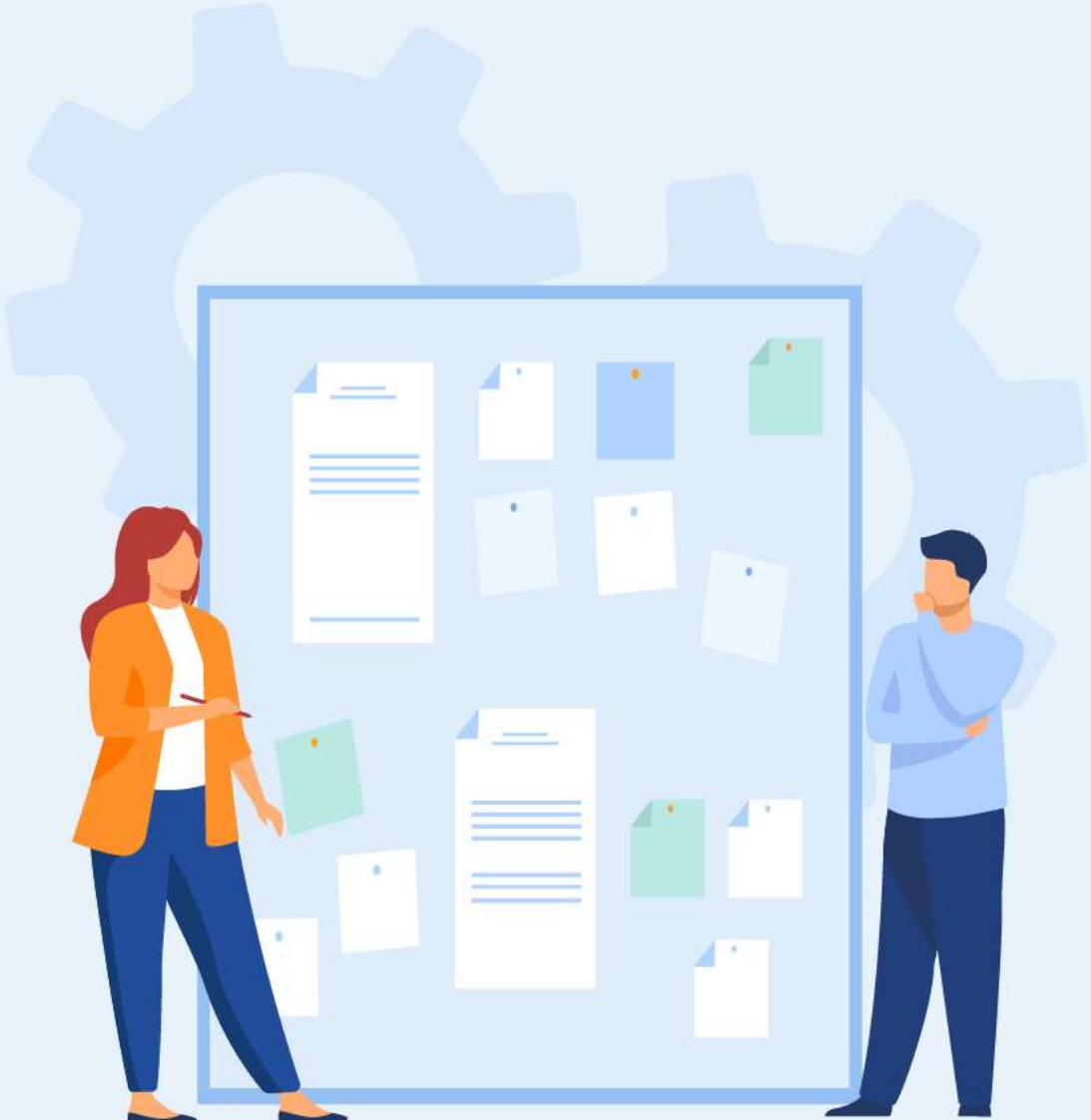
CHAPITRE 1

Inventorier les données

Ce que vous allez apprendre dans ce chapitre :

- Découvrir le catalogage des supports d'hébergement des données
- Découvrir les habilitations des utilisateurs sur les données

6 heures



CHAPITRE 1

Inventorier les données

1. **Catalogage des supports d’hébergement des données**
2. Habilitations des utilisateurs sur les données

Choisir l'option d'hébergement Azure appropriée

En tant que client, vous conservez la propriété des données client (contenu, données personnelles et autres) que vous fournissez à des fins de stockage et d'hébergement dans les services Azure. Vous contrôlez également toutes les zones géographiques supplémentaires où vous décidez de déployer vos solutions ou de répliquer vos données.

Lorsque la fonctionnalité d'un service nécessite une réplication de données globale, des détails sont disponibles ci-après.

Sécurité des données

Microsoft sécurise vos données à l'aide de plusieurs couches de sécurité et protocoles de chiffrement. Vous trouverez une vue d'ensemble de l'utilisation du chiffrement par Microsoft pour sécuriser vos données.

Par défaut, les clés gérées par Microsoft protègent vos données et les données client conservées sur support physique qui sont toujours chiffrées à l'aide de protocoles de chiffrement compatibles FIPS 140-2. Les clients peuvent également utiliser des clés gérées par le client (CMK), un double chiffrement et/ou des modules de sécurité matériels (HSM) pour renforcer la protection des données.

Tout le trafic de données circulant entre les centres de données est protégé par des normes de sécurité MAC IEEE 802.1 AE, ce qui évite des attaques de l'intercepteur physique. Pour maintenir la résilience, Microsoft utilise des chemins d'accès réseau variables qui franchissent parfois des limites géographiques, mais la réplication des données client entre régions est toujours transmise sur des connexions réseau chiffrées.

En outre, pour réduire les risques en matière de confidentialité, Microsoft génère des « identificateurs pseudonymes » qui lui permettent d'offrir un service cloud global (incluant des services d'exploitation et d'amélioration, de facturation et de protection contre la fraude). Dans tous les cas, les identificateurs pseudonymes ne peuvent être utilisés ni pour identifier directement un individu, ni pour accéder aux données client. Ces dernières qui identifient des personnes sont toujours protégées comme décrit ci-dessus.

Copyright - Tout droit réservé - OFPPT

Catalogage selon la technologie offerte par le support

Les supports d'hébergement de données sont très diversifiés sur le Cloud. Le bon choix d'un support approprié est un exercice qui doit se faire d'une manière très soigneuse avant d'héberger les données à l'intérieur.

Le catalogage des ces supports de données consiste à déterminer les critères permettant de les classifier et de les répertorier pour, d'une part, orienter convenablement le choix du support et, d'autre part, inventorier correctement les supports existants

Parmi les critères permettant de choisir un support approprié on trouve :

- Existence d'interfaces pour accéder aux données (exemple « API »
- Adaptation aux données massives ; on parle parfois de « lacs de données » ou « data lakes »
- Publication des données avec un contrôle public (open data)
- Exigence de formats favorisant l'interopérabilité pour pouvoir croiser et exploiter au mieux les données sur un territoire ou entre territoires.

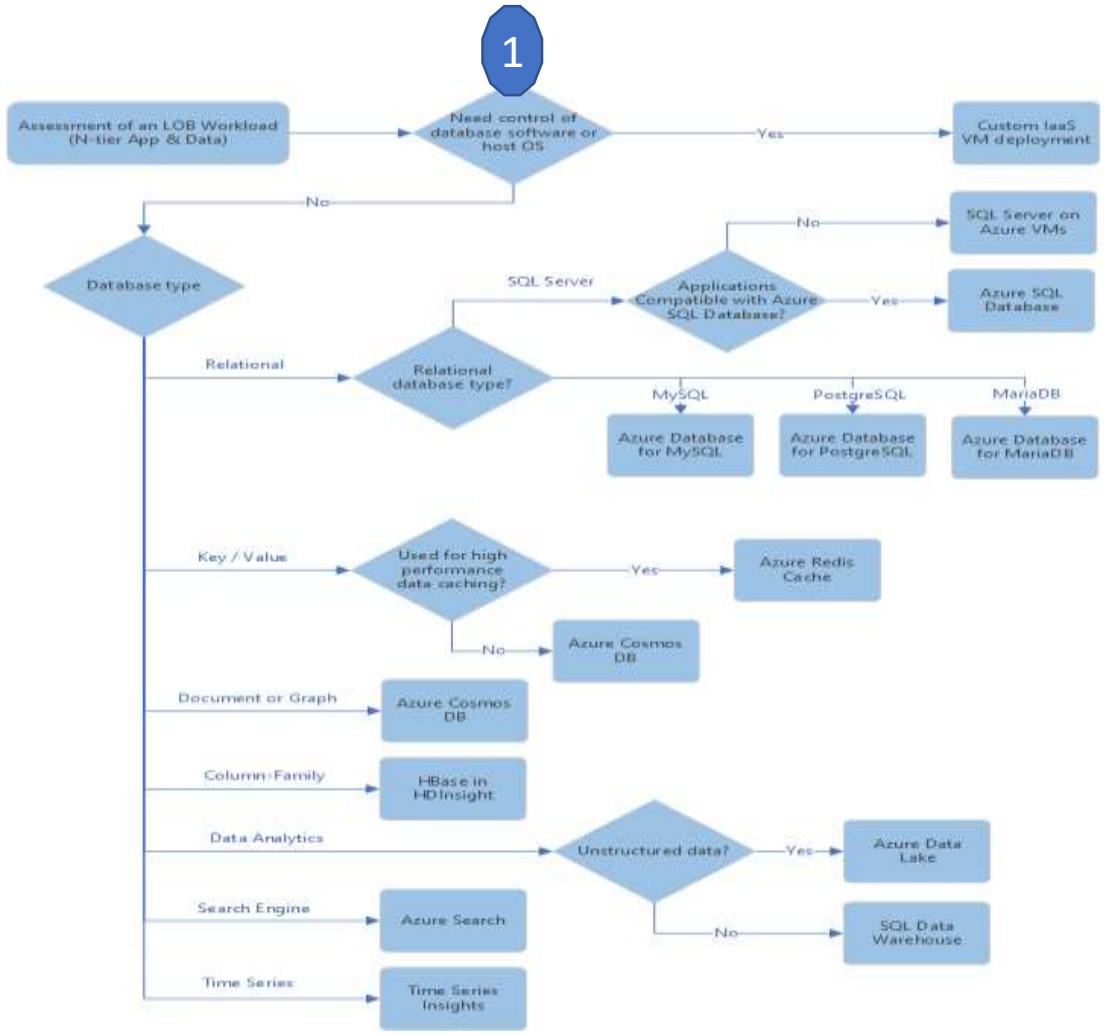
Copyright - Tout droit réservé - OFPPT

PARTIE 2

Arbre de décision des services de base de données Azure

1 Avez-vous besoin du contrôle total ou de la pleine propriété de votre logiciel de base de données ou de votre système d'exploitation hôte ?

Dans certains scénarios, vous devez disposer d'un niveau élevé de contrôle ou de propriété de la configuration logicielle et des serveurs hôtes pour vos charges de travail de base de données. Dans ces scénarios, vous pouvez déployer des machines virtuelles Infrastructure as a service (IaaS) personnalisées pour contrôler entièrement le déploiement et la configuration des services de données. Si vous n'avez pas ces exigences, les services de base de données PaaS (platform as a service) pourraient réduire vos coûts de gestion et d'exploitation.



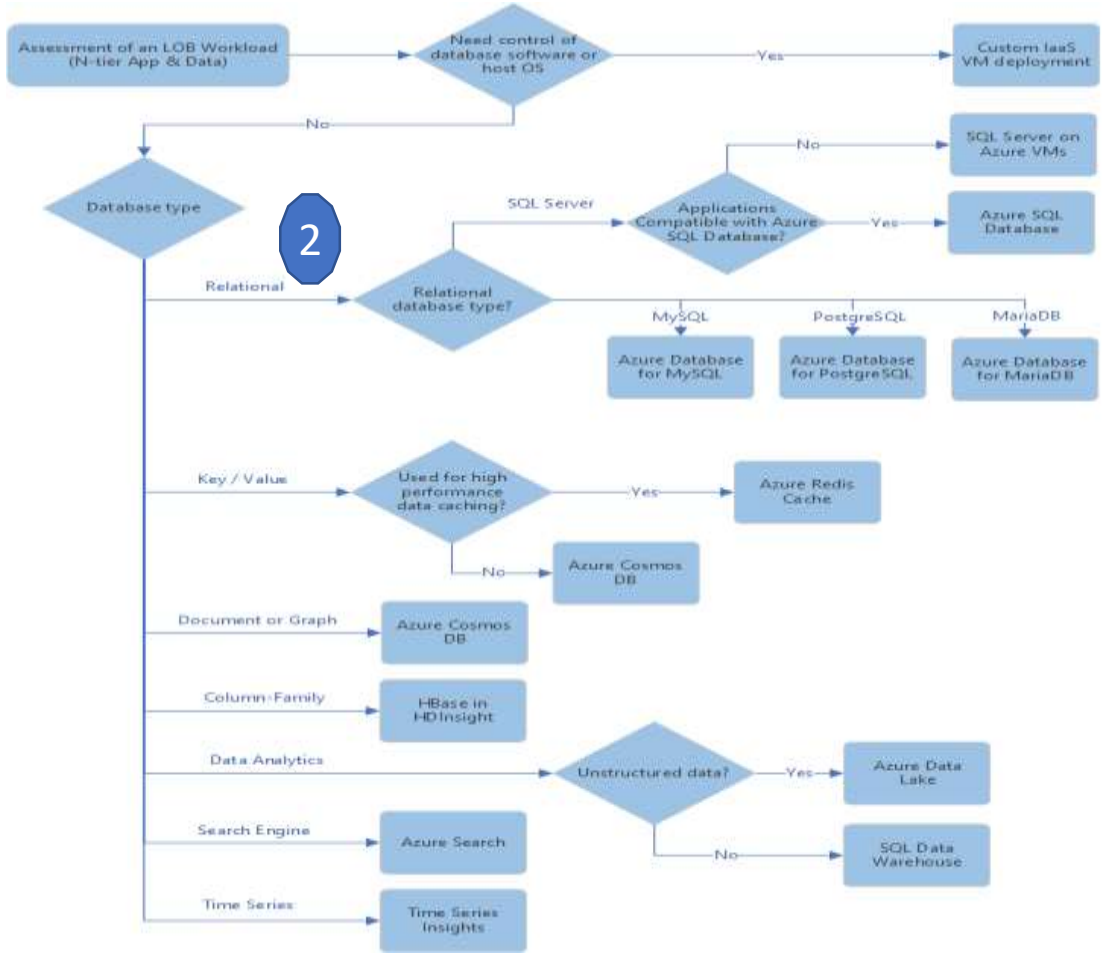
Copyright - Tout droit réservé - OFPPT

PARTIE 2

Arbre de décision des services de base de données Azure

2 Vos charges de travail utiliseront-elles une technologie de base de données relationnelle ?

Si oui, Azure fournit des fonctionnalités de base de données PaaS managées pour Azure SQL Database, MySQL, PostgreSQL et MariaDB.

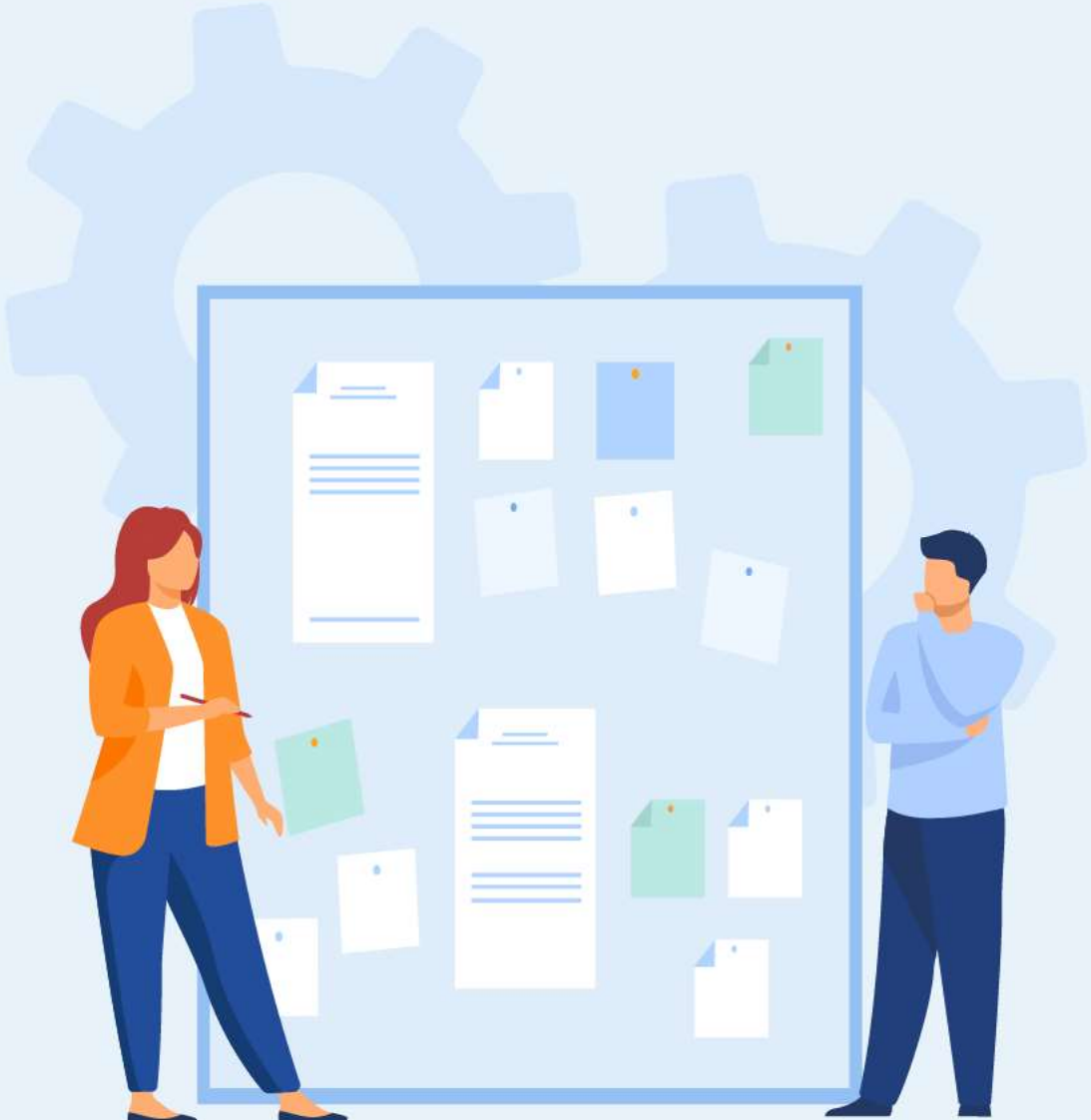


Copyright - Tout droit réservé - OFPPT

Quizz : Scénarios de base de données courants

Scénario	Service de données
J'ai besoin d'une base de données multi-modèle distribuée à l'échelle mondiale avec prise en charge des choix NoSQL.	Azure Cosmos DB

Copyright - Tout droit réservé - OFPPT



CHAPITRE 1

Inventorier les données

1. Catalogage des supports d’hébergement des données
2. **Habilitations des utilisateurs sur les données**

Méthodes d'authentification aux données

L'authentification aux données est le processus consistant à prouver que l'utilisateur est bien celui qu'il prétend être. Un utilisateur se connecte à une base de données à l'aide d'un compte d'utilisateur. Lorsqu'un utilisateur tente de se connecter à une base de données, il fournit un compte d'utilisateur et des informations d'authentification. L'utilisateur est authentifié à l'aide de l'une des deux méthodes d'authentification suivantes :

1. Authentification SQL

Avec cette méthode d'authentification, l'utilisateur envoie un nom de compte d'utilisateur et un mot de passe associé pour établir une connexion. Ce mot de passe est stocké dans la base de données master pour les comptes d'utilisateur liés à une connexion ou stockés dans la base de données contenant les comptes d'utilisateur non liés à une connexion.

2. Authentification Azure Active Directory

Avec cette méthode d'authentification, l'utilisateur soumet un nom de compte d'utilisateur et demande que le service utilise les informations d'identification stockées dans Azure Active Directory (Azure AD).

Copyright - Tout droit réservé - OFPPT

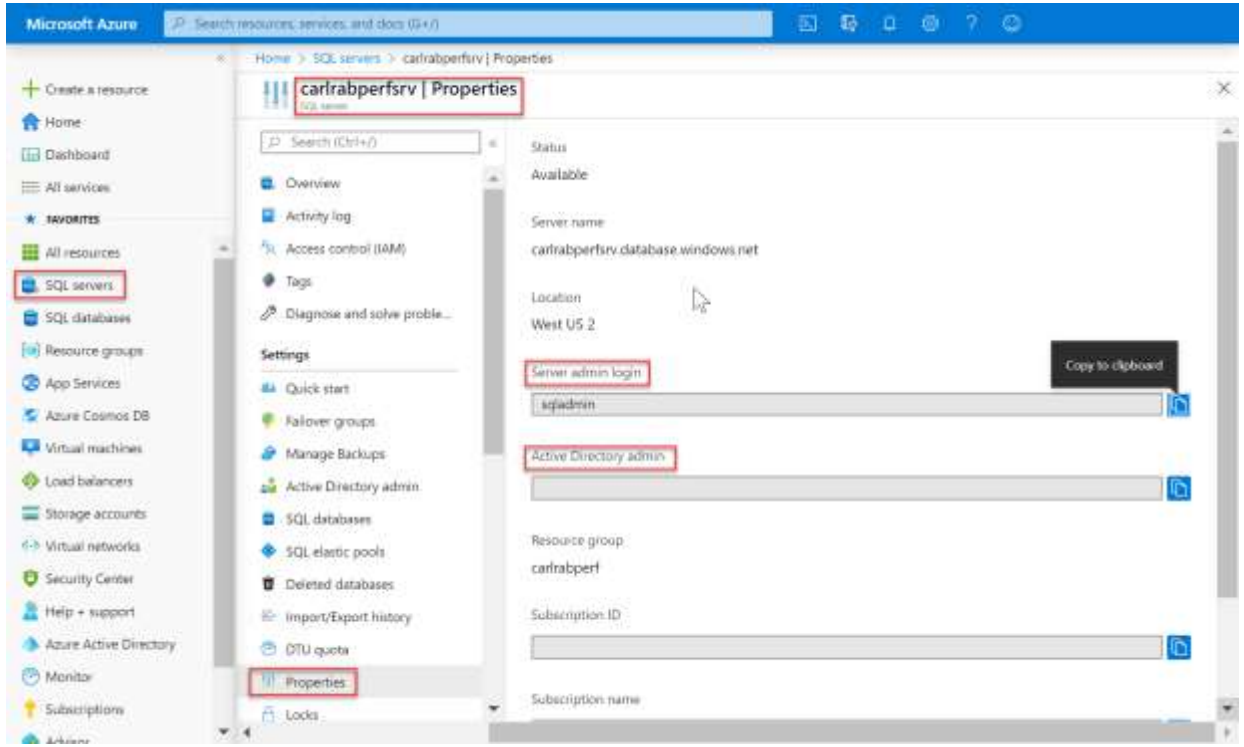
Base de données Azure SQL – Server Admin

Lorsque vous déployez Azure SQL pour la première fois, vous spécifiez une connexion d'administrateur et un mot de passe associé à cette connexion. Ce compte d'administration est appelé **Server Admin**

Pour identifier les comptes d'administrateur d'une base de données, ouvrez le Portail Azure, puis accédez à l'onglet **Propriétés** de votre serveur ou instance gérée.

Important

Une fois créé, le nom de connexion de Server Admin n'est pas modifiable. Pour réinitialiser son mot de passe, accédez au **portail Azure**, cliquez sur **Serveurs SQL**, sélectionnez le serveur dans la liste, pus cliquez sur **Réinitialiser le mot de passe**.



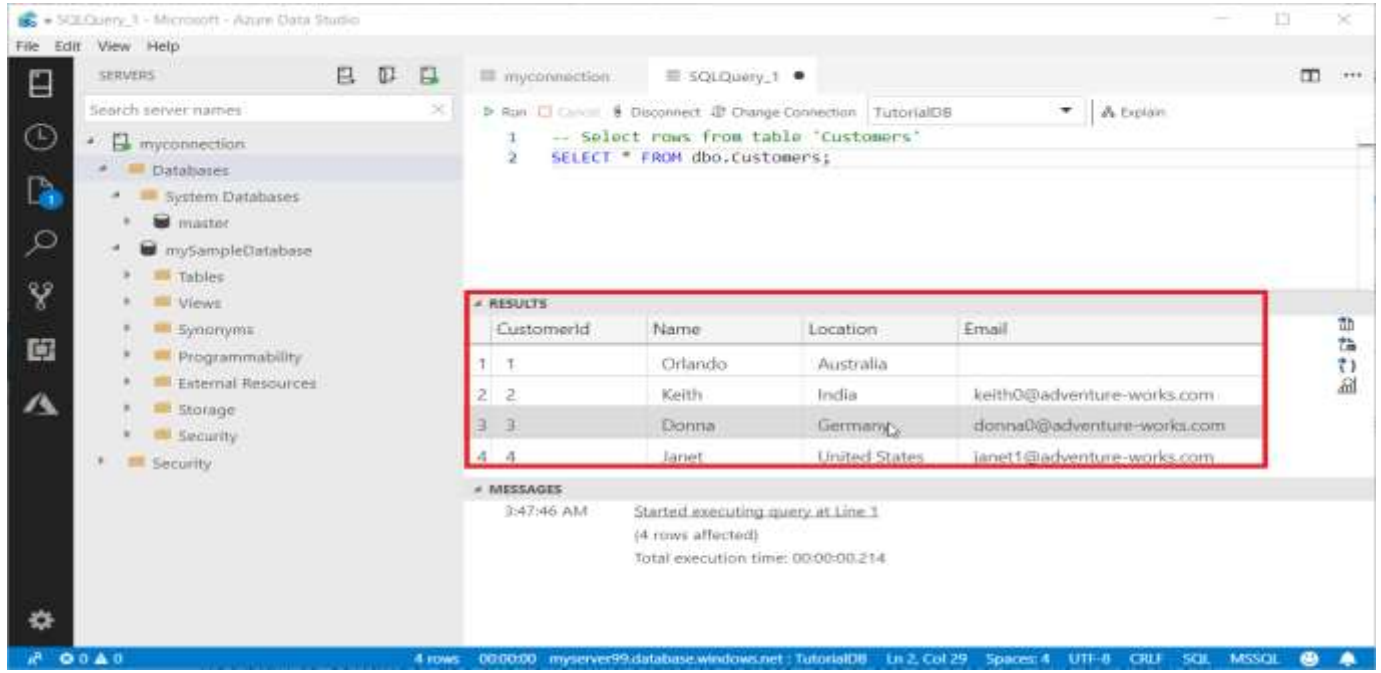
PARTIE 2

Copyright - Tout droit réservé - OFPPT

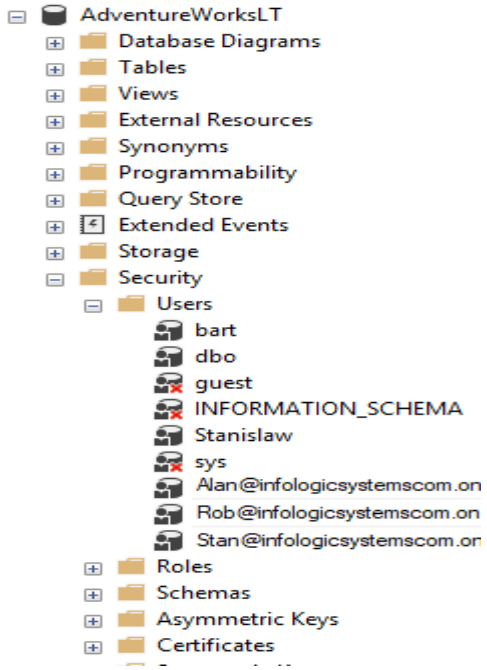
PARTIE 2

Base de données Azure SQL – Autres utilisateurs

Pour déterminer les utilisateurs sur les données d'une base de données Azure SQL, il faut accéder à cette base via un client (Azure Data Studio par exemple) et s'authentifier avec un compte ayant le droit d'accès comme par exemple le « Server Admin »



Liste des utilisateurs définis en interne dans une table de la base de données et qui accèdent via une application externe (En utilisation des requêtes SQL)



