Datacenter Virtuel Azure

Isolation, sécurité et confiance dans le Cloud Microsoft

par Mark Ozur
Hatay Tuna
Callum Coffin
Telmo Sampaio
Azure Engineering

Novembre 2017

Sommaire

Vue d'ensemble 5

PARTIE 1 QU'EST-CE QU'UN DATACENTER VIRTUEL AZURE ? 7

Introduction : les composants essentiels 8

Isolation logique des espaces de travail multiples 9

Infrastructure partagée de confiance 9

Plateforme globale 10

Infrastructure régionale 11

Confiance via l'isolation 12

Confiance via le chiffrement 13

Données en transit 14

Données stockées 14

Données en cours de traitement 15

DEUXIÈME PARTIE COMMENT CONTOSO COMPOSE UN CENTRE DE DONNÉES DE CONFIANCE 16

Contrôle d'accès centralisé et espaces de travail connectés 17

Connectivité sur site 18

Séparation des responsabilités dans le centre de données 18

Rôles d'administration 19

Gestion des identités avec Azure AD 20

Stratégie en différentes couches 20

Architecture proposée pour Contoso 20

Configuration initiale de l'environnement 22

Organisation de l'infrastructure centrale et des espaces de travail 22

Stratégies du Gestionnaire de ressources 23

Configuration du coffre des clés 24

Configuration du réseau virtuel du hub 24

Pare-feu central 25

Passerelles et réseaux de périmètre 27

Administration 28

Services partagés 29

Déployer des charges de travail dans des espaces de travail 31

Rôles d'administration d'un espace de travail 31
Choisir le bon modèle de service pour une charge de travail 31
Intégration d'un réseau virtuel avec PaaS 32
Audit et journalisation 33
Utilisation des outils de surveillance et de sécurité d'Azure 35
Architecture finale de Contoso 37
TROISIÈME PARTIE L'évolution du centre de données vers le Cloud 39
Équilibrer la gouvernance et l'agilité 40
Modèles pour un centre de données virtuel 40
Aller de l'avant avec un Datacenter Virtuel Azure 41
Automatisation du centre de données virtuel 42
Glossaire des principaux services et fonctionnalités 42
Pour en savoir plus 45
Plateforme Azure 45
Identités et Azure Active Directory 45
Isolation et sécurité 46
Chiffrement 46
Réseau virtuel 47
Opérations 48

Liste des figures

Figure 1. Les 4 composants du Datacenter Virtuel Azure : identité, chiffrement, réseau défini par logiciel et conformité. 5
Figure 2. Le respect de la conformité, la sécurité et l'application de stratégies constituent les bases de l'approche Datacenter Virtuel Azure pour développer la confiance, avec un audit automatisé pour révéler des problèmes potentiels. 8
Figure 3. Le tableau de bord de l'outil Microsoft Compliance Manager. 10
Figure 4. La plateforme Azure repose sur un nombre grandissant de centres de données dans le monde. 11
Figure 5. Architecture à haut niveau proposée par Contoso pour son centre de données virtuel. 17
Figure 6. Comment le pare-feu central utilise l'équilibrage de la charge et le routage du trafic. 25
Figure 7. Le sous-réseau de la passerelle route le trafic vers la partie appropriée de

l'infrastructure centrale. 27

Figure 8. Les administrateurs sur site utilisent des jumpboxes renforcés (hôtes bastions) pour configurer à distance le pare-feu central et gérer les machines virtuelles et les NVA via le réseau virtuel. Des NSG (groupes de sécurité réseau) restreignent l'accès à des ports et à des adresses IP spécifiques..... 29

Figure 9. La plateforme Azure propose différentes options pour répondre aux besoins de contrôle dont les DevOps ont besoin lorsqu'ils déploient des charges de travail dans le centre de données virtuel. 32

Figure 10. Les activités du centre de données virtuel sont contrôlées et enregistrées en permanence. Les données des journaux sont importées dans OMS et peuvent être exploitées par des analyses sur site..... 33

Figure 11. Architecture finale de Contoso avec les principaux composants, les flux de trafics (du site vers une charge de travail, d'une charge de travail vers le site, du site vers l'administration, et DNS). 38

Figure 12 : La gouvernance et le service informatique de l'entreprise doivent trouver un équilibre avec l'agilité du développement lors de l'évolution réussie d'un centre de données vers le Cloud..... 40

Figure 13 : Gamme de services de plateforme utilisables dans un centre de données virtuel. À gauche, les machines virtuelles IaaS n'utilisent que des données sur site. À droite, tous les services PaaS du Cloud sont exploités. 41

Vue d'ensemble

Le Datacenter Virtuel Azure est une approche qui permet d'obtenir le maximum des fonctionnalités de la plateforme de Cloud Azure, tout en respectant vos stratégies existantes en matière de réseau et de sécurité. Lorsqu'ils déploient des charges de travail dans le Cloud, les entreprises et les services informatiques doivent trouver le juste équilibre entre la gouvernance et l'agilité de développement. Le Datacenter Virtuel Azure fournit des modèles qui permettent de trouver cet équilibre, tout en mettant l'accent sur la gouvernance.

Le déploiement de charges de travail dans le Cloud introduit le besoin de développer et de garantir une confiance dans le Cloud comparable à celle que vous avez dans vos centres de données existants. Le premier modèle de Datacenter Virtuel Azure est conçu pour répondre à ce besoin via une approche fermée des infrastructures virtuelles. Cette approche ne concerne pas toutes les entreprises. Elle est conçue pour guider les services informatiques des entreprises dans l'extension de leurs infrastructures sur site vers le Cloud public Azure. Nous nommerons cette approche « modèle d'extension d'un centre de données de confiance ». Au fil du temps, d'autres modèles seront proposés, notamment celui qui permet d'accéder à Internet de façon sûre à partir d'un centre de données virtuel.

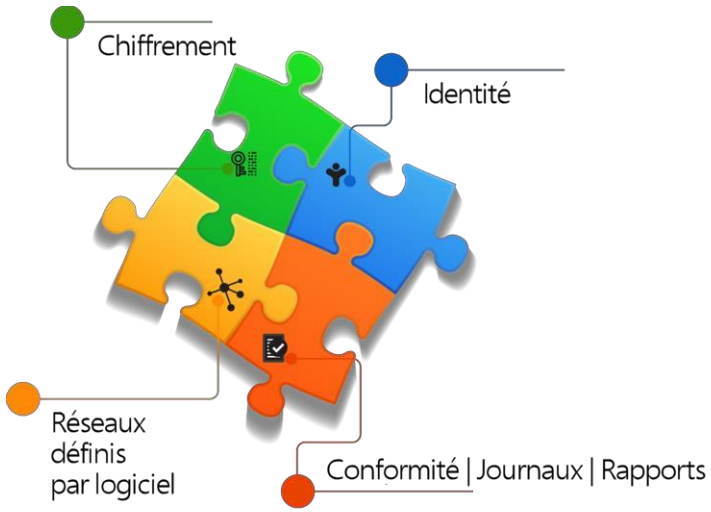

Figure 1. Les 4 composants du Datacenter Virtuel Azure : identité, chiffrement, réseau défini par logiciel et conformité.

Dans le modèle du Datacenter Virtuel Azure, vous pouvez appliquer des stratégies d'isolation, rendre le Cloud comparable aux centres de données physiques que vous connaissez, et atteindre les niveaux de sécurité et de confiance que vous souhaitez. Quatre composants, bien connus des services informatiques, permettent cela : réseau défini par logiciel, chiffrement, gestion des identités et conformité aux standards, normes et certifications de la plateforme Azure sous-jacente. Ces quatre composants sont la clé pour faire d'un centre de données virtuel, une extension digne de confiance de votre infrastructure existante.

Au cœur de ce modèle, votre infrastructure dans le Cloud a des frontières d'isolation définies

par votre *espace de noms*. Cet espace définit un Cloud isolé, qui vous est propre, dans Azure.

Dans cet espace virtuel, s'appliquent des contrôles de sécurité, des stratégies réseau et des règles de conformité. L'ensemble forme ne infrastructure dans Azure capable, en toute sécurité, de s'intégrer dans votre centre de données existant sur site.

Dans ce centre de données virtuel, vous pouvez déployer de nouveaux espaces de travail virtuels comme vous déploieriez une capacité supplémentaire dans votre centre de données physique. Ces espaces de travail virtuels sont des environnements intégrés qui permettent aux charges de travail de s'exécuter indépendamment les unes des autres, chaque équipe responsable d'une charge de travail ayant accès à l'espace de travail spécifique correspondant. Des espaces de travail permettent de construire des solutions et d'administrer des charges de travail avec une grande liberté, tout en respectant les stratégies de sécurité et d'accès définies au niveau global dans l'infrastructure informatique centrale.

Ce guide s'adresse aux architectes informatiques et aux dirigeants d'entreprises. En partant d'un centre de données physique, ce guide présente une approche pour concevoir des centres de données virtuels, sécurisés, dignes de confiance, sur la plateforme Azure. Un Datacenter Virtuel Azure n'est ni un service ni un produit spécifique mais un concept, une façon de penser des infrastructures dans le Cloud. Il décrit des pratiques et donne des conseils ayant fait leurs preuves afin de faciliter votre évolution vers le Cloud.

À la fin de ce guide, nous aborderons le prochain guide Automatisation d'un centre de données virtuel qui inclura un ensemble de scripts et des modèles du gestionnaire de ressources Azure qui vous aideront à construire un Datacenter Virtuel Azure en utilisant le modèle d'extension de confiance.

PARTIE 1
QU'EST-CE QU'UN DATACENTER VIRTUEL AZURE ?

Un Datacenter Virtuel Azure est un concept, une façon de penser le déploiement de vos applications dans une architecture basée sur le Cloud, tout en préservant les principaux aspects de votre gouvernance informatique actuelle et en tirant parti de l'agilité offerte par le Cloud.

Plusieurs différences très concrètes existent entre héberger vos applications dans le Cloud ou dans un centre de données traditionnel. Atteindre le niveau de gouvernance dans le Cloud que vous connaissez dans un centre de données traditionnel, implique une bonne compréhension des raisons pour lesquelles vous travaillez comme vous le faites aujourd'hui, et comment transposer cela dans Azure.

Contrairement à votre centre de données actuel sur site, le Cloud public Azure exploite une infrastructure physique partagée et une abstraction d'un environnement définie par logiciel. Le modèle du Datacenter Virtuel Azure vous permet de structurer des charges de travail isolées dans l'environnement mutualisé Azure, qui répondent à vos stratégies de gouvernance.

La gouvernance de vos charges de travail impose des processus d'administration intégrés, le respect des réglementations et des processus de sécurité dans le Cloud. Le modèle du Datacenter Virtuel Azure vous apporte des conseils de base pour créer une séparation des rôles, des responsabilités et des stratégies dans le Cloud.

Introduction : les composants essentiels

Un centre de données virtuel est un environnement isolé (comme un bâtiment avec des murs) pour des ressources hébergées dans le Cloud (comme des serveurs et des réseaux), qui prend en charge l'application de stratégies organisationnelles (comme la sécurité et la conformité). Cela commence par un abonnement à Azure, la porte d'entrée de l'environnement pour déployer des services et des ressources Azure.

Un principe fort du modèle de Datacenter Virtuel Azure est de faire assez peu confiance à l'environnement d'hébergement global. Par conséquence, un centre de données virtuel doit imposer des mesures d'isolation, de sécurité et de conformité dans son environnement, comme cela est le cas dans un centre de données physiques. La principale différence est comment ces mesures sont mises en œuvre. Un Datacenter Virtuel Azure s'appuie sur les principaux composants suivants :

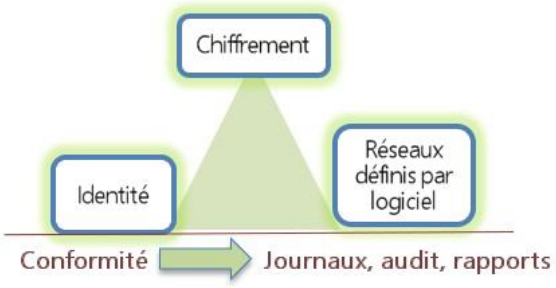

Figure 2. Le respect de la conformité, la sécurité et l'application de stratégies constituent les bases de l'approche Datacenter Virtuel Azure pour développer la confiance, avec un audit automatisé pour révéler des problèmes potentiels.

- **Un réseau défini par logiciel** définit des abstractions virtuelles d'éléments de votre réseau physique comme des topologies réseau des pare-feux, des mécanismes de détection d'intrusion, des systèmes d'équilibrage de la charge et des stratégies de routage. Vous pouvez créer, configurer et administrer des topologies réseau, une isolation du support et mettre en place des réseaux de périmètre.
- **La gestion des identités et un contrôle d'accès fondé sur les rôles (RBAC)** régissent l'accès au traitement, au réseau, aux données et aux applications dans le centre de données virtuel. Basé sur le contrôle d'accès de moindre privilège, le centre de données virtuel interdit par défaut tout accès aux ressources. Un accès doit être explicitement accordé à un utilisateur, un groupe ou une application spécifique, pour un rôle particulier.
- **Chiffrement**. Les données sont chiffrées, qu'elles soient en cours de transfert, stockées ou en cours de traitement. Le chiffrement isole les informations confidentielles du reste de l'environnement, y compris de la plateforme sous-jacente. Même les machines

virtuelles sont démarrées via des fichiers chiffrés. Cette approche très prudente n'est pas nécessaire pour tous les scénarios d'hébergement Azure mais elle est à la base du modèle de confiance intentionnellement strict du centre de données virtuel.

