Gestion de l'identité et de l'accès pour VMware Cloud on AWS

AWS Conseils prescriptifs

AWS Conseils prescriptifs: Gestion de l'identité et de l'accès pour VMware Cloud on AWS

Table of Contents

Gestion des identités et des accès pour VMware Cloud on AWS

Richard Milner-Watts, Abdenour Kansab et Chris Porter, Amazon Web Services (AWS)

Vern Bolinius, VMware

Juin 2023 (historique du document)

La gestion des identités et des accès est le principe qui consiste à limiter l'accès aux systèmes aux utilisateurs et applications autorisés, notamment en restreignant l'accès aux ressources réseau nécessaires. Dans les environnements cloud, les contrôles de gestion des identités et des accès comprennent généralement les stratégies et les services que vous utilisez pour identifier, authentifier et autoriser les utilisateurs, les groupes d'utilisateurs et les applications.

VMware Cloud on AWS prend en charge vos charges de travail basées sur VMware vSphere dans le AWS Cloud. Vous pouvez utiliser de nombreux services et outils VMware pour configurer, gérer, sauvegarder, surveiller et analyser cette infrastructure cloud. Les fonctionnalités et les contrôles que vous utilisez pour gérer les identités et les accès varient selon les services. Ce document fournit les bonnes pratiques et les recommandations relatives à la gestion des identités et des accès pour les services VMware suivants :

- VMware Aria Operations
- VMware Aria Operations for Logs
- VMware Aria Operations for Networks
- VMware Cloud Disaster Recovery
- VMware Cloud on AWS
- VMware Cloud Services Console
- VMware HCX
- VMware NSX
- VMware Site Recovery
- VMware vCenter Server

Ce guide fournit une vue d'ensemble et les bonnes pratiques en matière de gestion des identités et des accès pour VMware Cloud on AWS et les services VMware associés. Il inclut une brève

description de chaque service et aborde les considérations relatives à la gestion de l'accès et des identités pour ce service. Nous fournissons également des recommandations pour configurer le service dans le cadre de VMware Cloud on AWS.

> **Important**
>
> La plupart des services VMware décrits dans ce guide sont utilisés dans d'autres solutions VMware sur site ou cloud. Les recommandations et les bonnes pratiques de ce guide sont propres à VMware Cloud on AWS. Ces recommandations peuvent ne pas s'appliquer à d'autres environnements.

Public visé

Ce guide est destiné aux architectes et aux ingénieurs de sécurité chargés de l'implémentation de VMware Cloud on AWS dans leur environnement cloud ou hybride.

Résultats commerciaux ciblés

Ce guide vous aide à accomplir les tâches suivantes :

1. Découvrir les différents contrôles de gestion des identités et des accès pour VMware Cloud on AWS et les services VMware associés
2. Se familiariser avec les bonnes pratiques recommandées qui vous aident à exploiter VMware Cloud on AWS en toute sécurité
3. Découvrir les options disponibles pour l'authentification fédérée via un fournisseur d'identité externe

Vue d'ensemble de la gestion des identités

VMware utilise les concepts de conformité aux normes du secteur et la hiérarchie des identités suivants pour gérer l'identification, l'authentification et l'autorisation :

- Les utilisateurs sont les personnes qui accèdent à votre environnement à quelque titre que ce soit. Vous pouvez créer des utilisateurs locaux ou utiliser la fédération pour authentifier les utilisateurs auprès d'un fournisseur d'identité externe. Pour de plus amples informations, veuillez consulter Fédération d'identité et SSO.
- Les groupes fournissent un mécanisme permettant de regrouper logiquement un ensemble d'utilisateurs. Cela vous permet d'accorder des autorisations cohérentes à ces utilisateurs et de réduire la surcharge administrative. Les rôles servent à accorder des autorisations à un utilisateur ou à un groupe. Pour plus d'informations, veuillez consulter Rôles et autorisations dans le SDDC (documentation VMware).
- Les organisations dans VMware Cloud contrôlent l'accès à un ou plusieurs services VMware. Les utilisateurs et les groupes doivent appartenir à une organisation pour accéder à ses services. Vous pouvez activer la fonctionnalité Gouvernance et administration des identités permettant aux identités fédérées de demander en libre-service l'adhésion à une organisation VMware. Pour de plus amples informations, veuillez consulter VMware Cloud Services Console.

Les autorisations peuvent accorder l'accès à un objet spécifique ou elles peuvent être héritées d'objets parents. Si plusieurs autorisations qui se chevauchent sont attribuées à un utilisateur ou à un groupe, l'autorisation la plus permissive s'applique. Pour plus d'informations, veuillez consulter Héritage hiérarchique des autorisations (documentation VMware).

Vous pouvez utiliser ces éléments structurels pour adopter une stratégie de moindre privilège et établir des limites d'accès logiques au sein de votre infrastructure en fonction des besoins des utilisateurs. Le moindre privilège est le principe qui consiste à n'accorder aux utilisateurs et aux applications que l'accès minimum nécessaire à l'exécution de leurs tâches. En cas d'accès non autorisé, cette bonne pratique du secteur peut contribuer à limiter la capacité d'un pirate à endommager ou à voler des données sensibles. Et même pour les utilisateurs autorisés, ce principe peut empêcher les utilisateurs d'accéder à des données auxquelles ils n'auraient pas dû avoir accès. En donnant aux utilisateurs l'accès uniquement aux ressources nécessaires, il est également possible d'améliorer la productivité et de réduire le besoin d'assistance en matière de résolution des problèmes.

Lorsque vous utilisez VMware Cloud on AWS, il existe deux principaux services et outils de gestion des identités et des accès : VMware Cloud Services Console et VMware vCenter Server. Nous aborderons ces services plus en détail plus loin dans ce guide.

Fédération d'identité et SSO

De nombreuses entreprises souhaitent configurer une fédération avec un fournisseur d'identité (IdP) externe. Cela vous permet d'offrir à vos utilisateurs une authentification unique (SSO). VMware Cloud et vCenter Server prennent tous deux en charge la fédération d'entreprise :

- VMware Cloud prend en charge les IdP basés sur le langage SAML (Security Assertion Markup Language) 2.0 et le protocole LDAP (Lightweight Directory Access Protocol). Pour plus d'informations, veuillez consulter Qu'est-ce que la fédération d'entreprise et comment fonctionne-t-elle avec VMware Cloud Services ? (documentation VMware).
- Lorsque vous utilisez vCenter Server sur VMware Cloud on AWS, la fédération sur vCenter Server à l'aide d'un IdP externe n'est actuellement pas prise en charge. Seul l'IdP intégré qui prend en charge l'utilisation de Microsoft Active Directory via LDAP peut être utilisé. Pour plus d'informations, veuillez consulter Sources d'identité pour vCenter Server avec vCenter Single Sign-On (documentation VMware).

Certains des autres services VMware associés abordés dans ce guide prennent également en charge la fédération directe à partir d'un IdP. Cependant, la configuration de la fédération dans chaque service crée d'autres points de gestion des utilisateurs et devient difficile à gérer. Vous pouvez plutôt utiliser des groupes et des rôles dans VMware Cloud Services Console pour utiliser une source d'identité commune et configurer des autorisations pour d'autres services VMware Cloud. Vous pouvez également configurer le mode Hybrid Linked Mode afin d'utiliser les mêmes identités avec une instance de vCenter Server sur site. Cela permet de réduire le nombre de points de fédération et de gestion des identités à deux services. Pour plus d'informations sur Hybrid Linked Mode, veuillez consulter Configuration d'Hybrid Linked Mode (documentation VMware).

Bonnes pratiques d'ordre général

> **Important**
>
> La plupart des services VMware décrits dans ce guide sont utilisés dans d'autres solutions VMware sur site ou cloud. Les recommandations et les bonnes pratiques de ce guide sont propres à VMware Cloud on AWS. Ces recommandations peuvent ne pas s'appliquer à d'autres environnements.

