LIVRE ÉLECTRONIQUE

Microsoft Azure + EJBCA

Migrer vers Microsoft Azure avec une ICP moderne

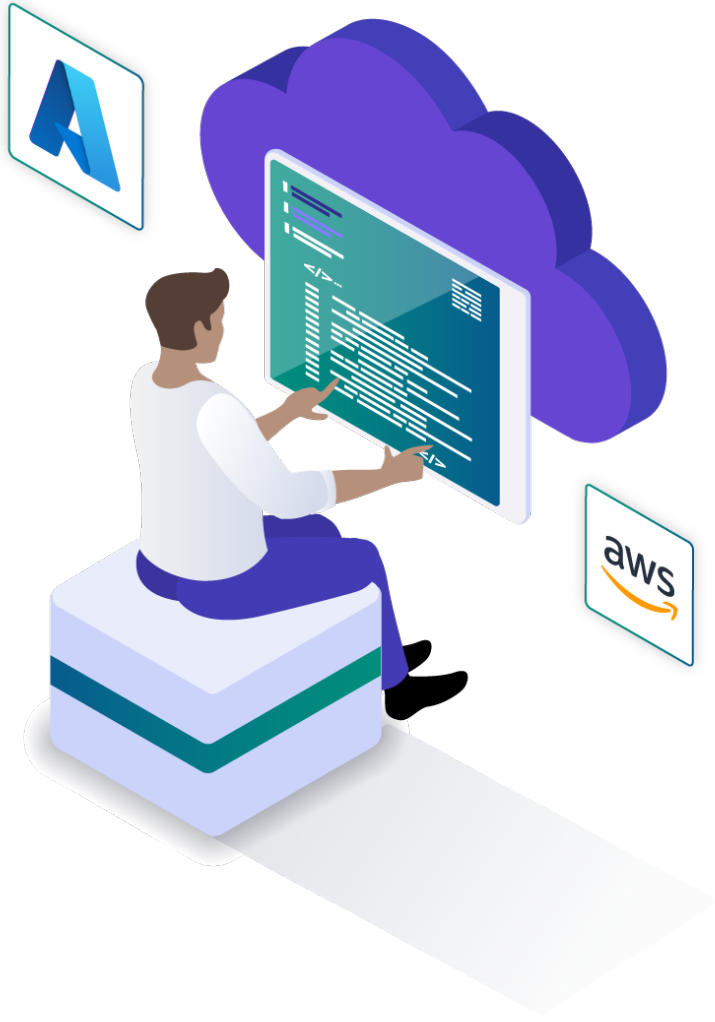
KEYFACTOR

Avantages du hybride et du multi-cloud

Les stratégies hybrides et multi-cloud ne sont pas seulement inévitables, elles sont déjà une réalité pour la plupart des organisations.

Ce n'est un secret pour personne que les organisations adoptent les services cloud pour accroître leur efficacité, permettre l'automatisation, et faire évoluer leur empreinte numérique pour répondre aux nouveaux besoins de l'entreprise. Comme les ordinateurs centraux avant eux, les centres de données deviennent graduellement obsolètes, remplacés par des solutions basées sur le cloud de plus en plus fiables et évolutives.

Dans une étude récente de HashiCorp, 76 % des répondants ont déclaré que leur entreprise utilise déjà une architecture multi-cloud. Dans deux ans, ce nombre passera à 9 entreprises sur 10[1]. En tant que fournisseur leader de services cloud, Microsoft Azure est devenu un incontournable pour l'infrastructure hybride et multi-cloud dans de nombreuses entreprises aujourd'hui.



[1] https://www.hashicorp.com/state-of-the-cloud

Défis de la migration vers le cloud

La transition des centres de données traditionnels vers l'infrastructure cloud est complexe et introduit plusieurs nouveaux défis pour les équipes d'identité et de sécurité.