- **Conformité**. Les services et l'infrastructure Azure répondent à de nombreux standards de conformité nationaux, internationaux ou liés à certains secteurs d'activité. Pour garantir la sécurité de vos données, Microsoft demande à des audits externes rigoureux de vérifier cette conformité afin de valider le respect par Azure des contrôles de sécurité imposés par ces standards. De plus, un centre de données virtuel utilise de nombreux systèmes de surveillance, de journalisation et de rapports, une grande rigueur d'exploitation, une transparence pour tous les rapports d'audits et des méthodes de tests agressifs développés par une équipe dédiée.

Isolation logique des espaces de travail multiples

Le centre de données virtuel est un espace de noms conceptuel qui regroupe toutes les ressources que vous utilisez dans ce centre de données. Cet espace de noms sert de murs virtuels pour isoler vos ressources des autres locataires de la plateforme et du reste d'Internet.

Les charges de travail, comme les applications métier, sont hébergées dans des espaces de travail distincts et isolés. Ces espaces de travail représentent l'infrastructure et les services d'administration pour déployer en toute sécurité les charges de travail et leurs ressources. Pour favoriser l'agilité des développeurs, ces espaces de travail se créent facilement et rapidement. Les espaces de travail adhèrent aux règles et au contrôle d'accès du centre de données virtuel. Il est possible d'ajouter des règles spécifiques pour certains espaces de travail. Des stratégies configurent les espaces de travail pour router tout le trafic externe via l'infrastructure informatique centrale où des règles organisationnelles s'appliquent. Il est possible de déployer plusieurs charges de travail dans un même espace de travail ou de leur attribuer un espace de travail distinct et isolé à chacune.

Infrastructure partagée de confiance

Pour utiliser un centre de données virtuel comme une extension digne de confiance d'un centre de données physique, vous devez connaître le niveau de contrôle que vous avez sur vos ressources, et le degré de confiance que vous placez sur des éléments spécifiques de la plateforme. La plateforme sous-jacente Azure assume toutes les responsabilités de la sécurité et de la maintenance de l'infrastructure physique. Dans un centre de données traditionnel sur site, c'est votre organisation qui assume ces responsabilités. En plus de cette responsabilité pour les matériels physiques de votre centre de données, vous devez aussi accorder votre confiance à la plateforme Azure qui vous fournit les contrôles et les outils

d'administration pour construire des solutions sécurisées dans un Cloud mutualisé.

En ce qui concerne la conformité, Microsoft élabore des produits qui facilitent la vie de ses clients. La plateforme Azure a reçu le plus grand nombre de certificats de conformité aux différentes normes industrielles et ce nombre continue de croître chaque année. Toutefois, si Microsoft assure la conformité au niveau de la plateforme, il est de votre responsabilité d'assurer la conformité des applications que vous créez sur la plateforme.

L'outil Microsoft Compliance Manager répertorie, dans une transparence totale, les contrôles gérés par la plateforme et ceux qui sont sous votre responsabilité. Cet outil vous aide aussi à comprendre comment s'applique la conformité sur ces contrôles. Qu'il s'agisse d'appliquer une configuration de la plateforme, comme le chiffrement ou une authentification à plusieurs niveaux, ou d'appliquer un article de la base de connaissances sur un processus comme l'affectation de rôles, l'objectif reste le même.

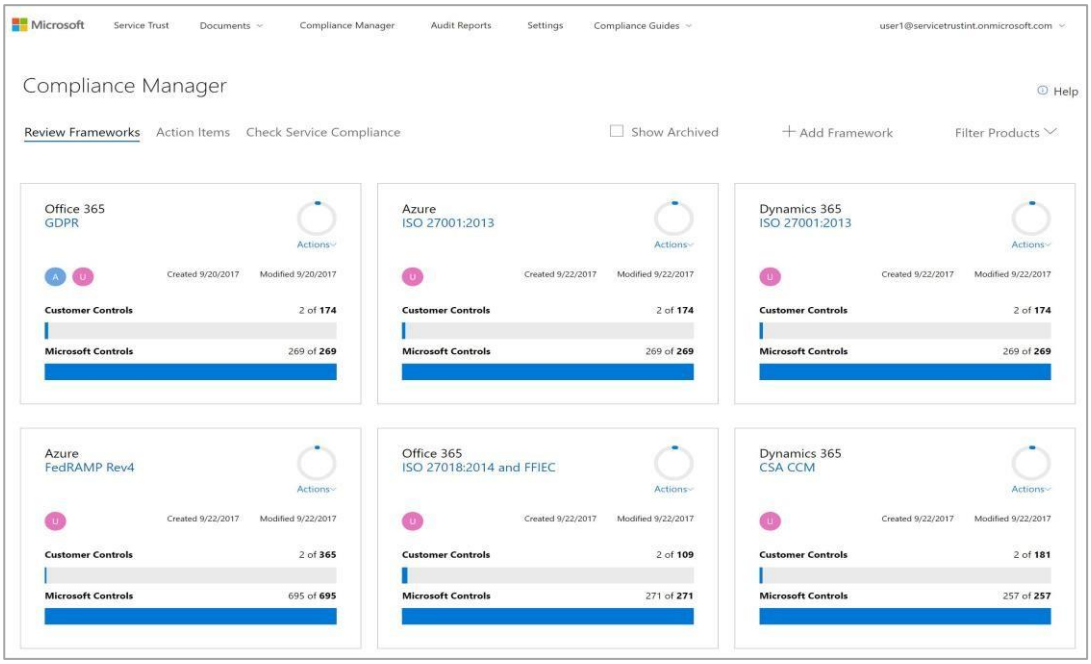

Figure 3. Le tableau de bord de l'outil Microsoft Compliance Manager.

Plateforme globale

Azure organise sa plateforme en différentes régions géographiques. Chaque région contient un ou plusieurs centres de données relativement proches les uns des autres afin de permettre des scénarios très fiables de basculement (haute disponibilité) entre centres, suite à un incident majeur. La carte du monde ci-dessous montre les centres de données Azure (à jour en octobre 2017) sur les différents continents. Cela vous permet de fournir vos solutions près de vos clients et de vos employés, et d'être présents sur de nouveaux marchés géographiques.

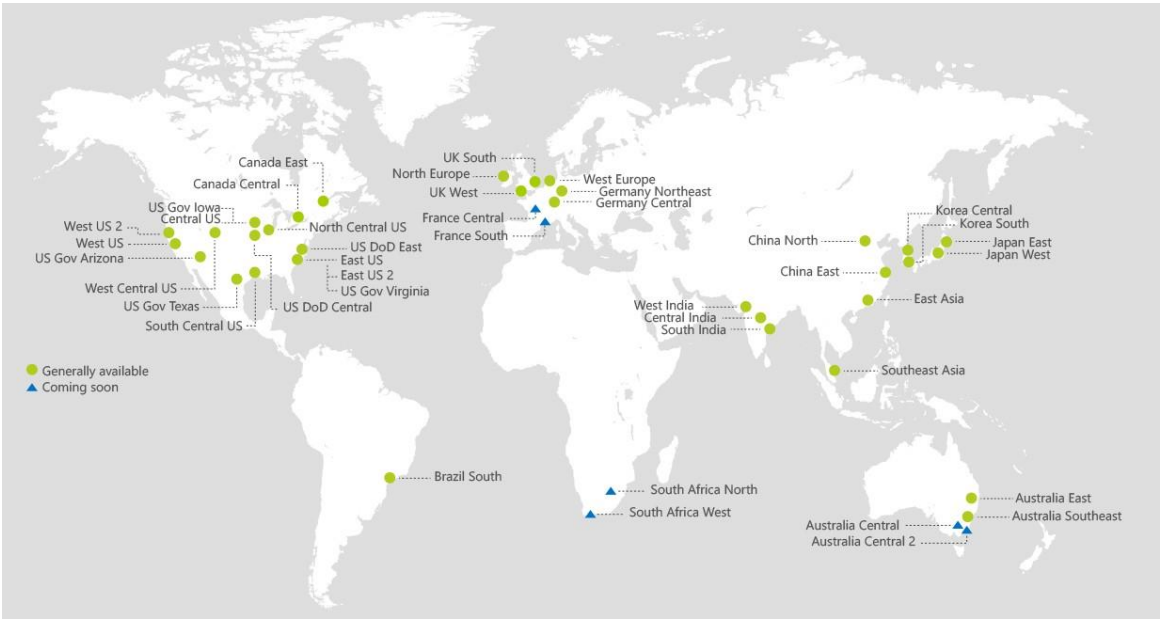

Figure 4. La plateforme Azure repose sur un nombre grandissant de centres de données dans le monde.

Les centres de données Azure contiennent des ordinateurs, des baies de stockage et des composants réseau comme n'importe quel centre de données physique traditionnel, mais à plus grande échelle. À un facteur d'échelle près, les mêmes impératifs de contrôle d'accès, de sécurité et de maintenance que vous appliquez déjà à votre centre de données physique, s'appliquent aux centres de données Azure. La principale différence est que ces impératifs sont régis par les équipes des centres de données Azure plutôt que par vos équipes.

Azure se répartissant dans le monde entier, l'aspect de la souveraineté des données peut poser un problème nouveau que vous ne connaissiez pas avec votre infrastructure sur site. Il est possible d'appliquer des stratégies de gouvernance à vos abonnements Azure pour que les ressources (vos données) ne soient déployées que dans certaines régions afin de répondre à vos impératifs de lieux de résidence de vos données. Pour définir la région Azure qui vous convient, visitez le site Web des centres de données Azure.

Infrastructure régionale

Pour permettre des scénarios de continuité métier et de récupération suite à un incident majeur, chaque région Azure est couplée à une région complémentaire sur le plan géopolitique (par exemple, la région Europe du Nord est couplée avec la région Europe de l'Ouest). Ces paires de régions (à l'exception du Brésil, de l'Asie de l'Est et d'Asie du Sud-Est) offrent la même souveraineté et les mêmes conditions de résidence des données pour les deux membres de chaque paire. Le fait de dupliquer les ressources entre des régions appariées réduit le risque que des désastres naturels, des guerres civiles, des coupures électriques ou des pannes des réseaux physiques affectent les deux régions en même temps.

Azure divise ensuite les régions en différentes zones de disponibilité, c'est-à-dire des environnements connectés à faible latence capables de prendre en charge des applications à haute disponibilité. Les zones de disponibilité protègent contre des pannes de courant potentielles dans un centre de données ou une région spécifique.

Par défaut, les ressources d'un centre de données virtuel existent dans une seule région Azure. Cela renforce la sécurité des connexions entre composants et réduit la latence du réseau. Comme vous dupliquez votre centre de données physique sur un autre site pour créer une infrastructure à haute disponibilité, il est possible de créer des instances du centre de données virtuel dans différentes régions. Les applications qui s'exécutent dans un espace de travail peuvent profiter de toutes les fonctionnalités de haute disponibilité Azure à l'intérieur d'une région ou entre régions. Par exemple, en utilisant un couplage VNet global, il est possible d'étendre le centre de données virtuel à n'importe quelles régions. Des fonctionnalités, comme la duplication géographique des bases de données SQL, permettent de synchroniser plusieurs instances de charges de travail actives, ce qui garantit leur disponibilité.

Confiance via l'isolation

Dans l'environnement mutualisé du Cloud, votre abonnement constitue le premier niveau d'isolation car il est lié à l'annuaire Azure Active Directory (Azure AD). Azure AD isole les informations d'identité et authentifie les utilisateurs pour leur donner accès à des ressources via leur abonnement. Azure AD prend en charge une authentification à plusieurs facteurs, technologie fortement recommandée qui constitue un deuxième niveau de sécurité pour l'authentification.

Les rôles Azure AD sont essentiels pour un centre de données virtuel qui utilise le contrôle d'accès basé sur les rôles (RBAC). RBAC contrôle l'accès à des ressources comme des services, des machines virtuelles, du stockage et des bases de données. RBAC autorise l'accès à une ressource pour un utilisateur, un groupe ou un rôle défini dans Azure AD. Cependant, les paramètres d'une ressource sont souvent régis par la configuration interne de cette ressource, pas par RBAC. Par exemple, l'accès au système d'exploitation d'une machine virtuelle est configuré dans ce système d'exploitation.

En plus du verrouillage des autorisations et des contrôles d'accès, des verrous de lecture seule ou contre l'effacement peuvent être posés sur des ressources individuelles ou sur des ensembles nommés groupes de ressources. Par exemple, les administrateurs centraux peuvent appliquer un verrou en lecture seule sur un réseau virtuel : les utilisateurs ou d'autres ressources peuvent utiliser ce réseau mais ne peuvent pas le modifier. Autre exemple : le propriétaire d'un espace de travail peut appliquer un verrou contre l'effacement sur une machine virtuelle dans son espace de travail ; l'équipe DevOps peut configurer cette machine mais ne peut pas la supprimer.

Quel que soit le niveau d'isolation et de sécurité appliqué à une ressource ou à un groupe de ressources, toute tentative d'accès, de modification ou de suppression d'une ressource est enregistrée dans un fichier journal d'audit. Le journal d'activité Azure enregistre toutes les activités sur les ressources, y compris les actions, les acteurs et les échecs et réussites d'actions.

