Réussir une migration simple et sécurisée vers AWS avec Zscaler

Mapper Zscaler Private Access avec AWS Cloud Adoption Framework

Table des matières

Introduction

Ce document a pour but de montrer comment Zscaler™ accélère l'adoption par les utilisateurs en supprimant les freins liés à l'atteinte des objectifs réseau et de sécurité. Comprendre comment Zscaler Private Access™ (ZPA™) s'applique aux cas d'utilisation de la migration vers AWS permettra de fournir une approche structurée de la solution globale et d'illustrer comment ZPA accélère la migration des applications.

Lorsque Zscaler est engagé dans des projets du secteur privé et public, l'architecture ZPA se positionne comme un outil permettant d'améliorer l'agilité des utilisateurs et des applications et d'accélérer la migration des applications.

La fonction principale de ZPA est de gérer de manière active l'accès des utilisateurs autorisés aux charges de travail – et leur interaction avec celles-ci – avant, pendant et après la migration vers le cloud, tout en améliorant l'expérience globale de l'utilisateur final.

Les meilleures pratiques architecturales liées à Zscaler Private Access jouent un rôle essentiel, notamment dans les phases de migration du client vers le cloud, comme par exemple:

- Préparation et planification
- Portefeuille et découverte
- Planification opérationnelle et exécution
- Migration et validation
- Fonctions opérationnelles continues

Avantages de Zscaler Private Access (ZPA) :

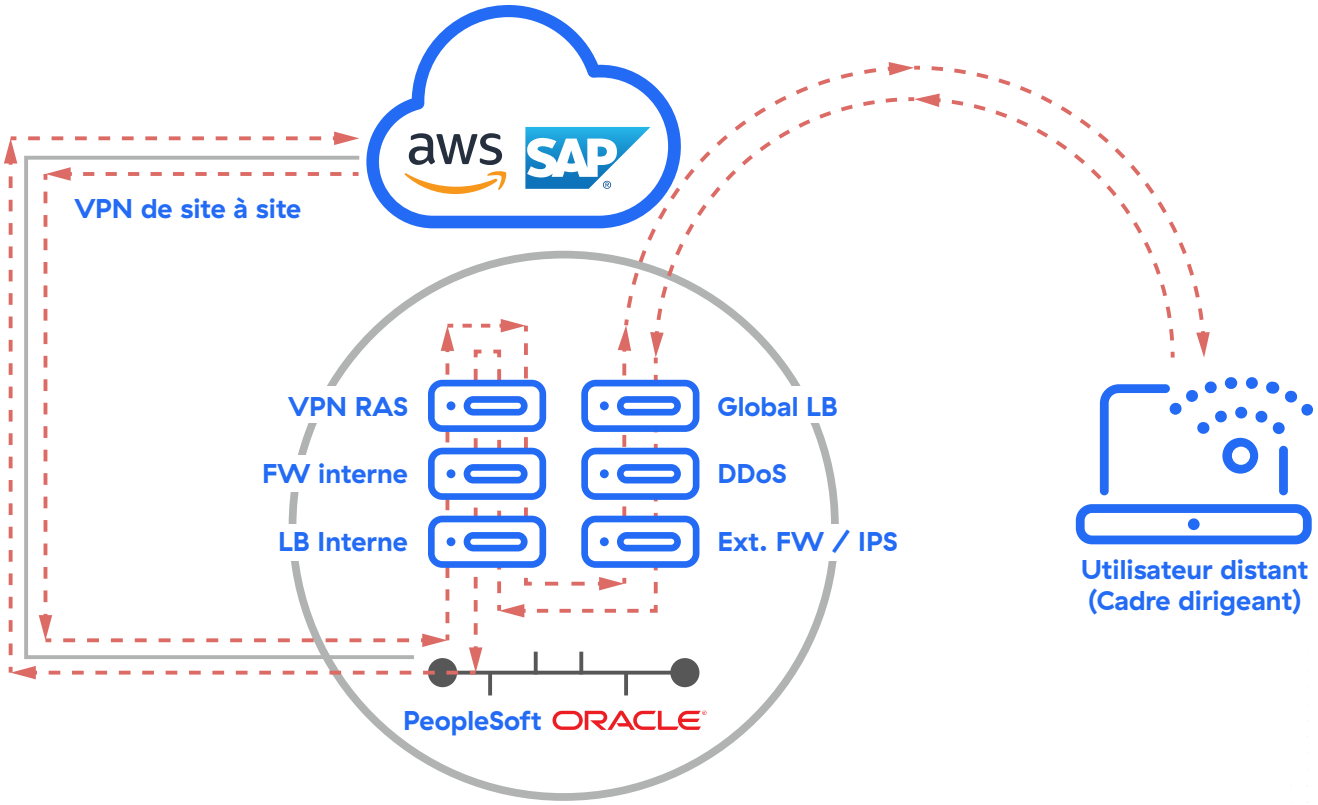
- **Accélérer la migration des applications et l'adoption du cloud**
- **Permettre un contrôle granulaire de l'accès des utilisateurs aux applications hébergées sur AWS**
- **Gérer activement l'accès aux charges de travail avant et après la migration**
- **Fournir une visibilité de bout en bout sur les applications et améliorer l'expérience utilisateur**