Tenez compte des recommandations AWS suivantes pour gérer l'identité et l'accès à votre infrastructure cloud VMware :

- Appliquez la stratégie du moindre privilège. Utilisez le contrôle d'accès basé sur les rôles (RBAC) pour accorder les autorisations et l'accès minimum dont ont besoin les utilisateurs dans le cadre de leurs fonctions.
- Dans la mesure du possible, accordez des autorisations à des groupes plutôt qu'à des utilisateurs individuels.
- Évitez de configurer des utilisateurs locaux. Authentifiez les utilisateurs auprès d'un fournisseur d'identité fédérée externe.
- Configurez l'authentification multifactorielle pour tous les utilisateurs.
- Votre stratégie de mot de passe doit inclure des exigences en matière de robustesse et de rotation des mots de passe.
- Documentez une procédure de bris de glace pour prendre le contrôle administratif total de l'organisation VMware et des services associés. Le bris de glace, qui tire son nom du fait de briser une vitre pour déclencher une alarme incendie, désigne un moyen permettant à une personne d'obtenir rapidement un accès administratif dans des circonstances exceptionnelles, en utilisant un processus approuvé et vérifié.
- Si vous disposez de centres de données sur site ou de plusieurs instances vCenter Server, utilisez Hybrid Linked Mode pour connecter votre instance cloud vCenter Server au domaine vCenter Single Sign-On sur site. Cela vous permet de gérer vos ressources cloud et sur site à partir d'une seule interface vSphere Client.
- Dans la mesure du possible, configurez les points de terminaison de gestion, tels que vCenter Server, HCX Cloud Manager et NSX Manager, pour qu'ils soient accessibles uniquement depuis des réseaux internes, plutôt que depuis l'Internet public.

- N'utilisez pas d'informations d'identification locales, telles que le compte cloudadmin, à des fins administratives. Réservez ces comptes pour les utiliser dans le cadre de votre procédure de bris de glace. Les actions effectuées à l'aide de comptes d'utilisateurs locaux administratifs ne peuvent pas être attribuées à une personne en particulier. Ces comptes peuvent donc être utilisés pour apporter des modifications sans responsabilité.
- Modifiez les mots de passe des comptes locaux, tels que les utilisateurs root et administratifs, pour qu'ils aient des valeurs fortes et stockez ces informations d'identification en toute sécurité dans un magasin de mots de passe vérifié. Établissez un processus d'approbation pour accorder l'accès à ces mots de passe.
- Si les informations d'identification locales doivent être conservées pendant de longues périodes, par exemple pendant plusieurs mois ou plus, établissez un processus de rotation des informations d'identification (par exemple, si vous utilisez VMware HCX pour étendre un réseau).

Ces recommandations s'appliquent à toutes les configurations de service VMware pour VMware Cloud on AWS. Des recommandations supplémentaires pour chaque service sont abordées plus loin dans ce guide.

Services de gestion des identités VMware

Lorsque vous utilisez VMware Cloud on AWS, il existe deux principaux services et outils de gestion des identités et des accès : VMware Cloud Services Console et VMware vCenter Server.

VMware Cloud Services Console

VMware Cloud Services Console (documentation VMware) vous aide à gérer votre portefeuille de services VMware Cloud, qui inclut VMware Cloud on AWS. Dans ce service, vous pouvez effectuer les actions suivantes :

- Gérer les entités, telles que les utilisateurs et les groupes
- Gérer les organisations qui contrôlent l'accès à d'autres services cloud, comme VMware Cloud Disaster Recovery (VCDR) et VMware Aria Suite
- Attribuer des rôles aux ressources et aux services
- Afficher les applications OAuth qui ont accès à votre organisation
- Configurer la fédération d'entreprise pour l'organisation
- Activer et déployer les services VMware Cloud, tels que VMware Aria et VMware Cloud on AWS
- Gérer la facturation et les abonnements
- Bénéficier de l'assistance VMware

Gestion des identités et des accès

En configurant correctement les utilisateurs, les groupes, les rôles et les organisations dans VMware Cloud Services Console, vous pouvez implémenter une stratégie d'accès fondée sur le principe du moindre privilège.

Il est essentiel de sécuriser l'accès à VMware Cloud Services Console, car les utilisateurs administratifs de ce service peuvent modifier les autorisations dans l'ensemble de votre environnement cloud VMware et accéder à des informations sensibles, telles que celles relatives à la facturation. Pour accéder à toutes les fonctionnalités de la console, telles que la facturation et l'assistance, les utilisateurs doivent également être associés à un profil VMware Customer Connect (anciennement appelé MyVMware).

Dans VMware Cloud Services Console, vous utilisez les types de rôles suivants pour accorder des autorisations aux utilisateurs et aux groupes :

- Rôles de l'organisation : ces rôles concernent directement l'organisation VMware Cloud et accordent des autorisations au sein de la console VMware Cloud Services. Il existe deux rôles standard. Le rôle Propriétaire de l'organisation dispose des autorisations complètes pour administrer l'organisation. Le rôle Membre de l'organisation dispose d'un accès en lecture à VMware Cloud Services Console. Pour plus d'informations, veuillez consulter Quels rôles d'organisation sont disponibles dans VMware Cloud Services ? (documentation VMware).
- Fonctions du service : ces rôles vous permettent d'attribuer des autorisations pour utiliser un service spécifique. Par exemple, une entité dotée de la fonction du service Admin DR peut administrer VMware Cloud Disaster Recovery (VCDR) dans la console de service dédiée. Chaque service disponible au sein de l'organisation est associé à une ou plusieurs fonctions du service. Pour plus d'informations sur les fonctions du service disponibles, veuillez consulter la documentation VMware relative au service qui vous intéresse.

VMware Cloud Services Console prend en charge les stratégies d'authentification. Celles-ci peuvent stipuler qu'un utilisateur doit fournir un deuxième jeton d'authentification lors de sa connexion, ce que l'on appelle également l'aauthentification multifactorielle (MFA).

Pour plus d'informations sur la gestion des identités et des accès dans ce service, veuillez consulter Gestion des identités et des accès (documentation VMware).

Recommandations concernant AWS

En plus des Bonnes pratiques d'ordre général, AWS adresse les recommandations suivantes lors de la configuration de VMware Cloud Services Console pour VMware Cloud on AWS :

- Lors de la création d'une organisation, utilisez un profil VMware Customer Connect et une adresse e-mail professionnelle associée qui n'appartiennent pas à une personne, comme vmwarecloudroot@exemple.com. Ce compte doit être traité comme un compte de service, ou root, et vous devez vérifier son utilisation et restreindre l'accès au compte de messagerie. Configurez immédiatement la fédération de comptes avec votre fournisseur d'identité (IdP) d'entreprise afin que les utilisateurs puissent accéder à l'organisation sans utiliser ce compte. Réservez ce compte à une utilisation dans le cadre d'une procédure de bris de glace visant à résoudre les problèmes liés à l'IdP fédéré.
- Utilisez des identités fédérées pour que l'organisation accorde l'accès à d'autres services cloud, tels que VMware Cloud Disaster Recovery (VCDR). Ne gérez pas individuellement les utilisateurs ou les fédérations dans plusieurs services. Cela simplifie la gestion de l'accès à plusieurs services, par exemple lorsque les utilisateurs rejoignent ou quittent l'entreprise.

- Accordez le rôle Propriétaire de l'organisation avec parcimonie. Les entités dotées de ce rôle peuvent s'octroyer un accès complet à tous les aspects de l'organisation et à tous les services cloud associés.

VMware vCenter Server

Serveur VMware vCenter (site Web de VMware) est un plan de gestion permettant d'administrer les environnements VMware vSphere. Dans vCenter Server, vous gérez les entités qui peuvent accéder aux ressources vSphere, telles que les machines virtuelles, et aux modules complémentaires, tels que VMware HCX et VMware Site Recovery. Vous gérez vCenter Server via l'application vSphere Client. Dans vCenter Server, vous pouvez effectuer les actions suivantes :

- Gérer les machines virtuelles, les hôtes VMware ESXi et le stockage VMware vSAN
- Configurer et gérer vCenter Single Sign-On

Si vous avez des centres de données sur site, vous pouvez utiliser Hybrid Linked Mode pour lier votre instance cloud vCenter Server à un domaine vCenter Single Sign-On sur site. Si le domaine vCenter Single Sign-On contient plusieurs instances de vCenter Server connectées via Enhanced Linked Mode, toutes ces instances sont liées à votre SDDC cloud. Ce mode vous permet de visualiser et de gérer vos centres de données sur site et cloud à partir d'une seule interface vSphere Client, et vous pouvez migrer les charges de travail entre votre centre de données sur site et le SDDC cloud. Pour plus d'informations, veuillez consulter Configuration d'Hybrid Linked Mode (documentation VMware).