Une autre façon d'isoler les ressources est d'activer le contrôle d'accès juste-à-temps des machines virtuelles. Cette fonctionnalité recommandée limite la durée pendant laquelle un point de terminaison d'administration, lié à une machine virtuelle, reste ouvert. Verrouiller le

trafic entrant de cette façon est une fonctionnalité particulièrement importante pour toutes les machines virtuelles utilisées à des tâches d'administration dans le centre de données virtuel.

Comme pour un centre de données sur site, des tests de sécurité doivent être régulièrement menés sur les ressources hébergées par Azure, via des processus automatisés et des examens manuels. Ces tests incluent le balayage de ports, des tentatives de pénétration et des tests aléatoires. L'Azure Security Center regroupe des fonctionnalités de prévention, de détection et de réponse aux menaces, intégrées dans Azure, et inclut des outils de limitation des risques comme la protection contre les logiciels malveillants dans les machines virtuelles.

Voir aussi :

Introduction à la sécurité d'Azure

Isolation dans le Cloud public

Sécurité du réseau Azure

Vue d'ensemble de la sécurité des machines virtuelles Azure

Guide de la sécurité du stockage Azure

Centre Microsoft de gestion de la confidentialité – Conception et sécurité opérationnelle

Confiance via le chiffrement

Le modèle du Datacenter Virtuel Azure considère le chiffrement comme une priorité absolue. Toutes les données devraient être chiffrées en permanence, qu'elles soient en cours de transfert ou stockées.

Le Coffre de clés Azure est le principal mécanisme qui stocke et gère les clés, les jetons secrets et les certificats associés aux processus avec non-reniement de chiffrement, d'authentification et de cryptographie dans le centre de données virtuel.

Toutes les clés de chiffrement, les chaînes de connexion, les certificats et autres jetons secrets utilisés par des applications et des ressources dans le centre de données virtuel doivent être gérés et stockés avec les plus grandes précautions. Le coffre de clés Azure adopte une sécurité matérielle de niveau 2, répondant à la norme FIPS 140-2, et vous permet de générer des clés en utilisant votre propre sécurité matérielle sur votre site, et de les transférer ensuite en toute sécurité dans le coffre de clés.

Les clés stockées dans le coffre servent à chiffrer les données stockées et à sécuriser des applications et des services PaaS. Par exemple, la chaîne de connexion à une base de données peut être stockée dans le coffre de clés, ce qui est bien plus sûr que dans un fichier de configuration de l'application ou dans une variable d'environnement. Les services et les applications autorisés dans le centre de données Azure peuvent utiliser les clés stockées dans le coffre mais ne peuvent pas les modifier. Seul le propriétaire d'une clé peut la modifier dans le coffre.

Données en transit

Le modèle du Datacenter Virtuel Azure utilise le chiffrement pour renforcer l'isolation des données lors de leurs transferts :

- Entre les réseaux sur site et le centre de données virtuel. Les données passent via une connexion VPN chiffrée de site à site ou une connexion isolée et privée ExpressRoute.
- Entre des applications qui s'exécutent dans des centres de données virtuels différents.
- Entre des applications qui s'exécutent dans un même centre de données virtuel.
- Entre des services de plateforme, y compris des points de terminaison internes et externes, des API d'administration, des bases de données et des comptes de stockage.

Dans tous ces scénarios, l'approche du Datacenter Virtuel Azure utilise les protocoles SSL/TLS pour échanger des données entre le centre de données virtuel et les composants des applications. Tout le trafic réseau est chiffré en permanence. De plus, toutes les communications entre les composants internes d'Azure, à l'intérieur même du centre de données virtuel, sont protégés par SSL/TLS et par un pare-feu dans l'infrastructure centrale.

Données stockées

Les données stockées sont aussi chiffrées, notamment celles placées dans le stockage Azure et celles des bases de données relationnelles, ces dernières pouvant bénéficier d'un chiffrement additionnel. Par exemple, une base de données Azure SQL inclut le chiffrement transparent des données.

L'infrastructure centrale utilise le Stockage Azure pour différentes tâches, notamment pour enregistrer les journaux. Le chiffrement du service de stockage assure le chiffrement pour tous les services de stockage Azure en chiffrant les données avant de les écrire dans les baies de stockage. Ce mécanisme déchiffre les données après leur lecture, juste avant leur utilisation. Les comptes de stockage Azure qui utilisent ce chiffrement, bénéficient de fonctionnalités de chiffrement, de déchiffrement et de gestion des clés, totalement transparentes pour les utilisateurs. Toutes les données sont chiffrées par le protocole AES avec des clés de 256 bits. Les clés peuvent être gérées par Microsoft ou par le client.

Le chiffrement de l'image disque d'une machine virtuelle est important pour assurer l'isolation et la sécurité d'une machine virtuelle dans un environnement mutualisé. Le modèle de Datacenter Virtuel Azure dépend de la capacité de la plateforme à créer et à héberger des machines virtuelles avec des disques chiffrés, et à y accéder. Azure prend en charge deux modèles de machines virtuelles chiffrées :

- Pour les machines virtuelles crées dans Azure, vous pouvez utiliser le chiffrement de disque Azure. Les fonctionnalités BitLocker de Windows et DM-Crypt de Linux permettent le chiffrement de volume pour des disques de données et pour ceux du système d'exploitation. Azure Marketplace contient des centaines d'images de machines virtuelles préconfigurées que vous pouvez rapidement déployer et chiffrer.
- Vous pouvez aussi chiffrer des machines virtuelles créées sur votre site en utilisant des

hôtes Hyper-V et un chiffrement DM-Crypt ou BitLocker, avec vos stratégies et vos configurations internes. Après avoir validé une image sur votre site, vous pouvez transférer les clés correspondantes dans votre coffre de clés Azure puis déployer l'image disque VHD déjà chiffrée comme machine virtuelle dans Azure.

Données en cours de traitement

Un autre ajout à la plateforme Azure est la prise en charge du traitement confidentiel via des environnements d'exécution approuvés, basés sur des technologies d'enclaves. Les Intel Secure Guard Extensions (SGX) et d'autres technologies d'enclaves permettent aux développeurs de créer des environnements d'exécution sécurisés et approuvés. Une enclave fournit une zone chiffrée pour des données et du code qui ne peuvent être traités que par des mécanismes de sécurité intégrés au processeur.

Microsoft investit aussi largement dans la recherche de nouvelles techniques de chiffrement. Par exemple, le chiffrement homomorphique permet de chiffrer des données pour les stocker ensuite dans un Cloud non sûr. Les applications peuvent utiliser ces données sans avoir besoin de les déchiffrer au préalable. Pour en savoir plus sur l'utilisation du chiffrement homomorphique dans un contexte de bioinformatique, lisez le document de Microsoft Research, Manual for Using Homomorphic Encryption for Bioinformatics.

Voir aussi :

Chiffrement dans le Cloud Microsoft

Qu'est le coffre des clés Azure ?

Chiffrement pour le service de stockage Azure

Chiffrement de disque Azure pour des machines virtuelles Windows et Linux

DEUXIÈME PARTIE COMMENT CONTOSO COMPOSE UN CENTRE DE DONNÉES DE CONFIANCE

Les centres de données virtuels introduisent de nouveaux défis pour l'administration des services. Associés aux principes du Datacenter Virtuel Azure, de bonnes procédures d'administration informatique aident les entreprises à profiter de tous les avantages d'un Cloud public, comme l'administration en libre-service, la capacité à monter en charge et l'élasticité (adaptation des ressources aux besoins).

Cette section décrit une mise en œuvre de référence pour Contoso, une entreprise fictive de services financiers. Elle s'inspire d'engagements réels d'organisations internationales qui ont réussi leur transition vers le Cloud tout en respectant les contraintes réglementaires imposées.

Contrôle d'accès centralisé et espaces de travail connectés

Le centre de données virtuel de Contoso définit un ensemble centralisé de fonctionnalités d'administration et de sécurité informatiques. Contoso souhaite que ses différents départements puissent déployer des charges de travail avec l'agilité et la flexibilité qui caractérisent les solutions Azure, tout en respectant les règles du service informatique central. L'infrastructure de base est prise en charge par une architecture réseau hub-and-spoke (en étoile) qui relie l'infrastructure centrale aux charges de travail.

L'entreprise désire mettre en place une connexion privée rapide entre le centre de données virtuel et ses réseaux sur site. Elle ne souhaite pas autoriser un accès direct à Internet ou à des réseaux externes autres que le sien. Tout le trafic Internet doit passer via le réseau sur site qui applique des restrictions de sécurité et des stratégies particulières.

La figure 5 montre leur proposition initiale. L'architecture finale adoptée par Contoso apparaît à la figure 11 à la fin de cette section.

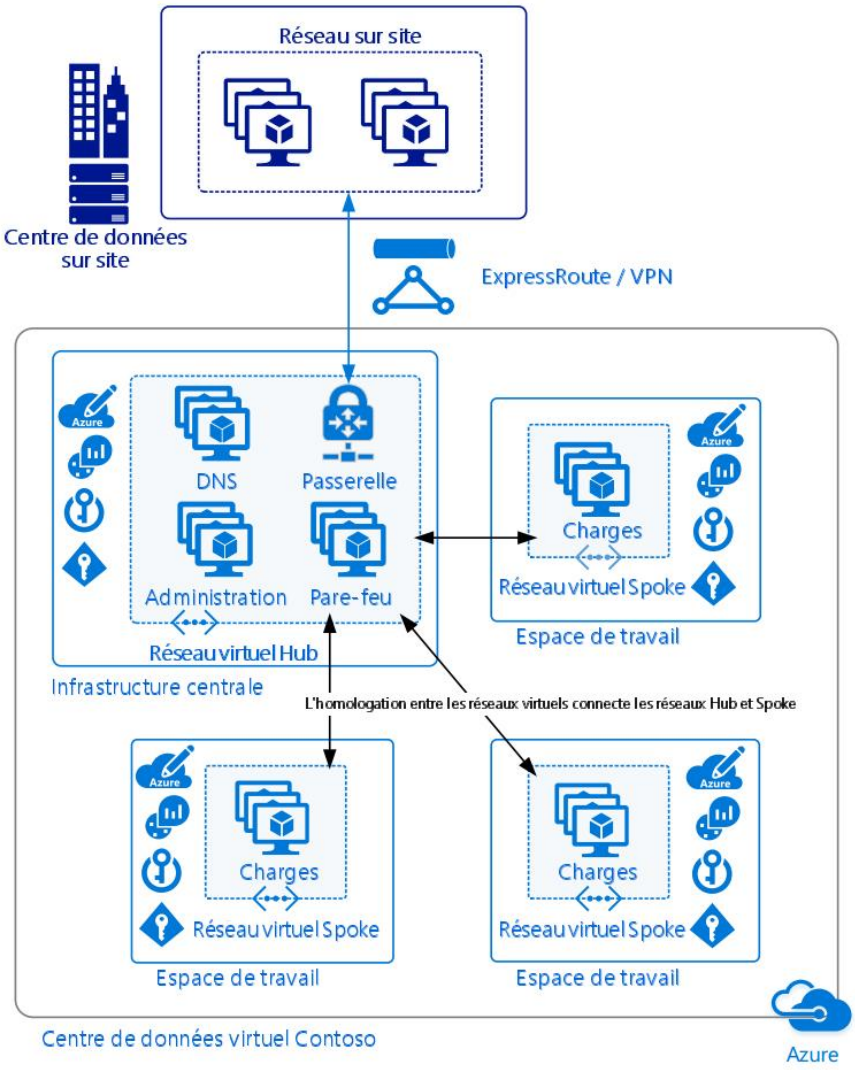

Figure 5. Architecture à haut niveau proposée par Contoso pour son centre de données virtuel.

Connectivité sur site

Pour éviter d'envoyer du trafic sur l'Internet public, Contoso souhaite mettre en place une connexion dédiée privée entre son réseau sur site et le centre de données virtuel. Le modèle du Datacenter Virtuel Azure pend en charge deux méthodes pour connecter un réseau sur site à un centre de données virtuel :

- ExpressRoute utilise une connexion dédiée, privée, fournie par un opérateur de télécommunications.
- Des passerelles VPN Azure créent une connexion de site à site qui transfère un trafic chiffré sur l'Internet public.

Contoso choisit une connexion ExpressRoute qui offre une plus grande fiabilité, des vitesses plus élevées et une latence plus faible que les connexions habituelles via Internet. ExpressRoute crée un lien direct entre Azure et le réseau sur le site de l'entreprise. Toutefois, les connexions ExpressRoute sont longues à acheter et à installer. En attendant qu'ExpressRoute soit opérationnel, Contoso peut immédiatement mettre en place une passerelle VPN, mécanisme couramment utilisé par de nombreuses entreprises pour exploiter rapidement les ressources Azure.

Lorsque la connexion ExpressRoute sera en place, Contoso convertira sa passerelle VPN en connexion de secours, dans l'éventualité d'une panne de la liaison ExpressRoute. Contoso pourrait aussi utiliser la connexion VPN comme route secondaire pour des charges de travail qui n'ont pas besoin de la vitesse élevée et de la faible latence d'ExpressRoute.

Séparation des responsabilités dans le centre de données

Contoso souhaite que la séparation des responsabilités qui existe dans l'exploitation sur site, se retrouve dans le centre de données virtuel. Pour organiser les responsabilités de chacun, Contoso a défini des rôles et les a affectés à des personnes physiques via le service d'annuaire sur site. L'annuaire Azure AD reprend ces rôles dans Azure. Ils peuvent donc servir dans la définition de règles d'accès à des ressources du centre de données virtuel.