Bien que le présent document se concentre sur la migration des charges de travail vers AWS, la solution ZPA et les solutions de périmètre défini par logiciel qui lui sont associées ne sont pas spécifiques aux déploiements AWS. ZPA prend en charge les environnements informatiques hybrides et peut être utilisé pour augmenter les cadres de migration des applications définis par les cabinets de conseil.

Zscaler Private Access : sécuriser l'accès aux applications internes

Zscaler Private Access fournit un accès sécurisé aux applications internes, qu'elles soient hébergées dans votre data center ou dans un cloud public. Zscaler réduit le coût et la complexité des problèmes de sécurité et de mise en réseau traditionnels, tout en améliorant l'expérience utilisateur relative à l'accès réseau traditionnel basé sur le VPN.

La plupart des clients commencent par une infrastructure réseau traditionnelle sur site, centrée sur le data center et basée sur le matériel, avec des solutions d'accès distant centralisées semblables à celle-ci:



AVANT ZSCALER : Approche traditionnelle d'accès à distance centrée sur le data center

Zscaler Private Access propose une solution de périmètre défini par logiciel (SDP). Cette méthodologie, axée sur l'expérience utilisateur, est totalement différente des solutions VPN d'accès à distance traditionnelles : elle est conçue spécifiquement pour répondre aux besoins d'évolution et aux autres besoins d'une communauté professionnelle agile et moderne migrant vers le cloud.

Zscaler Private Access s'appuie sur notre architecture cloud mondiale et établit un accès Zero Trust aux applications privées. La confiance n'est jamais acquise, mais basée sur l'authentification de l'utilisateur et de l'appareil via SAML. Une fois que chaque utilisateur est authentifié, une connexion de l'intérieur vers l'extérieur est établie depuis un App Connector dans AWS vers Zscaler Cloud, où une connexion sécurisée est établie entre les utilisateurs autorisés et leurs applications.

Avec Zscaler Private Access, l'accès aux applications est fédéré par un cloud mondial sécurisé, le réseau devenant un simple moyen de transport. Un accès granulaire, basé sur des politiques, est utilisé pour connecter les utilisateurs authentifiés aux applications auxquelles ils sont autorisés à accéder, afin que les clients puissent maintenir la caractère privé de leur cloud public.

AVEC ZSCALER : Accès sécurisé, basé sur des politiques, avec des utilisateurs en dehors du réseau

Comme la posture de sécurité de l'utilisateur et de l'appareil est évaluée avant que l'accès aux applications ne soit accordé, les applications sont invisibles pour les utilisateurs qui n'ont pas la permission d'y accéder. De plus, comme les applications sont fédérées par le cloud Zscaler, il n'y a pas de connexions entrantes vers l'instance AWS ou le data center du client. Les contrôles d'accès et stratégies, ainsi que les groupes de sécurité deviennent donc plus simples. La politique est basée sur les informations des utilisateurs et des appareils plutôt que sur les objets du réseau, ce qui offre une plus grande visibilité et une plus grande flexibilité.