Gestion des identités et des accès

Dans les centres de données définis par logiciel (SDDC) (site Web de VMware) pour VMware Cloud on AWS, le mode d'exploitation de vCenter Server est similaire à celui d'un SDDC sur site. La principale différence est que VMware Cloud on AWS est un service géré. VMware est donc responsable de certaines tâches administratives, telles que la gestion des hôtes, des clusters et des machines virtuelles de gestion. Pour plus d'informations, veuillez consulter Quelles sont les différences dans le cloud ? et Autorisations globales (documentation VMware).

Étant donné que VMware exécute certaines tâches administratives pour le SDDC, un administrateur cloud a besoin de moins de privilèges qu'un administrateur d'un centre de données sur site. Lorsque vous créez un SDDC VMware Cloud on AWS, un utilisateur cloudadmin est automatiquement créé et associé au rôle CloudAdmin (documentation VMware). Vous pouvez utiliser ce compte utilisateur local privilégié pour accéder à vCenter Server et à vCenter Single Sign-On. Les utilisateurs qui

disposent de la fonction du service Administrateur ou Administrateur (suppression restreinte) VMware Cloud on AWS dans VMware Cloud Services Console peuvent obtenir les informations d'identification pour l'utilisateur cloudadmin. Le rôle CloudAdmin dispose du maximum d'autorisations possibles dans vCenter Server pour un SDDC VMware Cloud on AWS. Pour plus d'informations sur cette fonction du service, veuillez consulter Privilèges de CloudAdmin (documentation VMware). L'utilisateur cloudadmin est le seul utilisateur local disponible pour vCenter Server dans VMware Cloud on AWS. Pour accorder l'accès à d'autres utilisateurs, utilisez une source d'identité externe.

vCenter Single Sign-On est un courtier d'authentification qui propose une infrastructure d'échange de jetons de sécurité. Lorsqu'un utilisateur s'authentifie auprès de vCenter Single Sign-On, il reçoit un jeton qui peut être utilisé pour s'authentifier auprès de vCenter Server et d'autres services complémentaires à l'aide d'appels d'API. L'utilisateur cloudadmin peut configurer une source d'identité externe pour vCenter Server. Pour plus d'informations, veuillez consulter Sources d'identité pour vCenter Server avec vCenter Single Sign-On (documentation VMware).

Dans vCenter Server, vous utilisez les trois types de rôles suivants pour accorder des autorisations aux utilisateurs et aux groupes :

- Rôles système : vous ne pouvez ni modifier ni supprimer ces rôles.
- Exemples de rôles : ces rôles représentent des combinaisons de tâches fréquemment effectuées. Vous pouvez copier, modifier ou supprimer ces rôles.
- Rôles personnalisés : si le système et les exemples de rôles ne fournissent pas le contrôle d'accès souhaité, vous pouvez créer des rôles personnalisés dans vSphere Client. Vous pouvez dupliquer et modifier un rôle existant, ou vous pouvez en créer un autre. Pour plus d'informations, veuillez consulter Créer un rôle personnalisé dans vCenter Server (documentation VMware).

Pour chaque objet de l'inventaire SDDC, vous ne pouvez attribuer qu'un seul rôle à un utilisateur ou à un groupe. Si, pour un seul objet, un utilisateur ou un groupe nécessite une combinaison de rôles intégrés, deux options s'offrent à vous. La première option consiste à créer un rôle personnalisé avec les autorisations requises. L'autre option consiste à créer deux groupes, à attribuer un rôle intégré à chacun, puis à ajouter l'utilisateur aux deux groupes.

Recommandations concernant AWS

En plus des Bonnes pratiques d'ordre général, AWS adresse les recommandations suivantes lors de la configuration de vCenter Server pour VMware Cloud on AWS :

- Utilisez le compte utilisateur cloudadmin pour configurer une source d'identité externe dans vCenter Single Sign-On. Attribuez les utilisateurs appropriés à partir de la source d'identité externe à utiliser à des fins administratives, puis cessez d'utiliser l'utilisateur cloudadmin. Pour connaître les bonnes pratiques en matière de configuration de vCenter Single Sign-On, veuillez consulter Information Security and Access for vCenter Server (documentation VMware).
- Dans vSphere Client, mettez à jour les informations d'identification cloudadmin pour chaque instance de vCenter Server vers une nouvelle valeur, puis stockez-les en toute sécurité. Cette modification n'est pas reflétée dans VMware Cloud Services Console. Par exemple, l'affichage des informations d'identification via Cloud Services Console affiche la valeur d'origine.

> **Note**
>
> En cas de perte des informations d'identification de ce compte, le support VMware peut les réinitialiser.

- N'utilisez pas le compte cloudadmin pour un accès quotidien. Réservez ce compte à une utilisation dans le cadre d'une procédure de bris de glace.
- Limitez l'accès réseau à vCenter Server aux réseaux privés.

Services VMware associés

Ce chapitre fournit les bonnes pratiques et les recommandations relatives à la gestion des identités et des accès pour les services VMware associés à VMware Cloud on AWS :

- Services gérés via VMware Cloud Services Console :
  - VMware Cloud on AWS
  - VMware NSX
  - VMware Aria Operations for Logs
  - VMware Aria Operations for Networks
  - VMware Aria Operations
  - VMware Cloud Disaster Recovery
- Services gérés via VMware vCenter Server :
  - VMware HCX
  - VMware Site Recovery

Ce guide fournit une brève description de chaque service, décrit les contrôles d'identité, d'accès et de gestion pour ce service, et inclut des recommandations AWS pour configurer ce service dans le cadre de VMware Cloud on AWS.

VMware Cloud on AWS

VMware Cloud on AWS (documentation VMware) est un service conçu conjointement par AWS et VMware pour vous aider à migrer et à étendre vos environnements sur site basés sur VMware vSphere vers le AWS Cloud.

Vous pouvez accéder à VMware Cloud on AWS via VMware Cloud Services Console, si vous appartenez à une organisation qui accorde l'accès à ce service. Dans VMware Cloud on AWS, vous pouvez effectuer les actions suivantes :

- Créer et supprimer des SDDC.
- Administrer des groupes SDDC.
- Administrer des SDDC, y compris les paramètres réseau et de cluster.

- Accéder aux informations d'identification d'utilisateur cloudadmin pour VMware vCenter Server. Pour plus d'informations sur cet utilisateur, veuillez consulter VMware vCenter Server dans ce guide.
- Accédez aux informations d'identification d'utilisateur cloud_admin pour VMware NSX. Pour plus d'informations sur cet utilisateur, veuillez consulter VMware NSX dans ce guide.
- Activez et déployez des services complémentaires au sein des SDDC, tels que VMware Site Recovery et VMware HCX.
- Accédez aux consoles pour les services complémentaires, notamment HCX et VMware Site Recovery.

Gestion des identités et des accès

Vous utilisez VMware Cloud Services Console pour gérer les identités et l'accès à VMware Cloud on AWS. Pour VMware Cloud on AWS, les fonctions du service suivantes sont disponibles :

- Administrateur : ce rôle dispose d'un accès complet à VMware Cloud on AWS.
- Administrateur (suppression restreinte) : ce rôle dispose d'un accès complet à VMware Cloud on AWS, à l'exception des opérations de suppression de SDDC.
- Administrateur de NSX Cloud
- Auditeur NSX Cloud

> **Note**
>
> Administrateur de NSX Cloud et Auditeur NSX Cloud sont liés à l'utilisation de VMware NSX. Pour de plus amples informations, veuillez consulter VMware NSX.

L'un des deux rôles Administrateur est nécessaire pour accéder à un SDDC dans le portail des services cloud. Les utilisateurs dépourvus de l'un des deux rôles NSX Cloud ne peuvent pas accéder à l'onglet Réseau et sécurité du SDDC dans le portail des services cloud. De plus, ils ne peuvent pas accéder aux informations d'identification d'administrateur NSX.