Le mécanisme RBAC (contrôle d'accès basé sur des rôles) permet à Contoso d'affecter des équipes différentes à diverses tâches d'administration du centre de données virtuel. L'informatique centrale conserve le contrôle de toutes les fonctionnalités de base de sécurité et d'accès mais elle utilise aussi une approche distribuée qui permet à des développeurs et à d'autres équipes de contrôler des charges de travail spécifiques.

Tout changement significatif des ressources ou de l'infrastructure implique la concertation de plusieurs rôles ; ainsi, plus d'une personne doit valider un quelconque changement. Cette séparation des responsabilités limite la possibilité qu'une personne isolée accède à des données sensibles ou introduise des vulnérabilités sans que cela ne soit connu des autres membres d'une équipe.

Par exemple, la personne de l'équipe Exploitation réseau, responsable de l'infrastructure du

réseau central, doit approuver certaines demandes d'infrastructure de la personne de son équipe qui supervise le réseau virtuel d'une application spécifique. Contoso a décidé que ces deux rôles similaires seraient séparés entre l'équipe centrale qui supervise les composants communs de l'architecture (Corporate NetOps) et toutes les personnes qui supervisent les déploiements individuels d'applications (Application NetOps). Par ailleurs, ils adoptent la même approche pour les opérations de sécurité et pour les autres rôles. Contoso peut administrer de façon centralisée les stratégies de l'entreprise tout en permettant à des équipes d'applications d'innover autour de ces stratégies.

Rôles d'administration

Le service informatique actuel de Contoso gère essentiellement les activités relatives à la conformité, aux configurations et aux audits. Pour gérer ces activités pour le nouveau centre de données virtuel, Contoso répartit les employés de ses équipes d'administration du service central et des applications selon les rôles suivants :

Groupe	Nom courant du rôle	Responsabilités
Sécurité	SecOps (opérateurs de la sécurité)	Assurent une surveillance générale de la sécurité. Établissent et appliquent une stratégie de sécurité, comme le chiffrement du stockage. Gèrent les clés de chiffrement. Gèrent les règles du pare-feu.
Réseau	NetOps (opérateurs réseaux)	Gèrent la configuration et l'exploitation des réseaux virtuels du centre de données virtuel, comme les routes et les couplages.
Système	SysOps (opérateurs systèmes)	Définissent des options de l'infrastructure de stockage et de traitement, et gèrent les ressources déployées.
Développement, test et exploitation	DevOps (développeurs)	Construisent des applications et des fonctionnalités pour des charges de travail. Gèrent des fonctionnalités et des applications pour assurer les niveaux de service (SLA) et d'autres standards de qualité. Les rôles DevOps ne sont généralement pas utilisés dans l'infrastructure centrale.

Selon les principes du Datacenter Virtuel Azure, l'accès et la sécurité des ressources de chaque espace de travail doivent être pris en charge par des groupes spécifiques à chaque espace de travail, indépendamment des groupes de l'infrastructure centrale. Les équipes des charges de travail gèrent leurs propres ressources, déploient des solutions et créent des stratégies d'accès tandis que les équipes de l'infrastructure centrale gardent le contrôle général du centre de données virtuel et des communications entrantes et sortantes.

Chaque groupe devrait avoir un nom unique, facilement compréhensible, qui indique la section du centre de données dont il est responsable. Contoso crée une nomenclature pour différencier les rôles associés à la gestion des services centraux du centre de données virtuel, des rôles associés à la gestion des espaces de travail et des charges de travail.

Groupes de l'infrastructure	Groupes spécifiques aux espaces de travail
CorpSecOps CorpNetOps CorpSysOps CorpDevOps	AppSecOps AppNetOps AppSysOps AppDevOps
	où « App » est un préfixe descriptif de l'espace de travail, par exemple NAVNetOps pour un espace de travail hébergeant une application métier Dynamics NAV.

Gestion des identités avec Azure AD

Contoso souhaite définir des identités communes pour gérer des ressources dans leur centre de données virtuel. Pour cela, Contoso prévoit d'intégrer son service d'annuaire sur site dans Azure AD. Azure AD Connect assure la synchronisation des utilisateurs et des rôles entre le service Active Directory sur site de Contoso et le service Azure AD associé au centre de données virtuel.

Des applications et des charges de travail individuelles hébergées dans les espaces de travail du centre de données virtuel peuvent, ou non, utiliser le partage des identités, mais toutes les ressources Azure utiliseront Azure AD pour le contrôle d'accès.

Voir aussi :

Solutions d'identités hybrides Microsoft

Fédération et connexion Azure AD

Stratégie en différentes couches

La stratégie globale se répartit en différentes couches, en utilisant les composants décrits dans la première partie de ce document : réseau défini par logiciel, chiffrement, gestion des identités et conformité.

Architecture proposée pour Contoso

Le cœur du centre de données virtuel de Contoso est une infrastructure centrale à travers

laquelle circule tout le trafic réseau. Sur cette infrastructure de base, s'appliquent des stratégies et une surveillance centrale. Cette infrastructure est segmentée dans son propre environnement ; elle fournit des services centraux de réseau et de sécurité, y compris un hub réseau virtuel qui établit les connexions avec les autres parties du centre de données. Elle gère aussi toutes les connexions externes utilisées par des ressources hébergées en dehors du centre de données virtuel.

Des espaces de travail isolés sont mis en place pour prendre en charge divers déploiements de charges de travail comme Microsoft SharePoint ou des services SAP. Chaque espace de travail a ses propres ressources d'administration et sa propre infrastructure de réseau virtuel en étoile. Les équipes peuvent ajouter d'autres stratégies pour contrôler les accès et l'utilisation des ressources dans leur propre espace de travail, tant que ces stratégies ne sont pas en contradiction avec les stratégies centrales.

L'infrastructure centrale et chaque espace de travail sont créés comme autant d'abonnements Azure distincts. Cette décision est prise pour accroître la flexibilité des charges de travail et pour éviter d'atteindre les limites d'un abonnement unique. Chaque abonnement est associé au client principal qui gère Azure AD, mais les équipes peuvent aussi définir des stratégies et des contrôles d'accès spécifiques à leurs espaces de travail. Par exemple, un contrôle d'accès basé sur les rôles (RBAC) au niveau d'un espace de travail permet à une équipe de déployer des ressources spécifiques à des charges de travail ou à des projets. Si une équipe souhaite déployer plusieurs charges de travail dans son espace de travail, elle peut le faire sans avoir besoin d'abonnement supplémentaire. L'application des stratégies globales définies au niveau de toute l'organisation, s'effectue sur tous les abonnements de l'entreprise.

L'infrastructure centrale du centre de données virtuel de Contoso inclut les éléments suivants :

- Définition de la stratégie de sécurité et des paramètres de supervision au niveau des abonnements.
- Définition de la stratégie réseau et des paramètres de supervision au niveau des abonnements.
- Toutes connexions sur les réseaux internes sur site ou sur Internet.
- Réseau virtuel du hub central, via lequel doit passer tout le trafic entre les charges de travail dans le Cloud et le réseau interne sur site.
- Pare-feu central qui, en accord avec le modèle d'extension approuvé, inspecte et redirige tout le trafic passant via le centre de données virtuel vers le réseau sur site.
- Outils d'exploitation et services d'administration partagés utilisés par le centre de données virtuel.

Les espaces de travail incluent les éléments suivants :

- Paramètres de stratégie du Gestionnaire de ressources, qui empêchent un accès direct aux réseaux externes et routent le trafic via l'infrastructure centrale.
- Réseau virtuel en étoile de l'espace de travail.
- Outils d'exploitation spécifiques aux charges de travail comme des outils de

journalisation ou de gestion des clés.

- Ressources des charges de travail.

Configuration initiale de l'environnement

Avant de créer des abonnements pour les espaces de travail, Contoso configure son compte Azure AD. Ce compte est créé lors de la signature du contrat Accord Entreprise Azure entre Contoso et Microsoft. Il servira pour l'authentification et le contrôle d'accès sur l'ensemble du centre de données virtuel. Contoso intègre la gestion des identités entre Azure AD et son installation d'Active Directory sur site, et utilise pour cela Azure AD Connect qui synchronise les informations de sécurité et les comptes entre les deux environnements.

Des abonnements pour l'infrastructure centrale et pour les différents espaces de travail sont ensuite créés par l'Administrateur du compte Azure de Contoso, qui vérifie que tous les abonnements créés pour le centre de données virtuel sont associés au compte principal Azure AD de l'organisation.

Lorsqu'un abonnement est créé, les rôles standards SecOps, NetOps, SysOps et DevOps correspondant à cet abonnement, sont ajoutés à Azure AD et reçoivent les autorisations appropriées.

Organisation de l'infrastructure centrale et des espaces de travail

Contoso organise les abonnements de l'infrastructure centrale et des espaces de travail en groupes de ressources fonctionnels. Contoso utilise des stratégies du Gestionnaire de ressources pour définir des règles sur les ressources qui pourront être déployées via ce gestionnaire. Ces stratégies peuvent aussi s'appliquer au niveau d'un groupe de ressources. Par exemple, il est possible d'appliquer des stratégies à un groupe de ressources créé pour des développeurs, afin de permettre la création de machines virtuelles et d'empêcher la création de ressources réseau ou de comptes de stockage. Les groupes de ressources servent aussi au contrôle d'accès. Contoso attribue des rôles spécifiques à certains groupes de ressources tout en leur interdisant d'accéder à un abonnement plus large.

Contoso créera les groupes de ressources suivants dans l'abonnement de l'infrastructure centralisée :

Groupe de	Description
Réseau	Contient le réseau virtuel et les stratégies qui y sont liées comme les routes personnalisées définies par des utilisateurs (UDR) et des groupes de sécurité réseau (NSG) utilisés par l'infrastructure centrale.
Opérations	Services de gestion des hôtes pour l'infrastructure centrale tels que les espaces de travail Microsoft Operations Management Suite (OMS) et les services de surveillance du réseau.

Coffre des clés	Donne accès au coffre des clés de l'infrastructure centrale.
Services partagés	Contient des machines virtuelles fournissant des services, comme le DNS, au centre de données virtuel.
Pare-feu central	Contient le pare-feu central assurant un filtrage sur le trafic sortant au niveau des couches 4 et 7 de la pile TCP/IP.
Administration	Contient les machines virtuelles qui assurent les fonctionnalités Jumpbox pour l'administration.

La répartition des groupes de ressources dans les espaces de travail dépend des besoins des charges de travail individuelles, mais Contoso fournira à chaque espace de travail, lors de sa création, les groupes suivants :

Groupe de	Description
Réseau	Contient le réseau virtuel, les NSG correspondants et les stratégies de routage personnalisées utilisées par l'espace de travail.
Opérations	Héberge des services d'administration propres à l'espace de travail tels que les espaces de travail OMS et les services de contrôle réseau.
Coffre des clés	Donne accès au coffre des clés spécifique à l'espace de travail.

Stratégies du Gestionnaire de ressources

Les stratégies de base du Gestionnaire de ressources définies pour un abonnement et pour des groupes de ressources sont héritées par toutes les ressources à l'intérieur de ce périmètre. Le centre de données virtuel Contoso implante les stratégies suivantes à la fois dans l'infrastructure centrale et dans tous les espaces de travail :

Stratégies	Description
Refuser toute adresse IP publique	Empêche la création d'un nouveau point de terminaison IP public. Pour les espaces de travail, cette stratégie s'applique au niveau de l'abonnement. L'infrastructure centrale applique cette stratégie sur tous les groupes de ressources et permet au propriétaire de l'abonnement d'ajouter une adresse IP publique pour établir, si nécessaire, une connexion VPN.
Imposer le chiffrement du stockage	Impose à tout compte de stockage créé d'utiliser le chiffrement. Cette stratégie s'applique au niveau de l'abonnement, pour l'infrastructure centrale et pour tous les espaces de travail.

Restreindre les régions autorisées	Restreint la création de ressources dans l'abonnement, à des régions Azure spécifiques. Contoso limite le déploiement de ressources à des régions situées aux États-Unis. Cette stratégie s'applique au niveau de l'abonnement, pour l'infrastructure centrale et pour tous les espaces de travail.

Configuration du coffre des clés

Avec la stratégie *Imposer le chiffrement du stockage* en place pour tous les abonnements, Contoso a besoin de stocker en toute sécurité les clés de chiffrement avant de déployer du stockage ou des machines virtuelles.

Après avoir créé des groupes de ressources, Contoso met en place un coffre des clés pour chaque environnement : les abonnements de l'infrastructure centrale et de chaque espace de travail. Lorsque cela est réalisé, une clé de chiffrement est créée et stockée dans chaque coffre. Elle servira aux opérations de chiffrement du stockage. Un compte de stockage chiffré est créé dans le groupe de ressources Coffre des clés pour stocker les informations de journalisation et d'audit relatives au coffre.

La modification des accès à ces clés et aux informations secrètes du coffre est restreinte au CorpSecOps ou à un rôle spécifique SecOps pour une charge de travail. D'autres rôles peuvent utiliser les clés pour chiffrer et déchiffrer le stockage et accéder à des machines virtuelles chiffrées, mais ces rôles ne peuvent ni modifier ces clés ni accéder d'une quelconque manière à d'autres clés.