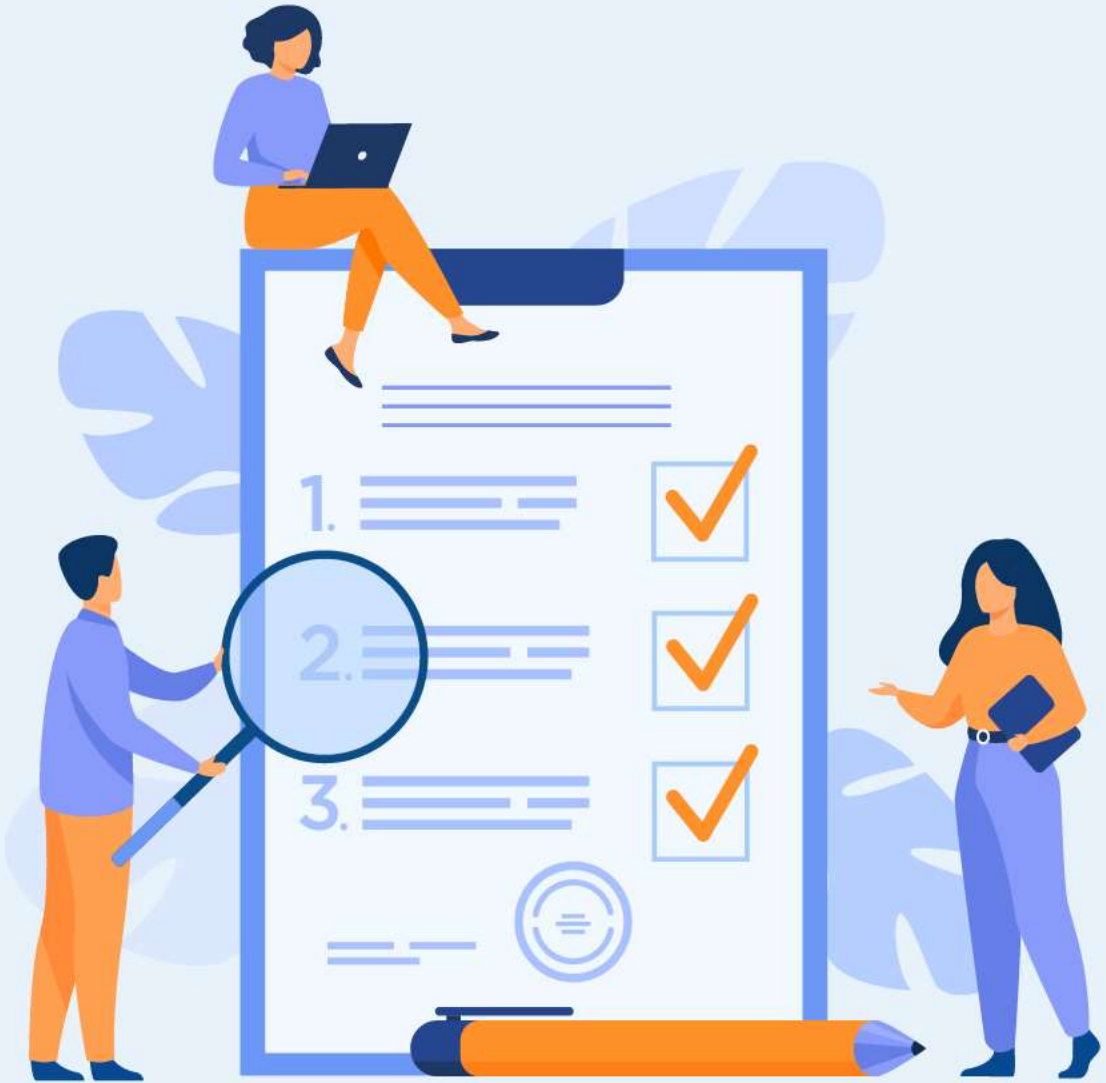
Liste des utilisateurs gestionnaires de la base de données définis en externe l'onglet « sécurité »

Copyright - Tout droit réservé - OFPPT

Les accès Microsoft aux données

PARTIE 2

Copyright - Tout droit réservé - OFPPT



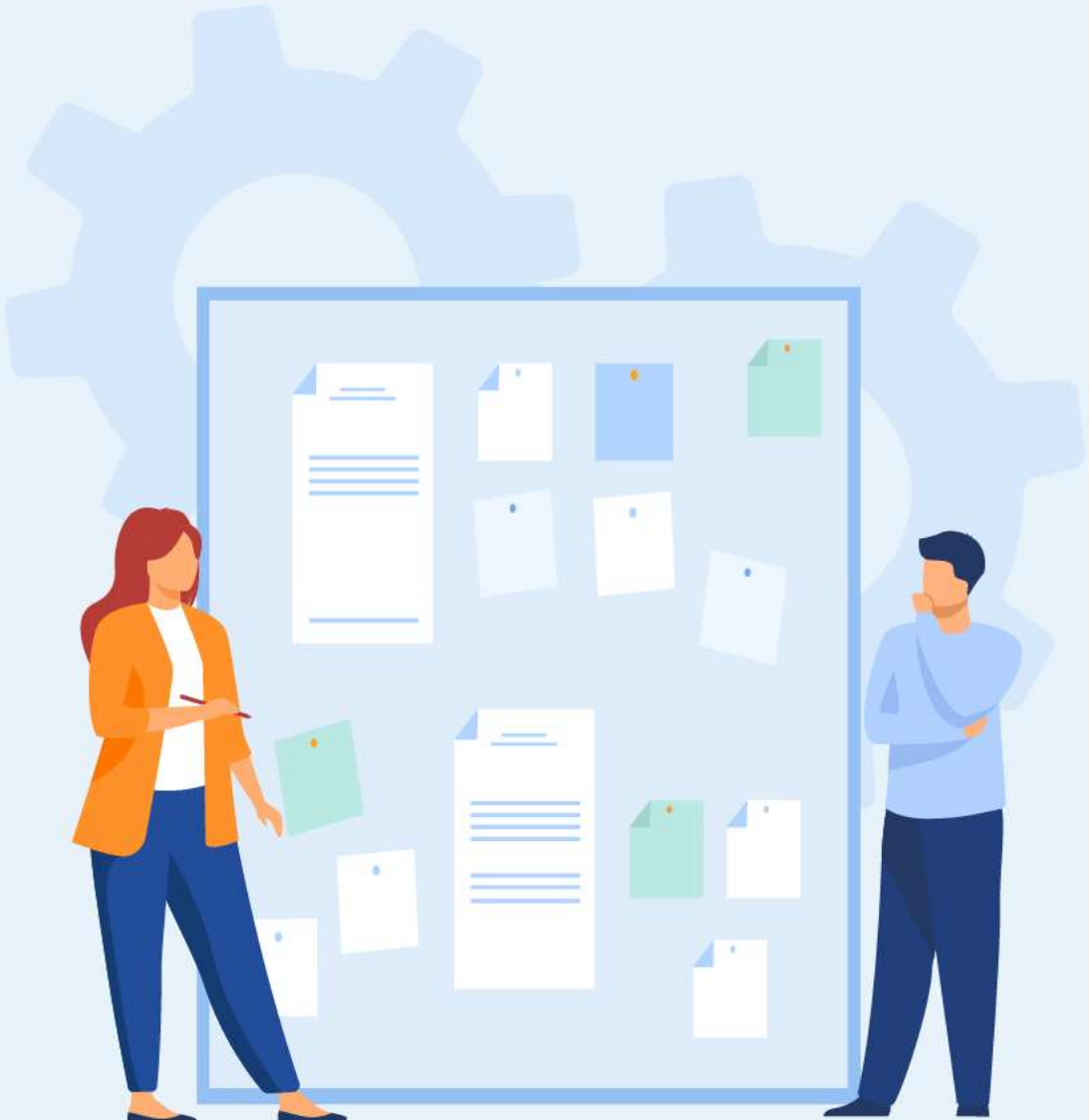
CHAPITRE 2

Cartographier les données

Ce que vous allez apprendre dans ce chapitre :

- Schémas des bases de données
- Flux des données
- Mappage des données

6 heures



CHAPITRE 2

Cartographier les données

1. **Schémas des bases de données**
2. Flux des données
3. Mappage des données

Présentation des schémas de base de données

L'Assistant Génération de schéma génère un schéma relationnel dénormalisé pour la base de données de la zone d'objet en fonction des dimensions et des groupes de mesures dans SQL Server Analysis Services. L'Assistant génère pour chaque dimension une table relationnelle appelée table de dimension, destinée à stocker les données de dimension, et pour chaque groupe de mesures une table relationnelle appelée table de faits, servant à stocker les données de faits. Lorsqu'il génère ces tables relationnelles, l'Assistant ignore les dimensions liées, les groupes de mesures liés et les dimensions de temps de serveur.

Validation

Avant de commencer à générer le schéma relationnel sous-jacent, l'Assistant Génération de schéma valide les SQL Server Analysis Services cubes et dimensions. Si l'Assistant détecte des erreurs, il s'arrête et signale les erreurs à la fenêtre Liste des tâches dans SQL Server Data Tools. Voici quelques exemples d'erreurs qui empêchent la génération :

- Les dimensions qui ont plus d'un attribut clé
- Les attributs parents qui ont des types de données différents de ceux des attributs clés
- Les groupes de mesures dépourvus de mesures
- Les dimensions dégénérées ou les mesures mal configurées
- Les clés de substitution mal configurées, par exemple plusieurs attributs utilisant le type d'attribut **ScdOriginalID** ou un attribut utilisant le type **ScdOriginalID** sans être lié à une colonne utilisant le type de données Integer.

Copyright - Tout droit réservé - OFPPT

Présentation des schémas de base de données

Tables de dimension

Pour chaque dimension, l'Assistant Génération de schéma crée une table de dimension à inclure dans la base de données de la zone de sujet. La structure de la table de dimension dépend des choix effectués lors de la conception de la dimension sur laquelle elle est basée.

Colonnes

L'Assistant génère une colonne pour les liaisons associées à chaque attribut de la dimension sur laquelle la table de dimension est basée, par exemple les liaisons pour les propriétés **KeyColumns**, **NameColumn**, **ValueColumn**, **CustomRollupColumn**, **CustomRollupPropertiesColumn** et **UnaryOperatorColumn** de chaque attribut.

Relations

L'Assistant génère une relation entre la colonne de chaque attribut parent et la clé primaire de la table de dimension.

L'Assistant crée également, s'il y a lieu, une relation à la clé primaire de chaque table de dimension supplémentaire définie comme dimension référencée du cube.

Contraintes

L'Assistant génère par défaut, pour chaque table de dimension, une contrainte de clé primaire basée sur l'attribut clé de la dimension. Si la contrainte de clé primaire est générée, une colonne de nom séparée est créée par défaut. Une clé primaire logique est créée dans la vue de source de données, même si vous décidez de ne pas créer la clé primaire dans la base de données.

Copyright - Tout droit réservé - OFPPT

Présentation des schémas de base de données

Tables de faits

Pour chaque groupe de mesures d'un cube, l'Assistant Génération de schéma crée une table de faits à inclure dans la base de données de la zone de sujet. La structure de la table de faits dépend des choix effectués lors de la conception du groupe de mesures sur lequel elle est basée et des relations établies entre le groupe de mesures et les dimensions incluses.

Colonnes

L'Assistant génère une colonne pour chaque mesure, sauf pour les mesures qui utilisent la fonction d'agrégation **Count** . En effet, de telles mesures ne nécessitent pas de colonne correspondante dans la table de faits.

L'Assistant génère également une colonne pour chaque colonne d'attribut de granularité de chaque relation de dimension régulière du groupe de mesures et, s'il y a lieu, une ou plusieurs colonnes pour les liaisons associées à chaque attribut d'une dimension qui entretient une relation de dimension de fait avec le groupe de mesures sur lequel cette table est basée.

Relations

L'Assistant génère une relation pour chaque relation de dimension régulière de la table de faits à l'attribut de granularité de la table de la dimension. Si la granularité est basée sur l'attribut clé de la table de dimension, la relation est créée dans la base de données et dans la vue de source de données. Si la granularité est basée sur un autre attribut, la relation n'est créée que dans la vue de source de données.

Si vous choisissez de générer les index dans l'Assistant, un index non-cluster est créé pour chacune de ces colonnes de relation.

Contraintes

Les clés primaires ne sont pas générées sur les tables de faits.

Si vous choisissez d'appliquer l'intégrité référentielle, des contraintes d'intégrité référentielle sont générées, le cas échéant, entre les tables de dimension et les tables de faits.

Copyright - Tout droit réservé - OFPPT

Présentation des schémas de base de données

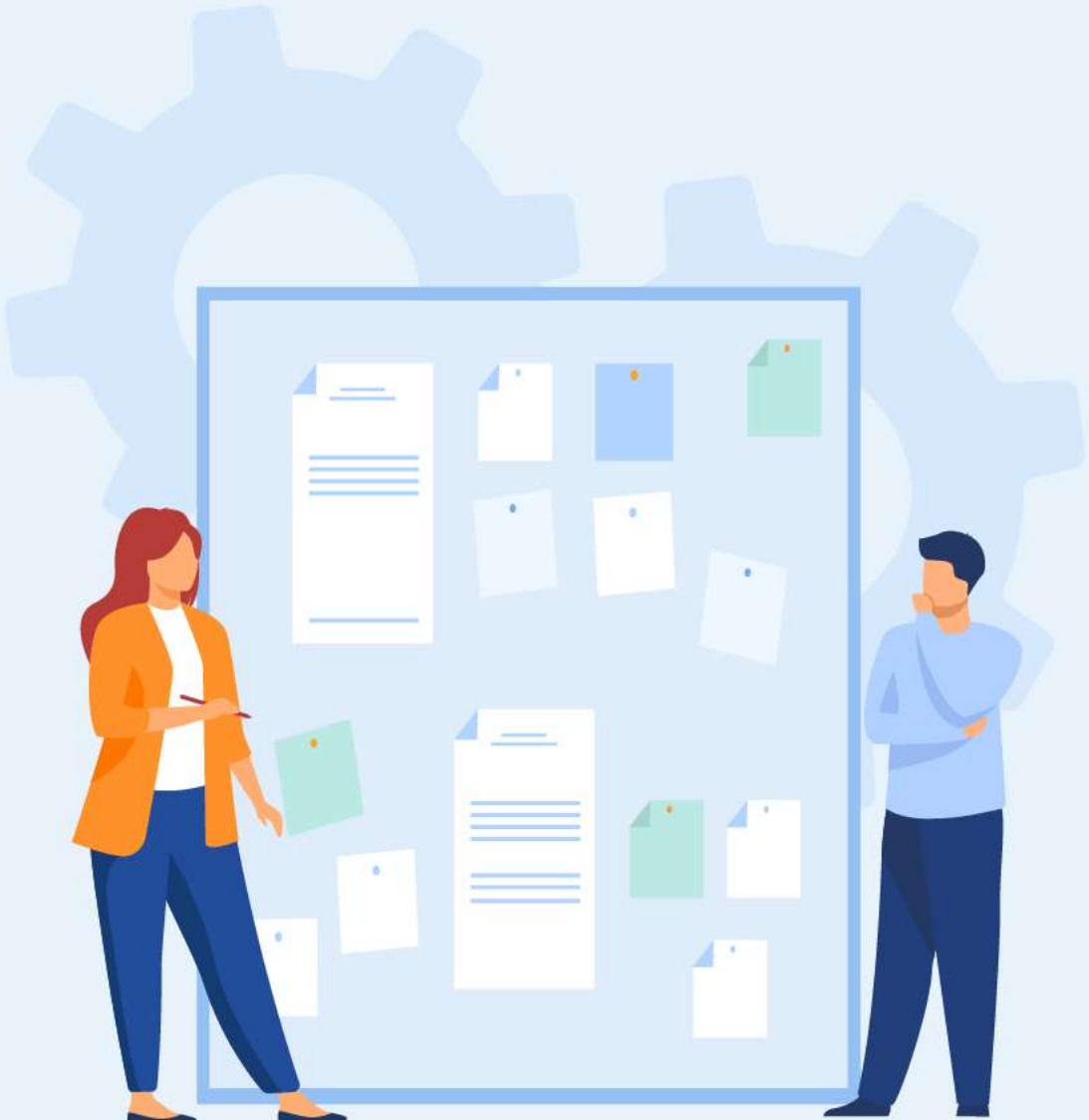
Conversion de type de données et longueurs par défaut

L'Assistant Génération de schéma ignore les types de données dans tous les cas, à l'exception des colonnes qui utilisent le type de données **wchar** SQL Server. Le type de données **wchar** se traduit directement en type de données **nvarchar** . Toutefois, si la longueur spécifiée d'une colonne utilisant le type **wchar** dépasse 4000 octets, l'Assistant Génération de schéma produit une erreur.

Le tableau suivant indique la longueur par défaut de la colonne si un élément de données, par exemple la liaison d'un attribut, n'a pas de longueur spécifiée.

Élément de données	Longueur par défaut (en octets)
KeyColumn	50
NameColumn	50
CustomRollupColumn	3000
CustomRollupPropertiesColumn	500
UnaryOperatorColumn	1

Copyright - Tout droit réservé - OFPPT



CHAPITRE 2

Cartographier les données

1. Schémas des bases de données
2. **Flux des données**
3. Mappage des données

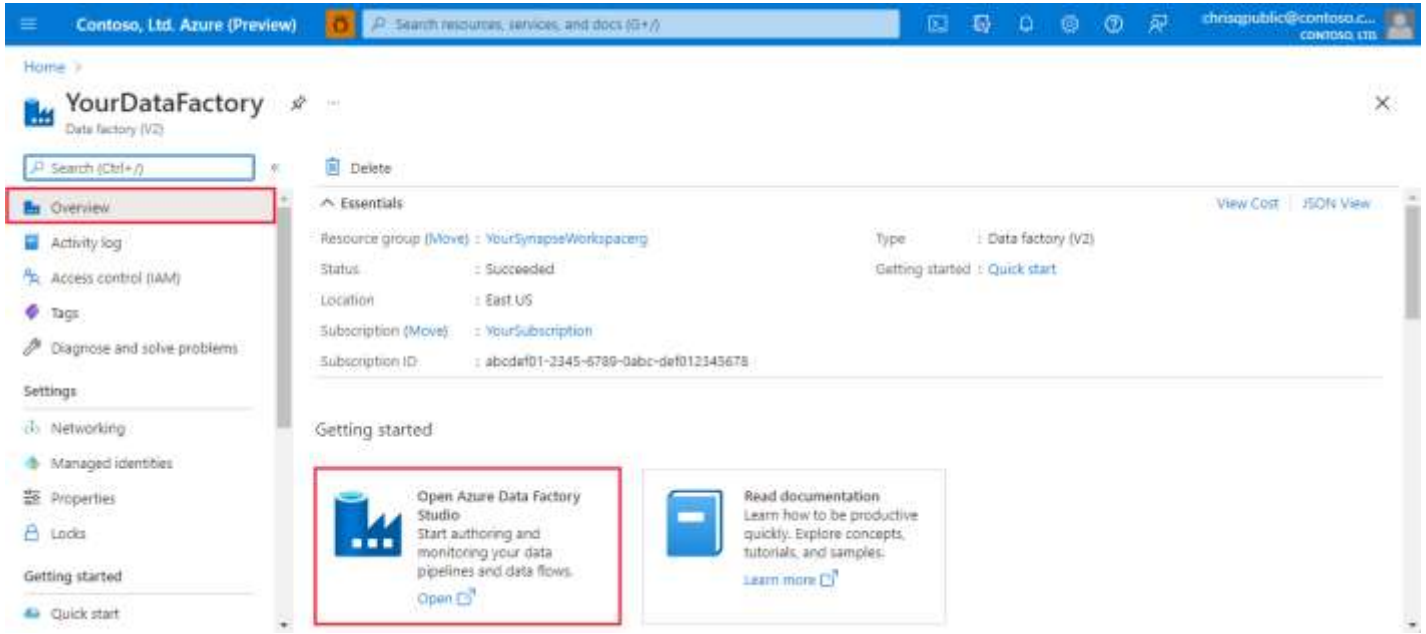
Créer des flux de données Azure Data Factory

Les flux de données sont disponibles à la fois dans les pipelines Azure Data Factory et Azure Synapse. Cet article s'applique aux flux de données de mappage.

Le mappage de flux de données permet de transformer des données à grande échelle sans aucun codage. Vous pouvez concevoir une tâche de transformation de données dans le concepteur de flux de données en créant une série de transformations. Commencez par un certain nombre de transformations sources, suivies par des étapes de transformation de données. Ensuite, réalisez votre flux de données avec un récepteur qui servira de destination à vos résultats.

Étapes de la création d'un flux de données

Commencez par créer un Data Factory V2 sur le portail Azure. Après avoir créé votre nouvelle fabrique, sélectionnez la vignette **Ouvrir Azure Data Factory Studio** dans le portail, pour lancer Data Factory Studio.

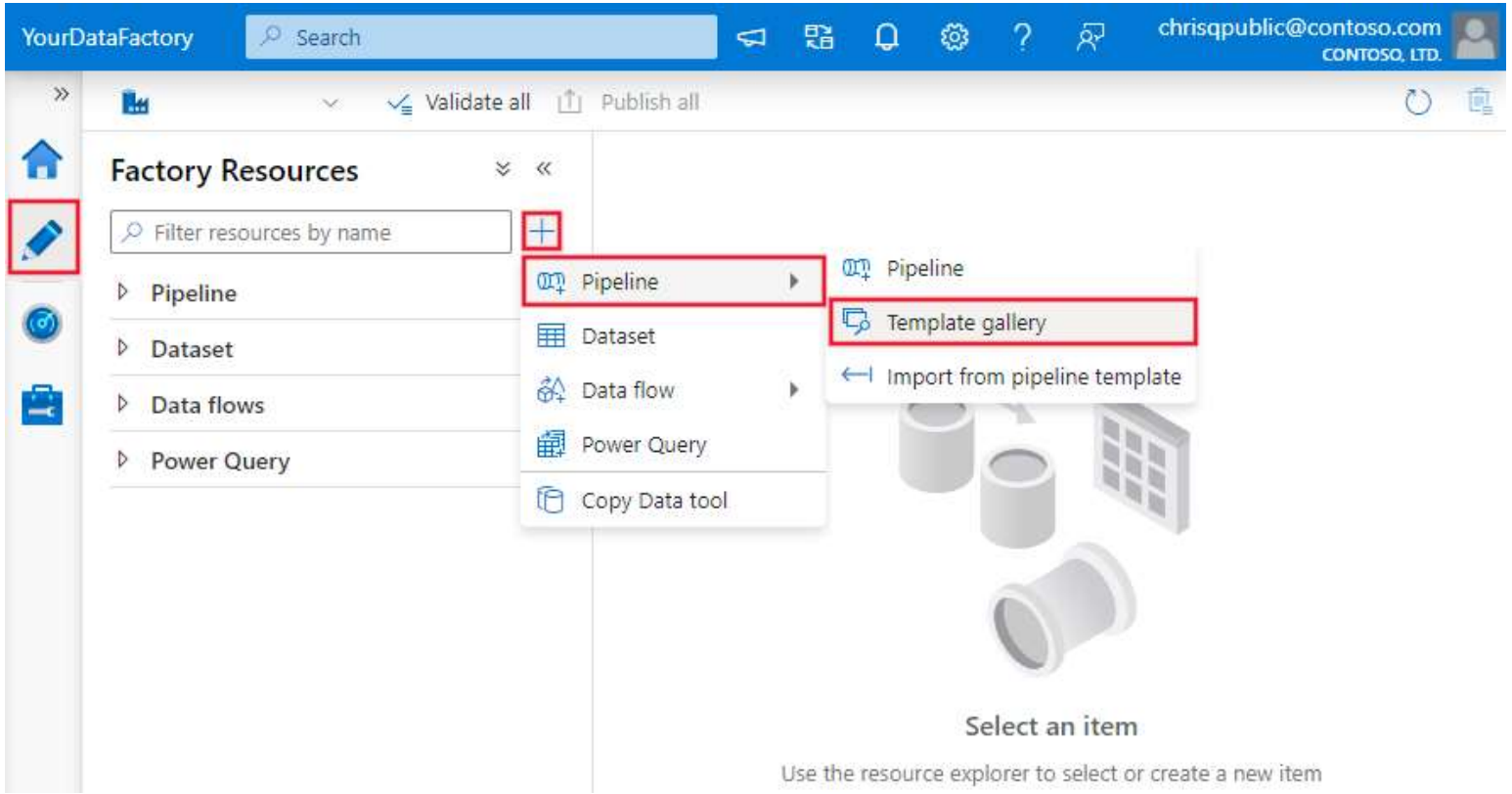


PARTIE 2

Copyright - Tout droit réservé - OFPPT

Créer des flux de données Azure Data Factory

Vous pouvez ajouter des exemples de flux de données à partir de la galerie de modèles. Pour parcourir la galerie, sélectionnez l'onglet **Auteur** dans Data Factory Studio, puis cliquez sur le signe plus pour choisir **Pipeline** | **Galerie de modèles**.



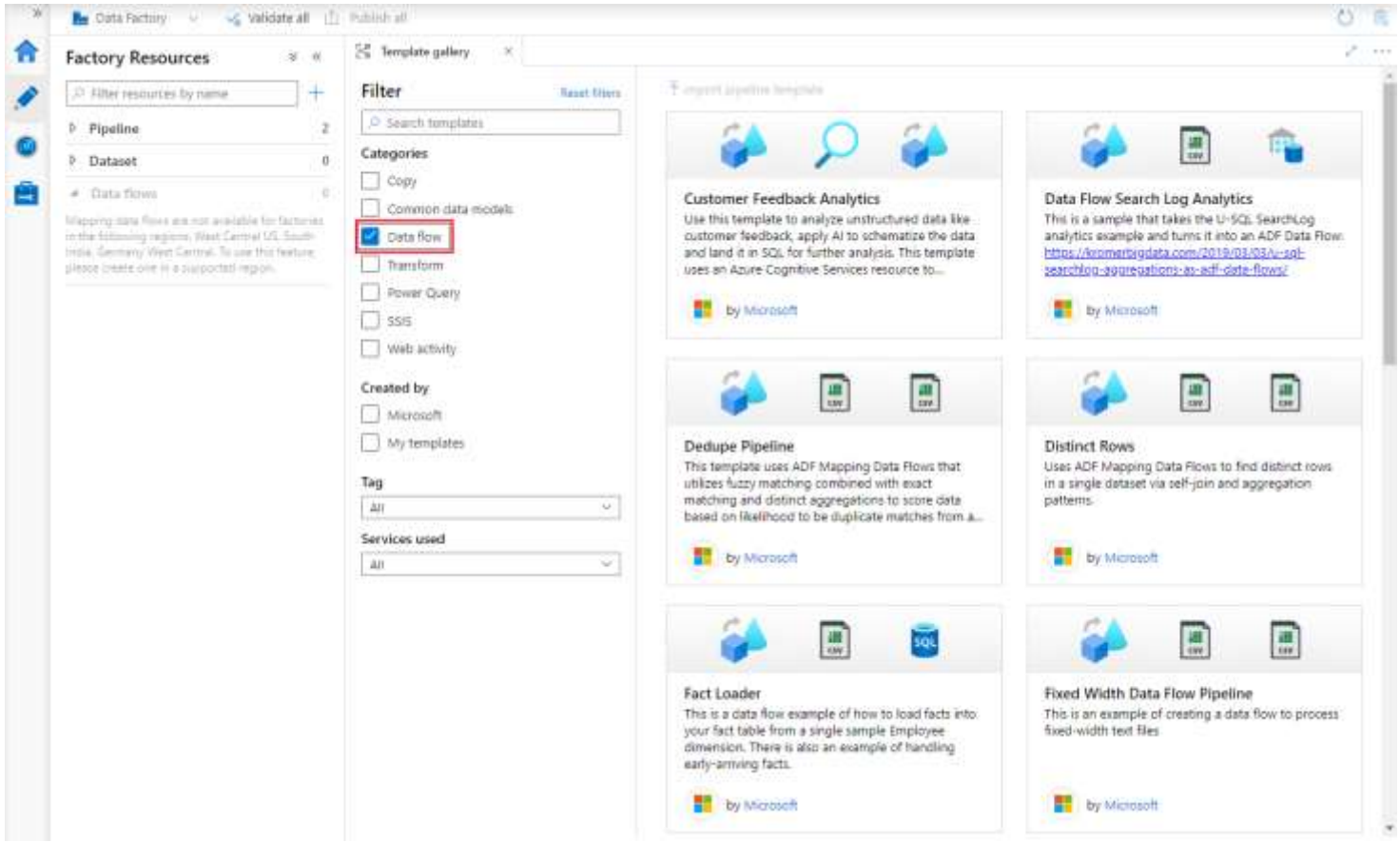
PARTIE 2

Copyright - Tout droit réservé - OFPPT

PARTIE 2

Créer des flux de données Azure Data Factory

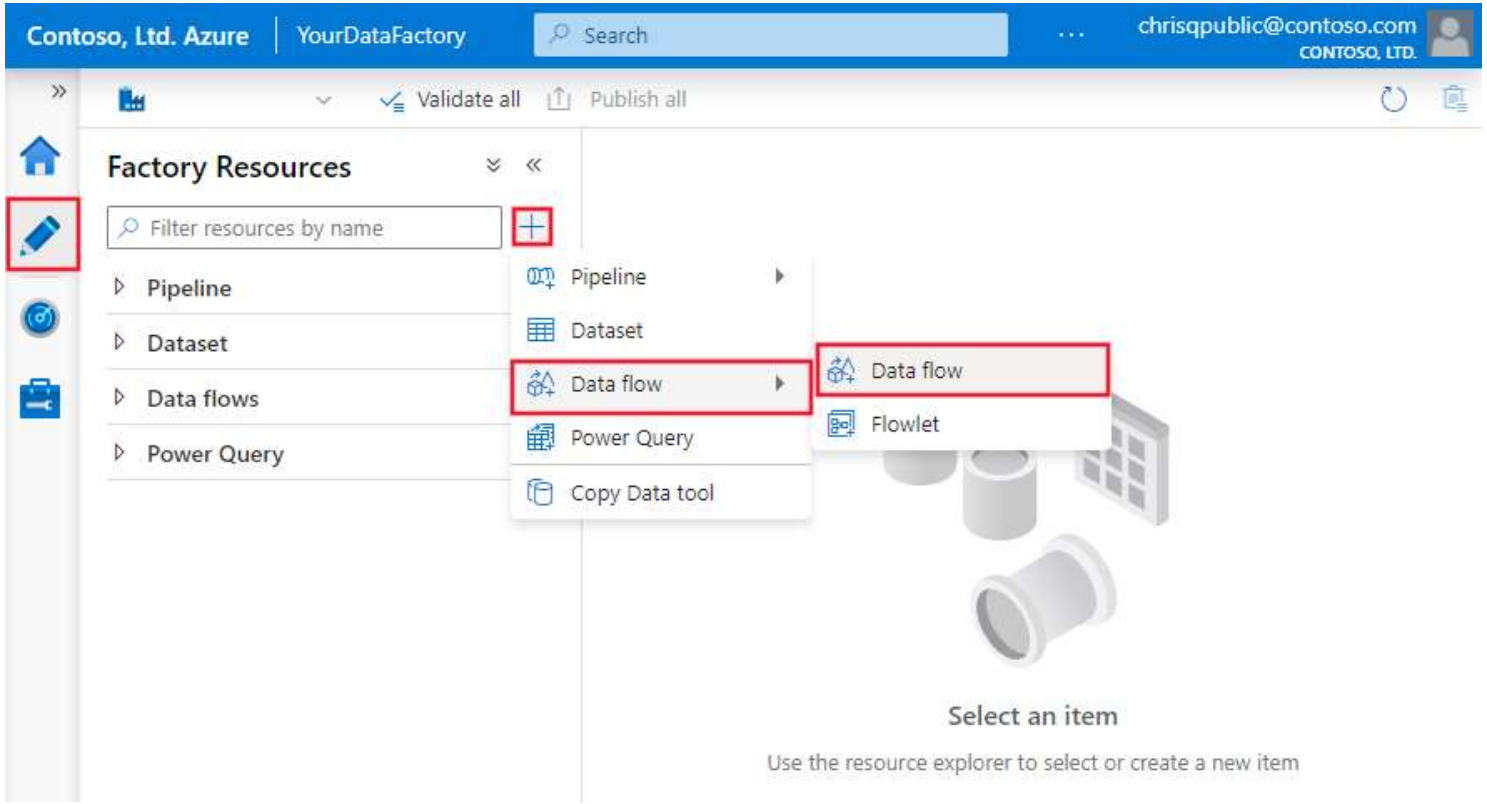
Sélectionnez la catégorie Data Flow pour effectuer une sélection parmi les modèles disponibles.