Recommandations concernant AWS

En plus des Bonnes pratiques d'ordre général, AWS adresse les recommandations suivantes lors de la configuration de VMware Cloud on AWS :

- Pour accorder l'accès aux administrateurs, utilisez uniquement le rôle Administrateur (suppression restreinte). Réservez le rôle Administrateur à un accès bris de glace lorsque vous devez supprimer un SDDC.
- N'accordez pas les rôles NSX à des utilisateurs qui n'ont pas besoin d'accéder aux configurations réseau et de pare-feu. Pour plus d'informations, consultez VMware NSX dans ce guide.
- Modifiez les mots de passe pour le compte utilisateur local cloudadmin pour qu'ils aient des valeurs fortes et stockez ces informations d'identification en toute sécurité dans un magasin de mots de passe vérifié. Vous pouvez modifier ce mot de passe dans VMware vCenter Server à l'aide de vSphere Web Client.

VMware NSX

VMware NSX (documentation VMware) fournit une couche de virtualisation réseau qui reproduit le modèle OSI (Open Systems Interconnection) de la couche 2 à la couche 7, avec des fonctionnalités telles que la commutation, le routage et les pare-feux. Il existe deux versions de NSX. La version d'origine (NSX-V) nécessite également le déploiement de vCenter Server. La nouvelle version (NSX-T) est découplée de vCenter Server, ce qui permet la prise en charge des architectures hybrides. VMware Cloud on AWS utilise NSX-T.

NSX, avec vSphere et vSAN, est un composant essentiel de VMware Cloud on AWS. NSX propose toutes les fonctionnalités de mise en réseau d'un SDDC et gère l'interaction entre le réseau de superposition et les composants natifs AWS qui constituent la sous-couche du réseau. NSX est étroitement associé à d'autres services, tels que vCenter Server et VMware HCX, qui font appel aux API NSX pour gérer les ressources.

Dans NSX, vous pouvez effectuer les actions suivantes :

- Gérer la commutation et le routage
- Gérer les pare-feux, notamment en utilisant un pare-feu distribué pour l'inspection en ligne entre les machines virtuelles ou entre le réseau et l'Internet public
- Gérer les réseaux privés virtuels (VPN)
- Configurer le protocole de configuration d'hôte dynamique (DHCP) et le système de nom de domaine (DNS)

Vous pouvez accéder à NSX depuis VMware Cloud Services Console ou via l'interface utilisateur Web de NSX Manager dédiée. L'interface utilisateur Web de NSX Manager propose des

fonctionnalités supplémentaires qui ne sont pas disponibles dans VMware Cloud Services Console. Pour plus d'informations, veuillez consulter Administration du réseau SDDC avec NSX Manager (documentation VMware).

Notez ce qui suit lorsque vous accédez à NSX dans VMware Cloud on AWS :

- Pour accéder à NSX via VMware Cloud Services Console, le rôle Administrateur VMware Cloud on AWS doit vous être attribué. Vous pouvez accéder à NSX sur l'onglet Réseau et sécurité du SDDC. Pour plus d'informations sur ce rôle, veuillez consulter VMware Cloud on AWS dans ce guide.
- Vous pouvez ouvrir l'interface utilisateur Web de NSX Manager en choisissant le lien sur l'onglet Paramètres du SDDC ou en choisissant Ouvrir NSX Manager sur la page Résumé du SDDC. Pour plus d'informations, veuillez consulter Ouvrir NSX Manager (documentation VMware).
- Si le SDDC est en mode Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS), vous ne pouvez pas accéder à NSX via l'onglet Réseau et sécurité dans VMware Cloud Services Console. Vous devez utiliser l'interface utilisateur Web de NSX Manager.

Gestion des identités et des accès

Vous utilisez VMware Cloud Services Console pour gérer les identités et les accès à VMware NSX. Pour NSX dans VMware Cloud on AWS, les fonctions du service suivantes sont disponibles :

- Administrateur de NSX Cloud : ce rôle permet d'administrer les fonctionnalités de VMware NSX avec VMware Cloud on AWS.
- Auditeur NSX Cloud : ce rôle peut consulter les paramètres et les événements du service NSX, mais ne peut apporter aucune modification.

> **Note**
>
> Malgré leur nom, ces rôles ne sont pas liés au service VMware NSX Cloud.

Les utilisateurs suivants peuvent accéder à NSX :

- L'utilisateur local cloud_admin, qui est un utilisateur NSX local intégré et hautement privilégié. Les utilisateurs qui disposent du rôle Administrateur de NSX Cloud peuvent accéder aux informations d'identification de ce compte utilisateur. Malgré leurs noms similaires, l'utilisateur cloud_admin est distinct de l'utilisateur local de vCenter Single Sign-On cloudadmin@vmc.local.

- Utilisateurs auxquels a été attribué une fonction du service Administrateur de NSX Cloud ou Auditeur NSX Cloud dans VMware Cloud Services Console. Ces utilisateurs peuvent être des utilisateurs de VMware Cloud Services Console ou des utilisateurs fédérés externes.
- Utilisateurs auxquels l'accès à NSX a été directement accordé à partir d'une source d'identité via LDAP.

Recommandations concernant AWS

En plus des Bonnes pratiques d'ordre général, AWS adresse les recommandations suivantes lors de la configuration de NSX pour VMware Cloud on AWS :

- Si des utilisateurs de votre entreprise sont chargés de gérer la mise en réseau et les pare-feux, mais pas de gérer les SDDC, accordez-leur l'un des rôles NSX, mais pas le rôle Administrateur. Ces utilisateurs doivent accéder à NSX via l'interface utilisateur Web de NSX Manager.
- Modifiez les mots de passe pour le compte utilisateur local cloud_admin pour qu'ils aient des valeurs fortes et stockez ces informations d'identification en toute sécurité dans un magasin de mots de passe vérifié. Pour modifier ce mot de passe, vous devez contacter le support VMware.
- Évitez d'accorder l'accès à des utilisateurs externes directement dans NSX. Configurez plutôt la fédération d'entreprise dans VMware Cloud Services Console, puis utilisez des rôles et des groupes pour accorder l'accès à ce service.

VMware Aria Operations for Logs

VMware Aria Operations for Logs (documentation VMware), anciennement VMware vRealize Log Insight Cloud, est un outil de stockage et d'analyse de journaux qui vous permet de visualiser et d'interroger les données de journal produites par vos SDDC VMware. Dans VMware Aria Operations for Logs, vous pouvez effectuer les actions suivantes :

- Effectuer une intégration aux instances sur site de vRealize Operations
- Collecter et analyser tous les types de données de journal générées par des machines
- Configuration des alertes
- Surveiller et analyser les journaux des autres services VMware

Il existe deux versions de ce service centralisé de gestion des journaux. VMware vRealize Log Insight est une version sur site qui peut être exécutée en tant qu'appareil au sein de votre SDDC. VMware

Aria Operations for Logs est une version logicielle en tant que service (SaaS). VMware Cloud on AWS utilise la version cloud comme service de journalisation par défaut, et cela ne peut pas être modifié. Si vous utilisez la version sur site, vous devez transférer les journaux de l'instance cloud vers votre instance sur site.

VMware Aria Operations for Logs est inclus dans VMware Cloud on AWS. La version incluse a une capacité d'ingestion et une durée de conservation du stockage limitées. Si nécessaire, vous pouvez passer à un abonnement premium pour augmenter ces limites. Pour plus d'informations, veuillez consulter Acheter et utiliser des abonnements VMware Aria Universal Suite (documentation VMware).

Gestion des identités et des accès

Vous utilisez VMware Cloud Services Console pour gérer les identités et l'accès à VMware Aria Operations for Logs. VMware Aria Operations for Logs utilise les mêmes utilisateurs, y compris les identités fédérées, et les mêmes groupes que ceux que vous avez configurés dans VMware Cloud Services Console. Pour accorder des autorisations pour ce service, vous pouvez attribuer une fonction du service ou configurer un rôle personnalisé dans VMware Aria Operations for Logs. Pour plus d'informations, veuillez consulter Service Roles (documentation VMware).

VMware vRealize Log Insight possède deux rôles par défaut. Le rôle Administrateur dispose d'un accès et d'un contrôle complets, tandis que le rôle Utilisateur dispose d'un accès en lecture et peut créer des tableaux de bord. Vous pouvez utiliser des rôles personnalisés pour n'autoriser l'accès qu'à des jeux de données spécifiques. Ces jeux de données contiennent des filtres qui limitent les données de journal accessibles à l'utilisateur. Pour plus d'informations, veuillez consulter Create a Data Set (documentation VMware).

Recommandations concernant AWS

Respectez les Bonnes pratiques d'ordre général décrites précédemment dans ce guide. Nous n'avons pas de recommandations supplémentaires concernant la gestion des identités et des accès dans ce service.