Configuration du réseau virtuel du hub

Contoso implante le hub de l'infrastructure centrale et les différentes espaces de travail (les rayons autour du hub) de leur centre de données virtuel sous la forme de réseaux virtuels distincts, chacun résidant dans son abonnement respectif. La conception du réseau virtuel repose sur la topologie en étoile hub-spoke proposée dans le document Centre de données virtuel dans le réseau Azure. Le groupe CorpNetOps de Contoso configure un couplage de réseaux virtuels pour assurer une connectivité de base entre le hub de l'infrastructure centrale et les réseaux virtuels des espaces de travail. Si un espace de travail ne respecte plus les règles de conformité, l'infrastructure centrale peut immédiatement couper la connexion de couplage, isolant ainsi les ressources de l'espace de travail affecté du reste du centre de données.

Une stratégie d'infrastructure Contoso nécessite un schéma d'adressage IP cohérent entre tous les réseaux virtuels et le centre de données virtuel. Ce schéma vérifie que les adresses ne se recouvrent pas avec les réseaux sur site, afin que le centre de données virtuel puisse coexister avec les réseaux internes lorsqu'une liaison VPN ou ExpressRoute est établie entre eux. De plus, à l'intérieur du centre de données virtuels, aucun recouvrement ne doit exister entre les plages d'adresses IP pour l'infrastructure centrale et celles des réseaux virtuels des

espaces de travail afin que le routage fonctionne correctement entre le hub central et les branches de l'étoile.

Pare-feu central

L'exfiltration des données constitue une menace majeure pour Contoso. Les administrateurs souhaitent installer un mécanisme de liste blanche au niveau 7 afin de contrôler les données qui sortent du centre de données virtuel. Les administrateurs mettent en place un pare-feu en utilisant une ou plusieurs appliances virtuelles réseaux (NVA) dans l'infrastructure centrale, et tout le trafic sortant d'un espace de travail à destination de l'extérieur doit passer par ce dispositif. Ces appareils virtuels prennent en charge les fonctionnalités sécurité et réseau traditionnellement gérés par des pare-feux physiques.

Via le pare-feu central, l'infrastructure centrale contrôle le trafic entrant et sortant du centre de données virtuel. Le pare-feu central gère les flux réseau à l'intérieur du centre de données et entre les ressources hébergées dans le centre de données virtuel et dans les environnements externes, comme le centre de données sur site.

Les UDR (routes définies par les utilisateurs) sur les sous-réseaux d'un espace de travail routent le trafic sortant vers le pare-feu central.

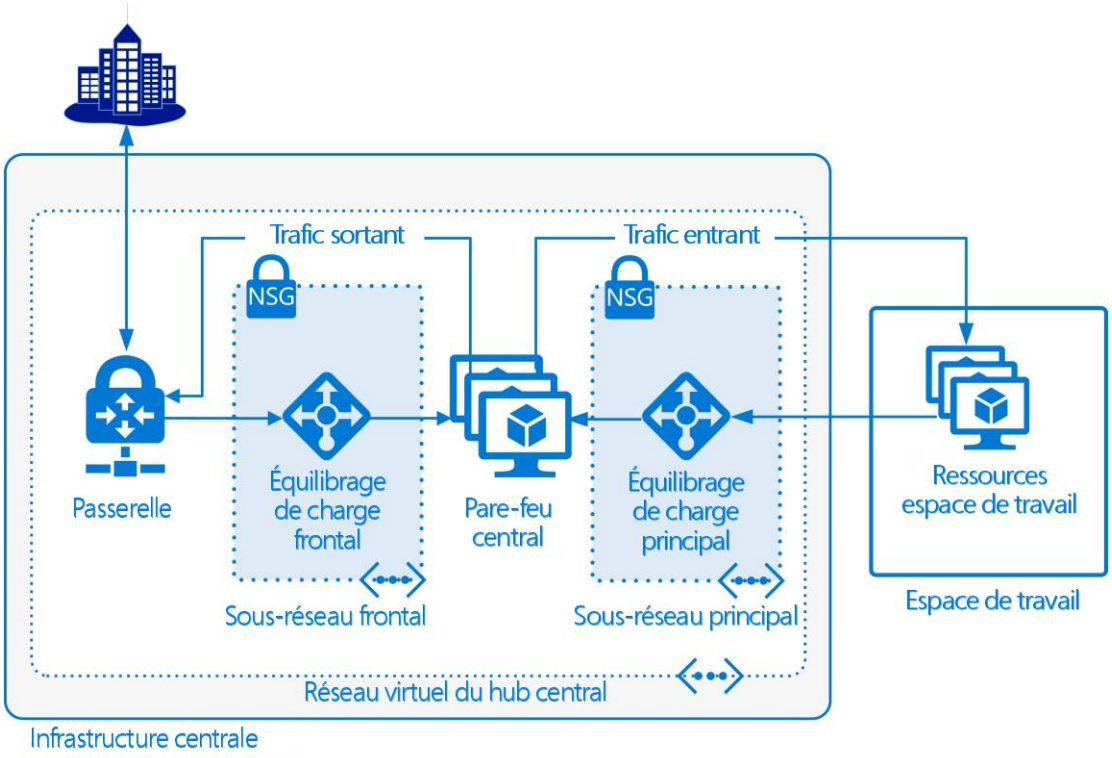

Figure 6. Comment le pare-feu central utilise l'équilibrage de la charge et le routage du trafic.

Contoso s'attend à un trafic important entre son réseau sur site et les charges de travail hébergées dans le centre de données virtuel. Pour y faire face et assurer une redondance, le pare-feu central se répartit sur plusieurs NVA (appliances virtuelles réseau). Deux systèmes d'équilibrage de la charge, qui utilisent la fonctionnalité de ports à haute disponibilité, répartissent le trafic : un système frontal d'équilibrage de la charge prend en charge le trafic en provenance du réseau sur site et destiné aux espaces de travail ; un autre système

d'équilibrage de la charge gère le trafic provenant des charges de travail à destination du réseau sur site.

Voir aussi :

Réseaux sécurisés par des appliances virtuelles

Routes définies par l'utilisateur et transfert IP (IP Forwarding)

Passerelles et réseaux de périmètre

Contoso a besoin de configurer un réseau de périmètre pour fournir une connectivité avec les réseaux du centre de données sur site. Dans un centre de données virtuel, les réseaux de périmètre sont généralement gérés en tant que sous-réseaux du réseau virtuel du hub de l'infrastructure centrale. Lorsque le réseau du hub et le réseau distant ont établi une relation d'approbation entre eux, le réseau de périmètre peut être mis en place en utilisant une simple passerelle qui vérifie que le trafic est correctement routé de et vers le pare-feu central.

Chez Contoso, dans la mise en œuvre du Cloud, une zone démilitarisée (DMZ) n'est pas nécessaire car tout le trafic circule uniquement entre le réseau sur site et le centre de données virtuel. Ce trafic passe soit via une connexion ExpressRoute isolée soit via un VPN sécurisé de site à site. De plus, une stratégie définie au niveau de l'abonnement empêche tout accès public sur le centre de données virtuel lui-même.

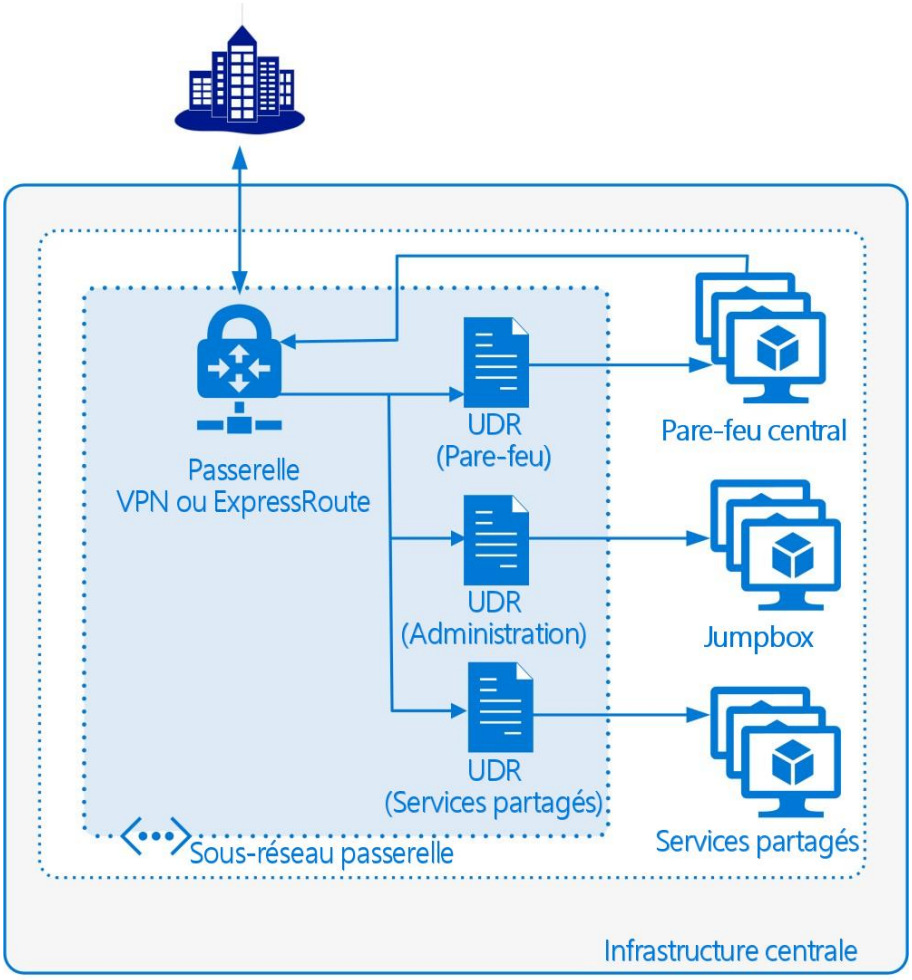

Figure 7. Le sous-réseau de la passerelle route le trafic vers la partie appropriée de l'infrastructure centrale.

Cette passerelle est configurée dans un sous-réseau du réseau virtuel du hub de

l'infrastructure centrale. Le sous-réseau met en œuvre des UDR (routes définies par l'utilisateur) pour envoyer le trafic entrant vers une des trois destinations. Les demandes de ressources d'espaces de travail sont traitées via le pare-feu central. Les demandes d'un administrateur pour accéder à distance afin de configurer des ressources réseau sont transmises aux jumpboxes d'administration. Des demandes de tâches comme une résolution de nom sont routées vers le sous-réseau des services partagés.

Dans tous les cas où le réseau de périmètre est en contact avec une source non approuvée, comme une connexion avec l'Internet public, le modèle du centre de données Azure impose la mise en place d'une zone démilitarisée (DMZ). Pour utiliser cette option, le réseau de périmètre de Contoso devrait inclure des UDR (routes définies par l'utilisateur) pour envoyer le trafic vers des NVA (appliances virtuelles réseau) hébergées sur le sous-réseau de la DMZ (zone démilitarisée). Le trafic est alors traité et seules les demandes approuvées sont orientées soit vers le réseau extérieur soit vers le réseau virtuel du hub de l'architecture centrale, où elles peuvent être transmises au réseau de l'espace de travail approprié.

Voir aussi :

Architectures de référence Azure : Connecter un réseau sur site à Azure

Architectures de référence Azure : DMZ entre Azure et Internet

Administration

Par défaut, le réseau sur le site de Contoso n'a pas d'accès direct aux ressources connectées ou aux réseaux virtuels du centre de données virtuel. Les administrateurs du groupe CorpSecOps doivent configurer le pare-feu central et effectuer d'autres tâches d'administration dans l'infrastructure centrale qui ne sont pas disponibles via le portail Azure ou les API d'administration. Contoso doit donc créer un ensemble de machines virtuelles Jumpbox sécurisées connectées au réseau du hub central. Les administrateurs configureront des règles UDR (routes définies par l'utilisateur) pour permettre à des administrateurs de se connecter à ces machines virtuelles à partir du réseau sur site, et d'accéder directement à des machines virtuelles et à des NVA (appliances virtuelles réseau) hébergées dans le centre de données virtuel.

Les jumpboxes sont créées dans un sous-réseau d'administration, et des règles NSG s'appliquent à ce sous-réseau pour réserver l'accès à des adresses IP spécifiques du réseau sur site. Contoso déploiera deux jumpboxes dans l'infrastructure centrale, en haute disponibilité. Pour accéder à ces machines virtuelles, les administrateurs doivent y être autorisés via le mécanisme de contrôle d'accès juste-à-temps.