Copyright - Tout droit réservé - OFPPT

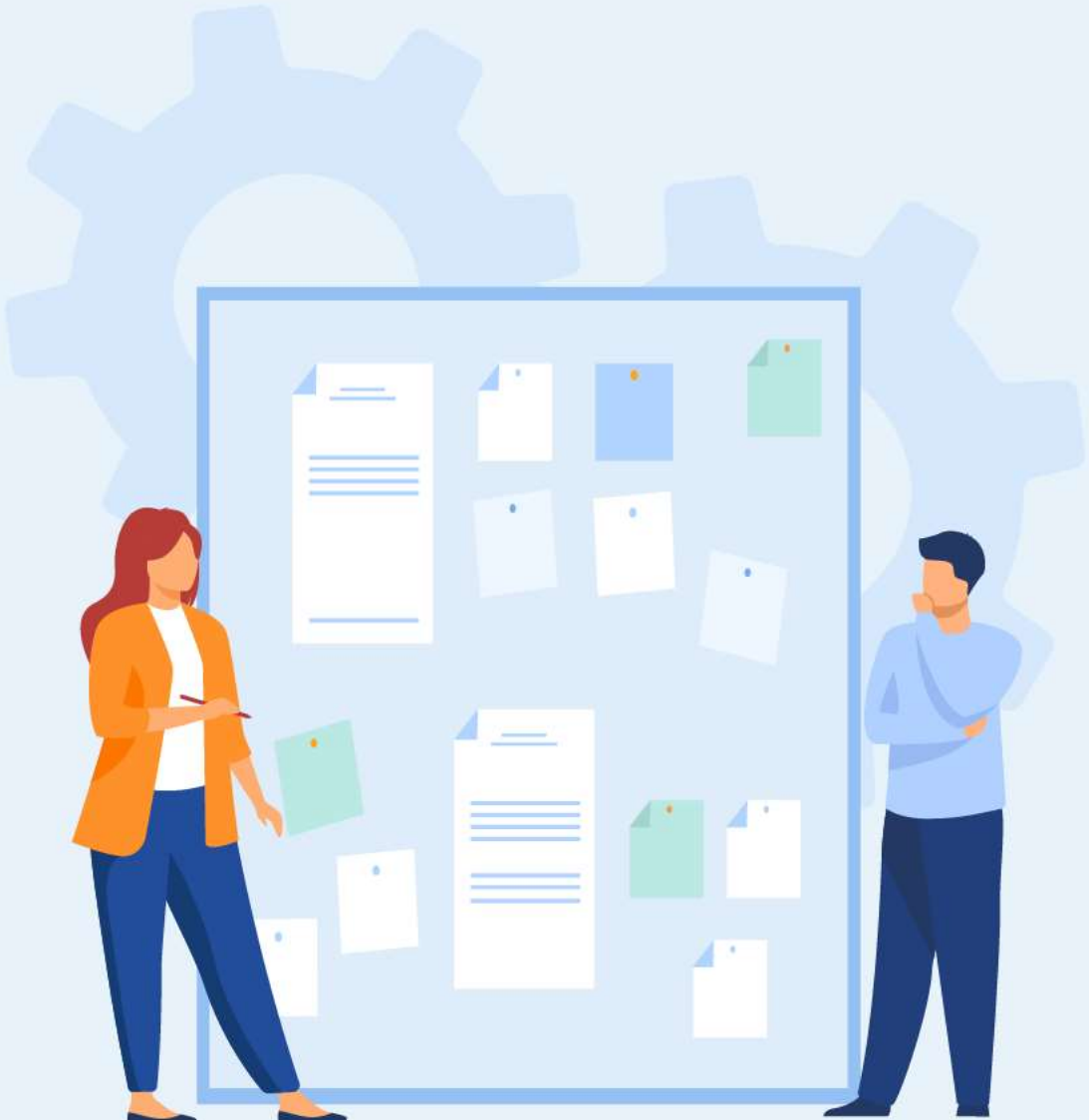
Créer des flux de données Azure Data Factory

Vous pouvez également ajouter des flux de données directement à votre fabrique de données sans utiliser de modèle. Sélectionnez l'onglet **Auteur** dans Data Factory Studio, puis cliquez sur le signe plus pour choisir **Data Flow** | **Data Flow**.



PARTIE 2

Copyright - Tout droit réservé - OFPPT



CHAPITRE 2

Cartographier les données

1. Schémas des bases de données
2. Flux des données
3. **Mappage des données**

Mappage des données

Les mappages de données sont utilisés pendant l'ingestion pour mapper les données entrantes aux colonnes à l'intérieur des tables.

L'Explorateur de données prend en charge différents types de mappages (`row-oriented` CSV, JSON, AVRO et W3CLOGFILE) et `column-oriented` (Parquet et ORC).

Chaque élément de la liste de mappage est construit à partir de trois propriétés :

Propriété	Description
Column	Nom de colonne cible dans la table
Datatype	(Facultatif) Type de données avec lequel créer la colonne mappée s'il n'existe pas déjà dans la table
Properties	(Facultatif) Conteneur de propriétés contenant des propriétés spécifiques à chaque mappage, comme décrit dans chaque section ci-dessous.

Copyright - Tout droit réservé - OFPPT

Mappage des données

Les mappages de données sont utilisés pendant l'ingestion pour mapper les données entrantes aux colonnes à l'intérieur des tables.

L'Explorateur de données prend en charge différents types de mappages (`row-oriented` CSV, JSON, AVRO et W3CLOGFILE) et `column-oriented` (Parquet et ORC).

Chaque élément de la liste de mappage est construit à partir de trois propriétés :

Propriété	Description
Column	Nom de colonne cible dans la table
Datatype	(Facultatif) Type de données avec lequel créer la colonne mappée s'il n'existe pas déjà dans la table
Properties	(Facultatif) Conteneur de propriétés contenant des propriétés spécifiques à chaque mappage, comme décrit dans chaque section ci-dessous.

Les mappages peuvent être précréés et référencés à partir de la commande d'ingestion à l'aide `ingestionMappingReference` de paramètres.

Copyright - Tout droit réservé - OFPPT

Mappage CSV

Lorsque le fichier source est un format CSV (ou un format séparé par un délimiteur) et que son schéma ne correspond pas au schéma de table actuel, un mappage CSV est mappé du schéma de fichier au schéma de table. Si la table n'existe pas dans Azure Data Explorer, elle est créée en fonction de ce mappage. Si certains champs du mappage sont manquants dans la table, ils sont ajoutés.

Le mappage CSV peut être appliqué à tous les formats tabulaires séparés par un délimiteur : CSV, TSV, PSV, SCSV, SOHsv et TXT.

Chaque élément de la liste décrit un mappage pour une colonne spécifique et doit contenir l'une des propriétés suivantes

Propriété	Description
Ordinal	Numéro de l'ordre des colonnes dans CSV.
ConstantValue	(Facultatif) Valeur constante à utiliser pour une colonne au lieu d'une valeur dans le fichier CSV.

Copyright - Tout droit réservé - OFPPT

JSON

```
[
  {"Column": "event_time", "Properties": {"Ordinal": "0"}},
  {"Column": "event_name", "Properties": {"Ordinal": "1"}},
  {"Column": "event_type", "Properties": {"Ordinal": "2"}},
  {"Column": "ingestion_time", "Properties": {"ConstValue": "2021-01-01T10:32:00"}}
]
```

```
.ingest into Table123 (@"source1", @"source2")
 with (
format="csv",
 ingestionMapping =
'['
 '{"Column": "column_a", "Properties": {"Ordinal": 0}},
' '{"Column": "column_b", "Properties": {"Ordinal": 1}}'
 ']'
 )
```

Exemple de mappage CSV

```
.ingest into Table123 (@"source1", @"source2")
    with
    (
        format="csv",
        ingestionMappingReference = "MappingName"
    )
```

```
.ingest into Table123 (@"source1", @"source2")
    with
    (
        format="csv"
    )
```

PARTIE 2

Copyright - Tout droit réservé - OFPPT

Mappage JSON

Lorsque le fichier source est au format JSON, le contenu du fichier est mappé à la table. La table doit exister dans la base de données, sauf si un type de données valide est spécifié pour toutes les colonnes mappées. Les colonnes mappées dans le mappage JSON doivent exister dans la table, sauf si un type de données est spécifié pour toutes les colonnes non existantes.

Chaque élément de la liste décrit un mappage pour une colonne spécifique et peut contenir les propriétés suivantes :

Propriété	Description
Path	Si la valeur commence par $: chemin JSON vers le champ qui deviendra le contenu de la colonne dans le document JSON (chemin JSON qui indique l'intégralité du document). Si la valeur ne commence pas par $: une valeur constante est utilisée. Les chemins JSON qui incluent des caractères spéciaux doivent être placés dans une séquence d'échappement en tant que [« Nom de propriété »].
ConstantValue	(Facultatif) Valeur constante à utiliser pour une colonne au lieu d'une valeur dans le fichier JSON.
Transform	(Facultatif) Transformation qui doit être appliquée au contenu avec des transformations de mappage.

Copyright - Tout droit réservé - OFPPT

Mappage JSON

Lorsque le fichier source est au format JSON, le contenu du fichier est mappé à la table. La table doit exister dans la base de données, sauf si un type de données valide est spécifié pour toutes les colonnes mappées. Les colonnes mappées dans le mappage JSON doivent exister dans la table, sauf si un type de données est spécifié pour toutes les colonnes non existantes.

Chaque élément de la liste décrit un mappage pour une colonne spécifique et peut contenir les propriétés suivantes :

Propriété	Description
Path	Si la valeur commence par $: chemin JSON vers le champ qui deviendra le contenu de la colonne dans le document JSON (chemin JSON qui indique l'intégralité du document). Si la valeur ne commence pas par $: une valeur constante est utilisée. Les chemins JSON qui incluent des caractères spéciaux doivent être placés dans une séquence d'échappement en tant que [« Nom de propriété »].
ConstantValue	(Facultatif) Valeur constante à utiliser pour une colonne au lieu d'une valeur dans le fichier JSON.
Transform	(Facultatif) Transformation qui doit être appliquée au contenu avec des transformations de mappage.

Copyright - Tout droit réservé - OFPPT

Exemple de mappage JSON

```
[
{"Column": "event_timestamp", "Properties": {"Path": "$.Timestamp"}}, {"Column": "event_name", "Properties": {"Path": "$.Event.Name"}},
 {"Column": "event_type", "Properties": {"Path": "$.Event.Type"}}, {"Column": "source_uri", "Properties": {"Transform": "SourceLocation"}},
 {"Column": "source_line", "Properties": {"Transform": "SourceLineNumber"}},
 {"Column": "event_time", "Properties": {"Path": "$.Timestamp", "Transform": "DateTimeFromUnixMilliseconds"}},
 {"Column": "ingestion_time", "Properties": {"ConstValue": "2021-01-01T10:32:00"}},
 {"Column": "full_record", "Properties": {"Path": "$"}}
]
```

Lorsque le mappage ci-dessus est fourni dans le cadre de la `.ingest` commande de contrôle, il est sérialisé en tant que chaîne JSON.

```
.ingest into Table123 (@"source1", @"source2")
 with (
 format = "json",
ingestionMapping = '['
 '{"Column": "column_a", "Properties": {"Path": "$.Obj.Property"}},' '{"Column": "column_b", "Properties": {"Path": "$.Property"}},' '{"Column": "custom_column", "Properties": {"Path": "$.[\'Property name with space\']"}}'
 ']'
)
```


Copyright - Tout droit réservé - OFPPT

Exemple de mappage JSON

Lorsque le mappage ci-dessus est précréé , il peut être référencé dans la commande de `.ingest` contrôle :

```
.ingest into Table123 (@"source1", @"source2")
    with
    (
        format="json",
        ingestionMappingReference = "Mapping_Name"
    )
```

L'ingestion est possible sans spécifier de mappage .

```
.ingest into Table123 (@"source1", @"source2")
    with
    (
        format="json"
    )
```


Copyright - Tout droit réservé - OFPPT

Exemple de copie de mappage JSON

Vous pouvez copier le mappage JSON d'une table existante et créer une table avec le même mappage à l'aide du processus suivant :

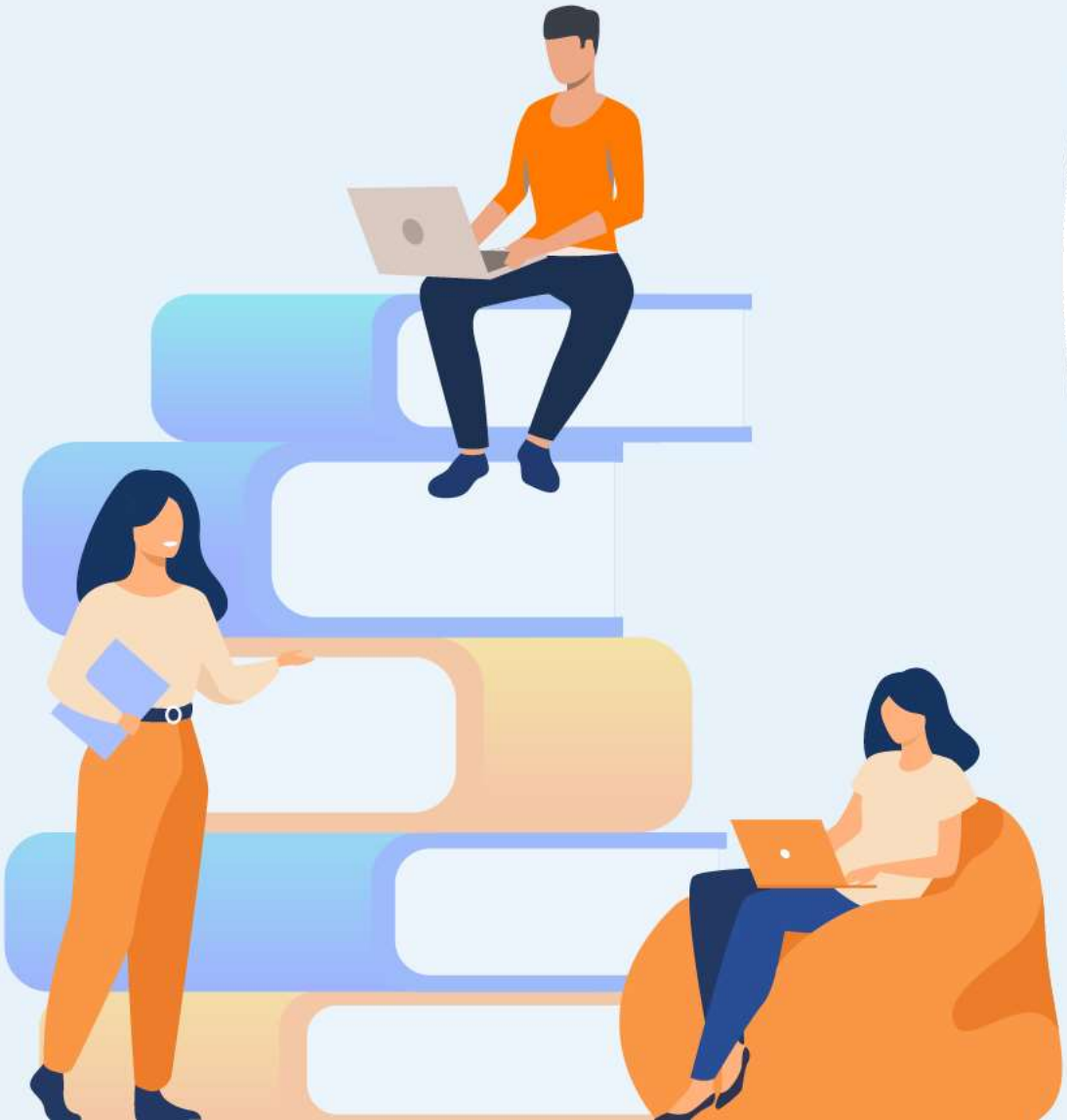
- Exécutez la commande suivante sur la table dont vous souhaitez copier le mappage :

```
.show table TABLENAME ingestion json mappings
| extend formatted_mapping = strcat("'",replace_string(Mapping, "'", "\\'"),"'")
| project formatted_mapping
```

- Utilisez la sortie de la commande ci-dessus pour créer une table avec le même mappage :

```
.create table TABLENAME ingestion json mapping "TABLENAME_Mapping" RESULT_OF_ABOVE_CMD
```


Copyright - Tout droit réservé - OFPPT



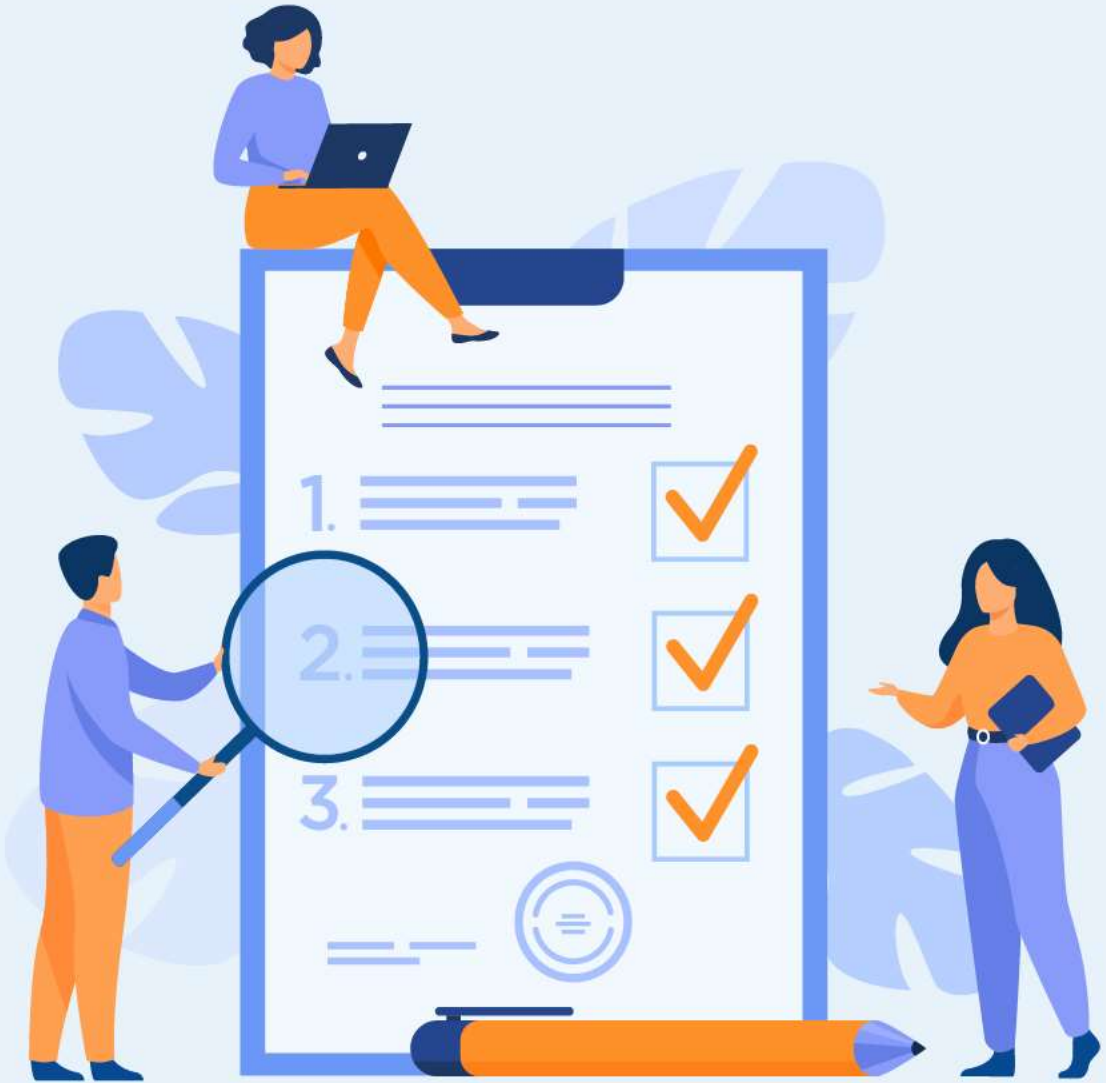
PARTIE 3

Établir des stratégies de transferts des données

Dans ce module, vous allez :

- Etablir des stratégies d'entrée
- Etablir des stratégies de sortie

9 heures



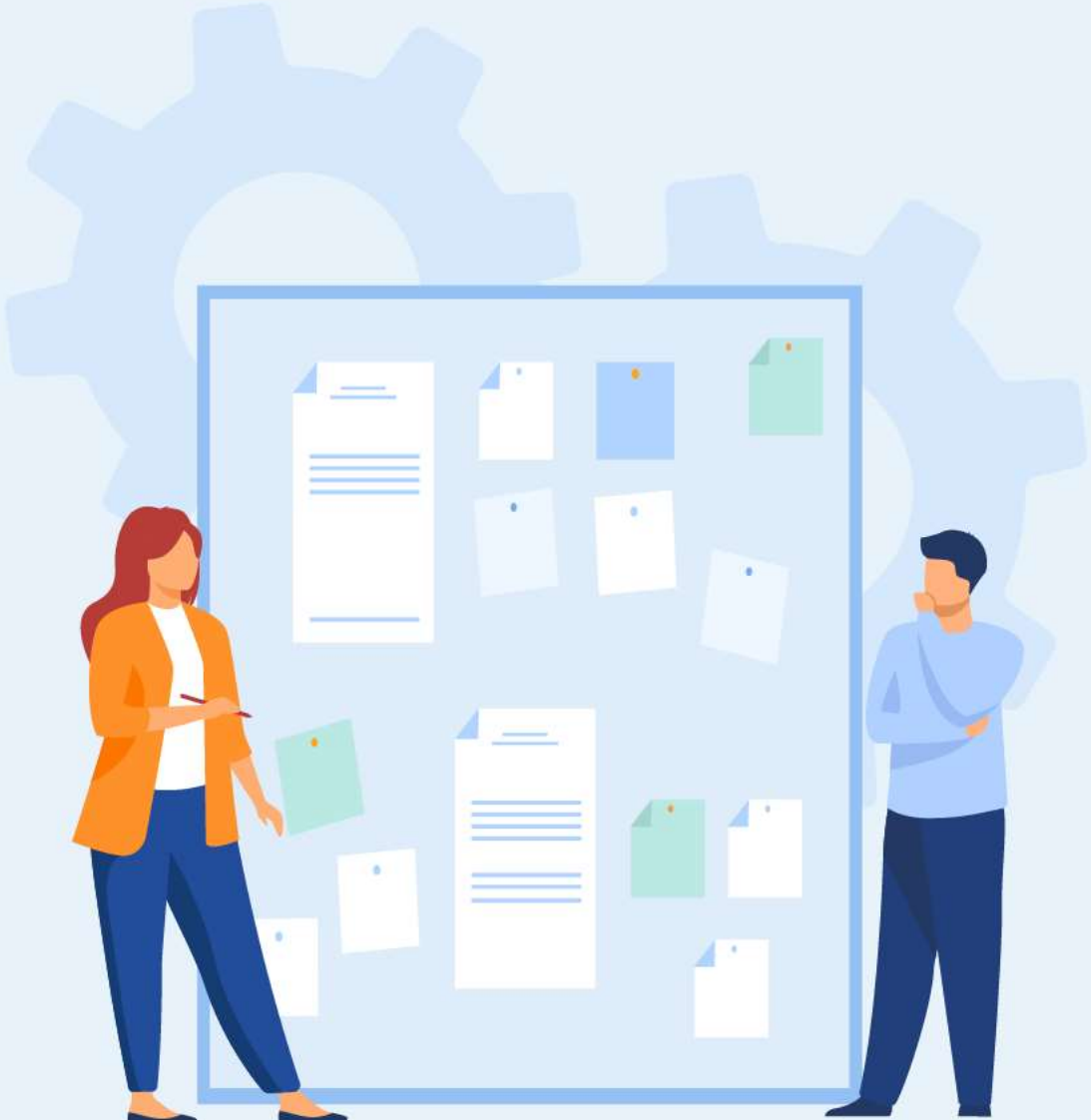
CHAPITRE 1

Etablir des stratégies d’entrée

Ce que vous allez apprendre dans ce chapitre :

- Production d’une stratégie de restauration
- Production d’une stratégie de réplication
- Production d’une stratégie d’import
- Production d’une stratégie de rétention

4,5 heures



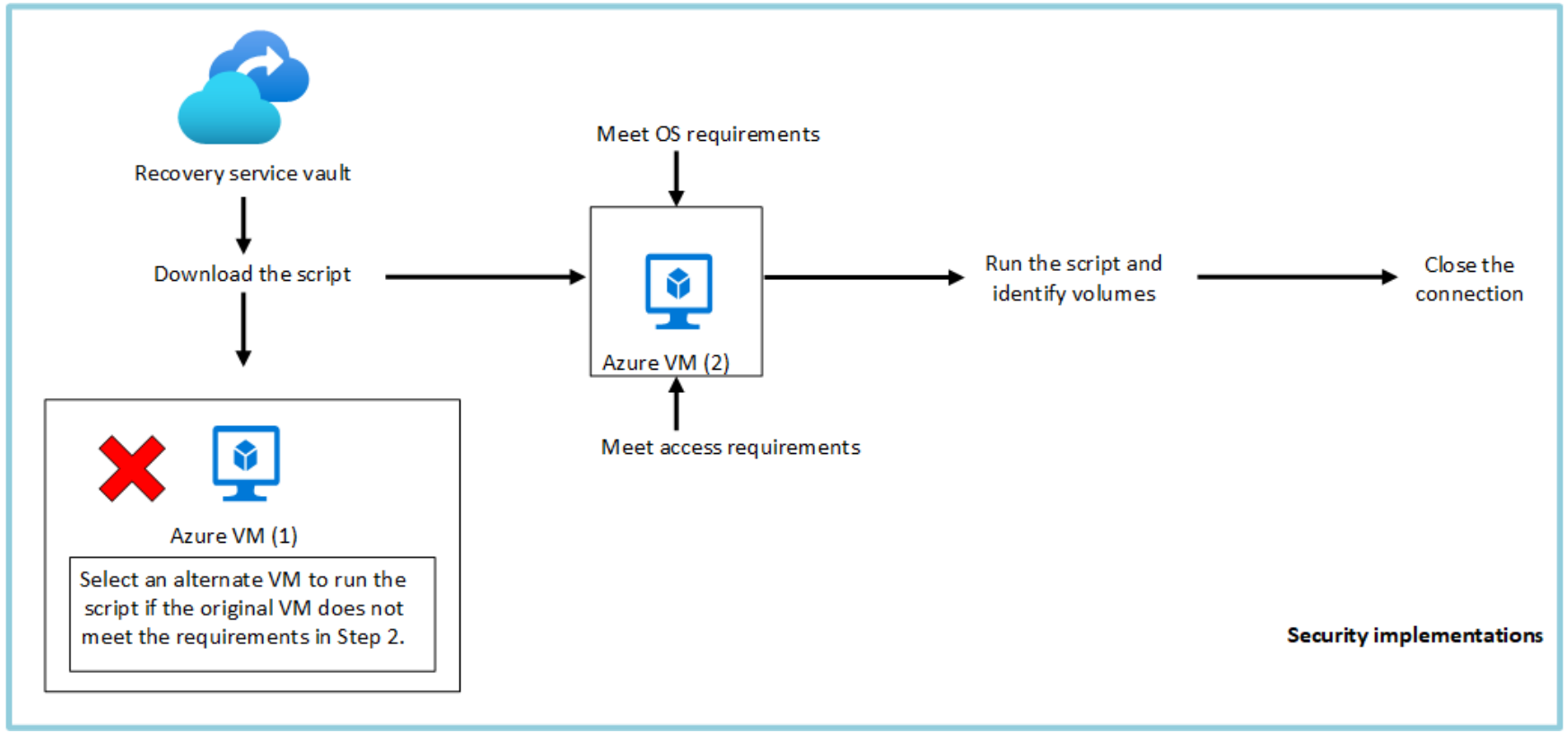
CHAPITRE 1

Etablir des stratégies d’entrée

1. **Production d’une stratégie de restauration**
2. Production d’une stratégie de réplication
3. Production d’une stratégie d’import
4. Production d’une stratégie de rétention

Récupérer des fichiers à partir d'une sauvegarde

La sauvegarde Azure offre la possibilité de restaurer des machines virtuelles et des disques Azure à partir de sauvegardes de machines virtuelles Azure, également appelées points de récupération. Cet article explique comment récupérer des fichiers et des dossiers à partir d'une sauvegarde de machine virtuelle Azure. La restauration des fichiers et des dossiers est disponible uniquement pour les machines virtuelles Azure déployées à l'aide du modèle Resource Manager et protégées dans un coffre Recovery Services.