Aujourd'hui, les applications doivent fonctionner partout et évoluer rapidement. Que votre organisation ait déjà une stratégie axée sur le cloud ou que vous migriez d'anciennes applications vers Microsoft Azure, l'infrastructure à clé publique (ICP) est un élément essentiel pour établir la confiance numérique et connecter en toute sécurité les charges de travail et les applications à grande échelle.

Tout le monde, des architectes de sécurité aux ingénieurs réseau en passant par les équipes d'application et d'exploitation, compte maintenant sur l'ICP et les certificats numériques pour sécuriser les connexions de machine à machine dans les environnements de cloud hybride. Cependant, le passage à des charges de travail et à l'infrastructure dynamiques en tant que code introduit de nouveaux défis pour les déploiements d'ICP.

Plus d'identités

Le nombre de machines et de charges de travail augmente de manière exponentielle, apportant beaucoup plus d'identités de machine dans le mélange.

Charges de travail dynamiques

La nature dynamique de l'infrastructure cloud augmente la vitesse d'émission, de déploiement et de révocation des certificats.

Complexité informatique

Différentes équipes déploient souvent plusieurs technologies d'autorité de certification et d'ICP pour soutenir des cas d'utilisation spécialisés, augmentant la complexité et les coûts.

ICP et identités machine dans Microsoft Azure

Alors que les organisations passent à une infrastructure cloud moderne avec Azure, l'identité joue un rôle central dans la protection des machines et des applications.

La migration ou la création de nouvelles applications dans Microsoft Azure aide les équipes à accroître l'efficacité et la valeur pour l'entreprise. Par conséquent, le nombre de charges de travail, comme les machines virtuelles, les conteneurs, et les microservices, augmente de façon exponentielle. Dans ce nouvel environnement, la sécurité repose sur l'assurance que chaque connexion est authentifiée, cryptée et autorisée à l'aide d'identités uniques et fiables.

Les identités de machine, telles que les certificats X.509, sont partout dans le cloud. Les développeurs et les ingénieurs qui utilisent Azure comptent sur les certificats chaque jour pour développer et exécuter leurs applications en toute sécurité. Une approche globale de la migration vers le cloud, y compris votre ICP et vos services de certificats, est donc essentielle pour garantir que vos équipes puissent profiter de tous les avantages d'Azure tout en restant sécurisées.

Azure AD

Les humains et les machines s'authentifient auprès d'un annuaire pour accéder aux ressources dans Azure via l'authentification basée sur les certificats (CBA).

Azure DevOps

Les services de gestion de conteneurs et les microservices utilisent des certificats pour mettre en œuvre l'authentification sécurisée au sein de l'écosystème Azure.

Azure IoT

Les dispositifs IoT et périphériques nécessitent des certificats en tant que composants de sécurité critiques pour l'authentification et la signature de code.

Microsoft Endpoint Manager

Les machines connectées à Microsoft Intune telles que les appareils mobiles et les ordinateurs portables sont authentifiées et autorisées à l'aide de certificats.

ICP obsolète : Un obstacle au succès du cloud

Lors de la migration des applications vers le cloud, la réalité est souvent que les outils et les processus autrefois utilisés pour sécuriser les environnements locaux traditionnels deviennent beaucoup moins efficaces. Ces anciens outils peuvent même devenir des obstacles opérationnels à la migration réussie vers le cloud dans de nombreux cas. L'ICP et la gestion des certificats ne font pas exception.

Les services de certificats Microsoft Active Directory (ADCS), souvent appelés Microsoft CA, ont longtemps été le choix de facto pour ICP dans les environnements informatiques traditionnels. C'est logique, c'est intégré à Active Directory (AD) et cela fonctionne bien avec l'infrastructure Microsoft. Cependant, la solution CA héritée n'est plus en mesure de répondre aux exigences courantes d'aujourd'hui.