Zscaler Private Access permet à un utilisateur d'accéder simultanément aux applications autorisées dans ses VPC AWS et ses data centers physiques. Séparer le réseau de l'utilisateur et fournir une connexion à l'application par le chemin le plus court améliore l'expérience de l'utilisateur, simplifie l'architecture du réseau et offre une plus grande visibilité et un meilleur contrôle de la sécurité.

Accélérer la migration des applications

Zscaler Private Access peut être utilisé pour un cas d'utilisation professionnel préliminaire impliquant une migration. La quantification d'une infrastructure d'application existante pose de nombreux défis. Avec cette approche, Zscaler fournit un cadre pour une expérience utilisateur fluide dans les environnements existants et AWS. Le contrôle d'accès basé sur les politiques remplace l'infrastructure traditionnelle, évitant ainsi la configuration et les besoins permanents d'administration qui y sont associés.

Le responsable de l'architecture ou le cabinet de conseil peut potentiellement raccourcir la durée globale de la migration. ZPA fournit une plate-forme à partir de laquelle l'accès des utilisateurs peut être contrôlé pendant la migration des charges de travail vers AWS sans avoir à effectuer la moindre modification sur l'infrastructure réseau existante. Il est possible d'éviter d'utiliser du matériel VPN traditionnel pour la connexion des utilisateurs à des applications privées hébergées sur AWS et de se servir d'AWS Direct Connect pour gérer le chemin non-optimal consistant à acheminer le trafic des utilisateurs distants par le data center avant qu'ils n'atteignent l'environnement AWS.

L'adoption de la plate-forme ZPA permet un contrôle détaillé de l'accès des utilisateurs aux applications hébergées sur AWS dans plusieurs régions et dans un environnement hybride. Dans la pratique, cette approche peut à la fois simplifier l'adoption du cloud et permettre au client d'établir une relation de confiance avec ses utilisateurs pendant la migration.

En améliorant l'expérience utilisateur, en réduisant considérablement les processus de contrôle des changements, en offrant une visibilité de bout en bout sur les applications et en permettant de choisir des groupes ou des sites discrets pour faciliter la migration grâce à une gestion centralisée des politiques, ZPA permet aux entreprises de migrer plus rapidement et d'offrir une expérience utilisateur optimale.

Amélioration de la gestion des identités et des accès :

- **Les applications sont invisibles pour les utilisateurs/appareils qui n'ont pas été pré-autorisés.**
- **Contribue à la lutte contre les menaces de sécurité modernes telles que les attaques DDoS et les accès non autorisés provenant de sources tierces.**
- **Limite la capacité de déplacement latéral des programmes malveillants sur votre réseau interne.**

Lorsque des applications métiers telles que SAP, Oracle ou les charges de travail de Microsoft sont migrées vers le système AWS, il arrive souvent que les questions liées au réseau et à la sécurité soient reportées pour être résolues plus tard dans le cycle de planification et d'exécution de la migration. Les architectes de solutions partenaires d'AWS et d'APN Consulting rapportent régulièrement être confrontés à des freins et aux retards qui en résultent. Intégrer une solution élégante et bien maîtrisée comme ZPA dans la boîte à outils de votre planification dès le début du projet permet de comprendre, d'anticiper et d'éviter cette friction.

Ce processus réunit souvent les architectes cloud, les équipes informatiques, les équipes réseau et de sécurité dans une collaboration productive qui, autrement, ne fait généralement pas partie de la phase de préparation et de planification.