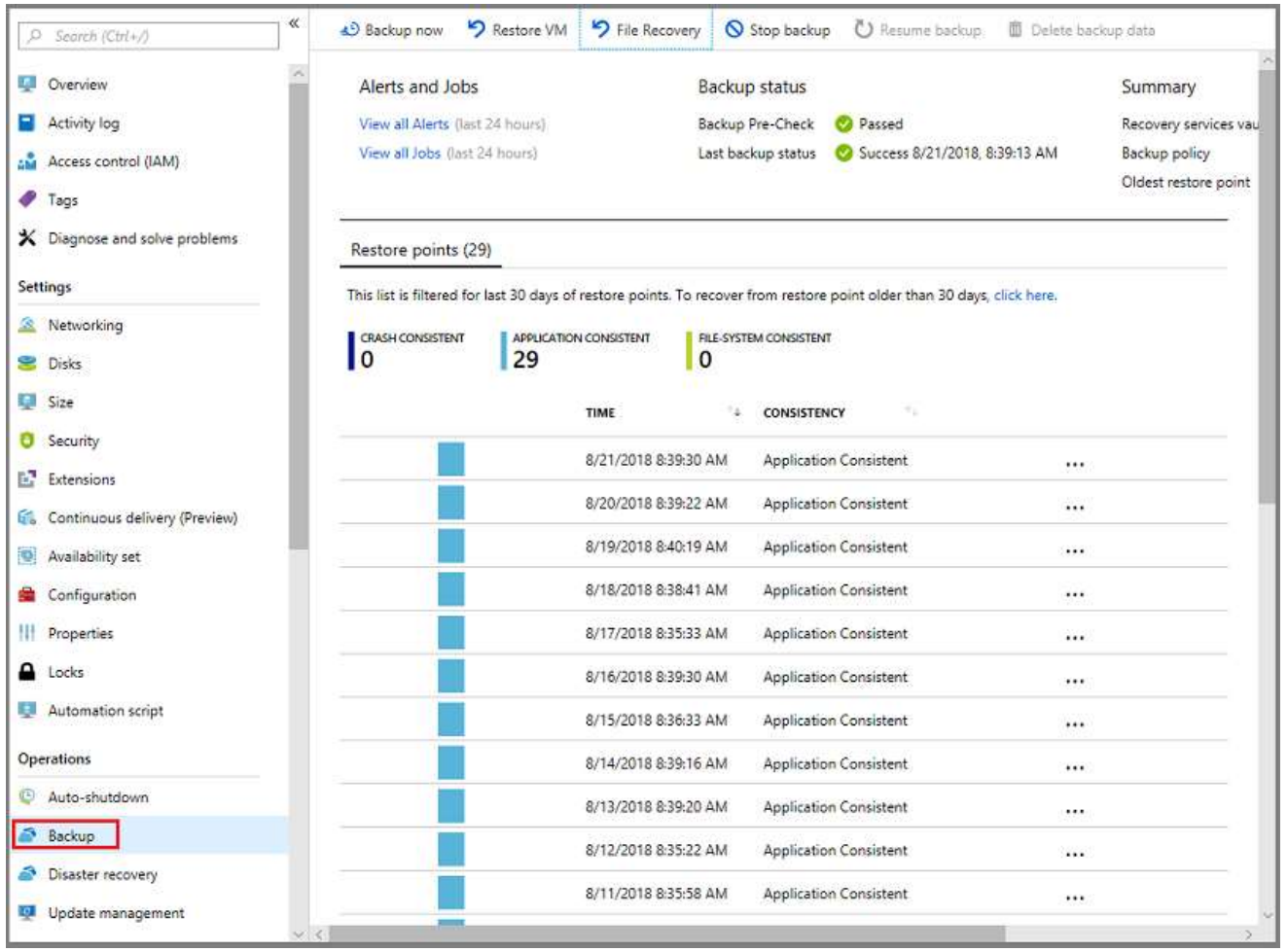
Copyright - Tout droit réservé - OFPPT

PARTIE 3

Étape 1 : Générer et télécharger un script pour parcourir et récupérer des fichiers

Pour restaurer des fichiers ou des dossiers à partir du point de récupération, accédez à la machine virtuelle et procédez comme suit :

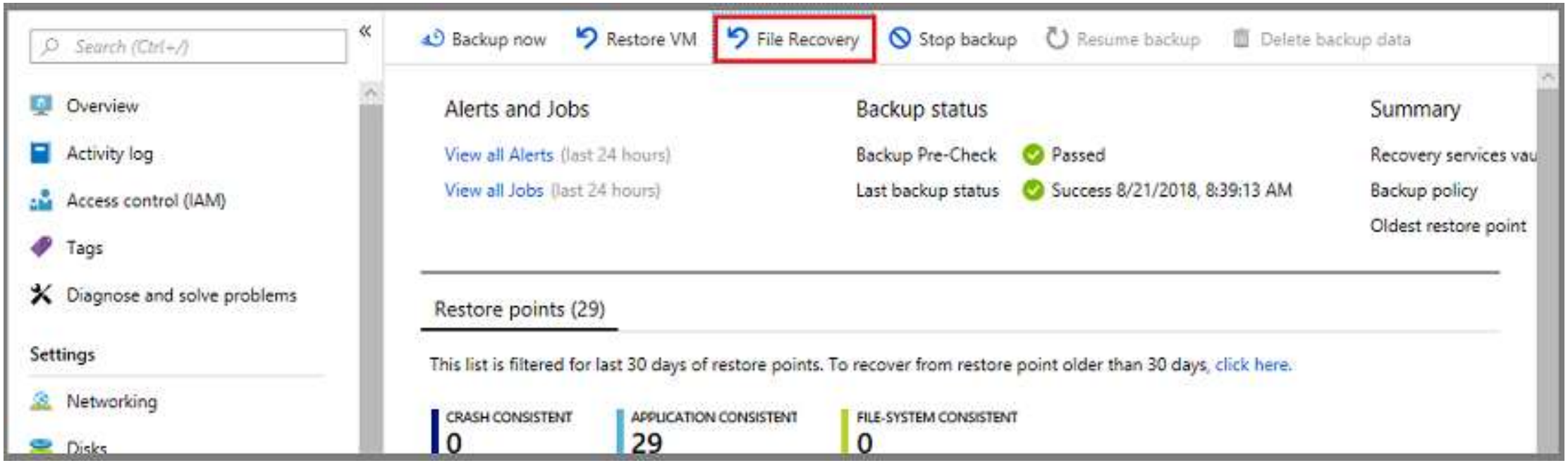
- Connectez-vous au Portail Azure, puis, dans le volet à gauche, sélectionnez **Machines virtuelles**. Dans la liste des machines virtuelles, sélectionnez la machine virtuelle pour ouvrir son tableau de bord.
- Dans le menu de la machine virtuelle, cliquez sur **Sauvegarde** pour ouvrir le tableau de bord Sauvegarde.



Copyright - Tout droit réservé - OFPPT

Étape 1 : Générer et télécharger un script pour parcourir et récupérer des fichiers

- Dans le menu du tableau de bord Sauvegarde, sélectionnez **Récupération de fichiers**.

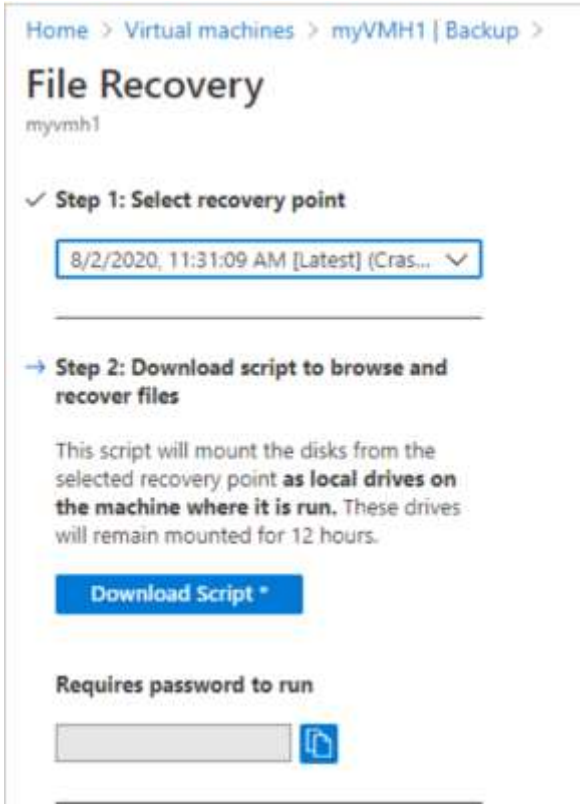


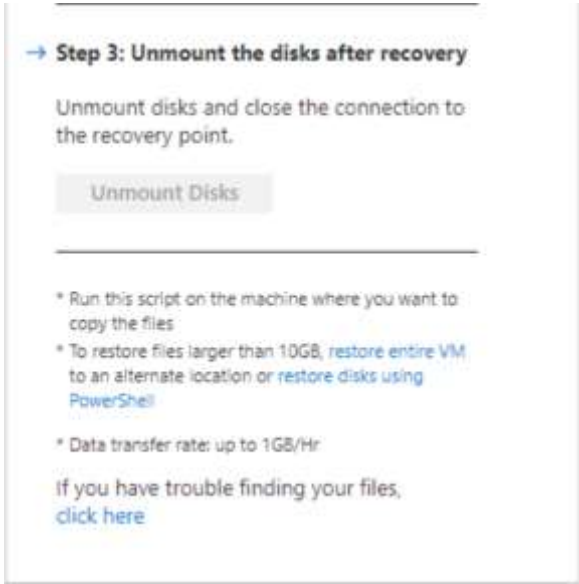
PARTIE 3

Copyright - Tout droit réservé - OFPPT

Étape 1 : Générer et télécharger un script pour parcourir et récupérer des fichiers

- Le menu **Récupération de fichiers** s'ouvre.
- Dans le menu déroulant **Sélectionner le point de récupération**, sélectionnez le point de récupération qui contient les fichiers dont vous avez besoin. Le dernier point de récupération est sélectionné par défaut.





PARTIE 3

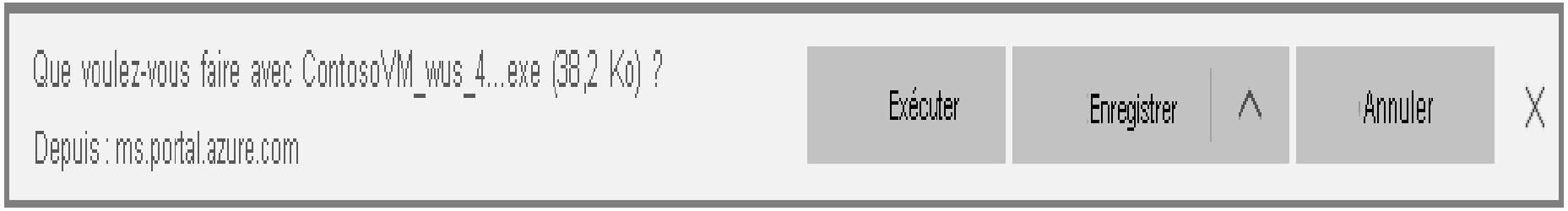
Copyright - Tout droit réservé - OFPPT

Étape 1 : Générer et télécharger un script pour parcourir et récupérer des fichiers

- Pour télécharger le logiciel utilisé pour copier des fichiers à partir du point de récupération, sélectionnez **Télécharger l'exécutable** (pour les machines virtuelles Windows Azure) ou **Télécharger le script** (pour les machines virtuelles Linux Azure, un script Python est généré).



- Azure télécharge le fichier exécutable ou le script sur l'ordinateur local.



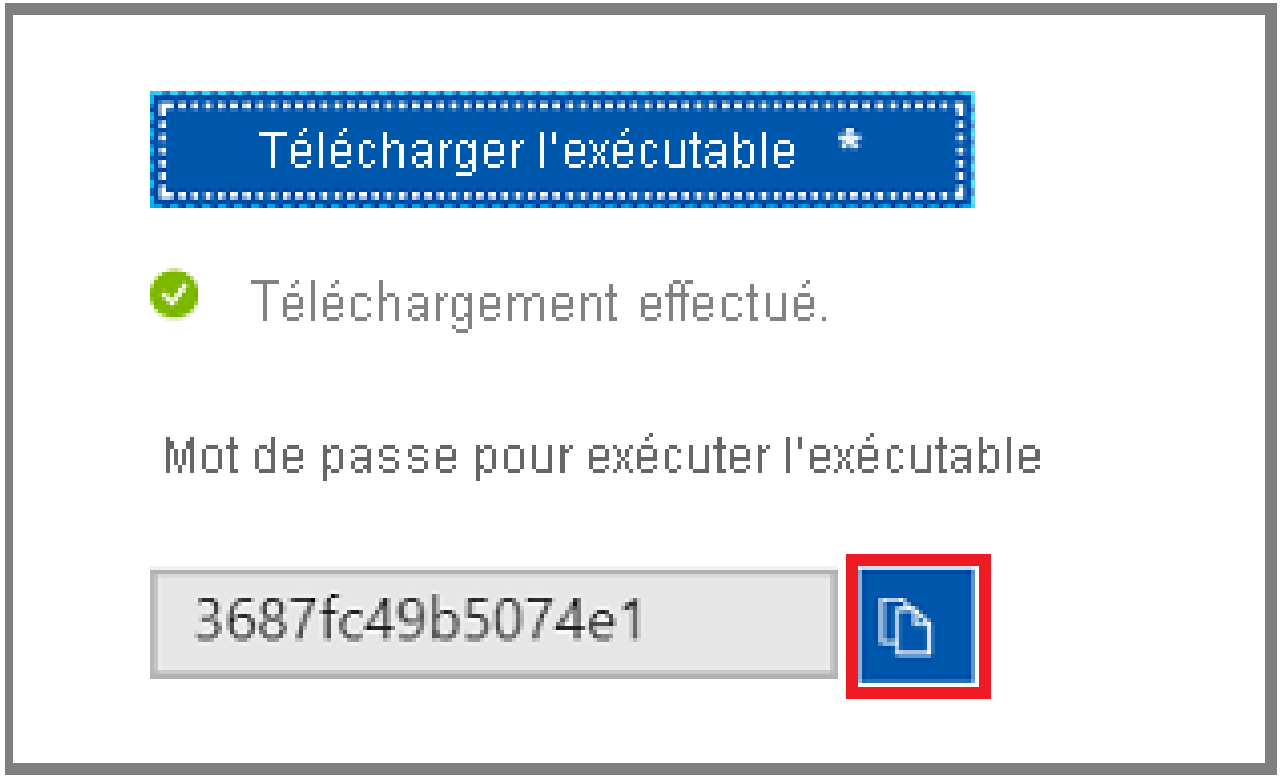
- Pour exécuter le fichier exécutable ou le script en tant qu'administrateur, il est recommandé d'enregistrer le fichier téléchargé sur votre ordinateur.

Copyright - Tout droit réservé - OFPPT

PARTIE 3

Étape 1 : Générer et télécharger un script pour parcourir et récupérer des fichiers

Le fichier exécutable ou le script est protégé par mot de passe et nécessite un mot de passe. Dans le menu **Récupération de fichiers**, sélectionnez le bouton Copier pour charger le mot de passe en mémoire



Copyright - Tout droit réservé - OFPPT

Étape 2 : Vérifier que la machine respecte la configuration requise avant d'exécuter le script

Une fois que le script a été téléchargé, vérifiez que vous disposez de la machine appropriée pour exécuter ce script. La machine virtuelle sur laquelle vous envisagez d'exécuter le script ne doit pas avoir l'une des configurations non prises en charge suivantes. **Si tel est le cas, choisissez un autre ordinateur qui répond aux exigences**.

Disques dynamiques

Vous ne pouvez pas exécuter le script exécutable sur la machine virtuelle avec l'une des caractéristiques suivantes : choisissez une autre machine.

- Volumes qui s'étendent sur plusieurs disques (volumes fractionnés et agrégés par bandes)
- Volumes à tolérance de pannes (volumes RAID-5 ou en miroir) sur des disques dynamiques.

Espaces de stockage Windows

Vous ne pouvez pas exécuter l'exécutable téléchargé sur la même machine virtuelle sauvegardée si la machine virtuelle sauvegardée contient des espaces de stockage Windows. Choisissez une autre machine.

Sauvegardes de machines virtuelles avec des disques de grande taille

Si la machine sauvegardée possède un grand nombre de disques (>16) ou des disques de grande taille (>4 To chacun), il n'est pas recommandé d'exécuter le script sur la même machine pour la restauration, car cela aura un impact significatif sur la machine virtuelle. Au lieu de cela, il est recommandé d'avoir une machine virtuelle distincte uniquement pour la récupération de fichiers (machines virtuelles Azure VM D2v3), puis de l'arrêter lorsqu'elle n'est pas nécessaire.

Copyright - Tout droit réservé - OFPPT

Étape 3 : Configuration requise du système d'exploitation pour exécuter correctement le script

La machine virtuelle sur laquelle vous souhaitez exécuter le script téléchargé doit remplir les conditions suivantes.

Pour système d'exploitation Windows

Le tableau suivant indique la compatibilité entre les systèmes d'exploitation des serveurs et des ordinateurs. Lors de la récupération de fichiers, vous ne pouvez pas restaurer des fichiers sur une version antérieure ou ultérieure du système d'exploitation. Par exemple, vous ne pouvez pas restaurer un fichier à partir d'une machine virtuelle sous Windows Server 2016 sur un ordinateur sous Windows Server 2012 ou Windows 8. Vous pouvez restaurer des fichiers à partir d'une machine virtuelle sur un système d'exploitation de serveur identique ou sur un système d'exploitation client compatible.

Système d'exploitation serveur	Système d'exploitation client compatible
Windows Server 2019	Windows 10
Windows Server 2016	Windows 10
Windows Server 2012 R2	Windows 8.1
Windows Server 2012	Windows 8
Windows Server 2008 R2	Windows 7

Copyright - Tout droit réservé - OFPPT

Étape 3 : Configuration requise du système d'exploitation pour exécuter correctement le script

Pour le système d'exploitation Linux

Sur Linux, le système d'exploitation de l'ordinateur utilisé pour restaurer des fichiers doit prendre en charge le système de fichiers de la machine virtuelle protégée. Lorsque vous sélectionnez un ordinateur pour exécuter le script, vérifiez que l'ordinateur possède un système d'exploitation compatible et utilise l'une des versions identifiées dans le tableau suivant :

Système d'exploitation Linux	Versions
Ubuntu	12.04 et versions ultérieures
CentOS	6.5 et versions ultérieures
RHEL	6.7 et versions ultérieures
Debian	7 et versions ultérieures
Oracle Linux	6.4 et versions ultérieures
SLES	12 et versions ultérieures
OpenSUSE	42.2 et versions ultérieures

Copyright - Tout droit réservé - OFPPT

Étape 3 : Configuration requise du système d'exploitation pour exécuter correctement le script

Le script requiert également les composants Python et bash pour exécuter et établir une connexion sécurisée avec le point de récupération.

Composant	Version
bash	4 et versions ultérieures
Python	2.6.6 et versions ultérieures
.NET	4.6.2 et versions ultérieures
TLS	La version 1.2 devrait être prise en charge

Assurez-vous aussi que vous disposez de la machine appropriée pour exécuter le script ILR et qu'elle est conforme aux conditions d'accès.

Copyright - Tout droit réservé - OFPPT

Étape 4 : Conditions d'accès pour exécuter correctement le script

Si vous exécutez le script sur un ordinateur disposant d'un accès restreint, assurez-vous qu'il a accès aux éléments suivants :

Étiquette de service download.microsoft.com ou AzureFrontDoor.FirstParty dans NSG sur le port 443 (sortant)

URL Recovery Services (GEO-NAME fait référence à la région où réside le coffre Recovery Services) sur le port 3260 (sortant)

https://pod01-rec2.GEO-NAME.backup.windowsazure.com (pour les régions publiques Azure) ou étiquette de service AzureBackup dans le groupe de sécurité réseau

https://pod01-rec2.GEO-NAME.backup.windowsazure.cn (pour Azure China 21Vianet) ou étiquette de service AzureBackup dans le groupe de sécurité réseau

https://pod01-rec2.GEO-NAME.backup.windowsazure.us (pour Azure US Government) ou étiquette de service AzureBackup dans le groupe de sécurité réseau

https://pod01-rec2.GEO-NAME.backup.windowsazure.de (pour Azure Allemagne) ou étiquette de service AzureBackup dans le groupe de sécurité réseau

Résolution de DNS public sur le port 53 (sortant)

Pour Linux, le script requiert les composants « open-iscsi » et « lshw » pour vous connecter au point de récupération. Si les composants n'existent pas sur l'ordinateur depuis lequel le script est exécuté, le script demande l'autorisation d'installer les composants. Autorisez l'installation des composants nécessaires.

L'accès à download.microsoft.com est requis pour télécharger les composants utilisés pour créer un canal sécurisé entre l'ordinateur sur lequel le script est exécuté et les données du point de récupération.

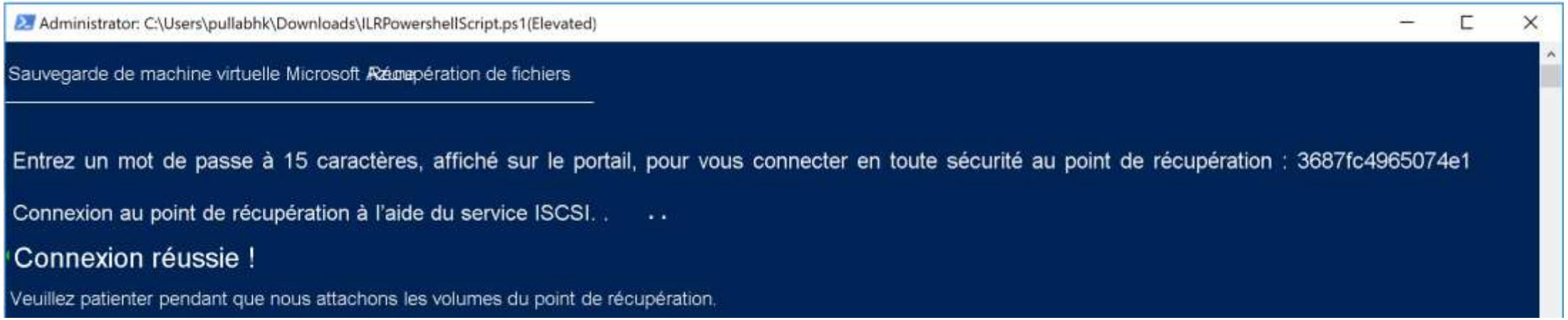
Assurez-vous aussi que vous disposez de la machine appropriée pour exécuter le script ILR et qu'elle est conforme à la configuration requise du système d'exploitation.

Copyright - Tout droit réservé - OFPPT

Étape 5 : Exécution du script et identification des volumes

Pour Windows

Une fois que vous avez rempli toutes les conditions énoncées à l'Étape 2, à l'Étape 3 et à l'Étape 4, copiez le script à partir de l'emplacement de téléchargement (généralement le dossier Téléchargements), consultez l'Étape 1 pour découvrir comment générer et télécharger le script. Cliquez avec le bouton droit sur le fichier exécutable, puis exécutez-le avec les informations d'identification d'administrateur. Lorsque vous y êtes invité, tapez le mot de passe ou collez le mot de passe en mémoire et appuyez sur Entrée. Une fois le mot de passe valide entré, le script se connecte au point de récupération.



Copyright - Tout droit réservé - OFPPT

Étape 5 : Exécution du script et identification des volumes

Lorsque vous exécutez l'exécutable, le système d'exploitation monte les nouveaux volumes et attribue des lettres de lecteur. Vous pouvez utiliser l'Explorateur Windows ou l'Explorateur de fichiers pour parcourir ces lecteurs. Les lettres de lecteur affectées aux volumes peuvent ne pas être les mêmes que celles de la machine virtuelle d'origine. Toutefois, le nom du volume est conservé. Par exemple, si le volume de la machine virtuelle d'origine était « Disque de données (E:\) », ce volume peut être connecté sur l'ordinateur local en tant que « Disque de données (n'importe quelle lettre:\) ». Parcourez tous les volumes mentionnés dans la sortie du script jusqu'à trouver vos fichiers ou votre dossier.

```
Connecting to recovery point using ISCSI service....

Connection succeeded!

Please wait while we attach volumes of the recovery point.

1 recovery volumes attached

D:\Local Disk

**********  Open Explorer to browse for files  **********

After recovery, to remove the disks and close the connection to the recovery point, please click 'Unmount Disks' in step
 3 of the portal.

Press 'Q/q' key to exit ...
```

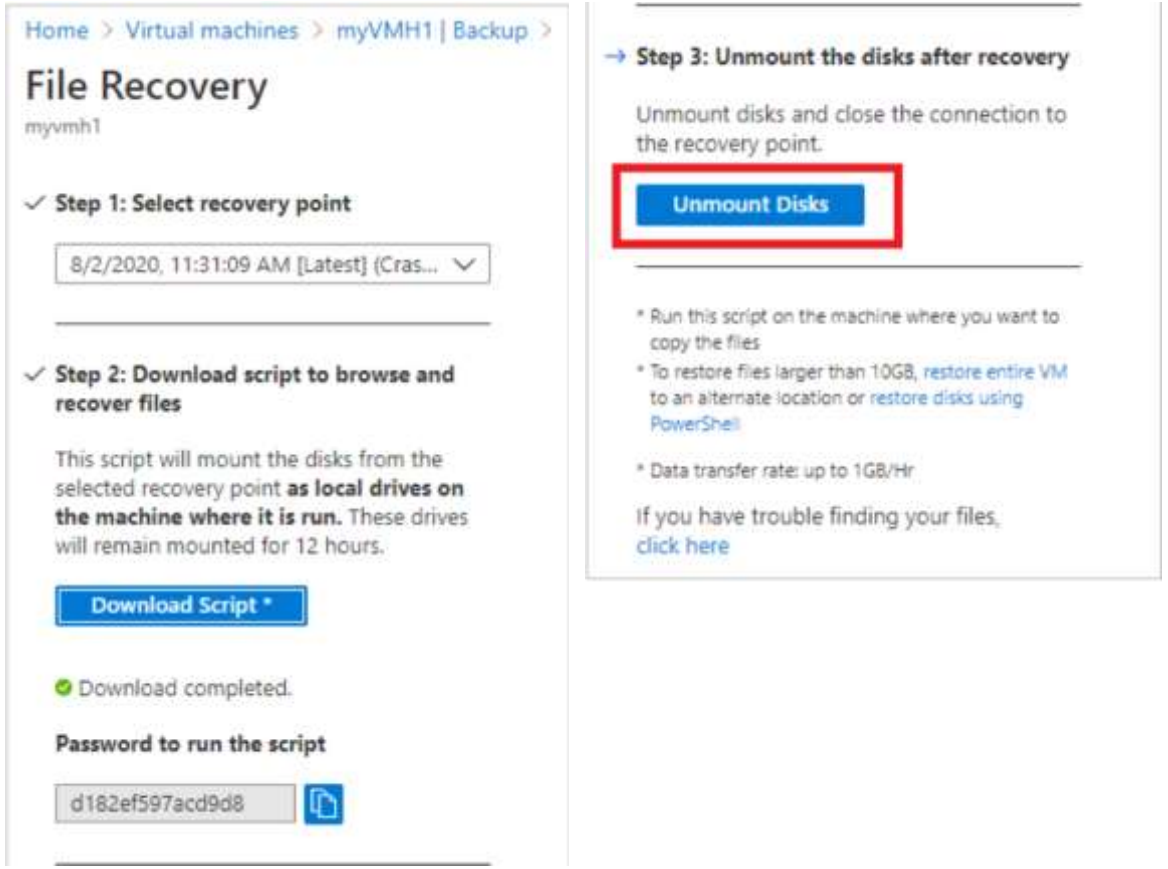

Copyright - Tout droit réservé - OFPPT

Étape 6 : Fermeture de la connexion

Après avoir identifié les fichiers et les avoir copiés dans un emplacement de stockage local, supprimez (ou démontez) les lecteurs supplémentaires. Pour démonter les lecteurs, dans le menu Récupération de fichier du portail Azure, cliquez sur Démonter les disques.