VMware Aria Operations for Networks

VMware Aria Operations for Networks, anciennement VMware vRealize Network Insight Cloud, est une version SaaS de vRealize Network Insight. VMware vRealize Network Insight (documentation VMware) vous aide à comprendre les flux de trafic liés à vos charges de travail. Vous pouvez utiliser ce service pour diagnostiquer les problèmes de mise en réseau et modéliser des règles de pare-feu

afin de prendre en charge la segmentation de charge de travail. Dans VMware Aria Operations for Networks, vous pouvez effectuer les actions suivantes :

- Visualiser vos environnements hybrides et multicloud
- Résoudre et analyser les problèmes de flux de trafic
- Découvrir et analyser des applications
- Mapper les dépendances entre les charges de travail

Il existe trois versions de ce service. VMware vRealize Network Insight est une version sur site uniquement. VMware Aria Operations for Networks est une version SaaS. vRealize Network Insight Universal peut être déployé en tant que solution sur site ou en tant que solution SaaS cloud fédérée. Toutes les versions sont compatibles avec VMware Cloud on AWS.

Gestion des identités et des accès

Vous utilisez VMware Cloud Services Console pour gérer les identités et l'accès à VMware Aria Operations for Networks. VMware Aria Operations for Networks utilise les mêmes utilisateurs, y compris les identités fédérées, et les mêmes groupes que ceux que vous avez configurés dans VMware Cloud Services Console. Pour VMware Aria Operations for Networks, les fonctions du service suivantes sont disponibles :

- Administrateur : ce rôle dispose d'un accès et d'un contrôle complets.
- Membre : l'accès de ce rôle est limité.
- Auditeur : ce rôle dispose d'un accès en lecture seule.

Recommandations concernant AWS

Respectez les Bonnes pratiques d'ordre général décrites précédemment dans ce guide. Nous n'avons pas de recommandations supplémentaires concernant la gestion des identités et des accès dans ce service.

VMware Aria Operations

VMware Aria Operations (documentation VMware), anciennement VMware vRealize Operations Cloud, est une plateforme de gestion des opérations pour VMware Cloud on AWS. Ce service a recours à l'intelligence artificielle et au machine learning (IA/ML) pour vous aider à optimiser, planifier

et mettre à l'échelle les applications et l'infrastructure de vos déploiements de cloud hybride. Dans VMware Aria Operations, vous pouvez effectuer les actions suivantes :

- Afficher les recommandations d'optimisation des performances et des capacités basées sur l'IA et le ML
- Gérer la conformité et les configurations des ressources
- Accéder à des outils pour vous aider à résoudre les problèmes, tels que les problèmes des clients ou la réponse aux alertes
- Utiliser des packs de gestion (documentation VMware) pour étendre les fonctionnalités de surveillance, de dépannage et de correction de ce service

Il existe deux versions de ce service centralisé de gestion des opérations. VMware vRealize Operations est une version sur site qui peut être exécutée en tant qu'appareil au sein de votre SDDC. VMware Aria Operations est une version logicielle en tant que service (SaaS) de vRealize Operations. Les deux versions sont compatibles avec VMware Cloud on AWS. Comme VMware Cloud on AWS est un service géré et que l'accès à certaines ressources est restreint, toutes les fonctionnalités de vRealize Operations ne sont pas prises en charge. Pour plus d'informations, veuillez consulter Limitations connues (documentation VMware).

Gestion des identités et des accès

Vous utilisez VMware Cloud Services Console pour gérer les identités et les accès à VMware Aria Operations. VMware Aria Operations utilise les mêmes utilisateurs, y compris les identités fédérées, que ceux que vous configurez dans VMware Cloud Services Console. Pour accorder des autorisations pour ce service, vous pouvez attribuer une fonction du service ou configurer un rôle personnalisé dans VMware Aria Operations. Pour plus d'informations sur les fonctions du service disponibles, veuillez consulter Rôles et privilèges (documentation VMware).

Il existe trois rôles intégrés : Administrateur, GeneralUser et ReadOnly. Au besoin, vous pouvez créer des rôles personnalisés pour répondre à des exigences d'autorisation spécifiques. Vous pouvez créer des groupes afin de réduire la surcharge administrative liée à la gestion des autorisations pour plusieurs utilisateurs.

La version locale de VMware vRealize Operations prend en charge les utilisateurs locaux, tandis que les versions cloud et sur site prennent en charge les utilisateurs fédérés. Toutefois, la fédération des utilisateurs sur un fournisseur d'identité externe varie entre les versions sur site et cloud de vRealize Operations. Pour la version sur site, vous pouvez fédérer directement les utilisateurs d'un IdP externe

via LDAP, ou vous pouvez utiliser les identités que vous avez fédérées dans vCenter Server. Pour la version cloud, vous utilisez les mêmes utilisateurs, y compris les utilisateurs fédérés, que ceux que vous configurez dans VMware Cloud Services Console.

Recommandations concernant AWS

En plus des Bonnes pratiques d'ordre général, AWS adresse les recommandations suivantes lors de la configuration de VMware Aria Operations pour VMware Cloud on AWS :

- Évitez de fédérer directement les utilisateurs. Pour la version cloud, fédérez les utilisateurs dans VMware Cloud Services Console, puis utilisez des rôles et des groupes pour accorder l'accès à ce service. Pour la version sur site de ce service, utilisez des identités provenant d'une source authentifiée ou activez l'authentification unique (SSO). Pour plus d'informations, veuillez consulter Sources d'authentification et Configurer une source d'authentification unique (documentation VMware).

VMware Cloud Disaster Recovery

VMware Cloud Disaster Recovery (VCDR) (documentation VMware) est une solution de reprise après sinistre en tant que service (DRaaS) qui propose une approche hiérarchisée de la reprise après sinistre. Vous pouvez ajuster les coûts et les délais pour votre objectif de point de reprise (RPO) et votre objectif de délai de reprise (RTO) afin de répondre aux exigences d'une charge de travail donnée. Cela vous permet de trouver un équilibre entre une protection fiable et une utilisation efficace des ressources de reprise après sinistre. Dans VCDR, vous pouvez effectuer les actions suivantes :

- Créer des sauvegardes de machines virtuelles
- Stocker des sauvegardes dans un espace de stockage cloud durable
- Choisissez entre des options de déploiement flexibles pour les cibles de restauration, de à la demande à zone hébergée
- Configurer des RPO et RTO personnalisés

Gestion des identités et des accès

Vous utilisez VMware Cloud Services Console pour gérer les identités et l'accès à VMware Cloud Disaster Recovery. VMware Cloud Disaster Recovery utilise les mêmes utilisateurs, y compris les identités fédérées, et les mêmes groupes que ceux que vous avez configurés dans VMware Cloud Services Console. Pour accorder des autorisations pour ce service, vous pouvez attribuer une

fonction du service VCDR ou créer un rôle personnalisé dans VMware Cloud Disaster Recovery. Pour plus d'informations sur les fonctions du service disponibles, veuillez consulter VMware Cloud Disaster Recovery Service Roles (documentation VMware).

VCDR inclut plusieurs rôles intégrés que vous pouvez utiliser pour faire fonctionner le service :

- Administrateur : contrôle total, à l'exclusion de l'accès aux jetons d'API.
- Auditeur : accès en lecture seule à l'interface utilisateur, à l'exclusion de la gestion des utilisateurs. Accès aux rapports de conformité.
- Admin DR : créez, testez et exécutez des plans de reprise après sinistre.
- Admin de sauvegardes : gérez les sites protégés et les groupes de protection. Accès pour restaurer des machines virtuelles.
- Testeur de plans : créez des plans de reprise après sinistre et exécutez des tests de restauration.
- Admin SDDC : gérer les SDDC.

Recommandations concernant AWS

Respectez les Bonnes pratiques d'ordre général décrites précédemment dans ce guide. Nous n'avons pas de recommandations supplémentaires concernant la gestion des identités et des accès dans ce service.