Pour ces applications, la migration vers l'IaaS sera attrayante et souvent évidente étant donné l'ampleur et la portée de leurs déploiements. Toutefois, nous constatons qu'un premier défi commun consiste à identifier toutes les applications auxquelles les utilisateurs accèdent et qui doivent également migrer. Parfois, le nombre d'applications découvertes dépasse celui que les responsables informatiques avaient estimé. ZPA permet de découvrir des applications privées et d'établir des rapports afin de fournir aux clients une visibilité sur toutes les applications auxquelles ils accèdent dans leur data center physique. Cela permet au cabinet de conseil et au client de déterminer l'ordre de priorité des applications à migrer vers l'IaaS et de renforcer les contrôles de sécurité autour de ces applications.

Les clients peuvent alors plus facilement identifier les charges de travail à migrer vers AWS, mais devront décider comment fournir les applications à leurs utilisateurs en toute sécurité : un véritable défi si l'application n'est pas conçue pour être fournie dans le cloud.

La gestion des identités et des accès est un facteur clé d'une mise en œuvre réussie de l'IaaS. Toutefois, ce contrôle d'accès peut être amélioré en rendant les applications invisibles à tous, sauf aux utilisateurs ou appareils qui ont été préalablement autorisés à y accéder. Cette méthode permet de faire face aux menaces de sécurité modernes, notamment les attaques DDoS, l'accès non autorisé par des sources tierces et la possibilité de déplacement latéral des logiciels malveillants sur le réseau interne.

Nous avons pu instaurer un modèle Zero Trust… et remplacer les approches traditionnelles par cette mise en œuvre moderne, sécurisée et cloud-first. Nous disposons également d'un contrôle granulaire sur les autorisations des utilisateurs, chaque employé et sous-traitant n'ayant accès qu'à ce à quoi il doit avoir accès.

Tony Fergusson, architecte d'infrastructure informatique,
MAN Energy Solutions

Sécurité renforcée

Zscaler Private Access fournit un cadre de politique granulaire permettant de connecter les utilisateurs aux applications, où qu'elles soient. ZPA ne connecte pas les utilisateurs au réseau, au contraire, il le sépare complètement de l'utilisateur. Cette connectivité des applications présente de nombreux avantages:

- Les utilisateurs peuvent accéder aux applications hébergées sur plusieurs environnements (AWS, sur site ou hybride) via des tunnels TLS cryptés qui sont activés à la demande.
- Les utilisateurs ont accès à des applications internes sans jamais être placés sur le réseau.
- L'adressage IP peut se chevaucher dans les data centers. Comme le réseau est séparé de l'utilisateur, le chevauchement n'a pas de conséquence.
- La politique d'accès aux applications est évaluée dans Zscaler Cloud. Ce n'est qu'une fois que l'accès d'un utilisateur et de son appareil est authentifié qu'une connexion sortante à l'application est établie via l'App Connector s'exécutant dans l'environnement de l'application. L'environnement d'application est « obscur » vis-à-vis d'Internet, ce qui signifie qu'il n'existe aucune connexion entrante vers l'appareil ou l'environnement d'application.
- Une politique granulaire basée sur des attributs pour chaque application ou utilisateur peut être rédigée et gérée par le client ou un programme de sécurité géré (MSP).

En permettant aux utilisateurs d'accéder uniquement aux applications dont ils ont besoin pour leur travail, et non à l'ensemble du réseau, ZPA offre une plus grande sécurité qu'une approche VPN traditionnelle. Cette approche permet une posture de sécurité intrinsèquement plus efficace contre les formes les plus courantes d'intrusion et de logiciels malveillants. En outre, Zscaler apporte son aide en matière d'assistance et d'accélération de l'adoption d'une approche Zero trust pour les clients AWS.

En ce qui concerne le cadre de la migration vers le système AWS, ZPA permet à l'utilisateur d'accéder à une application spécifique, ce qui assure une approche cohérente pour toutes les charges de travail déployées sur le système AWS. En limitant les utilisateurs aux seules applications spécifiques dont ils ont besoin dans le cadre de leurs fonctions, la sécurité de l'entreprise se trouve améliorée. En plus des rôles des utilisateurs, le statut de la gestion des appareils peut également être utilisé pour analyser la demande d'accès à une application. ZPA aide les clients AWS à appliquer le modèle de responsabilité partagée d'AWS en fournissant des mécanismes et des méthodologies pour gérer un contrôle granulaire des applications auxquelles un utilisateur se servant d'un appareil particulier peut avoir accès.