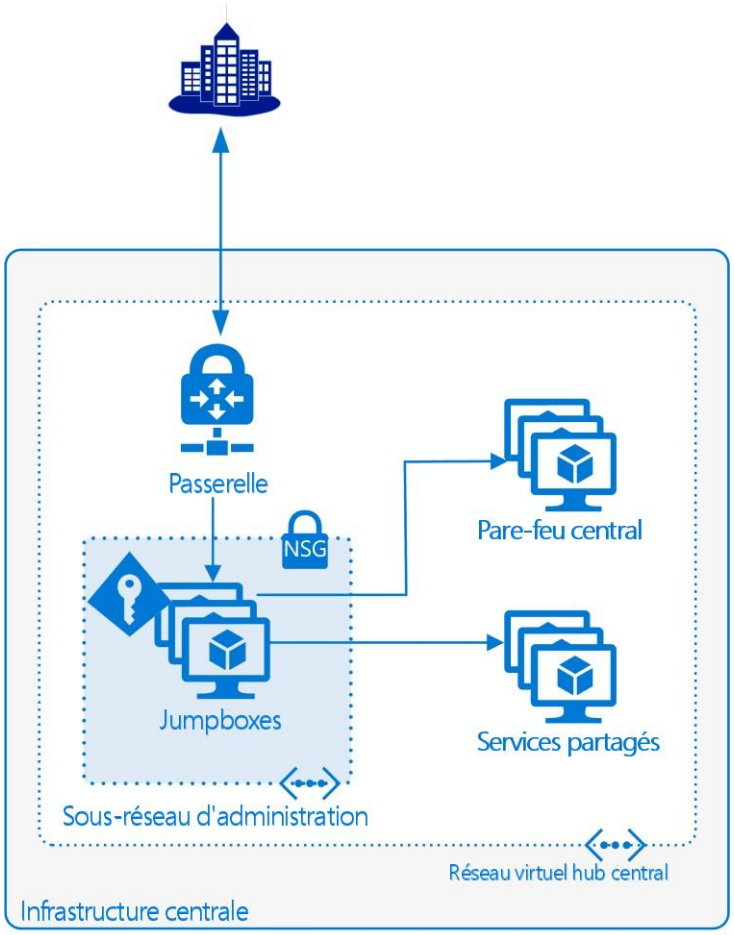

Figure 8. Les administrateurs sur site utilisent des jumpboxes renforcés (hôtes bastions) pour configurer à distance le pare-feu central et gérer les machines virtuelles et les NVA via le réseau virtuel. Des NSG (groupes de sécurité réseau) restreignent l'accès à des ports et à des adresses IP spécifiques.

Voir aussi :

Mise en œuvre d'hôtes d'administration sécurisés

Filtrer le trafic réseau avec des groupes de sécurité réseau

Services partagés

Le sous-réseau des services partagés représente un emplacement central pour déployer des fonctionnalités de base utilisées par les espaces de travail. Par exemple, les charges de travail installées dans le centre de données virtuel ont besoin de résoudre des noms pour des ressources sur site ; et le réseau sur site a besoin de résoudre des noms de ressources du centre de données virtuel. Pour cela, Contoso déploie un service DNS. C'est le premier service partagé mis en place. Contoso souhaite aussi intégrer son infrastructure DNS afin d'utiliser une résolution de noms cohérente entre les environnements sur site et virtuel.

Contoso fournira des services DNS en créant un contrôleur de domaine primaire et un contrôleur de domaine secondaire avec Azure Active Directory Domain Services (Azure AD DS) dans l'environnement de l'infrastructure centrale. Ces contrôleurs de domaine gèreront la résolution de noms pour le centre de données virtuel. Ces serveurs sont configurés pour

transmettre les demandes de résolution de noms en provenance du centre de données virtuel et qui concernent les machines sur site, vers l'environnement sur site et de façon symétrique, les serveurs DNS sur site sont configurés pour transmettre les demandes de résolution de noms des ressources des espaces de travail vers le service partagé DNS du centre de données virtuel.

Voir aussi :

Résolution de noms pour des machines virtuelles et des rôles

Déployer des charges de travail dans des espaces de travail

Dans l'implantation de son centre de données virtuel, Contoso pense en permanence aux développeurs exploitants (DevOps) afin que les équipes soient efficaces et qu'un maximum de processus puisse être automatisé. Les équipes de développement ont besoin d'une intégration continue et de pipelines de déploiement, et toutes les équipes doivent pouvoir contrôler leurs ressources et leurs charges de travail.

Une stratégie du centre de données virtuel de Contoso gère des espaces de travail comme des abonnements distincts, ce qui donne aux équipes des charges de travail un contrôle considérable sur leurs environnements de déploiements. Les développeurs bénéficient de l'agilité d'Azure tout en restant en conformité avec les stratégies de sécurité et d'isolation de Contoso définies au niveau de l'infrastructure centrale.

Rôles d'administration d'un espace de travail

Précédemment, Contoso a défini des rôles spécifiques à un espace de travail, les rôles SecOps, NetOps, SysOps et DevOps. Ces rôles d'administration d'un espace de travail ont le contrôle sur l'abonnement de l'espace de travail et sur toutes les ressources qu'ils déploient dans cet espace, tout en restant dans le cadre des stratégies définies sur l'architecture centrale. Lorsque l'abonnement de l'espace de travail est créé, des stratégies sont définies via le Gestionnaire de ressources, afin de limiter les accès de l'extérieur et de router tout le trafic sortant via l'infrastructure centrale.

Les rôles SecOps et NetOps de l'espace de travail ont la responsabilité de verrouiller les réseaux virtuels de l'espace de travail en fonction des stratégies définies par Contoso pour chaque charge de travail spécifique. Les équipes DevOps bénéficient d'une grande flexibilité pour déployer les ressources d'exploitation dont elles ont besoin pour gérer une charge de travail. Si les activités DevOps nécessitent un accès Internet ou ExpressRoute, le trafic transite par le réseau virtuel du hub central, contrôlé par l'équipe CorpSecOps de l'infrastructure centrale. Des règles doivent être définies sur le pare-feu central pour prendre en compte ce trafic et pour le router vers le réseau sur site. L'équipe CorpSecOps sera responsable de la validation et de l'implantation des mises à jour demandées sur le pare-feu.

Choisir le bon modèle de service pour une charge de travail

Lors de la planification des déploiements des charges de travail, les équipes DevOps décident elles-mêmes quel degré de confiance accorder à la plateforme. Les services Azure permettent de trouver un équilibre entre contrôle et confiance dans la plateforme. Les charges de travail se répartissent en trois grandes catégories : celles qui favorisent le contrôle et la confiance à une extrémité (IaaS), celles qui facilitent l'administration en faisant

confiance à la plateforme (SaaS) et celles situées entre les deux cas précédents, qui considèrent la plateforme comme un service (PaaS).

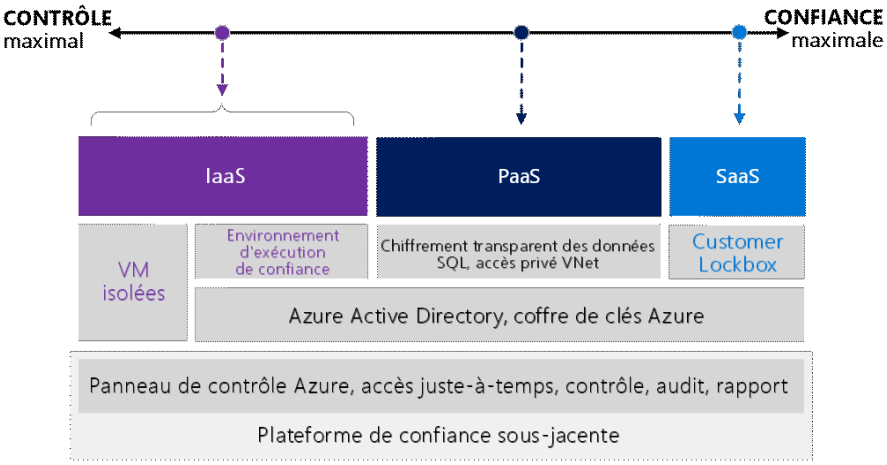

Figure 9. La plateforme Azure propose différentes options pour répondre aux besoins de contrôle dont les DevOps ont besoin lorsqu'ils déploient des charges de travail dans le centre de données virtuel.

Intégration d'un réseau virtuel avec PaaS

Certains départements de Contoso aimeraient exploiter les offres PaaS d'Azure telles que Azure Batch, les bases de données Azure SQL et le stockage Azure. Bien que ces services proposent des fonctionnalités de chiffrement et de sécurité, la plupart d'entre eux utilisent par défaut un point de terminaison public comme point d'accès. Les équipes réseau et sécurité de Contoso préfèrent éviter les services qui utilisent des points de terminaison publics. Elles souhaitent que les services soient accessibles uniquement à partir des réseaux virtuels situés à l'intérieur de l'espace de travail.

Elles intègrent les services Azure dans un réseau virtuel afin d'autoriser un accès privé et sécurisé aux services tels que HDInsight, Azure Batch et le stockage Azure. Deux schémas sont pris en charge. Dans le premier schéma, le service déploie des instances dédiées dans le réseau virtuel. Ces instances ne peuvent être utilisées que par des ressources qui ont accès à ce réseau. C'est le cas pour Azure Batch et HDInsight.

Dans le second schéma, des points de terminaison du réseau virtuel sont une fonctionnalité Azure qui étend les identités et l'espace d'adressage privé d'un réseau virtuel, à des services Azure via une connexion directe. Ce schéma permet de sécuriser des ressources de services en n'autorisant l'accès qu'à partir du réseau virtuel, en fournissant une connectivité privée à ces ressources et en empêchant tout accès depuis des réseaux externes. Les points de terminaison de service utilisent le réseau central Microsoft et permettent de restreindre des ressources PaaS à un unique réseau virtuel, ou à un unique sous-réseau, et d'utiliser des NSG (groupes de sécurité réseau) pour sécuriser encore davantage l'accès au réseau.

Le stockage Azure et la base de données SQL suivent ce schéma. D'autres services Azure suivront également ce schéma à l'avenir.

Voir aussi :

[Intégration d'un réseau virtuel pour des services Azure]

[Annonce de l'intégration d'un réseau virtuel pour le stockage Azure et Azure SQL]

[Points de terminaison de service dans un réseau virtuel]

Audit et journalisation

La gouvernance et le contrôle des charges de travail commencent par la collecte des données de journalisation mais Contoso a aussi besoin de déclencher des actions en fonction d'événements spécifiques. Dans le centre de données virtuel, les stratégies de journalisation des ressources Azure sont activées par défaut.

Différents types de services de contrôle et de journalisation sont disponibles pour suivre le comportement des ressources dans le centre de données virtuel. L'équipe SysOps de Contoso utilise les deux principaux types de journalisation proposés par Azure :

- **Les journaux d'audit** (aussi nommés journaux des opérations) qui montrent les opérations effectuées sur des ressources dans un abonnement Azure. Chaque ressource Azure dans un centre de données virtuel produit des journaux d'audit.
- **Les journaux de diagnostic** sont produits par une ressource et fournissent des données fréquentes et détaillées sur le fonctionnement de la ressource. Le contenu de ces journaux varie selon le type de la ressource.

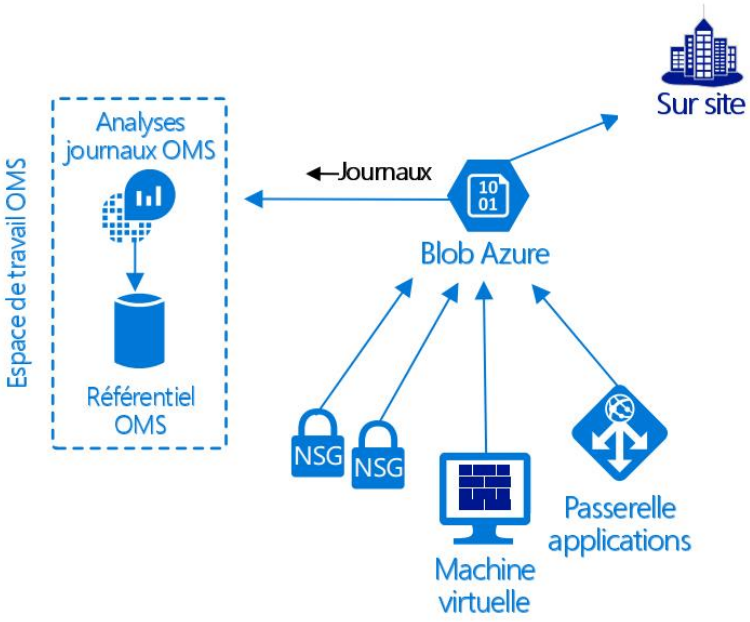

Figure 10. Les activités du centre de données virtuel sont contrôlées et enregistrées en permanence. Les données des journaux sont importées dans OMS et peuvent être exploitées par des analyses sur site.

Contoso souhaite étendre le cadre de contrôle standard déjà en place sur ses systèmes sur site afin d'y intégrer les journaux produits par les ressources du centre de données virtuel. Si les activités de journalisation peuvent rester dans le Cloud, Contoso peut utiliser OMS. Son analyseur collecte les données, analyse leur corrélation, effectue des recherches sur les données des journaux et des performances générées par les systèmes d'exploitation, les applications et l'infrastructure du Cloud.

Voir aussi :

Journalisation et audit dans Azure

Utilisation des outils de surveillance et de sécurité d'Azure

Des contrôles, des audits et des rapports effectués en permanence sont nécessaires pour assurer une bonne gouvernance. Azure fournit à Contoso un vaste ensemble de fonctionnalités d'administration pour que des personnes autorisées puissent surveiller les références de la configuration de la sécurité, les écarts par rapport aux stratégies définies, le trafic réseau, la détection d'intrusion et de nombreuses autres tâches d'administration des services. La plupart de ces opérations peuvent être prises en charge par OMS, Azure Security Center, Azure Network Watcher et Azure AD.