VMware HCX

VMware HCX (documentation VMware) est une plateforme de mobilité des applications qui permet de migrer des charges de travail entre les SDDC. VMware HCX est inclus dans VMware Cloud on AWS et peut être utilisé pour migrer des charges de travail. Dans VMware HCX, vous pouvez effectuer les opérations suivantes :

- Configurer des maillages multisites entre les SDDC
- Étendre les réseaux entre les sites HCX
- Migrer des machines virtuelles

Gestion des identités et des accès

Vous utilisez VMware vCenter Server pour gérer les identités et les accès à VMware HCX. VMware HCX a besoin d'accéder à d'autres services VMware pour créer et gérer des ressources et des

migrations, notamment l'accès à vCenter Server et à NSX. VMware HCX comporte deux services de composants :

- HCX Cloud Manager : dans VMware Cloud Services Console, vous activez VMware HCX pour le SDDC. Cela permet d'installer l'appareil HCX Cloud Manager dans le SDDC sélectionné. Pour plus d'informations, veuillez consulter Deploying the HCX Installer OVA in the vSphere Client (documentation VMware). Après le déploiement, vous pouvez utiliser lesinformations d'identification cloudadmin de vCenter Server pour accéder au service HCX Cloud Manager.
- HCX Connector : vous pouvez obtenir le fichier OVA (Open Virtualization Archive) HCX Connector via le service HCX Cloud Manager. Vous utilisez ce fichier pour installer un appareil HCX Cloud Manager sur n'importe quelle instance de vCenter Server, qui configure cette instance comme source de migration dans VMware HCX. Chaque instance de HCX Connector possède ses propres informations d'identification admin et root.

Après avoir déployé les deux services de composants, vous pouvez accéder à VMware HCX via vCenter Server. Le groupe Administrateurs vCenter Single Sign-On se voit automatiquement attribuer le rôle Administrateur HCX. L'installation de HCX ajoute de nombreux rôles et privilèges à vCenter Single Sign-On. Utilisez-les pour créer des contrôles d'accès précis pour VMware HCX, en fonction des différents types d'utilisateur.

Recommandations concernant AWS

En plus des Bonnes pratiques d'ordre général, AWS adresse les recommandations suivantes lors de la configuration de VMware HCX pour VMware Cloud on AWS :

- Utilisez les règles de Gateway Firewall pour restreindre l'accès réseau au service HCX Cloud Manager.
- Stockez en toute sécurité les informations d'identification admin et utilisateur root de HCX Connector sur site. Envisagez d'alterner ces informations d'identification conformément aux stratégies de votre entreprise. VMware gère ces informations d'identification en votre nom pour HCX Cloud Manager.
- Pour une instance de HCX Connector sur site, pensez à créer des rôles HCX personnalisés qui répondent aux besoins de vos différents types d'utilisateur HCX. Par exemple, créez un rôle plus permissif pour les utilisateurs qui configurent et administrent HCX, et créez un rôle moins permissif pour les utilisateurs qui gèrent uniquement les migrations.

- Lorsque vous associez VMware HCX à VMware Cloud on AWS, vous devez utiliser l'utilisateur cloudadmin. Pour plus d'informations, veuillez consulter la section Resolution de HCX - Site Pairing Connectivity Diagnostics (article 78340 de la base de connaissances VMware).
- Lorsque vous associez HCX Cloud à VMware Cloud on AWS, l'authentification n'est pas prise en charge entre le SDDC VMware Cloud on AWS et Active Directory. Pour plus d'informations, veuillez consulter [VMC on AWS] AD unsupported for HCX Cloud to Cloud setup (article 90433 de la base de connaissances VMware).

VMware Site Recovery

VMware Site Recovery (documentation VMware) est une solution de reprise après sinistre à la demande (DRaaS) basée sur le service VMware Site Recovery Manager pour les environnements sur site. Dans VMware Site Recovery, vous pouvez effectuer les actions suivantes :

- Implémenter la réplication, l'orchestration et l'automatisation pour protéger les charges de travail en cas de défaillance d'un site
- Créer une solution de reprise après sinistre de bout en bout pour protéger les SDDC

Gestion des identités et des accès

Vous utilisez VMware vCenter Server pour gérer les identités et l'accès à VMware Site Recovery. VMware Site Recovery exécute des opérations pour le compte des utilisateurs, telles que la réplication ou la mise hors tension d'une machine virtuelle. Site Recovery utilise des rôles et des privilèges pour garantir que seuls les utilisateurs disposant des autorisations appropriées peuvent effectuer des opérations de restauration, telles que l'exécution de toutes les étapes d'un plan de récupération.

Pour Site Recovery, les fonctions du service suivantes sont disponibles :

- SrmAdministrator : ce rôle peut effectuer toutes les opérations de configuration et d'administration de Site Recovery.
- HmsCloudAdmin : ce rôle peut répertorier les serveurs, mais il ne peut pas les ajouter ou les supprimer.

Lorsque vous configurez Site Recovery dans VMware Cloud on AWS, les mises à jour des groupes d'utilisateurs suivantes sont automatiquement configurées :

1. Un groupe Administrateurs SRM est créé et se voit assigner le rôle SrmAdministrator.
2. Un groupe HmsCloudAdministrators est créé et se voit assigner le rôle HmsCloudAdmin.
3. Le groupe CloudAdminGroup est ajouté à la fois au groupe Administrateurs SRM et au groupe HmsCloudAdministrators. Cela fournit au groupe CloudAdminGroup les autorisations transitives pour gérer la réplication Site Recovery Manager et vSphere.

Pour plus d'informations, veuillez consulter En savoir plus sur la configuration des autorisations pour VMware Site Recovery (documentation VMware).

Si vous utilisez des identités fédérées pour accéder à vCenter Server, vous devez utiliser Hybrid Linked Mode pour ajouter des entités à ces groupes. Pour plus d'informations, veuillez consulter Configuration d'Hybrid Linked Mode (documentation VMware).

Recommandations concernant AWS

En plus des Bonnes pratiques d'ordre général, AWS adresse les recommandations suivantes lors de la configuration de Site Recovery for VMware Cloud on AWS :

- Assurez-vous que les mêmes rôles sont attribués aux utilisateurs sur les sites source et cible. Cela garantit que les objets protégés et récupérés disposent des mêmes autorisations.
- Utilisez Hybrid Linked Mode pour gérer les attributions de rôles Site Recovery pour les identités fédérées au sein de vCenter Server.
- Site Recovery utilise des adresses IP privées uniquement au sein du SDDC. En respectant les Bonnes pratiques d'ordre général, assurez-vous que votre vCenter VMware Cloud on AWS correspond à une adresse IP privée.

Exemples de groupes et de rôles

Le tableau suivant fournit un exemple de stratégie de gestion des identités et des accès pour l'utilisation de VMware Cloud on AWS. Il décrit le profil de l'utilisateur, les services VMware auxquels il doit accéder, l'organisation et l'appartenance au groupe, les rôles assignés et le type d'identité utilisé (comme les utilisateurs locaux ou les identités fédérées). À l'aide de ce tableau comme point de départ, concevez une stratégie pour votre entreprise conforme aux bonnes pratiques recommandées dans ce guide.

Profil de l'utilisateur	Services consultés	Nom du groupe d'échantillons VMware Cloud	Fonctions du service VMware Cloud	Nom du groupe d'échantillons vCenter Single Sign-On	Rôle vCenter Single Sign-On	Source d'identité
Brise glace de l'organisation	VMware Cloud Services Console	Aucune	Propriétaire de l'organisation	Aucune	Aucun	Utilisateur local (adresse e-mail du compte de service)
Administrateur VMware	VMware Cloud Services Console vCenter Server HCX Site Recovery VCDR	`vmware_admins`	Propriétaire de l'organisation	`vmware_admins`	Administrateur	Fournisseur d'identité fédérée

Profil de l'utilisateur	Services consultés	Nom du groupe d'échantillons VMware Cloud	Fonctions du service VMware Cloud	Nom du groupe d'échantillons vCenter Single Sign-On	Rôle vCenter Single Sign-On	Source d'identité
	vRealize Operations					
Administrateur des sauvegardes	vCenter Server	Aucune	Aucun	`vmware_backups`	Utilisateur avancé	Fournisseur d'identité fédérée
Administrateur de reprise après sinistre	vCenter Server VMware Cloud Services Console Site Recovery VCDR	`vmware_dr`	Membre de l'organisation Administrateur de reprise après sinistre Administrateur SDDC de reprise après sinistre	`vmware_dr`	SrmAdministrator HmsCloudAdmin	Fournisseur d'identité fédérée