Comment Zscaler Private Access accélère la migration vers AWS

Préparation et planification

Zscaler Private Access peut être exploité pour accélérer l'adoption d'AWS et éviter les nombreuses phases de projet traditionnelles qui seraient autrement nécessaires pour répondre à cet objectif. Plus précisément, la solution établit une base de référence pour la partie la plus exigeante et la plus importante, mais souvent négligée, de toute migration : vos utilisateurs.

ZPA offrira aux clients les avantages suivants:

- Exploiter « l'identité » comme nouveau périmètre en fournissant une couche d'abstraction entre les utilisateurs et les applications qu'ils souhaitent utiliser.
- Adopter une posture de sécurité qui n'accorde pas une confiance par défaut aux utilisateurs selon qu'ils se trouvent à l'intérieur ou à l'extérieur du périmètre du réseau de l'entreprise. Les utilisateurs sont plutôt authentifiés via leur solution de gestion des identités et des accès (IAM) et se voient accorder l'accès à leurs applications en fonction d'un certain nombre de politiques de contrôle. Les contrôles peuvent être basés sur les attributs SAML renvoyés par la solution IAM.
- Mettre en place une approche basée sur le risque en utilisant l'authentification multifactorielle (AMF).
- Réduire la nécessité d'un accès à privilèges élevés et minimiser considérablement la surface d'attaque pour tout accès entrant. Pour ce faire, il faut intercepter les demandes des utilisateurs liées aux applications internes et appliquer la politique avant de connecter l'utilisateur à l'application, ce qui revient essentiellement à rendre les applications invisibles à la fois sur Internet et pour les utilisateurs internes non autorisés.
- Offrir une expérience utilisateur fluide en s'intégrant de manière transparente dans le flux de travail normal des utilisateurs, que l'utilisateur soit sur un réseau d'entreprise ou public. Avec le composant Zscaler Client Connector (anciennement Zscaler App) installé, aucune action n'est nécessaire de la part de l'utilisateur pour se connecter aux applications, quel que soit son emplacement ou l'appareil qu'il a choisi d'utiliser.

Cette section décrit plus en détail les avantages de chacune des étapes suivantes, mentionnées dans les recommandations et bonnes pratiques de migration vers le cloud AWS et souvent adaptées par les clients et divers cabinets de conseil :

- **Préparation et planification**
- **Portefeuille et découverte**
- **Planification opérationnelle et exécution**
- **Migration et validation**
- **Opérations en cours et investissements futurs**

Portefeuille et découverte

De nombreux clients sont désormais en passe de devenir des entreprises axées sur le cloud. Chez Zscaler, nous comprenons que lorsque les clients migrent vers le cloud, ils souhaitent éviter les défis suivants:

- Mauvaise expérience utilisateur lors du transfert des applications des data centers privés vers le cloud public, à la fois en raison de la nécessité permanente de former les utilisateurs à l'utilisation des applications et de la complexité des performances des applications.
- Complexité du réseau due à la connexion des data centers privés au cloud public.
- Le coût et la complexité liés au dimensionnement, à la gestion et à la projection de la capacité souhaitée par votre entreprise à l'échelle mondiale.
- Menaces et incertitudes importantes en matière de sécurité, causées par l'autorisation d'accès au réseau de l'entreprise accordée aux utilisateurs fiables ou douteux.

Zscaler Private Access relève ces défis en offrant une visibilité sur les applications internes grâce aux trois phases clés de conception de la sécurité suivantes:

- Détection : la détection d'applications basée sur les accès des utilisateurs permet de déterminer quelles applications internes sont utilisées au sein d'une entreprise, et par la suite, lesquelles sont utilisées à partir de AWS.
- Affinage : une fois qu'une application a été détectée, vous pouvez alors entreprendre l'affinage de la politique afin d'établir une base de référence avant la migration. Cela permet d'éviter toute exposition une fois l'application transférée vers le système AWS et de réduire également le délai de livraison finale.
- Production : la segmentation des applications vous permet d'appliquer rapidement et de manière granulaire une politique correspondant à la posture de sécurité et de déploiement requise pour une mise en production complète.