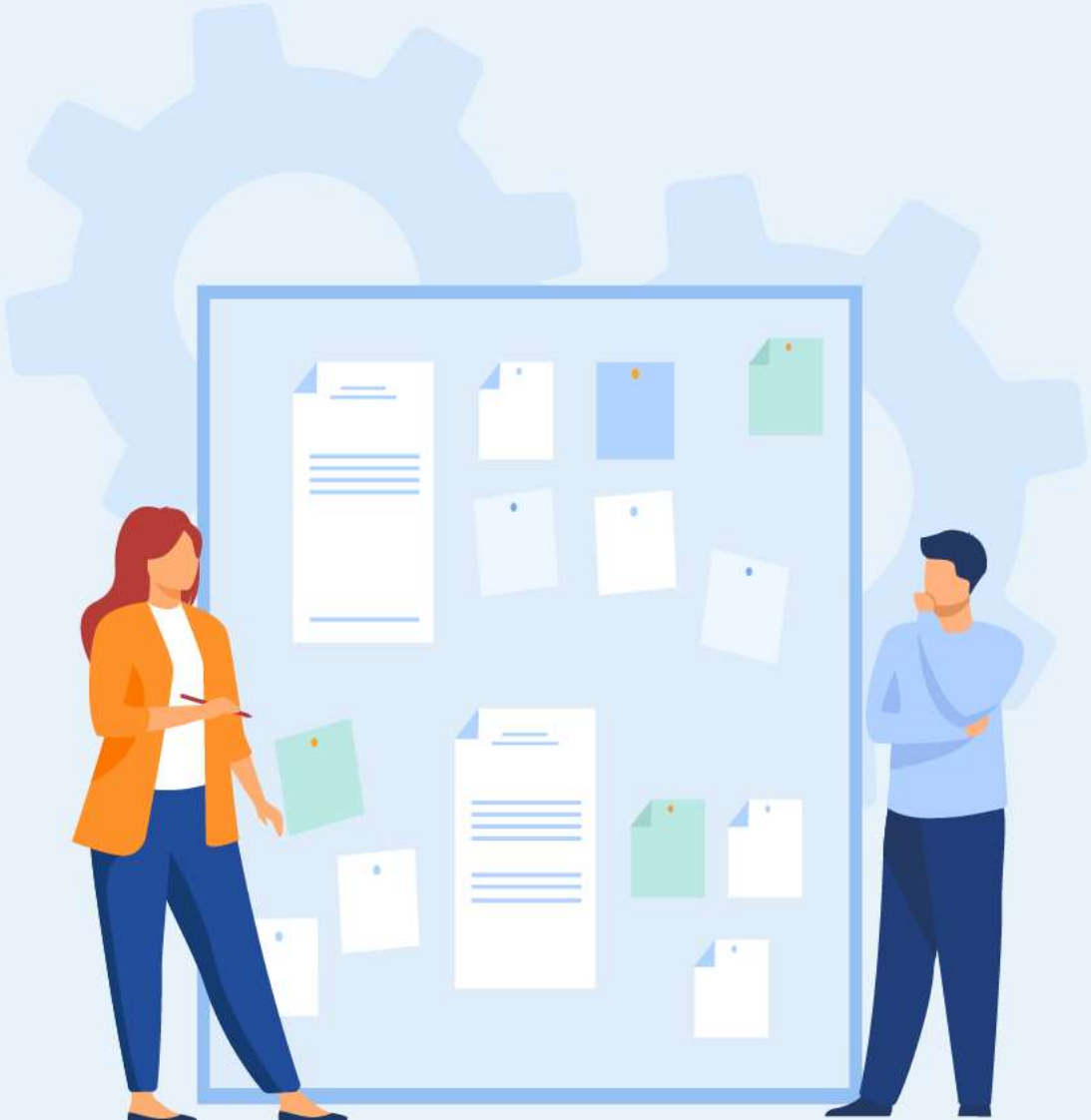
Une fois les disques démontés, vous recevez un message. L'actualisation de la connexion de sorte que vous pouvez supprimer les disques peut prendre quelques minutes.

Sous Linux, une fois la connexion au point de récupération interrompue, le système d'exploitation ne supprime pas les chemins d'accès de montage correspondants automatiquement. Les chemins d'accès de montage existent en tant que volumes « orphelins » et ils sont visibles, mais génèrent une erreur lorsque vous accédez aux fichiers ou écrivez dessus. Ils peuvent être supprimés manuellement. Le script, lorsqu'il est exécuté, identifie de tels volumes existants à partir des points de récupération précédents et les nettoie après accord.



PARTIE 3

Copyright - Tout droit réservé - OFPPT



CHAPITRE 1

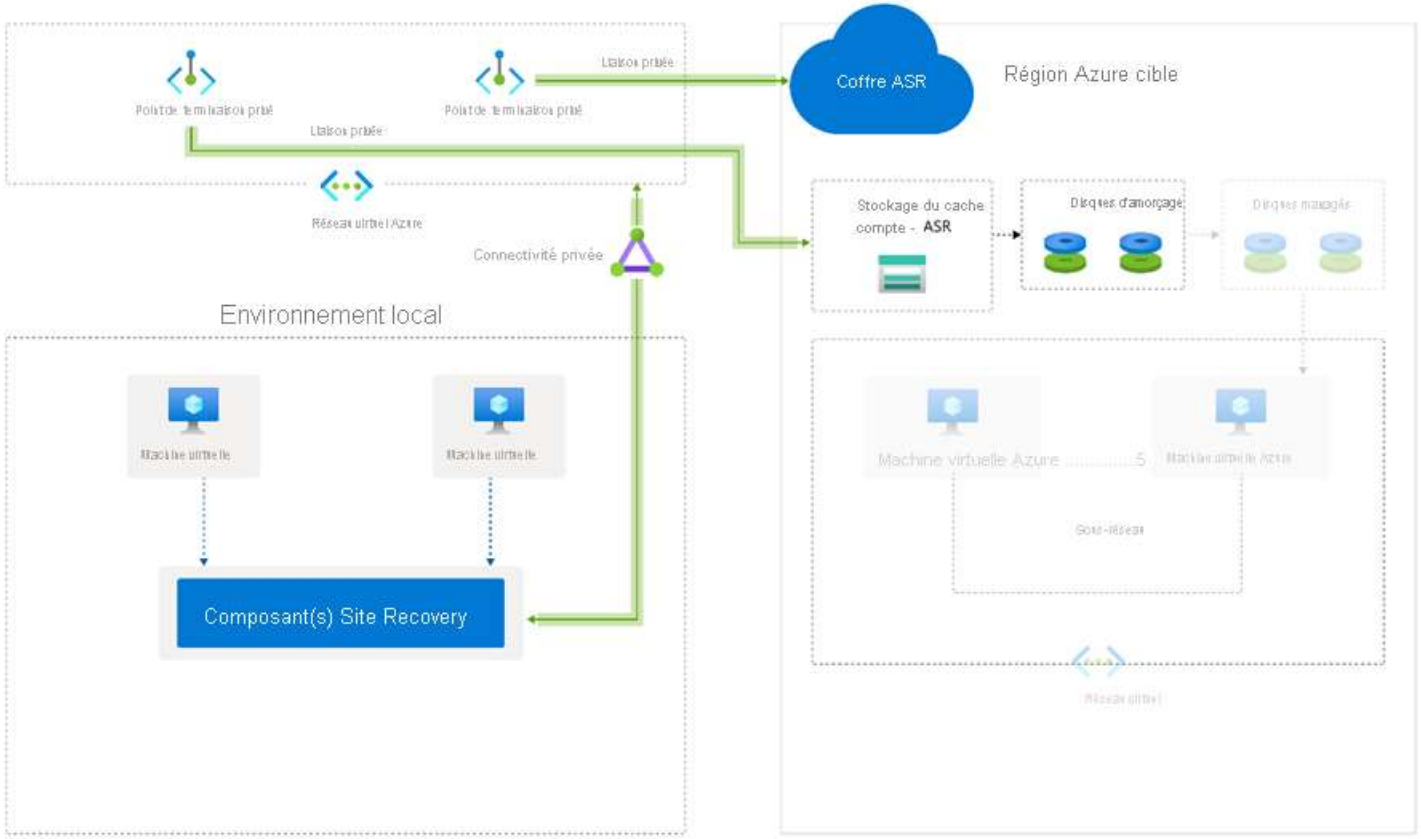
Etablir des stratégies d’entrée

1. Production d’une stratégie de restauration
2. **Production d’une stratégie de réplication**
3. Production d’une stratégie d’import
4. Production d’une stratégie de rétention

PARTIE 3

Répliquer des machines locales à l'aide de points de terminaison privés

Azure Site Recovery vous permet d'utiliser des points de terminaison privés Azure Private Link pour la réplication de vos machines locales vers un réseau virtuel dans Azure. Un accès de point de terminaison privé à un coffre de récupération est pris en charge dans toutes les régions Azure Commerce et Secteur public.



Copyright - Tout droit réservé - OFPPT

PARTIE 3

Créer et utiliser des points de terminaison privés pour Site Recovery

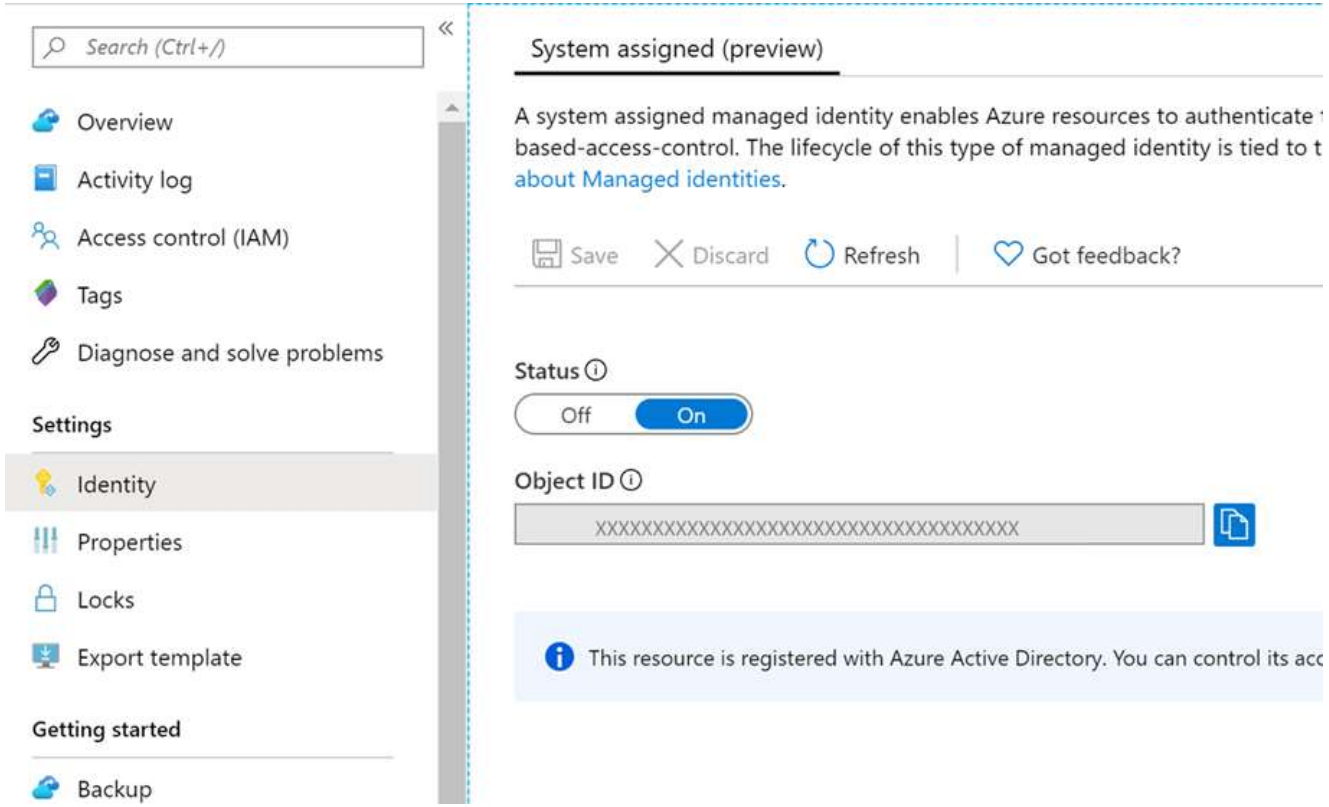
Créer un coffre Recovery Services

Un coffre Recovery Services contient les informations de réplication des machines. Il permet de déclencher des opérations Site Recovery. Pour savoir comment créer un coffre-fort Recovery Services dans la région Azure où vous souhaitez effectuer un basculement en cas de sinistre.

Activer l'identité managée pour le coffre

Une identité managée permet au coffre d'accéder à vos comptes de stockage. Site Recovery peut avoir à accéder au stockage cible et aux comptes de stockage de cache/journal en fonction de vos exigences. L'accès de l'identité managée est requis quand vous utilisez le service Azure Private Link pour le coffre.

- Accédez à votre coffre Recovery Services.
  Sélectionnez **Identité** sous **Paramètres** :



Copyright - Tout droit réservé - OFPPT

PARTIE 3

Créer et utiliser des points de terminaison privés pour Site Recovery

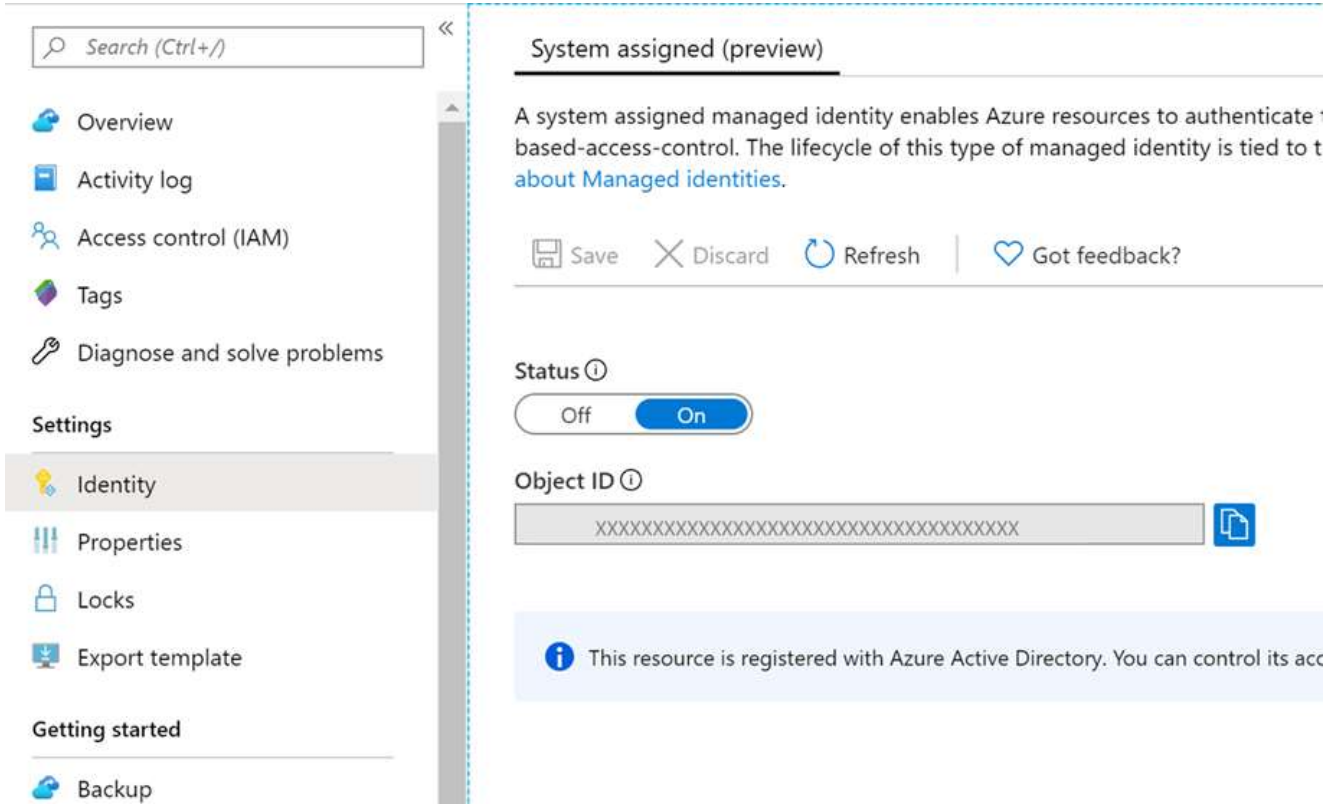
Créer un coffre Recovery Services

Un coffre Recovery Services contient les informations de réplication des machines. Il permet de déclencher des opérations Site Recovery. Pour savoir comment créer un coffre-fort Recovery Services dans la région Azure où vous souhaitez effectuer un basculement en cas de sinistre.

Activer l'identité managée pour le coffre

Une identité managée permet au coffre d'accéder à vos comptes de stockage. Site Recovery peut avoir à accéder au stockage cible et aux comptes de stockage de cache/journal en fonction de vos exigences. L'accès de l'identité managée est requis quand vous utilisez le service Azure Private Link pour le coffre.

- Accédez à votre coffre Recovery Services.
  Sélectionnez **Identité** sous **Paramètres** :



- Cliquez sur le bouton bascule sous **État** pour le définir sur la valeur **Activé**, puis sélectionnez **Enregistrer**.

Un ID d'objet est généré. Le coffre est à présent inscrit auprès d'Azure Active Directory

Copyright - Tout droit réservé - OFPPT

Créer et utiliser des points de terminaison privés pour Site Recovery

Créer des points de terminaison privés pour le coffre Recovery Services

Pour protéger les machines du réseau source local, vous aurez besoin d'un point de terminaison privé pour le coffre du réseau de contournement. Créez le point de terminaison privé à l'aide du centre Azure Private Link dans le Portail Azure ou par le biais d'Azure PowerShell.

Depuis la barre de recherche du Portail Microsoft Azure, recherchez «liaison privée». Sélectionnez Liaison privée pour accéder au Centre de liaisons privées :



Dans le volet gauche, sélectionnez **Points de terminaison privés**. Une fois dans le volet **Points de terminaison privés**, sélectionnez **Ajouter** pour démarrer le processus de création d'un point de terminaison privé pour votre coffre



PARTIE 3

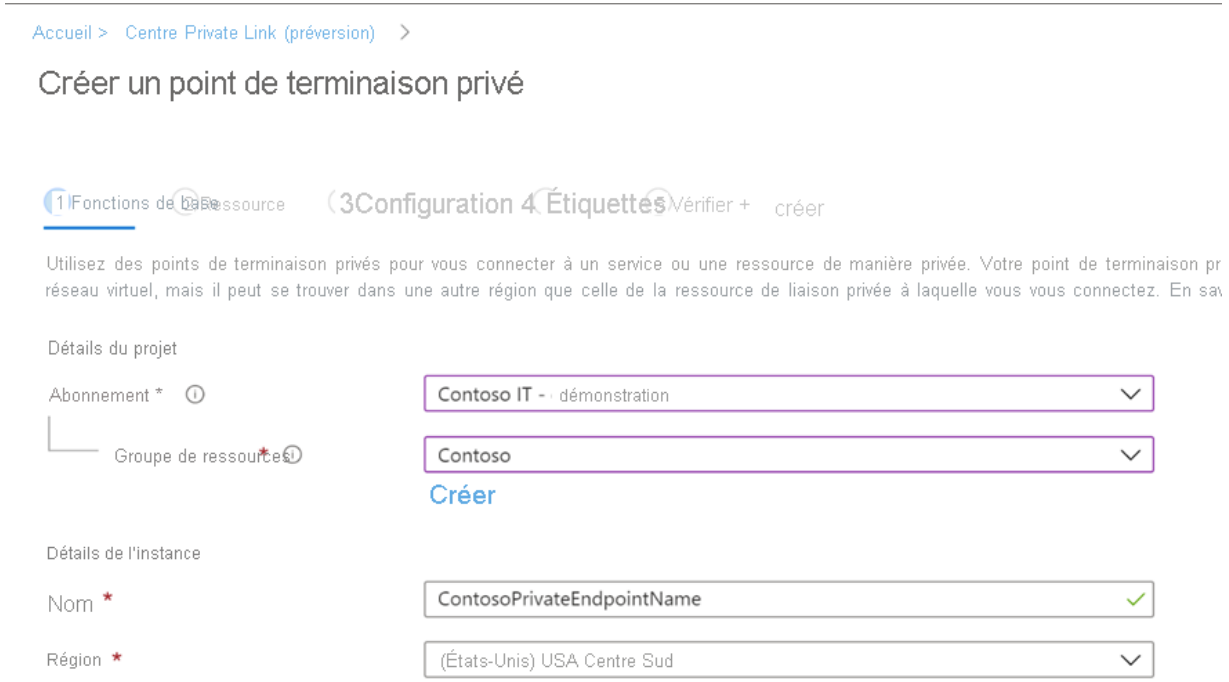
Copyright - Tout droit réservé - OFPPT

PARTIE 3

Créer et utiliser des points de terminaison privés pour Site Recovery

Dans la page **Créer un point de terminaison privé**, indiquez les détails pour créer votre connexion de point de terminaison privé.

- **Concepts de base**. Fournissez les informations de base de vos points de terminaison privés. Utilisez la région que vous avez utilisée pour le réseau de contournement :



Copyright - Tout droit réservé - OFPPT

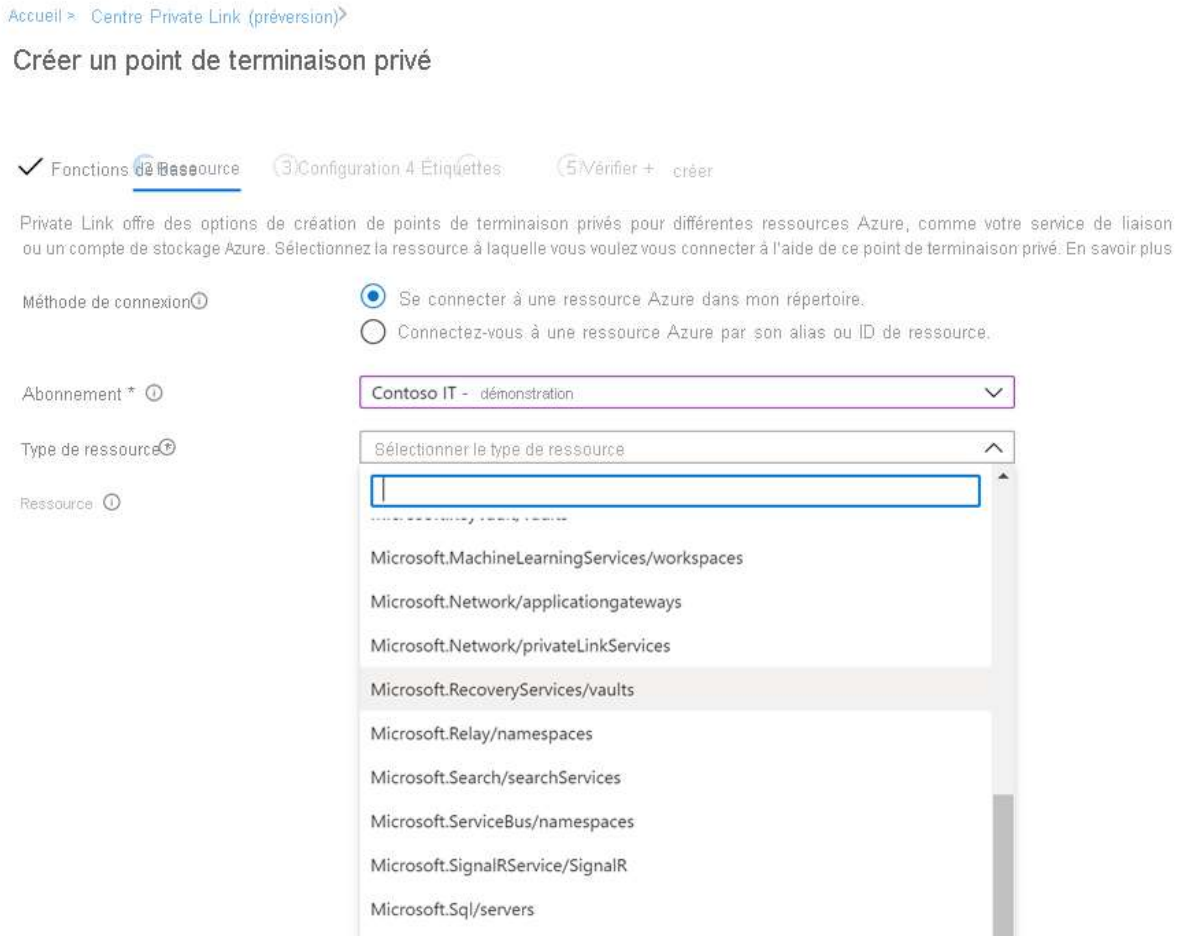
Créer et utiliser des points de terminaison privés pour Site Recovery

Ressource. Dans cet onglet, vous devez indiquer la ressource PaaS (plateforme en tant que service) pour laquelle vous souhaitez créer votre connexion.

Sous **Type de ressource** pour l'abonnement sélectionné, sélectionnez **Microsoft.RecoveryServices/vaults**.

Choisissez le nom de votre coffre Recovery Services sous **Ressource**.

Sélectionnez **Azure Site Recovery** en tant que **Sous-ressource cible**.



PARTIE 3

Copyright - Tout droit réservé - OFPPT

Créer et utiliser des points de terminaison privés pour Site Recovery

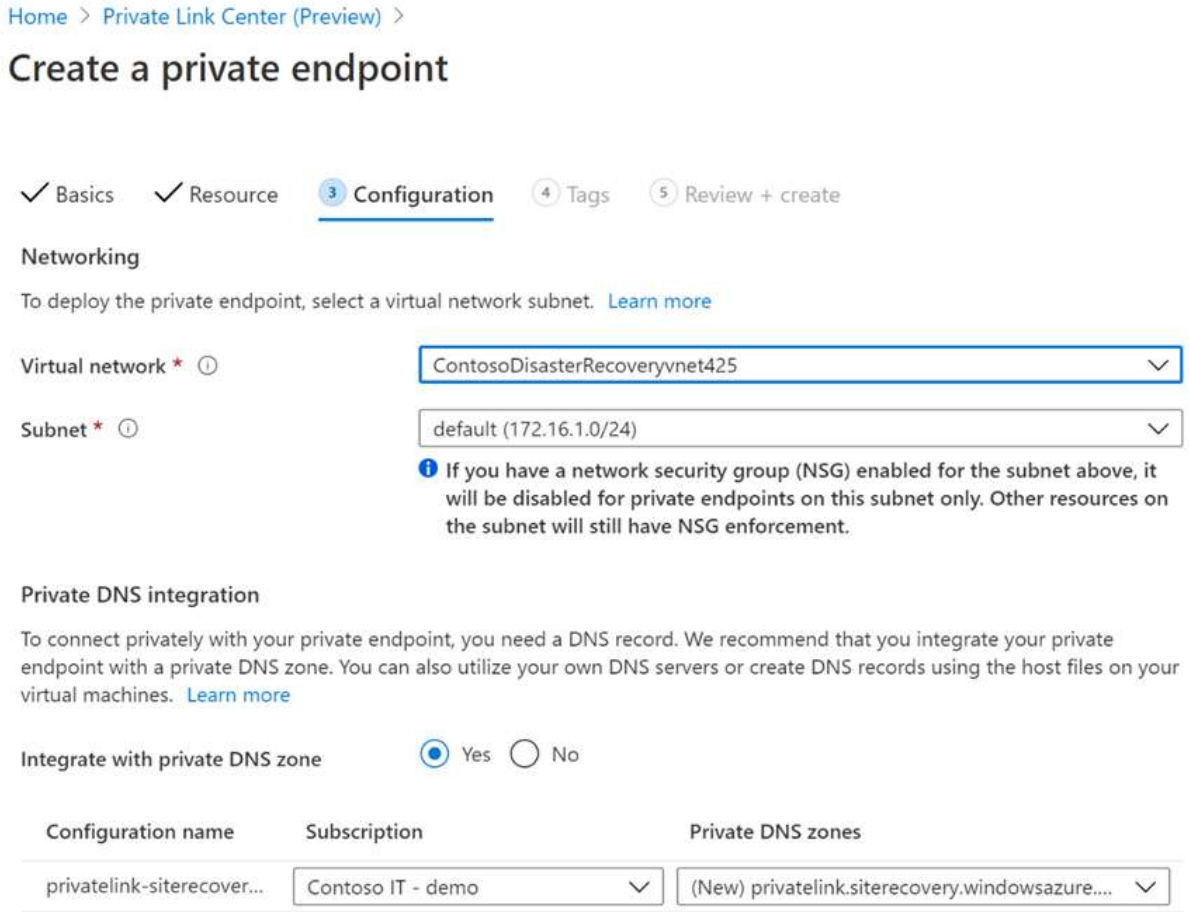
Configuration. Dans cet onglet, indiquez le réseau de contournement et le sous-réseau où vous souhaitez que le point de terminaison privé soit créé.

Activez l'intégration à la zone DNS privée en sélectionnant **Oui**. Choisissez une zone DNS existante ou en créez en une.

La sélection de l'option **Oui** associe automatiquement la zone au réseau de contournement. Cette action ajoute également les enregistrements DNS nécessaires à la résolution DNS des adresses IP et des noms de domaine complets créés pour le point de terminaison privé.

Veillez à créer une zone DNS pour chaque nouveau point de terminaison privé qui se connecte au même coffre. Si vous choisissez une zone DNS privée existante, les enregistrements CNAME précédents sont remplacés.

Si votre environnement a un modèle hub-and-spoke, vous n'avez besoin que d'un seul point de terminaison privé et d'une seule zone DNS privée pour l'ensemble de l'installation.



PARTIE 3

Copyright - Tout droit réservé - OFPPT

Créer et utiliser des points de terminaison privés pour Site Recovery

- **Tags** (balises). Si vous le souhaitez, vous pouvez ajouter des étiquettes à votre point de terminaison privé.
- **Vérifier + créer**. Une fois la validation terminée, sélectionnez **Créer** pour créer le point de terminaison privé.

Une fois le point de terminaison privé créé, cinq noms de domaine complets (FQDN) sont ajoutés à celui-ci. Ces liaisons permettent aux machines du réseau local d'accéder, via le réseau de contournement, à tous les microservices Site Recovery requis dans le contexte du coffre. Vous pouvez utiliser le même point de terminaison privé pour la protection de n'importe quelle machine Azure dans le réseau de contournement et tous les réseaux appairés.