Profil de l'utilisateur	Services consultés	Nom du groupe d'échantillons VMware Cloud	Fonctions du service VMware Cloud	Nom du groupe d'échantillons vCenter Single Sign-On	Rôle vCenter Single Sign-On	Source d'identité
Opérateur VMware	VMware Cloud Services Console vCenter Server HCX vRealize Operations	`vmware_ops`	Membre de l'organisation Administrateur vROps	`vmware_ops`	Utilisateur avancé	Fournisseur d'identité fédérée
Équipe de mise en réseau	VMware Cloud Services Console vCenter Server	`vmware_networks`	Membre de l'organisation Administrateur de NSX Cloud	`vmware_networks`	Readonly	Fournisseur d'identité fédérée

Profil de l'utilisateur	Services consultés	Nom du groupe d'échantillons VMware Cloud	Fonctions du service VMware Cloud	Nom du groupe d'échantillons vCenter Single Sign-On	Rôle vCenter Single Sign-On	Source d'identité
Équipe de sécurité	VMware Cloud Services Console vCenter Server HCX (accès temporaire) Site Recovery VCDR vRealize Operations	`vmware_security`	Membre de l'organisation vROps ReadOnly	`vmware_security`	Readonly	Fournisseur d'identité fédérée
Auditeurs	VMware Cloud Services Console vCenter Server	`vmware_audit`	Membre de l'organisation	`vmware_audit`	Readonly	Fournisseur d'identité fédérée

Étapes suivantes

Ce guide décrit les bonnes pratiques que nous recommandons pour gérer les identités et les accès pour VMware Cloud on AWS et les services VMware associés. Ces recommandations visent à vous aider à sécuriser votre infrastructure cloud et cloud hybride et à empêcher tout accès non autorisé, mais elles sont aussi conçues pour être évolutives et efficaces. En affectant des utilisateurs à des groupes, puis en attribuant des rôles aux groupes, vous pouvez accorder ou restreindre plus rapidement les autorisations et réduire la surcharge associée à la configuration individuelle des utilisateurs. En outre, en utilisant la fédération avec un fournisseur d'identité externe et vCenter Single Sign-On, vous pouvez proposer une expérience d'authentification unique et transparente à vos utilisateurs.

Utilisez la table Exemples de groupes et de rôles pour commencer à concevoir une stratégie de gestion des identités et des accès adaptée à votre entreprise. Après avoir pris connaissance des recommandations de ce guide, nous vous suggérons d'examiner les liens fournis dans la section Ressources. Ces ressources vous aideront à en savoir plus sur les services VMware Cloud et à configurer les bonnes pratiques décrites dans ce guide.

Ressources

Ressources connexes AWS

- Présentation et modèle d'exploitation de VMware Cloud on AWS
- Disaster recovery options for workloads on VMware Cloud on AWS
- Configuring storage offload options for VMware Cloud on AWS
- Deploy a VMware SDDC on AWS by using VMware Cloud on AWS
- Migrate VMware SDDC to VMware Cloud on AWS using VMware HCX

Documentation VMware

VMware Cloud on AWS

- Guide de configuration de la fédération d'entreprise avec VMware Cloud Services
- Gestion des identités et des accès

VMware vCenter Server et vCenter Single Sign-On

- Présentation des autorisations dans vSphere
- Administration de vSphere dans VMware Cloud on AWS
- Authentification vSphere à l'aide de vCenter Single Sign-On
- Configuration des sources d'identité vCenter Single Sign-On
- Héritage hiérarchique des autorisations
- Information Security and Access for vCenter Server
- Privilèges requis pour les tâches courantes

VMware NSX

- Guide d'administration de NSX
- Information Security and Access for NSX-T Data Center

VMware HCX

- Guide de l'utilisateur de VMware HCX
- VMware HCX User Account and Role Requirements

Suite VMware Aria et vRealize

- Documentation de vRealize Operations
- Rôles et privilèges dans VMware Aria Operations
- Fiche technique de VMware vRealize Log Insight
- Getting Started with VMware Aria Operations for Logs
- VMware Cloud Services Guide
- Configurer la gestion des utilisateurs de vRealize Network Insight

VMware Site Recovery

- Documentation VMware Site Recovery
- Privilèges, rôles et autorisations Site Recovery Manager
- En savoir plus sur la configuration des autorisations pour VMware Site Recovery sur VMware Cloud on AWS

VMware Cloud Disaster Recovery

- VMware Cloud Disaster Recovery User Roles

Historique du document

Le tableau suivant décrit les modifications importantes apportées à ce guide. Pour être averti des mises à jour à venir, abonnez-vous à un fil RSS.

Modification	Description	Date
Accès à VMware HCX	Nous avons mis à jour les recommandations AWS pour configurer VMware HCX pour VMware Cloud on AWS.	5 juin 2023
Publication initiale	—	3 novembre 2022

Glossaire des recommandations AWS

Les termes suivants sont couramment utilisés dans les politiques, les guides et les modèles fournis par les recommandations AWS. Pour suggérer des entrées, veuillez utiliser le lien Faire un commentaire à la fin du glossaire.

Nombres

7 R

Sept politiques de migration courantes pour transférer des applications vers le cloud. Ces politiques s'appuient sur les 5 R identifiés par Gartner en 2011 et sont les suivantes :

- Refactorisation/réarchitecture : transférez une application et modifiez son architecture en tirant pleinement parti des fonctionnalités natives cloud pour améliorer l'agilité, les performances et la capacité de mise à l'échelle. Cela implique généralement le transfert du système d'exploitation et de la base de données. Exemple : migrez votre base de données Oracle sur site vers Amazon Aurora Édition compatible avec PostgreSQL.
- Replateformer (déplacer et remodeler) : transférez une application vers le cloud et introduisez un certain niveau d'optimisation pour tirer parti des fonctionnalités du cloud. Exemple : migrez votre base de données Oracle sur site vers Amazon Relational Database Service (Amazon RDS) for Oracle dans le Cloud AWS.
- Racheter (rachat) : optez pour un autre produit, généralement en passant d'une licence traditionnelle à un modèle SaaS. Exemple : migrez votre système de gestion de la relation client (CRM) vers Salesforce.com.
- Réhéberger (lift and shift) : transférez une application vers le cloud sans apporter de modifications pour tirer parti des fonctionnalités du cloud. Exemple : migrez votre base de données Oracle sur site vers Oracle sur une instance EC2 dans le Cloud AWS.
- Relocaliser (lift and shift au niveau de l'hyperviseur) : transférez l'infrastructure vers le cloud sans acheter de nouveau matériel, réécrire des applications ou modifier vos opérations existantes. Ce scénario de migration est propre à VMware Cloud on AWS, qui prend en charge la compatibilité des machines virtuelles (VM) et la portabilité de la charge de travail entre votre environnement sur site et AWS. Vous pouvez utiliser les technologies VMware Cloud Foundation à partir de vos centres de données sur site lorsque vous migrez votre infrastructure vers VMware Cloud on AWS. Exemple : relocalisez l'hyperviseur hébergeant votre base de données Oracle vers VMware Cloud on AWS.

- Retenir : conservez les applications dans votre environnement source. Il peut s'agir d'applications nécessitant une refactorisation majeure, que vous souhaitez retarder, et d'applications existantes que vous souhaitez retenir, car rien ne justifie leur migration sur le plan commercial.
- Retirer : mettez hors service ou supprimez les applications dont vous n'avez plus besoin dans votre environnement source.

A

ABAC

Voir contrôle d'accès basé sur les attributs.

services abstraits

Consultez la section Services gérés.

ACIDE

Voir atomicité, consistance, isolation, durabilité.

migration active-active

Méthode de migration de base de données dans laquelle la synchronisation des bases de données source et cible est maintenue (à l'aide d'un outil de réplication bidirectionnelle ou d'opérations d'écriture double), tandis que les deux bases de données gèrent les transactions provenant de la connexion d'applications pendant la migration. Cette méthode prend en charge la migration par petits lots contrôlés au lieu d'exiger un basculement ponctuel. Elle est plus flexible mais demande plus de travail qu'une migration active-passive.

migration active-passive

Méthode de migration de base de données dans laquelle la synchronisation des bases de données source et cible est maintenue, mais seule la base de données source gère les transactions provenant de la connexion d'applications pendant que les données sont répliquées vers la base de données cible. La base de données cible n'accepte aucune transaction pendant la migration.

fonction d'agrégation

Fonction SQL qui agit sur un groupe de lignes et calcule une valeur de retour unique pour le groupe. Des exemples de fonctions d'agrégation incluent `SUM` et`MAX`.