Gros plan sur les clients :

Pour un grand fabricant mondial de boissons, le processus de détection a révélé plus de 500 applications sur site. Zscaler a permis au service informatique d'intervenir en 95 minutes ; l'affinage a porté sur l'authentification multi-facteur et d'autres attributs. Le déploiement de la production a très peu changé depuis le déploiement initial.

Zscaler Private Access contribue à accélérer la phase de détection en s'intégrant de manière transparente dans le flux de travail des utilisateurs. Les utilisateurs accèdent simplement à l'application qu'ils souhaitent utiliser, sans avoir à interagir au préalable avec un logiciel de sécurité tel qu'un client de terminal. Les utilisateurs n'ont plus besoin de comprendre comment on accède à une application, qu'elle soit nouvelle ou ancienne, et les administrateurs ont une visibilité totale de bout en bout des flux applicatifs.

Planification opérationnelle et exécution

À mesure que les clients identifient les applications à migrer vers AWS, ils décident comment fournir l'application aux utilisateurs. Ils le font essentiellement sous l'une des trois formes suivantes:

Virtualiser – Maintenir la confidentialité

- Comprendre l'architecture actuelle de l'application. Dans un environnement à trois niveaux (serveur web, serveur d'application, serveur de base de données), chaque composant serait virtualisé et migré vers AWS à tour de rôle.
- Le front-end peut être migré en premier pendant que les serveurs d'application et de base de données restent disponibles via VPN ou une connexion dédiée telle que Direct Connect.
- L'application reste « privée » et n'est accessible que via le VPN ou une connexion dédiée.

> « Grâce à Zscaler, nous avons pu faire preuve d'une grande agilité… Nous avons reçu énormément d'éloges de la part d'autres départements qui ont pu continuer à travailler à distance. Zscaler met fondamentalement fin à l'idée d'un VPN traditionnel. »
>
> Marc De Serio, Directeur technique, Henry M. Jackson Foundation (HJF)

Virtualiser – Rendre public

- Semblable à la première option. Toutefois, le serveur Web du front-end devient directement disponible sur Internet.
- La demande peut être résolue publiquement.
- L'obligation de mettre en œuvre un firewall d'application Web (WAF) pour contrôler le contenu entrant et sortant de l'application, les protections contre les DDoS, et de mettre en œuvre la gestion des identités et des accès pour restreindre l'accès des utilisateurs.

Révision de l'architecture pour la migration vers le cloud

- Les applications qui ne peuvent pas être migrées ou qui n'y parviennent pas dans leur forme actuelle.
- Le front-end passe au type EC2 ou au Serverless avec CloudFront : réaffectation et recodage du serveur web.
- Le niveau intermédiaire doit passer au type EC2 ou au Serverless – middleware à usage multiple.
- Le back-end doit passer à RDS/Aurora/etc – mise à jour du schéma, de la base de données, etc.
- L'IAM contrôle l'accès; le WAF contrôle le contenu.
- L'expérience utilisateur et l'accès changent en fonction de la migration vers une nouvelle architecture.

Rendre l'application publique comporte un risque de sécurité quantifiable. Pour certaines applications, ce risque tant pour la révision de l'architecture que pour la virtualisation, peut être acceptable pour l'entreprise. ZPA peut permettre aux clients de faire la promotion de leurs applications tout en offrant la même architecture de sécurité grâce à un accès par navigateur, ce qui nécessite la même authentification SAML dans ZPA, utilise la même architecture ZPA pour l'accès sans entrées et offre le même cadre de politiques et la même visibilité.