Les cinq noms de domaine sont mis en forme dans ce modèle :

```
{Vault-ID}-asr-pod01-{type}-.{target-geo-code}.siterecovery.windowsazure.com
```

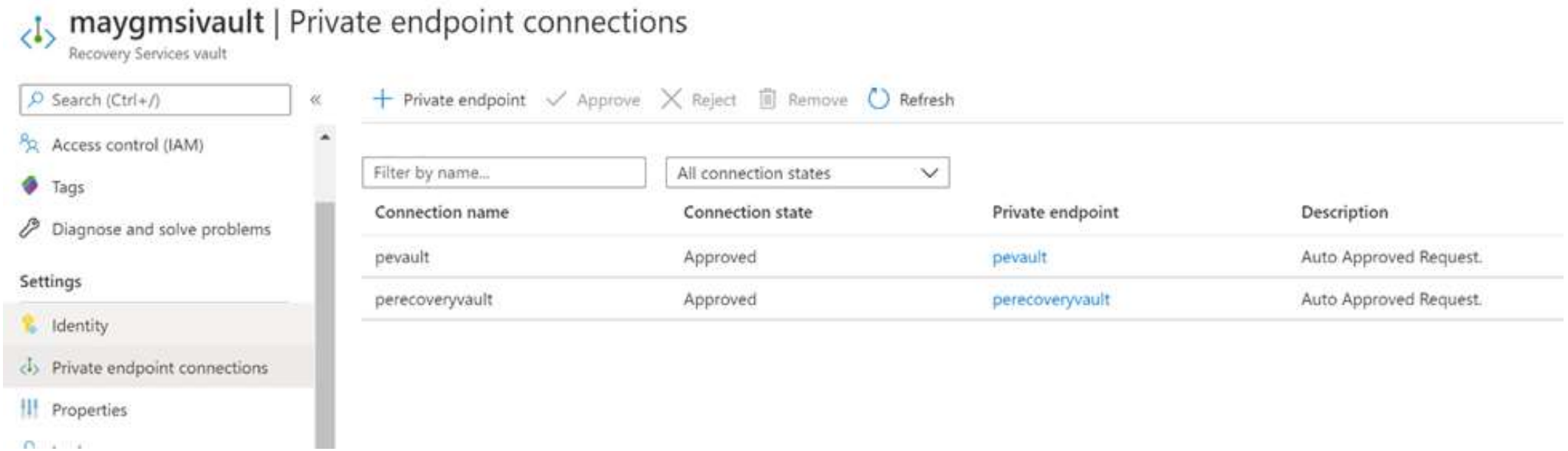

Copyright - Tout droit réservé - OFPPT

PARTIE 3

Approuver des points de terminaison privés pour Site Recovery

Si vous créez le point de terminaison privé et que vous êtes également le propriétaire du coffre-fort Recovery Services, le point de terminaison privé que vous avez créé précédemment est approuvé automatiquement en quelques minutes. Dans le cas contraire, le propriétaire du coffre doit approuver le point de terminaison privé avant que vous ne puissiez l'utiliser. Pour approuver ou rejeter une connexion de point de terminaison privée demandée, accédez à **Connexions des points de terminaison privés** sous **Paramètres** dans la page du coffre de récupération.

Vous pouvez accéder à la ressource de point de terminaison privé pour passer en revue l'état de la connexion avant de continuer :



Copyright - Tout droit réservé - OFPPT

Accorder les autorisations nécessaires au coffre

Selon votre configuration, vous pouvez avoir besoin d'un ou de plusieurs comptes de stockage dans la région Azure cible. Ensuite, accordez les autorisations d'identité managée pour tous les comptes de stockage de cache/journal requis par Site Recovery. Dans ce cas, vous devez créer les comptes de stockage requis à l'avance.

Avant d'activer la réplication des machines virtuelles, vous devez accorder à l'identité managée du coffre les autorisations de rôle suivantes en fonction du type de compte de stockage.

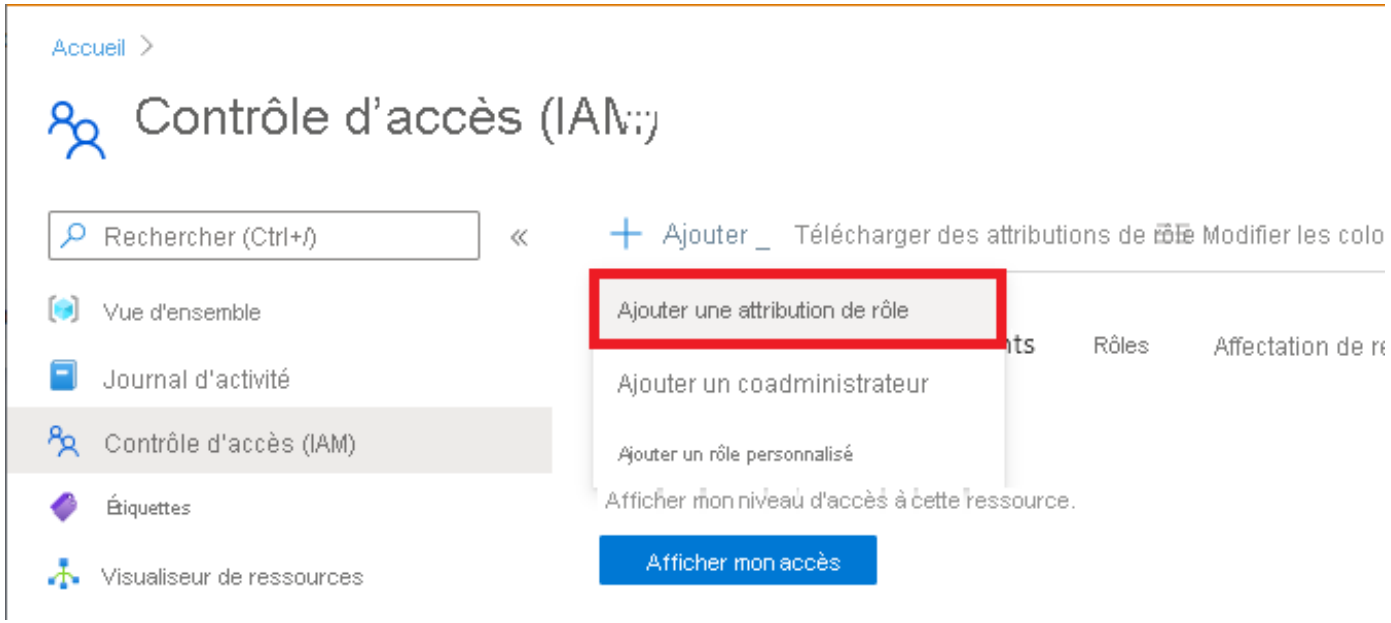
- Comptes de stockage basés sur Resource Manager (type Standard) :
  - Contributeur
  - Contributeur aux données Blob du stockage
- Comptes de stockage basés sur Resource Manager (type Premium) :
  - Contributeur
  - Propriétaire des données Blob du stockage
- Comptes de stockage Classic :
  - Contributeur de compte de stockage classique
  - Rôle de service d'opérateur de clé de compte de stockage classique

Les étapes suivantes expliquent comment ajouter une attribution de rôle à vos comptes de stockage.

Copyright - Tout droit réservé - OFPPT

Accorder les autorisations nécessaires au coffre

- Accédez au compte de stockage
- Sélectionnez **Contrôle d'accès (IAM)**
- Sélectionner **Ajouter> Ajouter une attribution de rôle**.



Copyright - Tout droit réservé - OFPPT

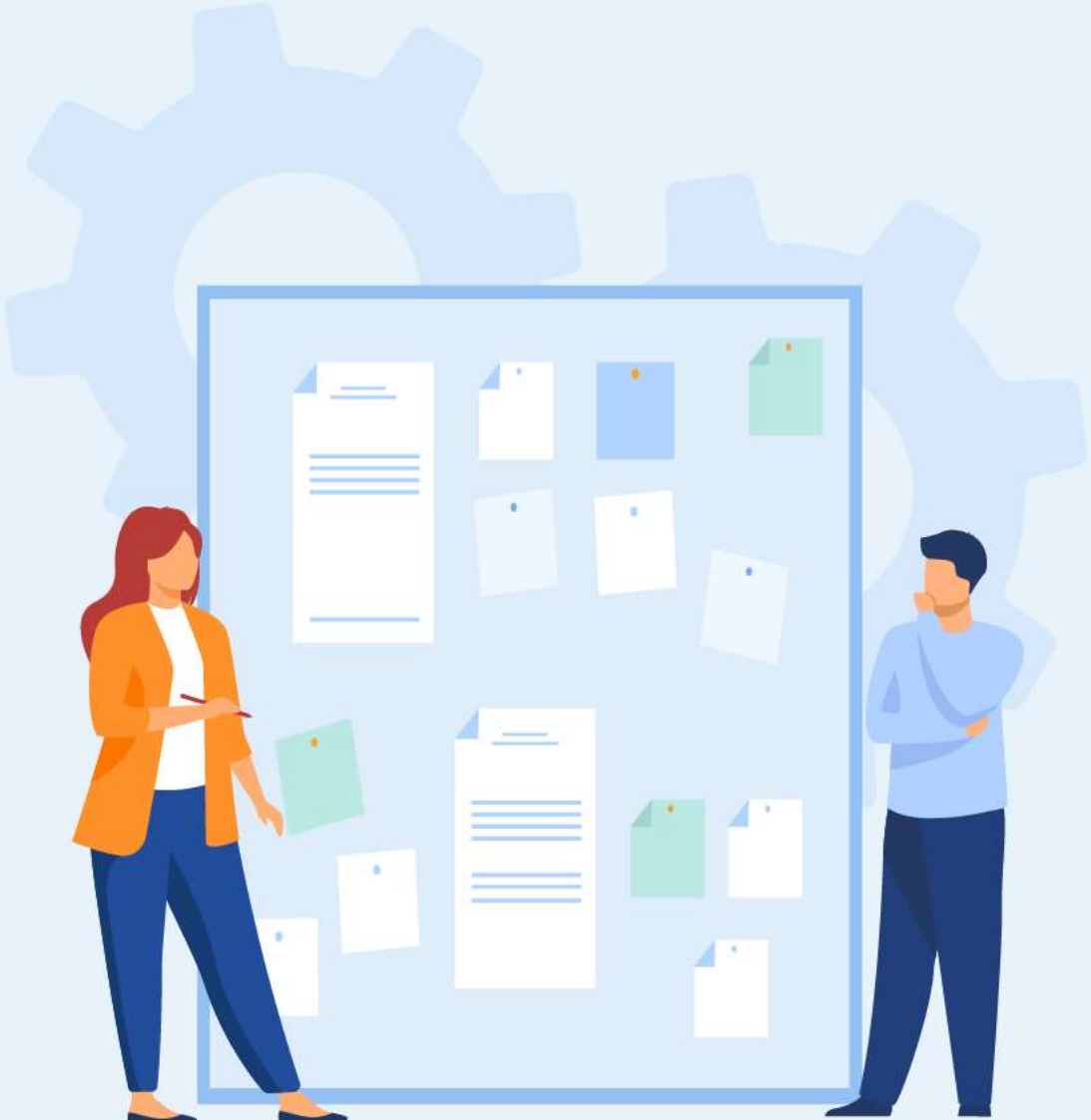
Accorder les autorisations nécessaires au coffre

- Sous l'onglet **Rôle**, sélectionnez l'un des rôles répertoriés au début de cette section
- Sous l'onglet **Membres**, sélectionnez **Identité managée**, puis **Sélectionner des membres**
- Sélectionnez votre abonnement Azure
- Sélectionnez **Identité managée affectée par le système**, recherchez un coffre, puis sélectionnez-le
- Dans l'onglet **Passer en revue + affecter**, sélectionnez **Passer en revue + affecter** pour affecter le rôle.

En plus de ces autorisations, vous devez autoriser l'accès aux services approuvés Microsoft. Pour ce faire, procédez comme suit :

- Accédez à **Pare-feu et réseaux virtuels**
- Dans **Exception**, sélectionnez **Autoriser les services Microsoft approuvés à accéder à ce compte de stockage**.

Copyright - Tout droit réservé - OFPPT



CHAPITRE 1

Etablir des stratégies d’entrée

1. Production d’une stratégie de restauration
2. Production d’une stratégie de réplication
3. **Production d’une stratégie d’import**
4. Production d’une stratégie de rétention

Qu'est-ce que le service Azure Import/Export ?

Le service Azure Import/Export est utilisé pour importer en toute sécurité des volumes importants de données dans Stockage Blob Azure et Azure Files en expédiant des lecteurs de disque vers un centre de données Azure. Vous pouvez également utiliser ce service pour transférer des données de Stockage Blob Azure vers des lecteurs de disque et les expédier vers vos sites locaux. Les données d'un ou plusieurs lecteurs de disque peuvent être importées dans le Stockage Blob Azure ou Azure Files.

Utilisez vos propres lecteurs de disque et transférez des données avec le service Azure Import/Export. Vous pouvez également utiliser les lecteurs de disque fournis par Microsoft.

Si vous souhaitez transférer des données à l'aide des lecteurs de disque fournis par Microsoft, vous pouvez utiliser un disque Azure Data Box pour importer des données dans Azure. Microsoft envoie jusqu'à 5 lecteurs de disque SSD chiffrés dotés d'une capacité totale de 40 To par commande à votre centre de données via un transporteur régional. Vous pouvez rapidement configurer les lecteurs de disque, y copiez des données via une connexion USB 3.0, puis les réexpédier à Azure. Pour plus d'informations, accédez à la vue d'ensemble d'Azure Data Box Disk.

Cas d'utilisation du service Azure Import/Export

Envisagez d'utiliser le service Azure Import/Export lorsque le chargement ou le téléchargement de données sur le réseau est trop lent ou lorsque l'obtention d'une bande passante réseau supplémentaire est coûteuse. Utilisez ce service dans les situations suivantes :

- **Migration des données vers le Cloud** : déplacez rapidement de grandes quantités de données vers Azure et à moindre coût
- **Distribution de contenu** : envoyez rapidement des données aux sites de vos clients
- **Sauvegarder** : sauvegardez vos données locales dans Stockage Azure
- **Récupération de données** : récupérez de grandes quantités de données stockées pour les transférer vers votre site local.

Copyright - Tout droit réservé - OFPPT

Composants du service Azure Import/Export

Le service Azure Import/Export utilise les composants suivants :

- **Service d'importation/exportation** : ce service disponible dans le portail Azure permet à l'utilisateur de créer des travaux d'importation (chargement) et d'exportation (téléchargement) de données et d'en effectuer le suivi.
- **Outil WAImportExport** : outil en ligne de commande qui effectue les opérations suivantes :
  - prépare vos lecteurs de disque expédiés à l'importation ;
  - facilite la copie de vos données sur le lecteur ;
  - Chiffre les données sur le lecteur avec BitLocker AES 256 bits. Vous pouvez utiliser un protecteur de clé externe pour protéger votre clé BitLocker.
  - génère les fichiers journaux de lecteur utilisés lors de la création de l'importation ;
  - permet d'identifier le nombre de disques requis pour les travaux d'exportation.

Lecteurs de disque : vous pouvez expédier des disques SSD (Solid-state drive) ou des disques HDD (Hard disk drive) au centre de données Azure. Lorsque vous créez un travail d'importation, vous expédiez les lecteurs de disque contenant vos données. Lorsque vous créez un travail d'exportation, vous expédiez des lecteurs vides au centre de données Azure.

Copyright - Tout droit réservé - OFPPT

Comment fonctionne le service Import/Export ?

Le service Azure Import/Export permet le transfert de données dans des objets blob Azure ou des fichiers Azure Files en créant des travaux. Utilisez le Portail Azure ou l'API REST Azure Resource Manager pour créer des travaux. Chaque travail est associé à un seul compte de stockage.

Il peut s'agir d'un travail d'importation ou d'exportation. Un travail d'importation vous permet d'importer des données dans des objets blob Azure ou des fichiers Azure Files, tandis que le travail d'exportation permet d'exporter des données à partir d'objets blob Azure. Dans le cas d'un travail d'importation, vous expédiez des disques contenant vos données. Lorsque vous créez un travail d'exportation, vous expédiez des lecteurs vides à un centre de données Azure. Dans les deux cas, vous pouvez expédier jusqu'à 10 lecteurs de disque par travail.

Dans un travail d'importation

Globalement, un travail d'importation comprend les opérations suivantes :

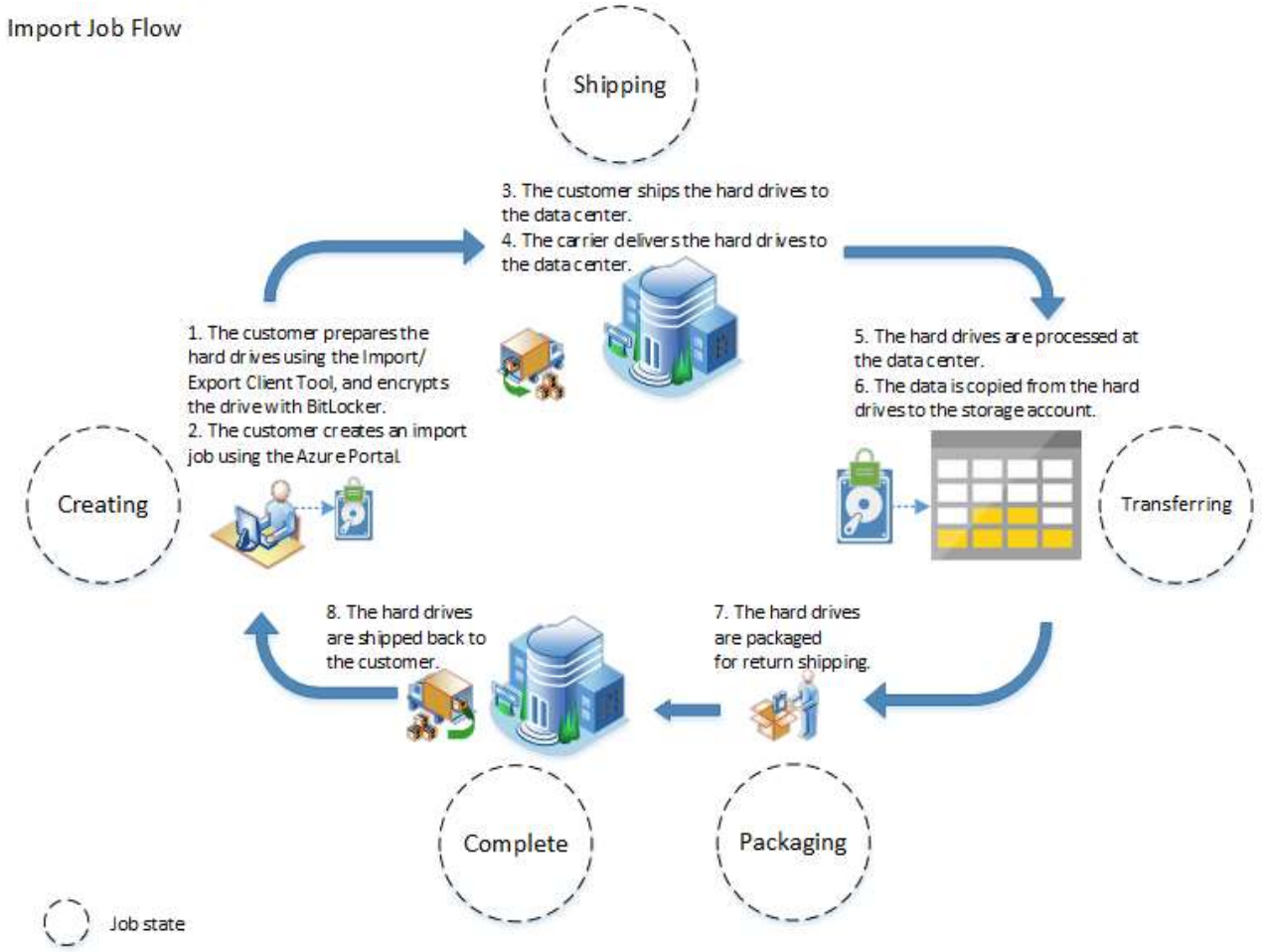
- Déterminer les données à importer, le nombre de disques dont vous avez besoin, l'emplacement de l'objet blob de destination de vos données dans Stockage Azure
- Utiliser l'outil WAImportExport pour copier les données sur les lecteurs de disque. Chiffrer les lecteurs de disque avec BitLocker
- Créer un travail d'importation dans votre compte de stockage cible dans le Portail Azure. Charger les fichiers journaux du lecteur
- Indiquer l'adresse de retour et le numéro de compte transporteur à utiliser pour le retour des disques
- Expédier les lecteurs de disque à l'adresse d'expédition indiquée lors de la création du travail
- Mettre à jour le numéro de suivi et envoyez le travail d'importation
- Les disques sont réceptionnés et traités dans le centre de données Azure
- Les disques sont expédiés à l'aide de votre compte de transporteur à l'adresse de retour indiquée dans le travail d'importation.

Copyright - Tout droit réservé - OFPPT

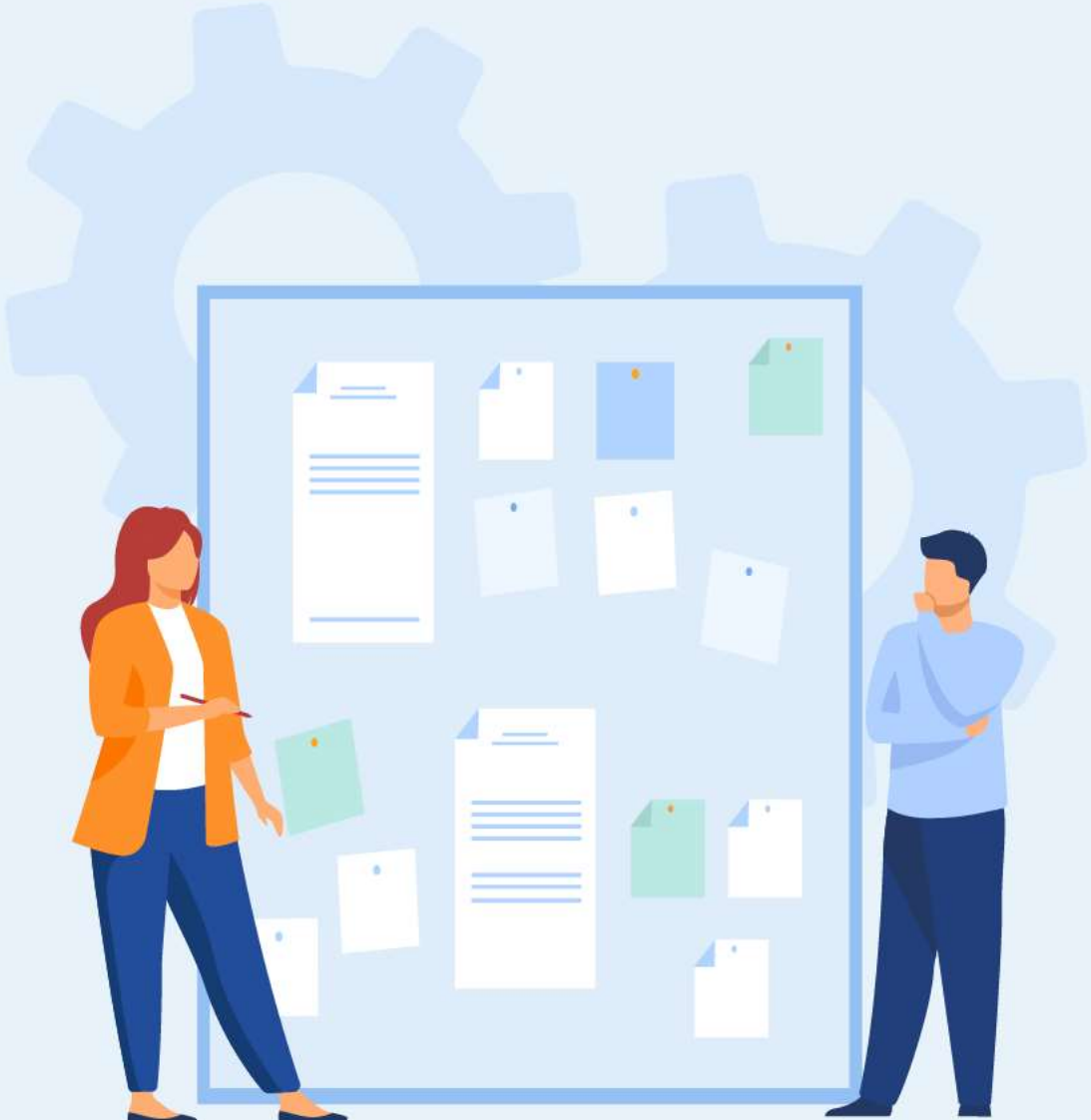
Comment fonctionne le service Import/Export ?

Pour les expéditions à l'échelle nationale (dans le pays / la région du centre de données), veuillez partager un compte de transporteur domestique.

Pour les expéditions à l'étranger (en dehors du pays /de la région du centre de données), veuillez partager un compte de transporteur international.



Copyright - Tout droit réservé - OFPPT



CHAPITRE 1

Etablir des stratégies d’entrée

1. Production d’une stratégie de restauration
2. Production d’une stratégie de réplication
3. Production d’une stratégie d’import
4. **Production d’une stratégie de rétention**

Définition d'une stratégie de conservation des données Storage Analytics

Par défaut, Storage Analytics ne supprimera aucun enregistrement ou données de métriques. Il existe deux manières de supprimer des données Storage Analytics : en effectuant manuellement des demandes de suppression ou en définissant une stratégie de rétention des données.

Important

Pour éviter les coûts inutiles, définissez une stratégie de rétention pour l'enregistrement et les métriques.

Définition d'une stratégie de rétention des données

Vous pouvez configurer deux stratégies de rétention des données : une pour l'enregistrement et une pour les métriques. Lorsqu'il est activé pour les deux, Storage Analytics supprimera les journaux et les entrées de table antérieurs à un nombre de jours spécifié. La période de rétention maximale est de 365 jours (1 année).

Nota

Lorsque vous effectuez des modifications à votre stratégie de rétention, l'application de vos paramètres peut prendre plusieurs minutes.