En fait, ADCS est devenu un obstacle opérationnel pour de nombreuses organisations qui adoptent le cloud. Pour commencer, il n'est pas pris en charge de manière native sur Azure. Ce qui est encore plus important, ADCS ne peut pas s'intégrer aux outils et aux plate-formes modernes, et puisqu'une seule CA peut être installée par serveur, il devient rapidement un élément d'infrastructure trop complexe et coûteux à mesure que vous évoluez.

Conclusion : Que vous commenciez tout juste votre migration vers Azure, ou que votre organisation dispose déjà d'une stratégie mature et multi-cloud, les demandes sur l'infrastructure ICP augmentent. Les anciens déploiements d'ICP ne peuvent fournir un soutien suffisant.

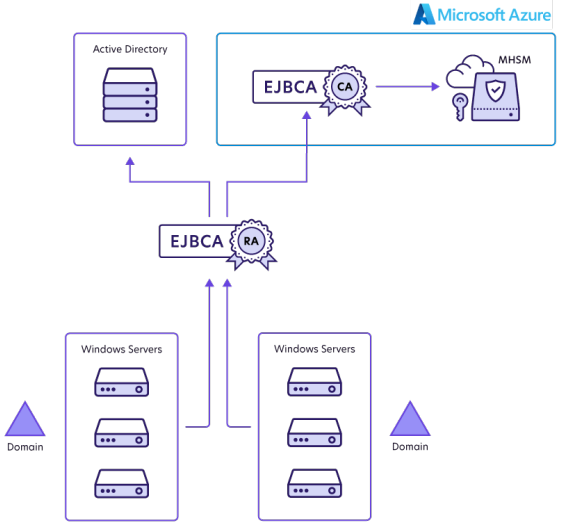
Moderniser ICP avec EJBCA pour Azure

Une plateforme ICP complète conçue pour prendre en charge l'échelle, la disponibilité et l'agilité des environnements hybrides et multi-cloud.

Il est clair que l'ICP et les identités des machines servent d'épine dorsale à la confiance numérique dans le cloud, sécurisant les services essentiels et permettant la connectivité à grande échelle. Pour tirer parti des avantages de la transformation numérique et de la migration vers le cloud, les organisations doivent simplifier et moderniser leur infrastructure ICP.

EJBCA de Keyfactor est une puissante plate-forme flexible d'autorité de certification (CA) et de gestion d'ICP pour émettre et fournir des certificats à l'échelle du cloud. Il s'intègre de manière transparente à votre infrastructure Microsoft et Azure, ce qui facilite l'émission de certificats pour tous les cas d'utilisation, que ce soit sur site ou dans le cloud. Mieux encore, les équipes peuvent déployer EJBCA directement depuis la place de marché cloud Azure ou AWS.

Bâti sur des normes ouvertes et une plateforme open-source, EJBCA apporte la maturité et la transparence attendues d'une infrastructure de sécurité moderne. Il est conçu pour l'évolutivité et la disponibilité du cloud, tout en garantissant la robustesse et la conformité aux bonnes pratiques et aux normes du secteur comme les critères communs.



EJBCA s'exécute dans Azure et s'intègre à votre environnement d'application cloud Azure.

Avantages EJBCA pour Microsoft Azure

Intégration Azure

EJBCA s'intègre aux plates-formes natives Microsoft et Azure via l'inscription automatique, SCEP et la prise en charge d'Intune. L'authentification et l'autorisation de gérer EJBCA se font via l'authentification par certificat ou Azure OAuth, et la visibilité et la surveillance de votre ICP peuvent être gérées via Azure Insight.

Cas d'utilisation multiples

EJBCA prend en charge tous les cas d'utilisation de certificats et tous les formats de certificats sur une seule plateforme. Grâce à une intégration et un support d'automatisation étendus, via des protocoles et des API standard, tels que EST, SCEP, CMP, ACME, REST et des services Web, EJBCA est facilement extensible.