Cependant, pour un certain nombre d'applications, telles que SAP, le risque d'exposer l'application directement à Internet est trop grand. En effet, la migration vers AWS nécessite un renforcement de la sécurité. ZPA permet aux clients de planifier leur migration, de renforcer la sécurité dans le cadre de cette migration et de préserver la confidentialité des applications.

Migration et validation

Au cours de la migration, il est important de pouvoir déterminer où des progrès ont été réalisés. Zscaler Private Access offre une visibilité sur les emplacements où les applications sont utilisées, ainsi que sur les politiques de sécurité qui les entourent.

Zscaler Private Access agit comme une couche d'abstraction entre l'utilisateur et l'application. L'application peut être déplacée du data center vers le cloud public ou d'un VPC à l'autre, sans qu'il n'y ait aucun impact négatif sur l'expérience utilisateur. Les utilisateurs ne se connectent jamais directement aux applications ; le trafic doit transiter par le service cloud de ZPA. En outre, les utilisateurs ne sont jamais placés sur le réseau, ce qui renforce la sécurité. Toutes les communications effectuées par ZPA sont des connexions sortantes issues du data center ou du cloud public vers le service cloud de ZPA. De ce fait, les pare-feu ou les ACL du data center peuvent maintenant être configurés pour refuser toutes les connexions entrantes, et le data center ou le VPC peut devenir complètement invisible pour le reste du monde.

Zscaler Private Access s'intègre au centre des opérations de sécurité (SOC) d'un client pour les flux et les rapports (ou les analyses) SIEM. La représentation graphique des applications et des utilisateurs est fournie via la console de gestion de ZPA, et des changements de politique peuvent être apportés pour contrôler l'accès des utilisateurs aux applications.

Zscaler ne fournit pas de services de migration. Cependant, Zscaler renforce le processus de validation de la migration et s'assure que l'expérience utilisateur fournie est conforme aux exigences de l'entreprise. La visibilité des clients et des consultants sur la progression des migrations d'applications est un besoin clé pris en charge par ZPA.

Gros plan sur les clients :

Pour le gouvernement britannique, ZPA est désormais un outil complet utilisé pour fournir des applications et des accès dans AWS. Ce client a adopté un modèle Zero Trust. TOUTES les applications sont accessibles uniquement via ZPA.

Opérations en cours et investissements futurs

Zscaler Private Access permet à AWS et à nos administrateurs clients de créer à l'échelle mondiale des politiques personnalisées en fonction des applications et des utilisateurs. Cette méthode peut réduire la complexité imposée par la segmentation basée sur le réseau.

- Des politiques simples sont utilisées pour segmenter l'accès en fonction de l'identité et de l'application.
- La nécessité de créer et de mettre en œuvre des politiques complexes basées sur les adresses IP est éliminée. En d'autres termes, les opérations peuvent être agiles en interne sans affecter l'utilisateur. Le DevSecOps peut être exploité pour migrer les applications du cloud privé vers le cloud public, tout en maintenant la confidentialité du cloud public.
- Vous pouvez fournir aux clients une plus grande visibilité et un meilleur contrôle des applications auxquelles peuvent accéder les tiers et les sous-traitants.
- Zscaler investit continuellement dans le cloud Zscaler et dans l'amélioration de ses capacités. Ces progrès sont basés sur une bonne connaissance des clients et de leurs exigences acquise par une analyse du trafic de nombreuses organisations à travers le monde qui leur a offert une portée et une visibilité qu'aucune organisation ne peut obtenir par elle même. Cette visibilité apportera une valeur ajoutée permanente à votre investissement lié à ZPA.