Copyright - Tout droit réservé - OFPPT

Définition d'une stratégie de conservation des données Storage Analytics

Pour configurer une stratégie qui supprime les données de journalisation et de métriques après 7 jours, effectuez une demande pour définir les propriétés du service Blob, définissez les propriétés du servicetable ou définissez l'opération Définir les propriétés du service de file d'attente avec les <RetentionPolicy> nœuds configurés comme indiqué :

Copier

```
…
<RetentionPolicy>
    <Enabled>true</Enabled>
    <Days>7</Days>
</RetentionPolicy>
…
```


Copyright - Tout droit réservé - OFPPT

Définition d'une stratégie de conservation des données Storage Analytics

Le code XML suivant montre les nœuds <RetentionPolicy> dans le contexte de la charge utile complète pour une demande Set Blob Service Properties

```xml
<?xml version="1.0" encoding="utf-8"?>
<StorageServiceProperties>
    <Logging>
        <Version>1.0</Version>
        <Delete>true</Delete>
        <Read>false</Read>
        <Write>true </Write>
        <RetentionPolicy>
            <Enabled>true</Enabled>
            <Days>7</Days>
        </RetentionPolicy>
    </Logging>
    <HourMetrics>
        <Version>1.0</Version>
        <Enabled>true</Enabled>
        <IncludeAPIs>false</IncludeAPIs>
        <RetentionPolicy>
            <Enabled>true</Enabled>
            <Days>7</Days>
        </RetentionPolicy>
    </HourMetrics>
    <MinuteMetrics>
        <Version>1.0</Version>
        <Enabled>true</Enabled>
        <IncludeAPIs>false</IncludeAPIs>
        <RetentionPolicy>
            <Enabled>true</Enabled>
            <Days>7</Days>
        </RetentionPolicy>
    </MinuteMetrics>
    <DefaultServiceVersion>2013-08-15</DefaultServiceVersion>
</StorageServiceProperties>
```


Copyright - Tout droit réservé - OFPPT

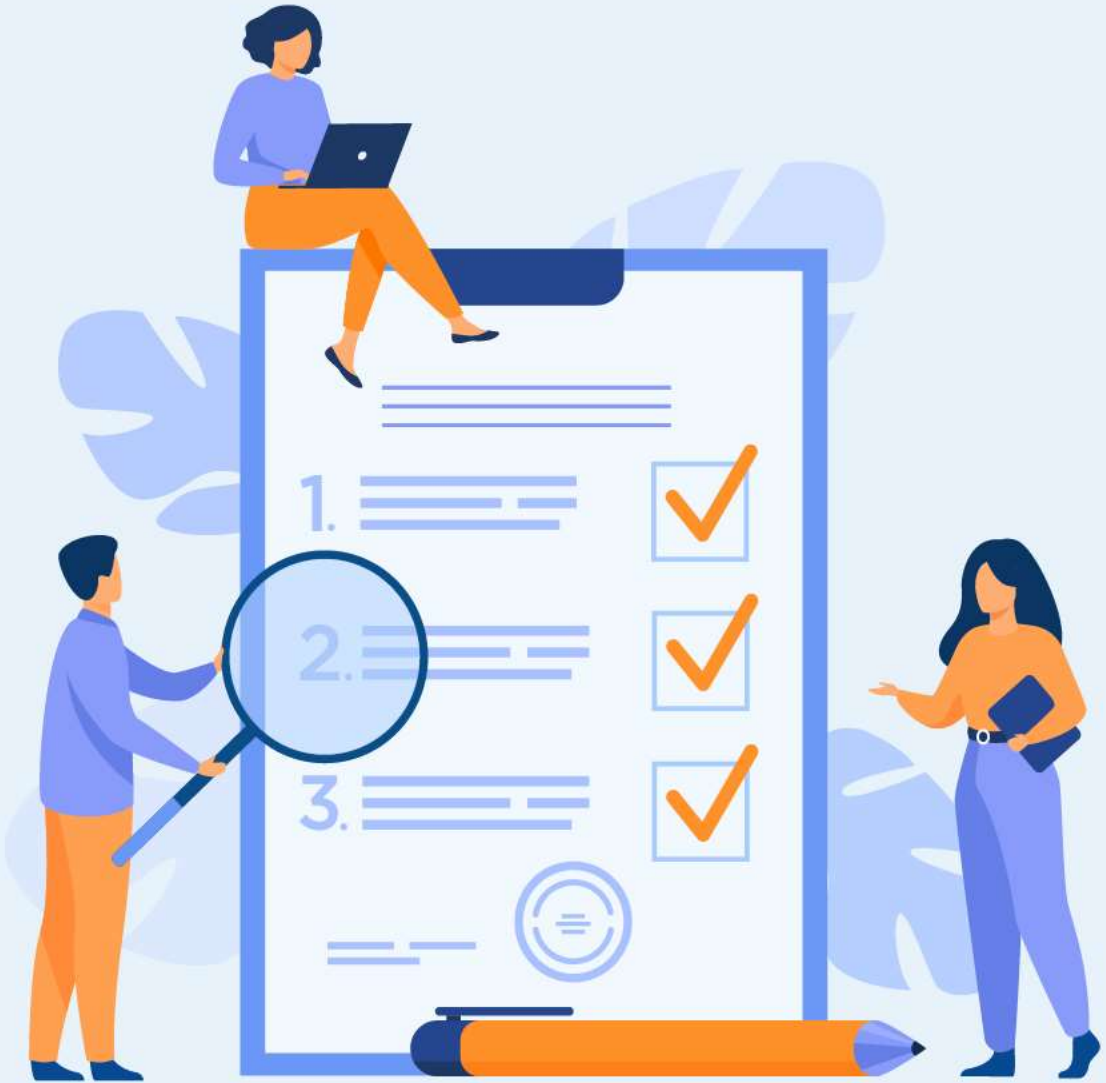
Définition d'une stratégie de conservation des données Storage Analytics

Vous pouvez également configurer une stratégie de rétention qui utilise différentes périodes pour l'enregistrement et les métriques. Pour désactiver une stratégie de rétention à l'avenir, appelez l'opération Set Blob Service Properties avec le nœud <Enabled> défini sur **false**, comme indiqué

Copier

```
…
<RetentionPolicy>
    <Enabled>false</Enabled>
    <Days>7</Days>
</RetentionPolicy>
…
```


Copyright - Tout droit réservé - OFPPT



CHAPITRE 2

Etablir des stratégies de sortie

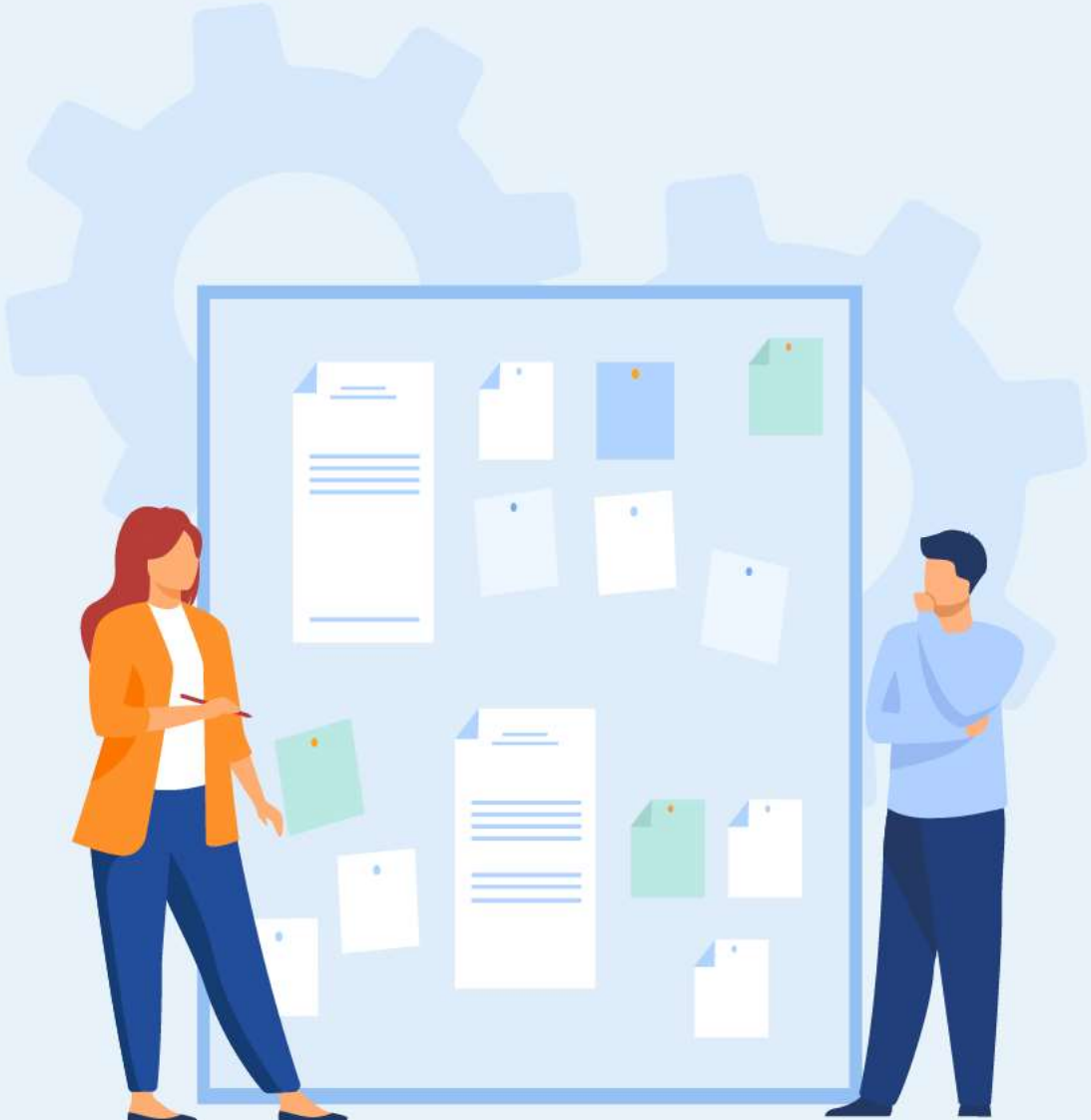
Ce que vous allez apprendre dans ce chapitre :

- Sauvegarde et Réplication
- Interopérabilité
- Export
- Coût

4,5 heures

CHAPITRE 2

Etablir des stratégies de sortie

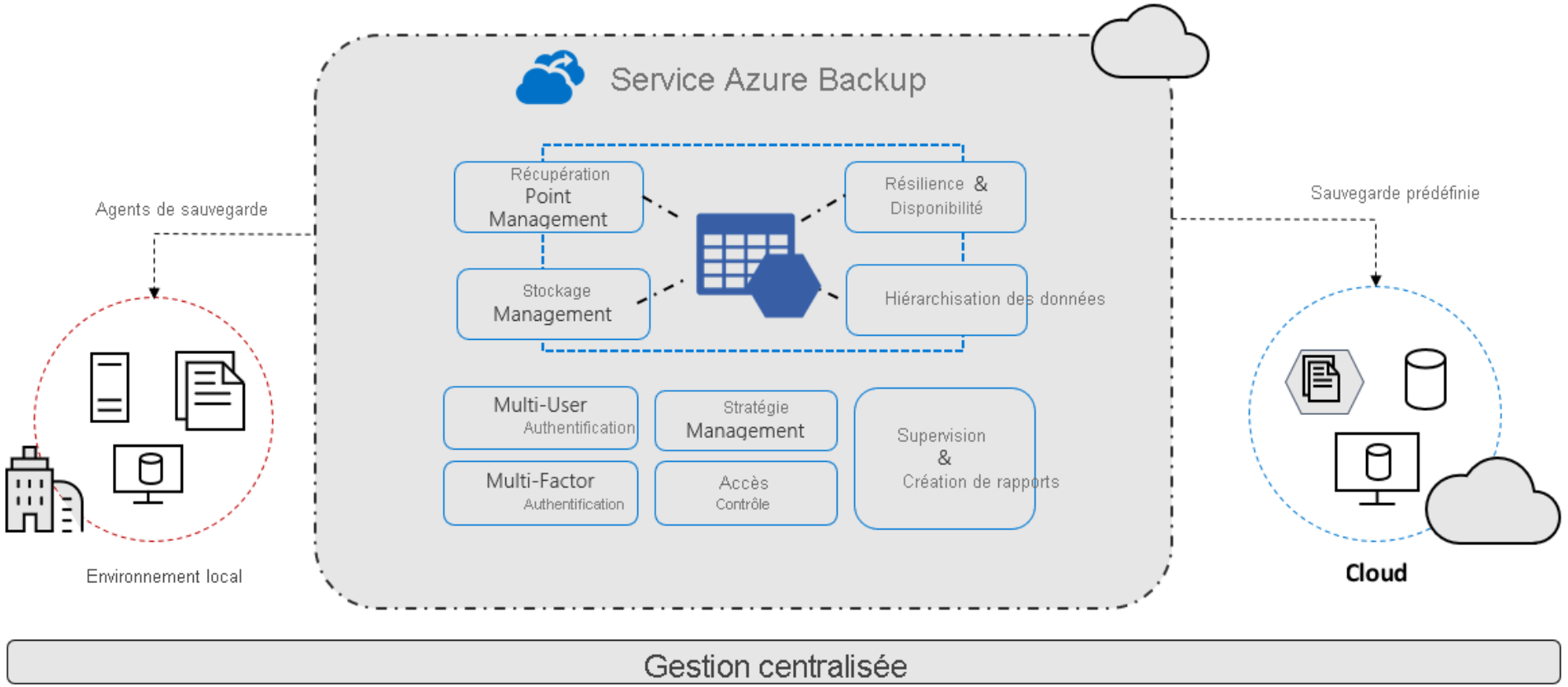


- Sauvegarde et Réplication
- Interopérabilité
- Export
- Coût

PARTIE 3

Qu'est-ce que le service Sauvegarde Azure ?

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



Copyright - Tout droit réservé - OFPPT

Que puis-je sauvegarder ?

- **Localement** - Sauvegardez des fichiers, des dossiers et l'état du système à l'aide de l'agent Microsoft Azure Recovery Services (MARS). Ou utilisez l'agent DPM ou Serveur de **sauvegarde Azure (MABS) pour protéger les machines virtuelles locales (Hyper-V et VMware) et d'autres charges de travail locales**
- **Machines virtuelles Azure** Sauvegardez des machines virtuelles Windows/Linux entières (à l'aide d'extensions de sauvegarde) ou sauvegardez des fichiers, des dossiers et l'état du système à l'aide de l'agent MARS
- **Disques managés Azure** Vous pouvez sauvegarder les disques managés Azure
- **Partages Azure Files** Sauvegardez des partages de fichiers Azure sur un compte de stockage
- **SQL Server sur des machines virtuelles Azure** Sauvegardez des bases de données SQL Server qui s'exécutent sur les machines virtuelles Azure
- **Bases de données SAP HANA sur des machines virtuelles Azure** Sauvegardez des bases de données SAP HANA qui s'exécutent sur des machines virtuelles Azure
- **Serveurs Azure Database pour PostgreSQL** -Sauvegarder des bases de données Azure PostgreSQL et conserver les sauvegardes pendant 10 ans maximum
- **Objets blob Azure** Vue d'ensemble de la sauvegarde opérationnelle des objets blob Azure.

Copyright - Tout droit réservé - OFPPT

Pourquoi utiliser Azure Backup ?

Le service Sauvegarde Azure offre les principaux avantages suivants :

- **Sauvegarde locale de déchargement** : Le service Sauvegarde Azure offre une solution simple pour la sauvegarde de vos ressources locales dans le Cloud. Obtenez une sauvegarde à court terme et à long terme sans avoir besoin de déployer des solutions de sauvegarde locale complexes.
- **Sauvegarder des machines virtuelles Azure IaaS** : Le service Sauvegarde Azure fournit des sauvegardes indépendantes et isolées pour éviter une destruction accidentelle des données d'origine. Les sauvegardes sont stockées dans un coffre Recovery Services avec gestion intégrée des points de récupération. La configuration et la scalabilité sont simples : les sauvegardes sont optimisées et vous pouvez facilement effectuer des restaurations en fonction des besoins.
- **Mettre à l'échelle facilement** : Sauvegarde Azure utilise la puissance sous-jacente et la mise à l'échelle illimitée du Cloud Azure pour offrir une haute disponibilité, sans tâche supplémentaire de maintenance ou de supervision.
- **Obtenir un transfert de données illimitées** : Le service Sauvegarde Azure ne limite pas la quantité de données entrantes ou sortantes que vous transférez, et ne génère pas de frais pour les données transférées.
    - Les données sortantes sont les données transférées à partir d'un coffre Recovery Services pendant une opération de restauration.
    - Si vous effectuez une sauvegarde initiale hors connexion avec le service Azure Import/Export pour importer de grandes quantités de données, des frais associés aux données entrantes sont facturés.
- **Sécuriser les données** : Le service Sauvegarde Azure fournit des solutions pour sécuriser les données en transit et au repos.
- **Supervision et gestion centralisées** : Sauvegarde Azure fournit des fonctionnalités intégrées de supervision et d'alerte dans un coffre Recovery Services. Ces fonctionnalités sont disponibles sans infrastructure de gestion supplémentaire. Vous pouvez également augmenter l'échelle de votre supervision et de vos rapports à l'aide d'Azure Monitor.

Copyright - Tout droit réservé - OFPPT

Pourquoi utiliser Azure Backup ?

- **Obtenir des sauvegardes cohérentes au niveau application** : une sauvegarde cohérente au niveau application signifie qu'un point de récupération dispose de toutes les données nécessaires pour restaurer la copie de sauvegarde. Le service Sauvegarde Azure fournit des sauvegardes cohérentes avec les applications, qui garantissent qu'aucun correctif supplémentaire n'est requis pour restaurer les données. La restauration de données cohérentes avec les applications réduit le délai de restauration, ce qui permet de rétablir rapidement le fonctionnement normal.
- **Conserver des données à court et à long terme** : Vous pouvez utiliser des coffres Recovery Services pour la conservation des données à court et à long termes.
- **Gestion automatique du stockage** : les environnements hybrides impliquent souvent un stockage hétérogène (une partie en local et une autre dans le Cloud). Avec le service Sauvegarde Azure, l'utilisation d'appareils de stockage locaux ne génère aucun coût. Azure Backup alloue et gère automatiquement le stockage de sauvegarde sur la base d'un modèle de paiement à l'utilisation. Vous payez uniquement le stockage que vous consommez. **Plusieurs options de stockage** : Sauvegarde Azure offre trois types de réplication pour conserver votre stockage/vos données hautement disponibles.
    - Le stockage localement redondant (LRS) réplique vos données trois fois (il crée trois copies de vos données) dans une unité d'échelle de stockage d'un centre de données. Toutes les copies des données existent dans la même région. Le stockage LRS est une option à faible coût qui protège vos données contre les défaillances matérielles locales.
    - Le stockage géoredondant (GRS) est l'option de réplication par défaut : c'est l'option recommandée. Le stockage géo-redondant réplique vos données vers une région secondaire, distante de plusieurs centaines de kilomètres de l'emplacement principal des données sources. Le stockage GRS est plus onéreux que le stockage LRS, mais il offre une durabilité des données supérieure, même en cas de panne au niveau régional.
    - Le stockage redondant interzone (ZRS) réplique vos données dans des zones de disponibilité, garantissant ainsi la résidence et la résilience des données dans la même région. Le stockage redondant interzone n'a pas de temps d'arrêt. Vos charges de travail critiques qui nécessitent la résidence des données et qui ne doivent pas avoir de temps d'arrêt peuvent donc être sauvegardées dans un stockage redondant interzone.

Copyright - Tout droit réservé - OFPPT

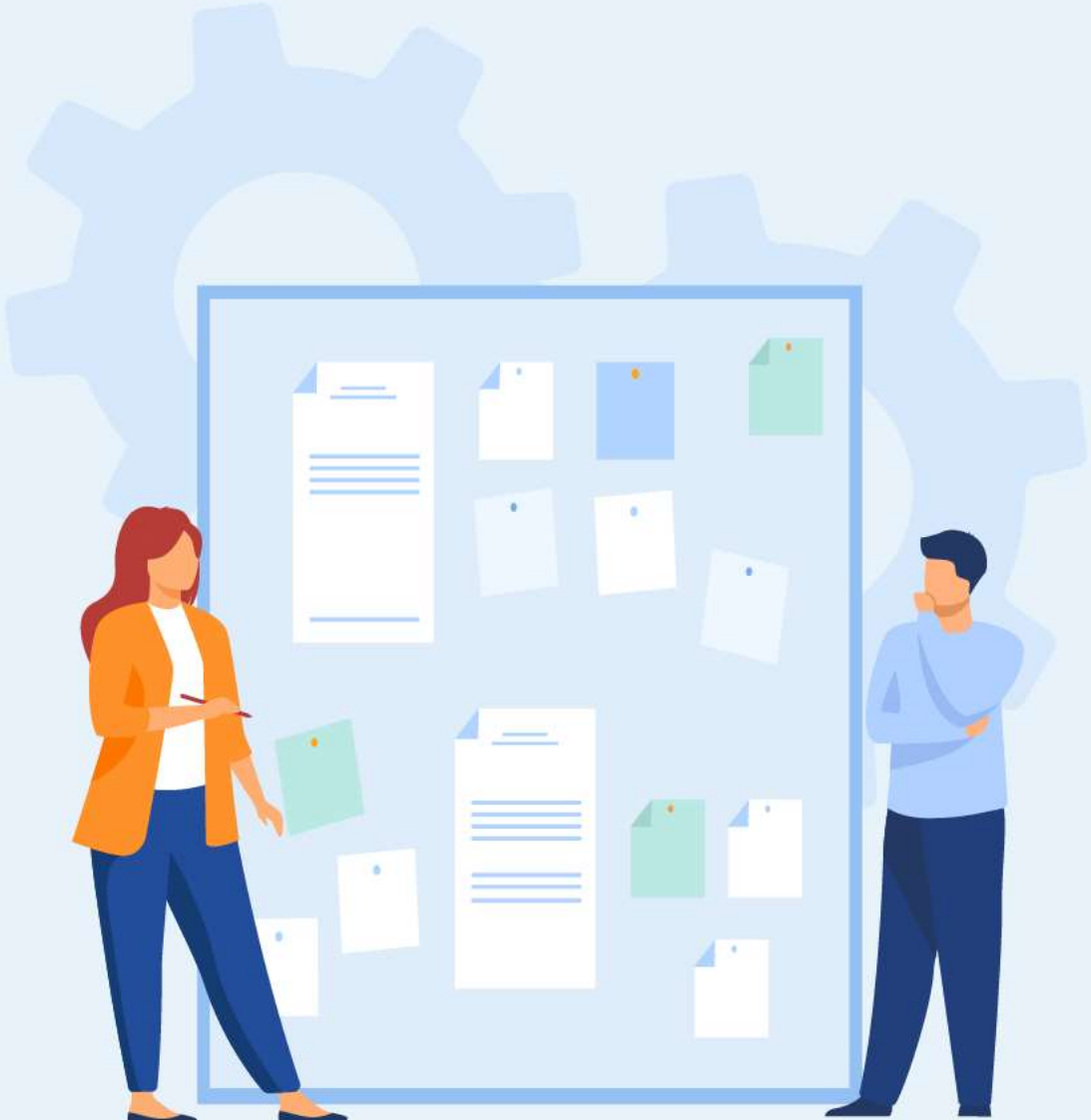
Comment le service Sauvegarde Azure protège-t-il contre les rançongiciels ?

Le service Sauvegarde Azure vous aide à protéger vos systèmes d'entreprise critiques et données de sauvegarde contre les attaques par rançongiciel en implémentant des mesures préventives et en fournissant des outils qui protègent votre organisation contre toute action que des pirates informatiques effectuent pour infiltrer vos systèmes. Il assure la sécurité de votre environnement de sauvegarde, tant lorsque vos données sont en transit que quand elles sont au repos.

Copyright - Tout droit réservé - OFPPT

CHAPITRE 2

Etablir des stratégies de sortie



- Sauvegarde et Réplication
- Interopérabilité
- Export
- Coût

PARTIE 3

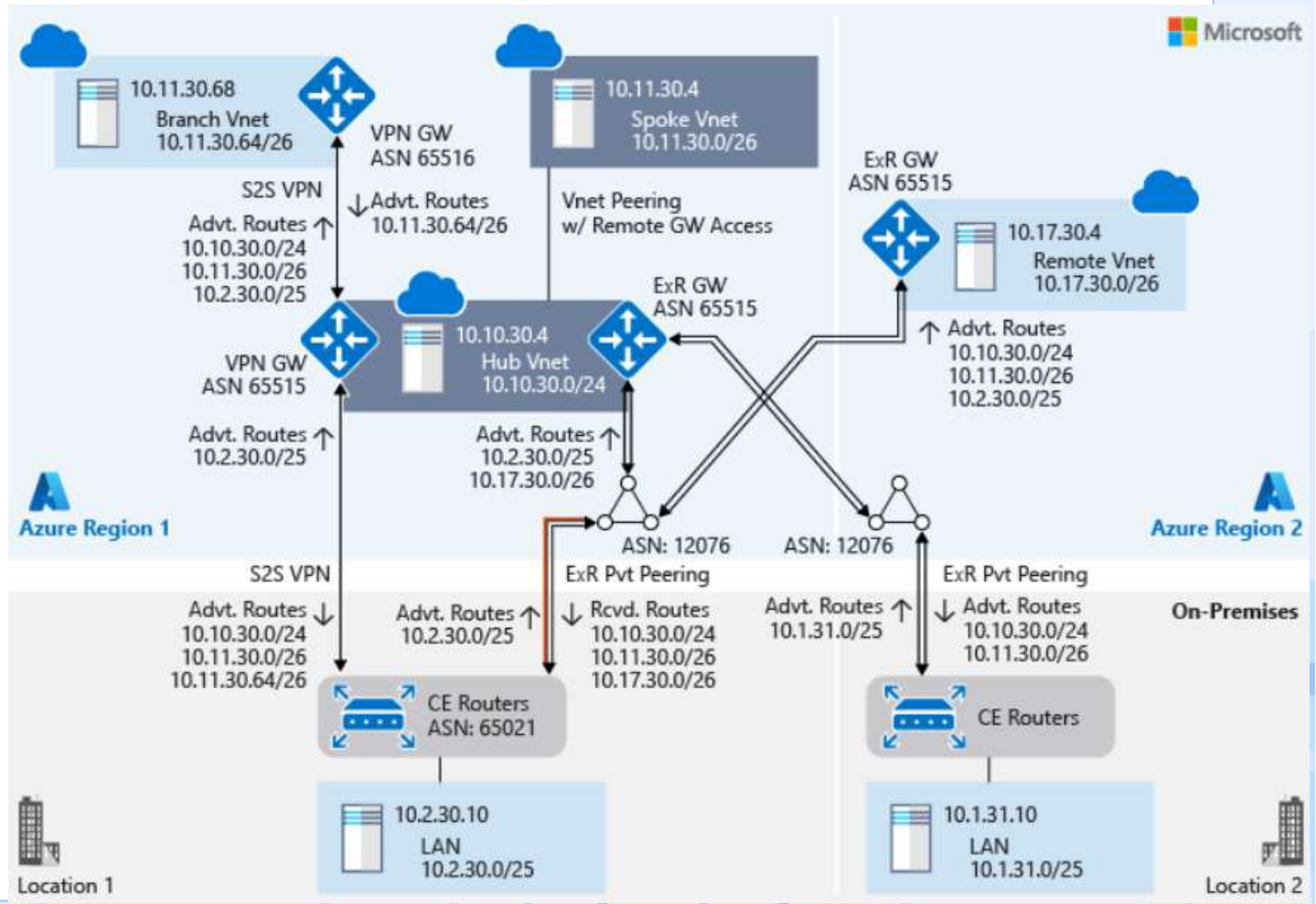
Interopérabilité dans Azure : Analyse du plan de contrôle

L'analyse du plan de contrôle examine essentiellement les itinéraires qui sont échangés entre des réseaux au sein d'une topologie. L'analyse du plan de contrôle vous permet de comprendre comment des réseaux différents affichent la topologie.

Perspective du réseau virtuel hub and spoke

La figure suivante illustre le réseau du point de vue d'un réseau virtuel hub (VNet) et d'un réseau virtuel spoke (en bleu). Cette figure montre également le numéro de système autonome (ASN) de différents réseaux et les itinéraires qui sont échangés entre réseaux différents

L'ASN de la passerelle Azure ExpressRoute du réseau virtuel est différent de l'ASN des routeurs Microsoft Enterprise Edge (MSEE). Une passerelle ExpressRoute utilise un ASN privé (valeur de **65515**) et les MSEE utilisent un ASN public (valeur de **12076**) dans le monde entier. Lorsque vous configurez le peering ExpressRoute, étant donné que le MSEE est l'homologue, vous utilisez l'ASN d'homologue **12076**. Du côté Azure, MSEE établit le peering eBGP la passerelle ExpressRoute. Le double peering eBGP que MSEE établit pour chaque peering ExpressRoute est transparent au niveau du plan de contrôle. Par conséquent, lorsque vous visualisez une table de routage ExpressRoute, l'ASN de la passerelle ExpressRoute du réseau virtuel s'affiche pour les préfixes du réseau virtuel.



Copyright - Tout droit réservé - OFPPT

Interopérabilité dans Azure : Analyse du plan de contrôle

La figure montre un exemple de table de routage ExpressRoute

Route table (Primary)
AzurePrivatePeering - ASH-Cust30-ER

Download | Show secondary

Showing only top 200 primary records, click Download above to see all.

NETWORK	NEXT HOP	LOCPRF	WEIGHT	PATH
10.2.30.0/25	192.168.30.17		0	65021
10.2.30.125/32	192.168.30.17		0	65021 65515
10.10.30.0/24	10.10.30.141		0	65515
	10.10.30.140		0	65515
10.11.30.0/26	10.10.30.141		0	65515
	10.10.30.140		0	65515

Dans Azure, l'ASN n'est significatif que de la perspective du peering. Par défaut, l'ASN de la passerelle ExpressRoute et de la passerelle du réseau privé virtuel est **65515** dans la passerelle VPN Azure.

PARTIE 3

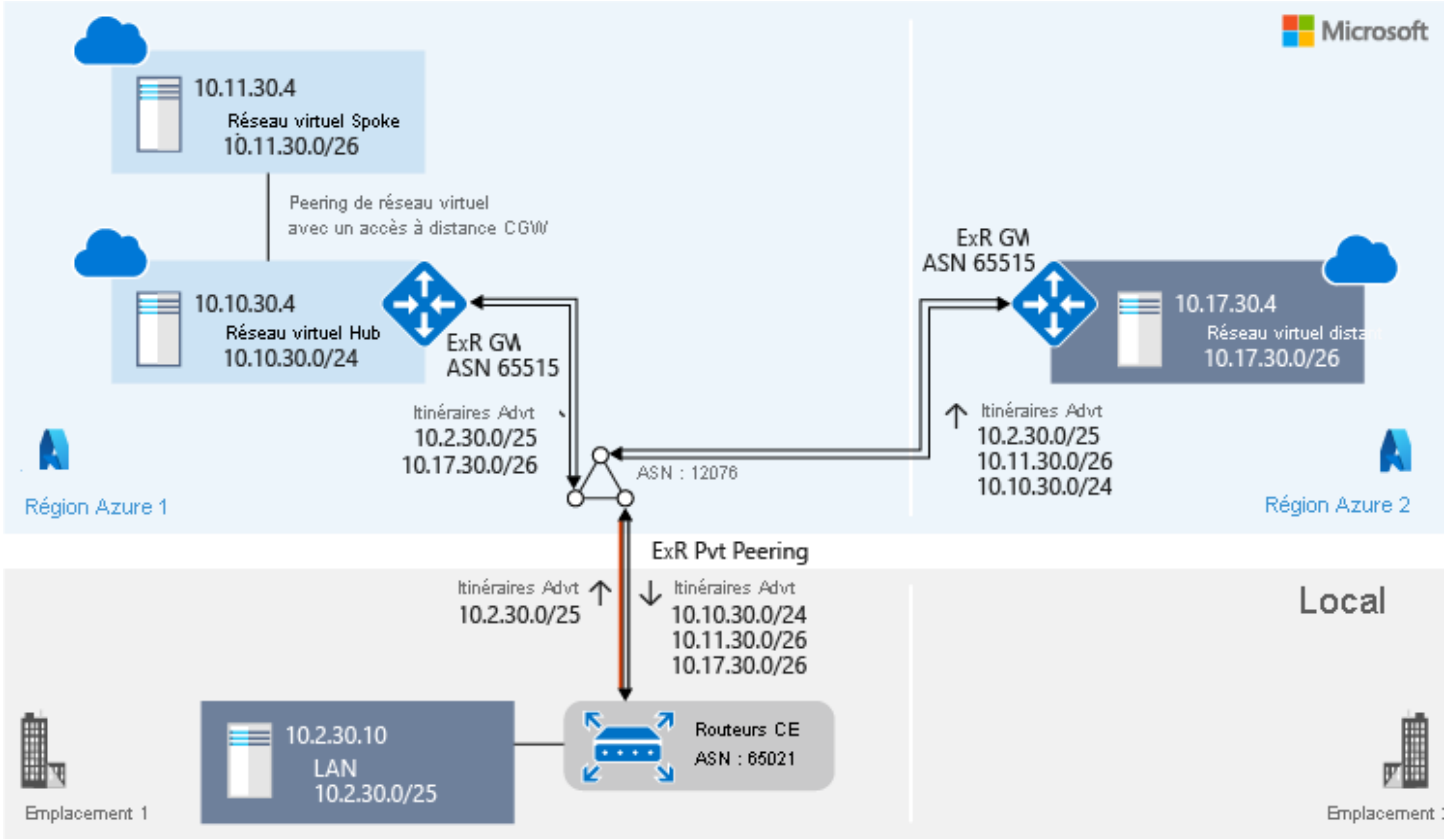
Copyright - Tout droit réservé - OFPPT

PARTIE 3

Perspective du réseau local Location 1 et du réseau virtuel distant via ExpressRoute 1

Le réseau local Location 1 et du réseau virtuel distant sont connectés au réseau virtuel du hub via ExpressRoute 1.