Outil	Description
OMS	• Donne aux équipes la visibilité et le contrôle sur des implantations hybrides avec une gestion simplifiée des opérations et de la sécurité. • Permet une analyse opérationnelle en temps réel via des tableaux de bord personnalisés et une recherche intégrée, sur tous les enregistrements de toutes les charges de travail dans un centre de données virtuel.
Azure Monitor	• Contrôle les ressources Azure. • Prend en compte les valeurs de performances et la journalisation des diagnostics. • S'intègre avec la base de données SQL, les NSG et le stockage de blogs Azure. • Prend en charge des règles d'alerte personnalisées pour avertir des équipes lorsque des problèmes de performances se produisent et pour déclencher des actions automatiques.
Azure AD	• Aide à sécuriser les ressources d'un centre de données virtuel en fournissant des rapports de diagnostic. • Fournit des rapports sur des anomalies d'ouvertures de sessions, sur l'utilisation d'applications intégrées, sur des erreurs et même sur des utilisateurs spécifiques. Propose des journaux d'activité sur tous les événements audités, les activités des groupes, les réinitialisations de mots de passe et les activités d'inscription.

Azure Security Center	• Détecte des menaces ou des failles de sécurité dans le centre de données virtuel et aide à détecter des menaces sur des ressources hébergées, à les bloquer et à y répondre. • Fournit un contrôle de la sécurité et une gestion centralisée des stratégies entre les abonnements Azure d'un centre de données virtuel. • Prend en charge la définition des stratégies de sécurité pour des ressources ou un groupe de ressources dans un abonnement spécifique. Alerte les équipes de sécurité appropriées de toute violation d'une stratégie. Suggère des corrections. • Collecte, analyse et fusionne des données de journaux en provenance de services de traitement, des ressources réseau et de solutions partenaires comme des pare-feu. • Prend en charge le Microsoft Digital Crimes Unit, le Microsoft Security Response Center (MSRC) et d'autres ressources conçues pour bloquer les attaques et empêcher de futures attaques.
Azure Network Watcher	• Fournit des fonctionnalités de contrôle du réseau. Vous pouvez visualiser les topologies réseau et identifier des ressources et des connexions peu sûres. • Inclut des diagnostics sur la connectivité, la latence, le DNS, les routes utilisées, la vérification du flux IP, les groupes de sécurité, le prochain saut et la capture de paquets. • Analyse les performances et le statut via des analyses de flux, des analyses de la sécurité, l'utilisation de la bande passante, un analyseur de protocoles et les limites de l'abonnement réseau. • Montre les configurations et affiche toutes les alertes et les journaux du réseau.

Voir aussi :

Meilleures pratiques de sécurité opérationnelle Azure

Meilleures pratiques pour créer des solutions d'administration dans OMS (Operations Management Suite)

Azure Architecture Center – Pratiques recommandées : Contrôle et diagnostics

Architecture finale de Contoso

L'architecture finale de Contoso définit une extension complète pour un centre de données de confiance, ajoutée à l'infrastructure existante sur site. Le tableau ci-dessous résume les décisions prises. Le résultat final apparaît à la figure 11.

Domaine	Décisions
Gestion des identités	• Rôles en place • Règles RBAC configurées pour l'infrastructure centrale • Règles RBAC configurées pour les espaces de travail • Azure AD Connect configuré pour synchroniser les utilisateurs et les rôles avec Active Directory sur site
Abonnement	• Abonnements séparés pour l'infrastructure centrale et pour chaque espace de travail • Stratégies et contrôle d'accès définis au niveau de chaque abonnement
Réseau	• Aucun accès autorisé depuis l'Internet public vers le centre de données virtuel • Services DNS configurés et intégrés dans le réseau sur site • Connexion ExpressRoute établie entre le centre de données virtuel et le réseau sur site • Réseau du hub central • Pare-feu central pour examiner le trafic entre le réseau sur site et les réseaux des espaces de travail • Connectivité entre l'architecture centrale et les réseaux virtuels des espaces de travail via des couplages de réseaux virtuels • Stratégies sur les espaces de travail, NSG (groupes de sécurité réseau) et UDR (règles de routage définies par l'utilisateur)
Administration	• Jumpboxes d'administration accessibles uniquement à partir du réseau sur site ; accès autorisé par le mécanisme d'autorisation juste-à-temps

Au final, le centre de données virtuel Contoso déploie des charges de travail uniquement accessibles via l'infrastructure centrale. Il est régi par des contrôles d'accès, des stratégies et une configuration réseau appliqués par l'équipe d'administration centrale de Contoso.

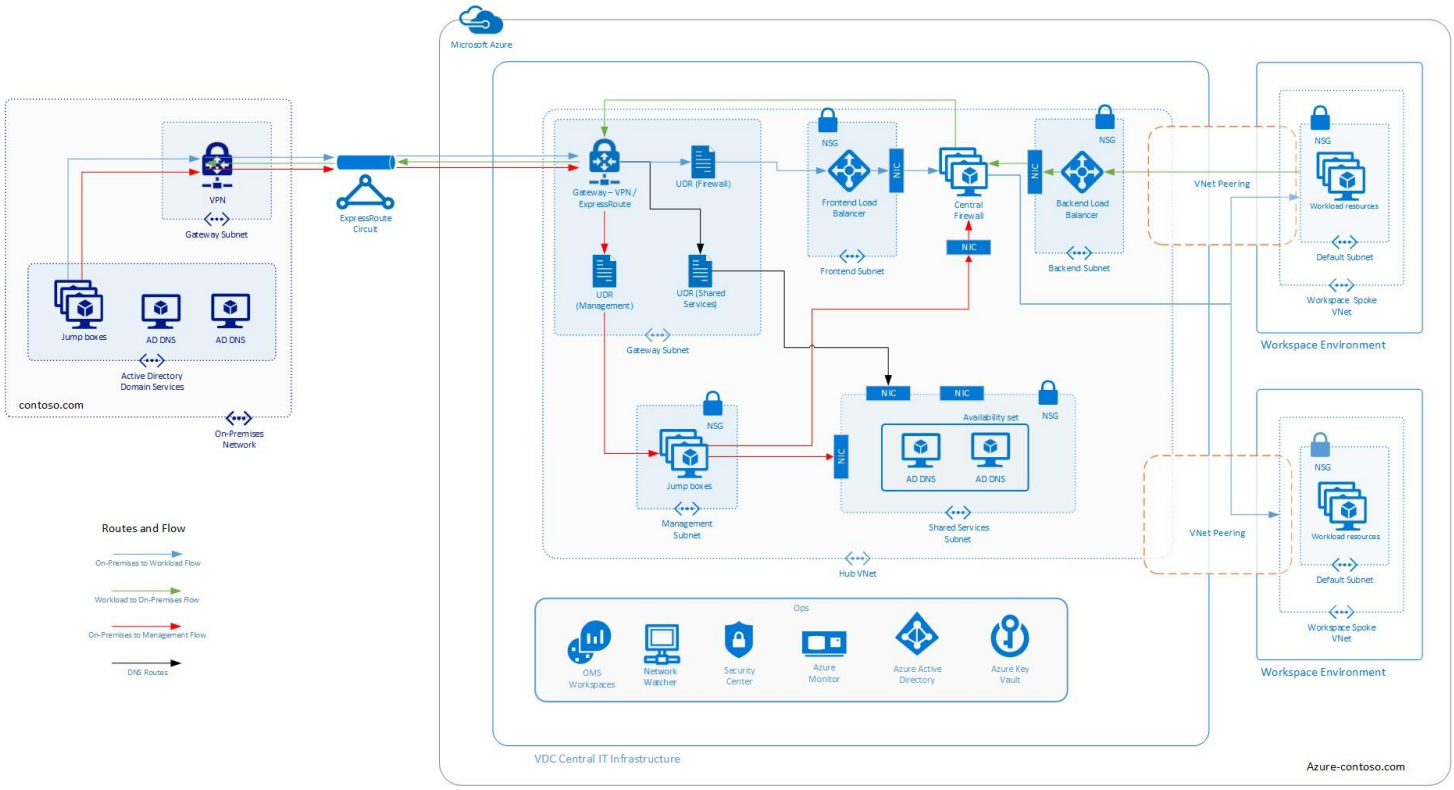

Figure 11. Architecture finale de Contoso avec les principaux composants, les flux de trafics (du site vers une charge de travail, d'une charge de travail vers le site, du site vers l'administration, et DNS).

TROISIÈME PARTIE
L'évolution du centre de données vers le Cloud

L'évolution du centre de données vers le Cloud est un processus continu qui vise à moderniser votre infrastructure et à tirer parti au maximum du Cloud. Dans le cadre de ce processus, votre organisation doit planifier comment utiliser le Cloud Azure et comment structurer au mieux les charges de travail pour utiliser de la façon la plus efficace vos investissements sur site en association avec les ressources du Cloud. Le modèle du Datacenter Virtuel Azure constitue un point de départ pour cette transformation.

Équilibrer la gouvernance et l'agilité

Dans le cadre de l'évolution du centre de données vers le Cloud, les équipes de gouvernance et celles du service informatique de l'entreprise ont deux objectifs prioritaires : la capacité d'isoler les applications et la capacité d'appliquer ces isolations par des stratégies. Les développeurs et les responsables des applications métier ont aussi leurs objectifs : tirer le maximum de l'agilité offerte par le Cloud afin d'obtenir des avantages concurrentiels. Le modèle de Datacenter Virtuel Azure a pour objectif de trouver un équilibre entre ces deux facteurs.

Figure 12 : La gouvernance et le service informatique de l'entreprise doivent trouver un équilibre avec l'agilité du développement lors de l'évolution réussie d'un centre de données vers le Cloud.

Le service informatique souhaite que les applications basées dans le Cloud soient régies par les mêmes stratégies que celles utilisées sur site. Même des applications qui n'existent que dans le Cloud, comme des offres PaaS mutualisées et des applications SaaS comme Office 365, doivent être bien isolées et régies par des stratégies basées sur des rôles. Le modèle de Datacenter Virtuel Azure commence à donner au service informatique de l'entreprise les contrôles nécessaires pour faire respecter la gouvernance.

Modèles pour un centre de données virtuel

Dans la transformation du centre de données et des applications, trois modèles de charges de travail apparaissent :

- Ressources de traitement IaaS, les données restant dans le centre de données sur site.
- IaaS avec les données stockées dans le Cloud, mais utilisation minimale d'autres PaaS (à part le stockage).
- Applications dans le Cloud entièrement composées de services de plateformes.

Figure 13 : Gamme de services de plateforme utilisables dans un centre de données virtuel. À gauche, les machines virtuelles IaaS n'utilisent que des données sur site. À droite, tous les services PaaS du Cloud sont exploités.

Le premier modèle correspond généralement à une évolution partielle vers le Cloud, purement IaaS, sans que des services de plateforme ne soient consommés. Dans ce cas, les machines virtuelles qui traitent les données, sont hébergées dans le Cloud mais toutes les données sont stockées sur site et accessibles via ExpressRoute. Même les services Active Directory restent sur site. Ce modèle inclut des scénarios où les données peuvent circuler vers le Cloud de façon anonyme ou avec un jeton. Ces scénarios ne gèrent pas des données sensibles mais limitent les types de traitement applicables à ces données.

Le deuxième modèle implique une intégration limitée de ressources IaaS pour construire une infrastructure de Cloud basique. Par exemple, des machines virtuelles peuvent utiliser des services PaaS essentiels comme le stockage ou un coffre de clés. Certains services additionnels, comme une base de données Azure SQL, peuvent être consommés pour permettre des économies et faciliter l'administration.

Le troisième modèle utilise pleinement les services PaaS pour construire une solution complète comme un pipeline d'analyses de données dans Azure (hub IoT, apprentissage automatique (machine learning) dans Azure, HDInsight, Azure Data Lake).

Aller de l'avant avec un Datacenter Virtuel Azure

Le modèle de Datacenter Virtuel Azure propose des conseils pour un déploiement cohérent de charges de travail dans le Cloud Azure. La première édition de ce modèle se concentre sur la création d'une extension de confiance pour des charges de travail hébergées dans des machines virtuelles, elles-mêmes déployées dans le Cloud public.

Les prochaines éditions de ce modèle montreront comment des éléments additionnels permettent le renforcement de l'isolation pour des scénarios plus complexes, comme des charges de travail basées sur un orchestrateur, ou des charges de travail composées de services de plateforme. D'autres modèles pendront en charge un accès sécurisé à Internet, directement à partir du centre de données virtuel.

Automatisation du centre de données virtuel

L'automatisation du centre de données virtuel (utilisée actuellement en avant-première dans quelques déploiements) repose sur un ensemble de scripts Python et Azure CLI v2, des modèles du Gestionnaire de ressources et de la documentation. Cet ensemble donne tous les conseils nécessaires pour créer un exemple fonctionnel d'un centre de données virtuel dans Azure.

La première version de ces conseils en automatisation se concentre sur la création d'une extension d'un centre de données, comme l'exemple Contoso décrit dans ce document. Cela implique la création d'un centre de données virtuel isolé connecté aux réseaux sur site via une connexion VPN ou ExpressRoute. Cette version inclut des instructions pour configurer les paramètres nécessaires à la création d'un centre de données virtuel capable de se connecter à vos ressources réseau existantes.

Pour en savoir plus sur l'automatisation d'un centre de données virtuel, contactez votre Responsable de compte Microsoft et visitez le site de référence Architecture d'Azure.