L'infrastructure VPN traditionnelle d'accès distant présente un risque pour toute stratégie de migration, car elle élargit la surface de la menace en plaçant toujours l'utilisateur sur le réseau. Zscaler Private Access permet d'éviter ce risque en mettant en œuvre les quatre principes de sécurité clés ci-après :

- Connecter les utilisateurs à des applications privées (dans un VPC ou data center physique) sans les placer sur les réseaux internes
- Ne jamais exposer les applications à des utilisateurs non autorisés
- Permettre la segmentation des applications sans s'appuyer sur une segmentation complexe et coûteuse du réseau, mais en s'alignant étroitement sur les VPC, les groupes de sécurité et/ou d'autres fonctionnalités de service
- Utiliser Internet comme un réseau de transport sécurisé sans recourir aux VPN qui peuvent augmenter la surface d'attaque et nuire à l'expérience utilisateur

Cette approche signifie qu'il ne peut y avoir de mouvement latéral vers des demandes non autorisées. De plus, les applications auxquelles l'utilisateur n'a pas accès restent complètement invisibles. Elles ne peuvent pas être détectées par des scanners de port ou tout autre outil exécuté localement ou depuis Internet et visant l'environnement hébergé. Les applications ne reçoivent aucune connexion entrante provenant directement des utilisateurs.

Gros plan sur les clients :

MAN Energy Solutions fournit désormais aux développeurs partenaires un accès limité aux environnements DevOps et applications nécessaires. L'accès des partenaires représentait une surface d'attaque potentielle ; elle est maintenant contenue, car les contrôles d'accès basés sur l'identité maintiennent ces utilisateurs et leurs appareils hors du réseau.

Conclusion

La fonction principale de Zscaler Private Access est de gérer de manière active l'accès des utilisateurs autorisés aux charges de travail, ainsi que leur interaction avec celles-ci, avant, pendant et après la migration vers le cloud, tout en améliorant l'expérience utilisateur globale.

Les principaux avantages de la transformation sont les suivants :

- Réduction des délais des projets de transformation et de migration
- Amélioration de la posture de sécurité grâce aux applications migrées
- Amélioration de l'expérience utilisateur pendant et après la migration des applications

Voici quelques cas d'utilisation de ZPA :

- Adoption du cloud et migration des applications
- Fusions et acquisitions
- Accès par des tiers

Zscaler Private Access peut être déployé selon des modalités limitées ou globales. ZPA est conçu sur AWS, et ZPA Public Service Edge est déployé sur AWS et sur d'autres sites dans le monde. Les App Connectors de Zscaler se trouvent dans les VPC. Zscaler Client Connector est une application légère qui prend en charge tous les principaux systèmes d'exploitation des PC et des appareils mobiles. Contactez-nous pour un essai gratuit, une démonstration de faisabilité officielle ou un déploiement de production incrémentiel qui tient lieu de démonstration de faisabilité. ZPA est disponible sur AWS Marketplace en tant que liste de contrats SaaS, prenant en charge les offres privées.

Références

Voici quelques ressources supplémentaires utiles :

Page d'accueil de Zscaler : www.zscaler.fr

Page d'accueil de ZPA : www.zscaler.fr/products/zscaler-private-access

Page d'accueil de ZPA pour AWS : www.zscaler.fr/products/zpa-for-aws

Assistance et documentation technique : help.zscaler.com/zia?filter=documentation

MAN Energy Solutions : https://www.zscaler.fr/resources/case-studies/man-energy-solutions-fr.pdf

Cadre d'adoption des technologies cloud d'AWS : aws.amazon.com/professional-services/CAF/

Modèle de responsabilité partagée d'AWS : aws.amazon.com/compliance/shared-responsibility-model/

zscaler™ | Experience your world, secured.™

À propos de Zscaler
Zscaler (NASDAQ: ZS) accélère la transformation digitale de sorte que les clients deviennent plus agiles, plus efficaces, plus résilients et plus en sécurité. La plateforme Zscaler Zero Trust Exchange protège des milliers de clients contre les cyberattaques et la perte des données en connectant de manière sécurisée les utilisateurs, les appareils et les applications indépendamment de l'emplacement. Distribué à travers plus de 150 data centers dans le monde, Zero Trust Exchange basé sur SASE est la plus grande plateforme de sécurité cloud inline. Pour en savoir plus, rendez-vous sur **zscaler.fr** ou suivez-nous sur Twitter **@zscaler**.

+1 408 533 0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.fr