Évolutivité infinie

Contrairement à MS ADCS, EJBCA peut héberger plusieurs infrastructures CA et ICP dans une seule installation. Le déploiement multi-domaines et multi-forêts est pris en charge, ce qui vous permet de consolider les cas d'utilisation de l'ICP sur une seule plate-forme. Vous ne payez que ce que vous utilisez.

Prise en charge HSM intégrée

L'utilisation d'un HSM apporte une sécurité et une conformité de niveau entreprise et maintient toutes les clés cryptographiques en sécurité. EJBCA s'intègre à tous les HSM, y compris Azure Key Vault et Azure Key Vault Managed HSM, ainsi qu'à Thales DPoD et à la plupart des HSM certifiés FIPS et CC du marché.

Déploiement flexible

Pour relever les défis commerciaux uniques de votre organisation, vous pouvez déployer EJBCA selon vos besoins. Il est disponible sur Azure Cloud en tant que service hébergé et géré ou en tant qu'infrastructure en tant que service (IaaS), ainsi que des appliances matérielles ou logicielles pour une conformité spécifique ou d'autres exigences.

Automatisation du cycle de vie des certificats

En ajoutant Keyfactor Command, vous pouvez combiner une ICP hautement évolutive avec une automatisation complète du cycle de vie des certificats. Keyfactor Command offre une visibilité et un contrôle de tous les certificats de votre environnement, qu'ils soient émis par EJBCA ou tout autre service CA public, privé ou basé sur le cloud.

Choisissez la stratégie de migration qui vous convient le mieux

Trouvez le moyen le plus sûr et le plus efficace pour votre organisation de moderniser l'ICP dans Azure.

Les enjeux sont importants lors de la migration ou de la consolidation de l'infrastructure ICP d'entreprise. Il est impératif que les solutions actuelles rendues possibles par les services de certificat existants continuent de fonctionner avec peu d'interruptions, que le projet de migration gère les interfaces et les intégrations existantes avec les systèmes externes, et que la solidité de l'infrastructure soit maintenue - ou améliorée - avec la migration.

Avec EJBCA, vous pouvez choisir la stratégie de migration qui convient le mieux à votre situation actuelle. Voici trois options de migration courantes :

Nouveau départ

Démarrez un nouveau déploiement EJBCA pour de nouveaux cas d'utilisation et migrez les services de certificats existants en aval.

Migrez

Simplifiez et consolidez votre infrastructure ICP avec une couverture complète vers EJBCA et la migration de tous les cas d'utilisation existants.

Étendez

Conservez votre autorité de certification Microsoft, mais implémentez EJBCA pour les cas d'utilisation modernes qui nécessitent plus de flexibilité et d'évolutivité.

Commencez avec EJBCA Cloud

Si vous êtes prêt à moderniser votre ICP, vous pouvez commencer à essayer EJBCA Cloud dès aujourd'hui - et gratuitement.

Essayez EJBCA sur Azure | Essayez EJBCA sur AWS

Découvrez des cas d'utilisation :

- Utiliser Keyfactor Command avec EJBCA pour l'automatisation du cycle de vie des certificats
- Migration d'ADCS vers EJBCA
- Sécuriser votre environnement Microsoft avec EJBCA
- Intégrer EJBCA avec Microsoft Intune

KEYFACTOR

À propos de Keyfactor

Keyfactor est la plate-forme d'identité machine et IoT pour les entreprises modernes. L'entreprise aide les équipes de sécurité à gérer la cryptographie comme une infrastructure critique en simplifiant l'ICP, en automatisant la gestion du cycle de vie des certificats, et en favorisant l'agilité cryptographique à grande échelle.

Pour en savoir plus, visitez www.keyfactor.com ou suivez-nous sur LinkedIn, Twitter, et Facebook.

Bâti sur la confiance et la sécurité, Keyfactor est un fier employeur garantissant l'égalité des chances, un partisan et un défenseur de la création d'un lieu de travail fiable, sécurisé, diversifié et inclusif.

Contactez-nous

- www.keyfactor.com
- +1.216.785.2946