Glossaire des principaux services et fonctionnalités

Les technologies, fonctionnalités et concepts ci-dessous sont essentiels pour composer une extension digne de confiance d'un centre de données, à partir du modèle d'un centre de donnes virtuel Azure.

Abonnement Environnement global dans Azure qui contient toutes les ressources virtuelles, les applications et toutes les constructions utilisées pour l'administration et la facturation d'un compte. Chaque abonnement a une relation approuvée avec un seul annuaire Azure AD.

Accès juste-à-temps Accès à une machine virtuelle pendant une période de temps définie afin de limiter le trafic entrant dans vos machines virtuelles Azure, de réduire leur exposition à des attaques et de permettre un accès facile aux machines virtuelles lorsque cela est nécessaire.

Appliance virtuelle réseau (NVA) Une image de machine virtuelle dédiée et préconfigurée conçue pour prendre en charge le type de fonctionnalités sécurité et réseau traditionnellement prise en charge par des passerelles, des routeurs et des pare-feux.

Azure Active Directory Assure l'authentification et le contrôle d'accès pour des ressources dans Azure. Azure AD est un service de gestion des identités et un annuaire mutualisé. Il est basé dans le Cloud. Azure AD s'intègre avec des gestionnaires d'identités sur site et prend en charge RBAC ainsi que les contrôles d'accès juste-à-temps. Azure AD prend en charge

des authentifications à plusieurs facteurs via un téléphone, du texte, une appli mobile ou des méthodes personnalisées, via un jeton oAuth. Une pratique recommandée consiste à activer l'authentification à plusieurs facteurs pour les rôles du service informatique et les utilisateurs d'applications.

Chiffrement homomorphique Technique spéciale de chiffrement qui permet d'effectuer des traitements sur des données chiffrées sans avoir besoin d'une clé de déchiffrement. Les résultats des traitements restent chiffrés et ne peuvent être lus en clair que par le propriétaire de la clé secrète.

Coffre de clés Azure Mécanisme principal pour stocker, gérer et utiliser les clés de chiffrement dans la plateforme Azure. Le coffre de clés est un service centralisé qui permet l'administration des certificats, des chaînes de connexions, des secrets et des clés utilisés pour chiffrer le stockage et sécuriser des services PaaS ou des applications. Le coffre de clés accepte des clés générées et administrées par Microsoft ou des clés générées par votre service informatique et stockées dans ce coffre. Il prend en charge un service de conteneur virtuel HSM qui donne accès à des HSM physiques.

Équilibrage de la charge Dans Azure, un système d'équilibrage de la charge au niveau de la couche 4 (TCP, UDP) répartit le trafic entrant sur les ressources de votre réseau virtuel.

ExpressRoute Prend en charge des connexions privées entre les centres de données Azure et l'infrastructure sur site, dans un environnement mutualisé. Les connexions ExpressRoute ne passent pas via l'Internet public ; les clients bénéficient d'une plus grande fiabilité, d'un débit plus élevé, de latences plus faibles et d'une plus grande sécurité qu'avec les connexions Internet habituelles.

FIPS Federal Information Processing Standard.

Gestionnaire de ressources Azure Fournit le mécanisme pour créer et administrer des ressources dans un centre de données virtuel. Le Gestionnaire de ressources et les API correspondantes vous permettent d'implanter des stratégies sur le lieu de résidence des données lors de la création d'une ressource.

Groupe de ressources Un ensemble de ressources Azure, comme des machines virtuelles, des services et des équipements réseau, à l'intérieur d'un abonnement. Vous pouvez appliquer un contrôle d'accès et des stratégies de sécurité au niveau d'un groupe de ressources plutôt que gérer individuellement chaque ressource.

Groupe de sécurité réseau (NSG) Équipement d'inspection simple des paquets qui permet la création de règles Accepter/Refuser sur le trafic réseau. Un NSG peut interdire ou autoriser le trafic de ou vers une adresse IP, de ou vers plusieurs adresses IP, et même de ou vers des sous-réseaux entiers. Lorsqu'un NSG est associé à un sous-réseau, les règles s'appliquent à toutes les ressources connectées à ce sous-réseau. Le trafic peut être davantage restreint en appliquant des NSG supplémentaires à des machines virtuelles.

HSM Hardware Security Module.

IaaS Infrastructure as a Service.

Machine virtuelle (VM) Une ressource de traitement Azure disponible sur demande et capable de monter en charge. Une machine virtuelle peut exécuter des charges de travail Windows ou Linux dans l'environnement virtuel Azure.

Machine virtuelle protégée Une future fonctionnalité dans Azure qui protègera les machines virtuelles contre des administrateurs malveillants. Une machine virtuelle protégée chiffre son disque et son état ; seuls la machine virtuelle et les administrateurs du compte principal peuvent y accéder. Une machine virtuelle protégée utilise un module virtuel TPM. Le disque est chiffré via BitLocker et la machine virtuelle ne peut s'exécuter que sur un hôte approuvé.

MFA Authentification à plusieurs facteurs.

NVA Network Virtual Appliance. Voir Appliance virtuelle réseau.

PaaS Platform as a Service.

Passerelle VPN Type de connexion réseau qui transmet un trafic chiffré via un réseau public ou partagé. Le service Passerelle VPN Azure connecte vos réseaux sur site, à Azure via des VPN de site à site, similaire à ce que vous faites pour connecter une de vos filiales ou agences à votre maison-mère. Cette connectivité utilise les protocoles standards IPSec (Internet Protocol Security) et Internet Key Exchange (IKE).

RBAC Contrôle d'accès basé sur les rôles.

Récupération suite à un incident majeur Processus utilisé pour restaurer des données et assurer la continuité métier dans le cas d'une panne importante des systèmes et de l'infrastructure informatique.

Réseau virtuel Une représentation logique de votre réseau dans le Cloud. Dans la plateforme Azure, les réseaux virtuels sont comparables dans le Cloud à vos réseaux physiques sur site. Les réseaux virtuels assurent aussi l'isolation par défaut entre les ressources de la plateforme. Un réseau virtuel est parfois nommé VNet.

Route définie par l'utilisateur (UDR) Table de routage personnalisée qui sert à créer vos réseaux virtuels. Les UDR sont liées à des sous-réseaux dans vos réseaux virtuels. Une UDR définit le prochain saut et les règles de transferts pour tout le trafic sortant de ce sous-réseau.

Secure Boot Démarrage sécurisé. Une fonctionnalité à venir dans azure. Secure Boot vérifiera que chaque composant chargé au cours du processus de démarrage est signé et validé.

SSE Storage Service Encryption.

SSL Secure Sockets Layer.

TLS Transport Layer Security.

VM Voir machine virtuelle.

VPN Réseau privé virtuel.

Pour en savoir plus

Plateforme Azure

- Centres de données Azure : https://azure.microsoft.com/en-us/overview/datacenters/
- Présentation des zones de disponibilité dans Azure : https://docs.microsoft.com/en-us/azure/availability- zones/az-overview
- Haute disponibilité pour les applications construites sur Microsoft Azure https://docs.microsoft.com/en- us/azure/architecture/resiliency/high-availability-azure-applications
- Souscription Azure et limites de service, quotas et contraintes : https://docs.microsoft.com/en- us/azure/azure-subscription-service-limits
- Azure Security Center : https://azure.microsoft.com/en-us/services/security-center/
- Centre Microsoft de gestion de la confidentialité – Conformité : https://www.microsoft.com/en- us/TrustCenter/Compliance/default.aspx
- Centre Microsoft de gestion de la confidentialité – Conception et sécurité opérationnelle : https://www.microsoft.com/en-us/trustcenter/security/designopsecurity
- Centre Microsoft de gestion de la confidentialité – Transparence : https://www.microsoft.com/en- us/trustcenter/about/transparency
- Équipe rouge : Simuler des attaques pour renforcer les protections du Cloud Microsoft : https://azure.microsoft.com/en-us/blog/red-teaming-using-cutting-edge-threat-simulation-to-harden-the-microsoft-enterprise-cloud/

Identités et Azure Active Directory

- Documentation d'Azure Active Directory : https://docs.microsoft.com/en-us/azure/active- directory/
- Qu'est-ce que l'authentification Azure à plusieurs facteurs ? https://docs.microsoft.com/en-us/azure/multi- factor-authentication/multi-factor-authentication
- Solutions d'identités hybrides Microsoft : https://docs.microsoft.com/en-us/azure/active- directory/choose-hybrid-identity-solution
- Intégration de vos annuaires sur site dans Azure Active Directory https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect
- Fédération et Azure AD Connect : https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnectfed-whatis

Isolation et sécurité

- Documents Microsoft Service Trust : https://servicetrust.microsoft.com/Documents/TrustDocuments
- Introduction à la sécurité d'Azure : https://docs.microsoft.com/en-us/azure/security/azure- security
- Isolation dans le Cloud public Azure : https://docs.microsoft.com/en-us/azure/security/azure- isolation
- Sécurité du Cloud Microsoft pour des architectes d'entreprises : https://www.microsoft.com/en- us/download/48121
- Sécurité réseau d'Azure : https://docs.microsoft.com/en-us/azure/security/azure-network- security
- Vue d'ensemble de la sécurité des machines virtuelles Azure : https://docs.microsoft.com/en- us/azure/security/security-virtual-machines-overview
- Administration de l'accès juste-à-temps d'une machine virtuelle : https://docs.microsoft.com/en- us/azure/security-center/security-center-just-in-time
- Guide de la sécurité du stockage Azure : https://docs.microsoft.com/en-us/azure/storage/common/storage-security-guide

Chiffrement

- Chiffrement dans le Cloud Microsoft : https://www.microsoft.com/en-us/download/details.aspx?id=55848
- Qu'est le coffre des clés Azure ? https://docs.microsoft.com/en-us/azure/key-vault/key-vault-whatis
- Chiffrement des données dans le service de stockage Azure : https://docs.microsoft.com/en- us/azure/storage/common/storage-service-encryption
- Chiffrement du disque Azure pour des machines virtuelles IaaS Windows et Linux : https://docs.microsoft.com/en- us/azure/security/azure-security-disk-encryption
- Comment générer et transférer des clés protégées par HSM vers le coffre de clés Azure : https://docs.microsoft.com/en-us/azure/key-vault/key-vault-hsm-protected-keys
- Introduction au traitement confidentiel Azure : https://azure.microsoft.com/en-us/blog/introducing-azure-confidential-computing/
- Chiffrement homomorphique : https://www.microsoft.com/en-us/research/project/homomorphic- encryption/
- Manuel d'utilisation du chiffrement homomorphique en bioinformatique : https://www.microsoft.com/en-us/research/publication/manual-for-using-

homomorphic- encryption-for-bioinformatics/

- Blog de la sécurité de Dubaï – Analyse du Secure Boot : https://blogs.technet.microsoft.com/dubaisec/2016/03/14/diving-into-secure-boot/
- Analyse approfondie des machines virtuelles protégées dans Windows Server 2016 : https://blogs.technet.microsoft.com/windowsserver/2016/05/10/a-closer-look-at-shielded- vms-in-windows-server-2016/

Réseau virtuel

- Centre de données virtuel Microsoft Azure (centré sur VNet) : https://docs.microsoft.com/en- us/azure/networking/networking-virtual-datacenter
- Groupes de sécurité réseau dans Azure : https://docs.microsoft.com/en-us/azure/virtual- network/virtual-networks-nsg
- Routes définies par l'utilisateur et transfert IP (IP Forwarding) dans Azure : https://docs.microsoft.com/en- us/azure/virtual-network/virtual-networks-udr-overview
- Appliance virtuelle réseau : https://azure.microsoft.com/en-us/solutions/network-appliances/
- Scénario d'appliance virtuelle réseau : https://docs.microsoft.com/en-us/azure/virtual-network/virtual- network-scenario-udr-gw-nva
- Connecter un réseau sur site à Azure : https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/
- Installer une zone démilitarisée (DMZ) entre Azure et Internet : https://docs.microsoft.com/en- us/azure/architecture/reference-architectures/dmz/secure-vnet-dmz
- Mise en œuvre d'hôtes d'administration sécurisés : https://docs.microsoft.com/en-us/windows- server/identity/ad-ds/plan/security-best-practices/implementing-secure-administrative-hosts
- Résolution de noms pour des machines virtuelles et des rôles : https://docs.microsoft.com/en-us/azure/virtual- network/virtual-networks-name-resolution-for-vms-and-role-instances
- Réseau virtuel pour des services Azure : https://docs.microsoft.com/en-us/azure/virtual- network/virtual-network-for-azure-services
- Annonce de l'intégration d'un réseau virtuel pour le stockage Azure et Azure SQL : https://azure.microsoft.com/en-us/blog/announcing-virtual-network-integration-for-azure- storage-and-azure-sql/
- Points de terminaison de service dans un réseau virtuel Azure : https://docs.microsoft.com/en-us/azure/virtual- network/virtual-network-service-endpoints-overview
- Présentation des ports de haute disponibilité : https://docs.microsoft.com/en-

us/azure/load-balancer/load- balancer-ha-ports-overview

Opérations

- Meilleures pratiques de sécurité opérationnelle Azure : https://docs.microsoft.com/en- us/azure/security/azure-operational-security-best-practices
- Meilleures pratiques pour une solution d'administration OMS : https://docs.microsoft.com/en- us/azure/operations-management-suite/operations-management-suite-solutions-best- practices
- Conseils en contrôle et diagnostics : https://docs.microsoft.com/en-us/azure/architecture/best-practices/monitoring