Ils partagent la même perspective de la topologie, comme le montre le schéma

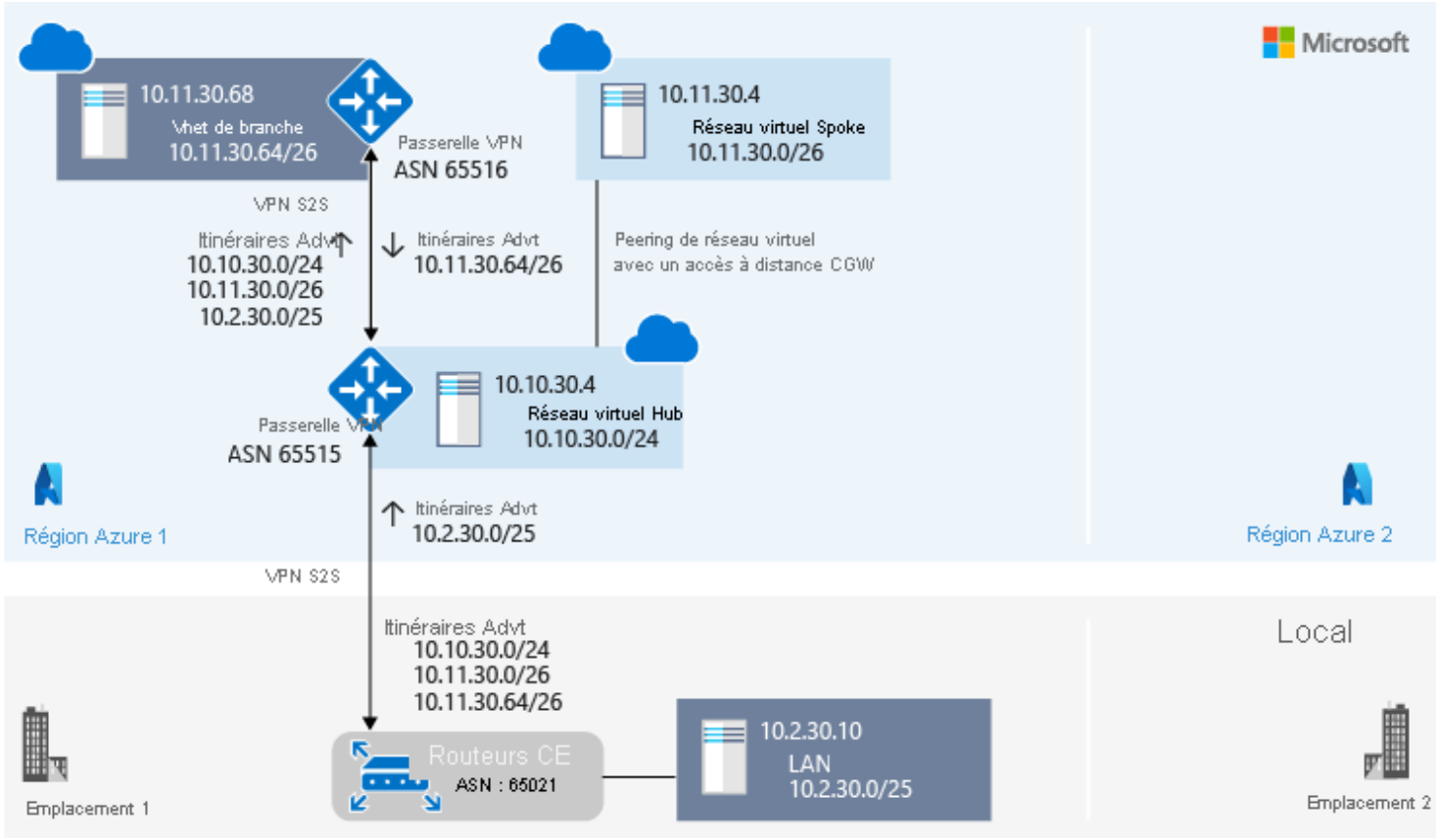


Copyright - Tout droit réservé - OFPPT

PARTIE 3

Perspective du réseau local Location 1 et du réseau virtuel branche via le VPN de site à site

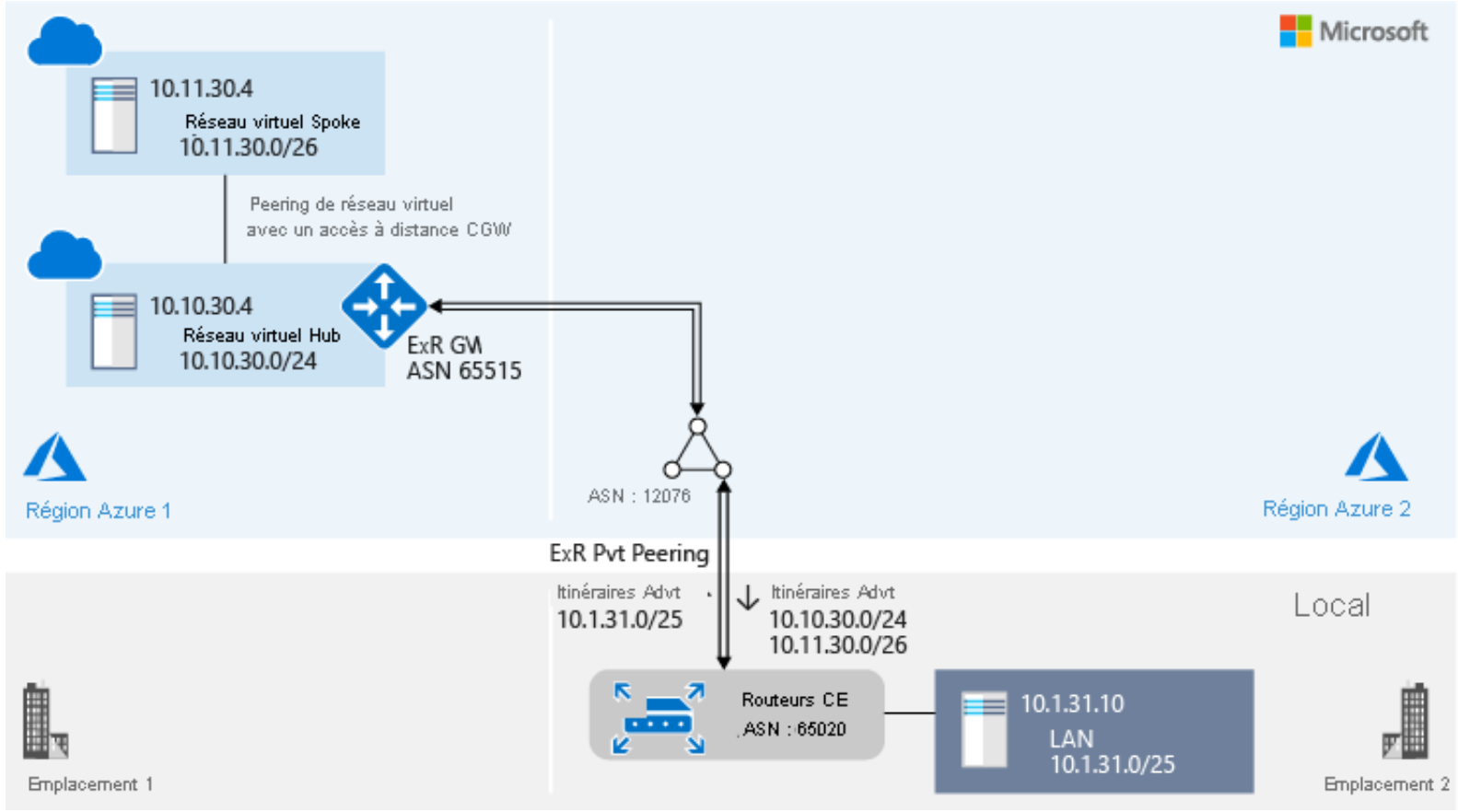
Le réseau local Location 1 et le réseau virtuel branche sont tous deux connectés à la passerelle VPN du réseau virtuel Hub via les connexions VPN de site à site. Ils partagent la même perspective de la topologie, comme le montre le schéma



Copyright - Tout droit réservé - OFPPT

Perspective du réseau local Location 2

Le réseau local Location 2 est connecté au réseau local hub via le peering privé d'ExpressRoute 2



PARTIE 3

Copyright - Tout droit réservé - OFPPT

Connectivité ExpressRoute et VPN de site à site en tandem

VPN de site à site sur ExpressRoute

Vous pouvez configurer un VPN de site à site à l'aide du peering Microsoft ExpressRoute pour échanger des données de façon privée entre votre réseau local et vos réseaux virtuels Azure. Avec cette configuration, vous pouvez échanger des données en garantissant confidentialité, authenticité et intégrité. L'échange de données est également soumis à un système anti-relecture. Pour plus d'informations sur la configuration d'un VPN IPSec de site à site en mode tunnel via le peering Microsoft ExpressRoute, consultez l'article [Configurer un réseau VPN de site à site via le peering Microsoft ExpressRoute][S2S-Over-ExR].

La principale limitation liée à la configuration d'un VPN de site à site qui utilise le peering Microsoft est le débit. Le débit sur le tunnel IPsec est limité par la capacité de la passerelle VPN. Le débit d'une passerelle VPN est inférieur au débit ExpressRoute. Dans ce scénario, le fait d'utiliser le tunnel IPsec pour un trafic très sécurisé et d'utiliser le peering privé pour toutes les autres catégories de trafic permet d'optimiser l'utilisation de la bande passante ExpressRoute.

VPN de site à site en tant que chemin de basculement sécurisé pour ExpressRoute

ExpressRoute est utilisé comme une paire de circuits redondants pour garantir une haute disponibilité. Vous pouvez configurer une connectivité ExpressRoute géo-redondante dans différentes régions Azure. En outre, comme nous l'avons démontré dans notre initialisation (tearDown) de test, dans une région Azure, vous pouvez utiliser un VPN de site à site pour créer un chemin de basculement pour votre connectivité ExpressRoute. Quand les mêmes préfixes sont publiés sur ExpressRoute et un VPN de site à site, Azure choisit en priorité ExpressRoute. Pour éviter un routage asymétrique entre ExpressRoute et le VPN de site à site, la configuration réseau locale doit en faire autant en utilisant la connectivité ExpressRoute avant la connectivité VPN de site à site.

Pour plus d'informations sur la façon de configurer des connexions coexistantes pour ExpressRoute et un VPN de site à site, consultez [Coexistence de connexions ExpressRoute et de site à site][ExR-S2S-CoEx].

Copyright - Tout droit réservé - OFPPT

Étendre la connectivité de back-end à des réseaux virtuels spoke et à des emplacements branch

Connectivité de réseau virtuel spoke via le peering de réseaux virtuels

L'architecture des réseaux virtuels hub et spoke est largement utilisée. Le hub est un réseau virtuel dans Azure qui centralise la connectivité entre vos réseaux virtuels spoke et votre réseau local. Les spokes sont des réseaux virtuels appairés avec le hub et que vous pouvez utiliser pour isoler les charges de travail. Le trafic circule entre le centre de données local et le hub via une connexion ExpressRoute ou VPN. Pour plus d'informations sur l'architecture, consultez [Implémenter une topologie réseau hub-and-spoke dans Azure][Hub-n-Spoke].

Dans le peering de réseau virtuel dans une région, les réseaux virtuels spoke peuvent utiliser des passerelles de réseau virtuel hub (les passerelles VPN et ExpressRoute) pour communiquer avec des réseaux distants.

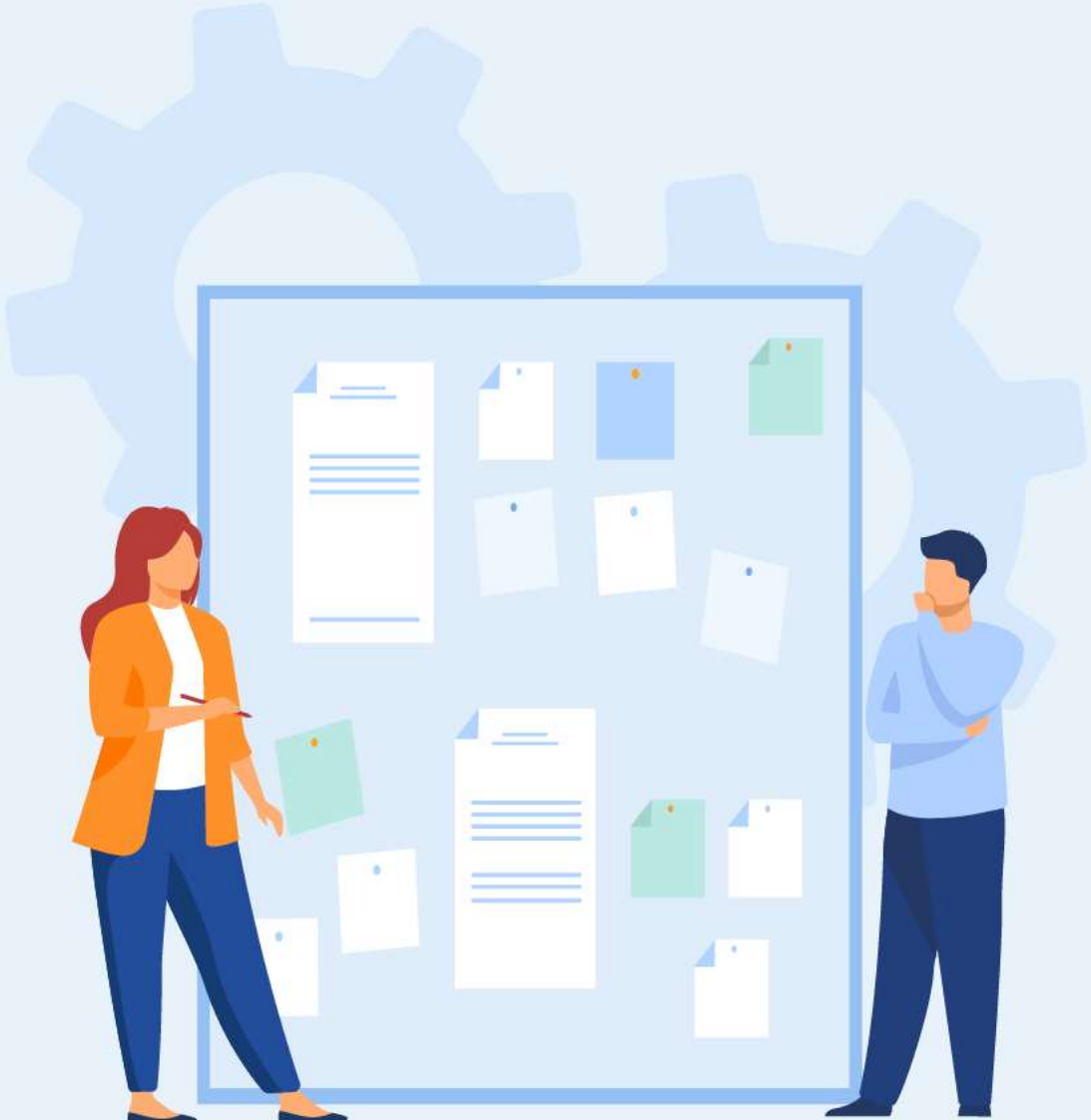
Connectivité de réseau virtuel branch à l'aide d'un VPN de site à site

Vous pouvez souhaiter que les réseaux virtuels branch, qui se trouvent dans différentes régions, et les réseaux locaux communiquent entre eux via un réseau virtuel hub. La solution Azure native pour cette configuration est la connectivité VPN de site à site à l'aide d'un VPN. Une autre solution consiste à utiliser une appliance virtuelle réseau (NVA) pour le routage dans le hub.

Copyright - Tout droit réservé - OFPPT

CHAPITRE 2

Etablir des stratégies de sortie



- Sauvegarde et Réplication
- Interopérabilité
- Export
- Coût

Export

Globalement, un travail d'exportation comprend les opérations suivantes :

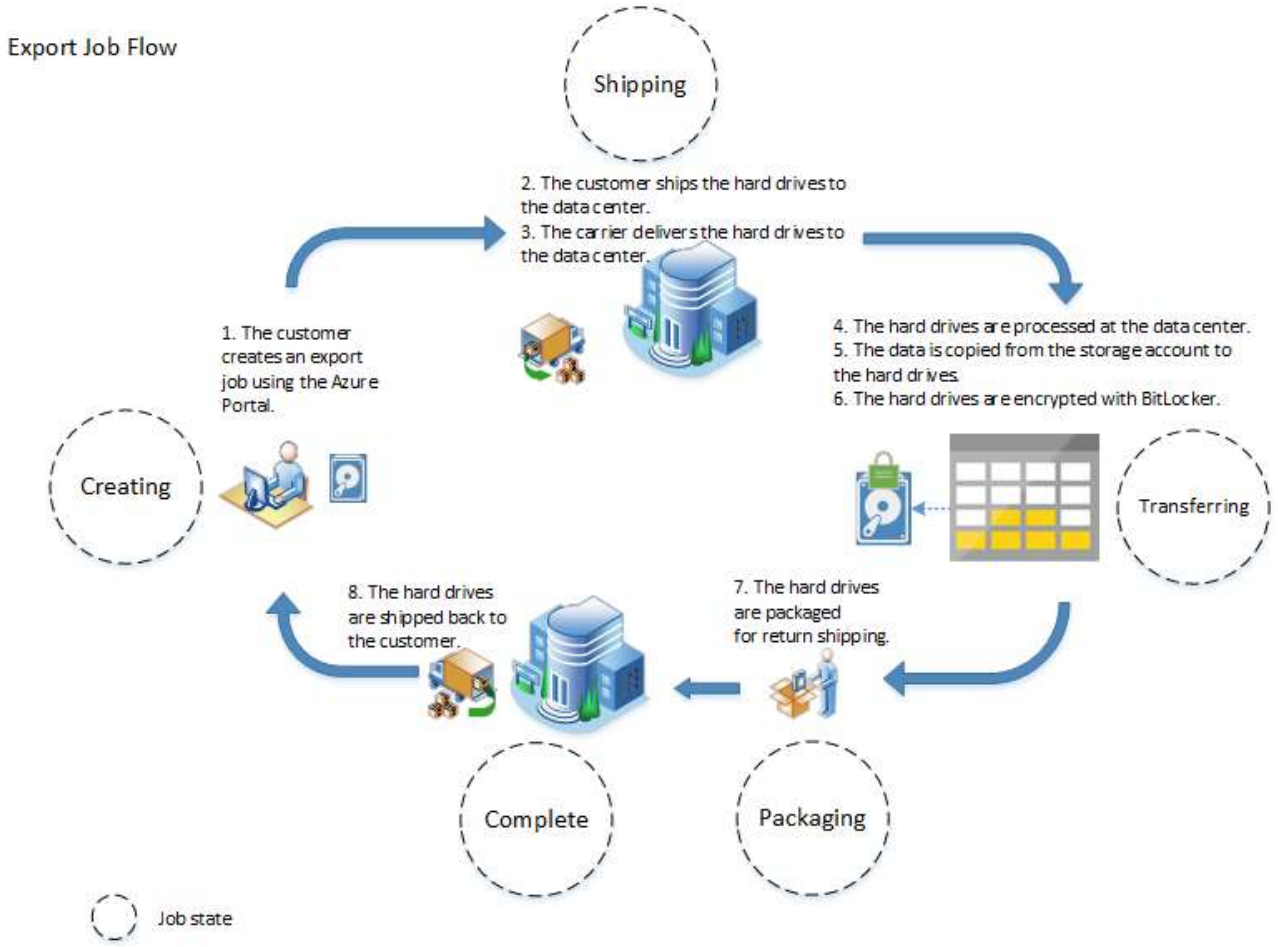
- Déterminer les données à exporter, le nombre de lecteurs vous besoin, les objets blob sources ou les chemins de conteneur de vos données dans le stockage blob
- Créer un travail d'importation dans votre compte de stockage source dans le Portail Azure
- Spécifier les objets blob sources ou les chemins de conteneur de vos données à exporter
- Indiquer l'adresse de retour et le numéro de compte transporteur à utiliser pour le retour des disques
- Expédier les lecteurs de disque à l'adresse d'expédition indiquée lors de la création du travail
- Mettre à jour le numéro de suivi et envoyez le travail d'exportation
- Les disques sont réceptionnés et traités dans le centre de données Azure
- Les disques sont chiffrés à l'aide de BitLocker et les clés sont disponibles via le Portail Azure
- Les disques sont expédiés à l'aide de votre compte de transporteur à l'adresse de retour indiquée dans le travail d'importation.

Copyright - Tout droit réservé - OFPPT

Export

Pour les expéditions à l'échelle nationale (dans le pays / la région du centre de données), veuillez partager un compte de transporteur domestique.

Pour les expéditions à l'étranger (en dehors du pays/de la région du centre de données), veuillez partager un compte de transporteur international.



Copyright - Tout droit réservé - OFPPT

Export

Disponibilité des régions

Le service Azure Import/Export prend en charge la copie des données vers et depuis tous les comptes de stockage Azure. Vous pouvez expédier des lecteurs de disque aux emplacements suivants. Si votre compte de stockage se trouve dans un emplacement Azure qui n'est pas spécifié ici, un emplacement d'expédition de remplacement est proposé lorsque vous créez le travail.

Emplacements d'expédition pris en charge

Pays/région	Pays/région	Pays/région	Pays/région
USA Est	Europe Nord	Inde centrale	US Gov Iowa
USA Ouest	Europe Ouest	Inde Sud	Est des États-Unis – US DoD
USA Est 2	Asie Est	Inde Ouest	Centre des États-Unis – US DoD
USA Ouest 2	Asie Sud-Est	Centre du Canada	Chine orientale
USA Centre	Australie Est	Est du Canada	Chine du Nord
Centre-Nord des États-Unis	Sud-Australie Est	Brésil Sud	Sud du Royaume-Uni
États-Unis - partie centrale méridionale	OuJapon Est	Centre de la Corée	Centre de l'Allemagne
Centre-USA Ouest	Japon Est	Gouvernement américain - Virginie	Nord-Est de l'Allemagne
Afrique du Sud Ouest	Afrique du Sud Nord		

Copyright - Tout droit réservé - OFPPT

Export

Considérations relatives à la sécurité

Les données présentes sur le lecteur doivent être chiffrées à l'aide du chiffrement de lecteur BitLocker AES 256 bits. Ce chiffrement permet de protéger vos données en transit.

Pour les travaux d'importation, les lecteurs sont chiffrés de deux manières.

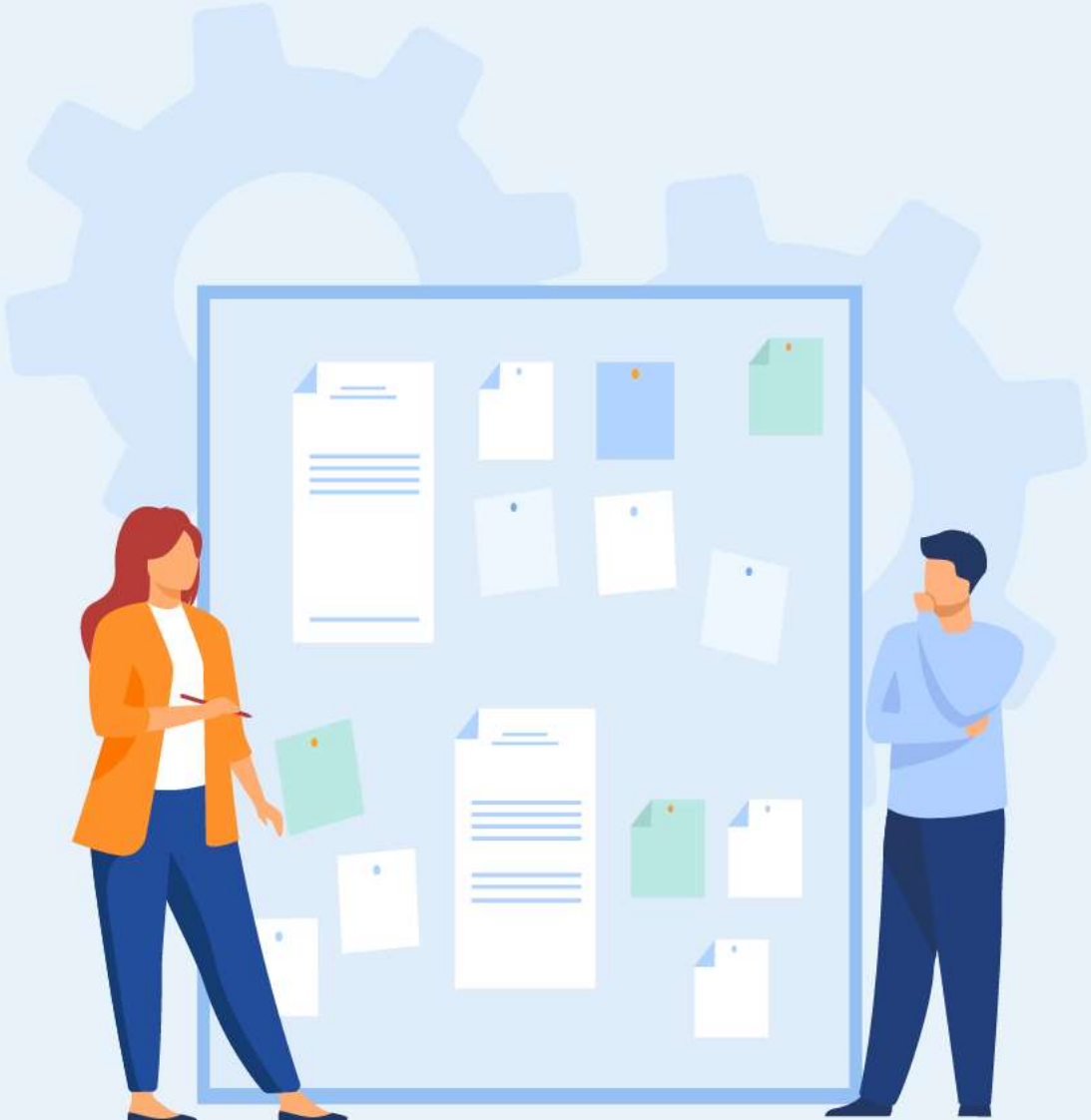
1. Spécifiez l'option lors de l'utilisation du fichier *dataset.csv* pendant l'exécution de l'outil WAImportExport pour préparer le disque.
2. Activez le chiffrement BitLocker manuellement sur le disque. Spécifiez la clé de chiffrement dans le fichier *driveset.csv* lors de l'exécution de la ligne de commande de l'outil WAImportExport pendant la préparation du disque. La clé de chiffrement BitLocker peut être davantage protégée à l'aide d'un protecteur de clé externe (également appelé « clé gérée par Microsoft ») ou d'une clé gérée par le client.

Pour les travaux d'exportation, une fois vos données copiées sur le disque, le service chiffre le disque à l'aide de BitLocker avant de vous le renvoyer. La clé de chiffrement vous est fournie par le biais du Portail Azure. Le lecteur doit être déverrouillé à l'aide de l'outil WAImporExport en utilisant la clé.

Copyright - Tout droit réservé - OFPPT

CHAPITRE 2

Etablir des stratégies de sortie



- Sauvegarde et Réplication
- Interopérabilité
- Export
- Coût

Coût

Frais de manipulation de disque

Des frais de manipulation sont appliqués pour chaque disque traité dans le cadre de votre travail d'importation/exportation.

Les prix sont uniquement des estimations et ne constituent pas des prix réels. Les prix réels peuvent varier en fonction du type d'accord conclu avec Microsoft, de la date d'achat et du taux de change. Les prix sont calculés en dollars US et convertis à l'aide des taux de référence Thomson Reuters actualisés le premier jour de chaque mois civil. Connectez-vous à la Calculatrice de prix Azure pour consulter la tarification en fonction de votre programme/offre actuel avec Microsoft.

Frais d'expédition

Lorsque vous envoyez des disques à Azure, vous payez le coût d'expédition au transporteur. Lorsque Microsoft vous renvoie les disques, les frais d'expédition sont facturés au compte de transporteur que vous avez spécifié lors de la création du travail.

Frais de transaction

Les frais de transaction de stockage standard s'appliquent pour l'importation et l'exportation des données. Des frais de sortie standard sont également applicables avec les frais de transaction de stockage lorsque les données sont exportées depuis le stockage Azure.

Gestion des périphériques : tarif fixe de $80 par dispositif de stockage géré. Aucuns frais de transfert de données entre le périphérique et le stockage Azure dans le même centre de données. Les coûts normaux des transactions Stockage d'Azure s'appliquent.

Retour de périphériques : les frais de retour encourus seront facturés sur le compte du transporteur du client.

*Des frais de stockage et de transaction standard sont facturés séparément.

Copyright - Tout droit réservé - OFPPT