AI

Voir intelligence artificielle.

AIOps

Voir les opérations d'intelligence artificielle.

anonymisation

Processus de suppression définitive d'informations personnelles dans un ensemble de données. L'anonymisation peut contribuer à protéger la vie privée. Les données anonymisées ne sont plus considérées comme des données personnelles.

anti-motif

Solution fréquemment utilisée pour un problème récurrent lorsque la solution est contre-productive, inefficace ou moins efficace qu'une alternative.

contrôle des applications

Une approche de sécurité qui permet d'utiliser uniquement des applications approuvées afin de protéger un système contre les logiciels malveillants.

portefeuille d'applications

Ensemble d'informations détaillées sur chaque application utilisée par une organisation, y compris le coût de génération et de maintenance de l'application, ainsi que sa valeur métier. Ces informations sont essentielles pour le processus de découverte et d'analyse du portefeuille et permettent d'identifier et de prioriser les applications à migrer, à moderniser et à optimiser.

intelligence artificielle (IA)

Domaine de l'informatique consacré à l'utilisation des technologies de calcul pour exécuter des fonctions cognitives généralement associées aux humains, telles que l'apprentissage, la résolution de problèmes et la reconnaissance de modèles. Pour plus d'informations, veuillez consulter Qu'est-ce que l'intelligence artificielle ?

opérations d'intelligence artificielle (AIOps)

Processus consistant à utiliser des techniques de machine learning pour résoudre les problèmes opérationnels, réduire les incidents opérationnels et les interventions humaines, mais aussi améliorer la qualité du service. Pour plus d'informations sur la façon dont les AIOps sont utilisées dans la stratégie de migration AWS, veuillez consulter le guide d'intégration des opérations.

chiffrement asymétrique

Algorithme de chiffrement qui utilise une paire de clés, une clé publique pour le chiffrement et une clé privée pour le déchiffrement. Vous pouvez partager la clé publique, car elle n'est pas utilisée pour le déchiffrement, mais l'accès à la clé privée doit être très restreint.

atomicité, cohérence, isolement, durabilité (ACID)

Ensemble de propriétés logicielles garantissant la validité des données et la fiabilité opérationnelle d'une base de données, même en cas d'erreur, de panne de courant ou d'autres problèmes.

contrôle d'accès par attributs (ABAC)

Pratique qui consiste à créer des autorisations détaillées en fonction des attributs de l'utilisateur, tels que le service, le poste et le nom de l'équipe. Pour plus d'informations, veuillez consulter ABAC for AWS dans la documentation AWS Identity and Access Management (IAM).

source de données faisant autorité

Emplacement où vous stockez la version principale des données, considérée comme la source d'information la plus fiable. Vous pouvez copier les données de la source de données officielle vers d'autres emplacements à des fins de traitement ou de modification des données, par exemple en les anonymisant, en les expurgant ou en les pseudonymisant.

Zone de disponibilité

Emplacement distinct au sein d'une Région AWS qui est à l'abri des dysfonctionnements d'autres zones de disponibilité et offre une connectivité réseau peu coûteuse et de faible latence par rapport aux autres zones de disponibilité de la même région.

Framework d'adoption du Cloud AWS (AWS CAF)

Un cadre de directives et de bonnes pratiques d'AWS pour aider les entreprises à élaborer un plan efficient et efficace pour réussir leur migration vers le Cloud AWS. Le CAF organise ses conseils en six domaines prioritaires appelés perspectives : l'entreprise, les personnes, la gouvernance, la plateforme, la sécurité et les opérations. Les perspectives d'entreprise, de personnes et de gouvernance mettent l'accent sur les compétences et les processus métier, tandis que les perspectives relatives à la plateforme, à la sécurité et aux opérations se concentrent sur les compétences et les processus techniques. Par exemple, la perspective liée aux personnes cible les parties prenantes qui s'occupent des ressources humaines (RH), des fonctions de dotation en personnel et de la gestion des personnes. Dans cette perspective, AWS CAF fournit des conseils pour le développement du personnel, la formation et les communications

afin de préparer l'organisation à une adoption réussie du cloud. Pour plus d'informations, veuillez consulter le site Web AWS CAF et le livre blanc AWS CAF.

AWS Workload Qualification Framework (AWS WQF)

Outil qui évalue les charges de travail de migration de base de données, recommande des politiques de migration et fournit des estimations de travail. AWS WQF est inclus avec AWS Schema Conversion Tool (AWS SCT). Il analyse les schémas de base de données et les objets de code, le code d'application, les dépendances et les caractéristiques de performance, et fournit des rapports d'évaluation.

B

BCP

Consultez la section Planification de la continuité des activités.

graphique de comportement

Vue unifiée et interactive des comportements des ressources et des interactions au fil du temps. Vous pouvez utiliser un graphique de comportement avec Amazon Detective pour examiner les tentatives de connexion infructueuses, les appels d'API suspects et les actions similaires. Pour plus d'informations, veuillez consulter Data in a behavior graph dans la documentation Detective.

système de poids fort

Système qui stocke d'abord l'octet le plus significatif. Voir aussi endianité.

classification binaire

Processus qui prédit un résultat binaire (l'une des deux classes possibles). Par exemple, votre modèle de machine learning peut avoir besoin de prévoir des problèmes tels que « Cet e-mail est-il du spam ou non ? » ou « Ce produit est-il un livre ou une voiture ? ».

filtre de Bloom

Structure de données probabiliste et efficace en termes de mémoire qui est utilisée pour tester si un élément fait partie d'un ensemble.

branche

Zone contenue d'un référentiel de code. La première branche créée dans un référentiel est la branche principale. Vous pouvez créer une branche à partir d'une branche existante, puis développer des fonctionnalités ou corriger des bogues dans la nouvelle branche. Une branche

que vous créez pour générer une fonctionnalité est communément appelée branche de fonctionnalités. Lorsque la fonctionnalité est prête à être publiée, vous fusionnez à nouveau la branche de fonctionnalités dans la branche principale. Pour plus d'informations, consultez À propos des branches (GitHub documentation).

accès par brise-vitre

Dans des circonstances exceptionnelles et par le biais d'un processus approuvé, c'est un moyen rapide pour un utilisateur d'accéder à un accès auquel Compte AWS il n'est généralement pas autorisé. Pour plus d'informations, consultez l'indicateur Implementation break-glass procedures dans le guide Well-ArchitectedAWS.

stratégie existante (brownfield)

L'infrastructure existante de votre environnement. Lorsque vous adoptez une stratégie existante pour une architecture système, vous concevez l'architecture en fonction des contraintes des systèmes et de l'infrastructure actuels. Si vous étendez l'infrastructure existante, vous pouvez combiner des politiques brownfield (existantes) et greenfield (inédites).

cache de tampon

Zone de mémoire dans laquelle sont stockées les données les plus fréquemment consultées.

capacité métier

Ce que fait une entreprise pour générer de la valeur (par exemple, les ventes, le service client ou le marketing). Les architectures de microservices et les décisions de développement peuvent être dictées par les capacités métier. Pour plus d'informations, veuillez consulter la section Organisation en fonction des capacités métier du livre blanc Exécution de microservices conteneurisés sur AWS.

planification de la continuité des activités (BCP)

Plan qui tient compte de l'impact potentiel d'un événement perturbateur, tel qu'une migration à grande échelle, sur les opérations, et qui permet à une entreprise de reprendre ses activités rapidement.

C

CAF

Voir le cadre d'adoption du AWS cloud.

CCoE

Voir le Centre d'excellence du cloud.

CDC

Voir capture des données de modification.

capture des données de modification (CDC)

Processus de suivi des modifications apportées à une source de données, telle qu'une table de base de données, et d'enregistrement des métadonnées relatives à ces modifications. Vous pouvez utiliser la CDC à diverses fins, telles que l'audit ou la réplication des modifications dans un système cible afin de maintenir la synchronisation.

ingénierie du chaos

Introduire intentionnellement des défaillances ou des événements perturbateurs pour tester la résilience d'un système. Vous pouvez utiliser AWS Fault Injection Service(AWS FIS) pour effectuer des expériences qui stressent vos AWS charges de travail et évaluer leur réponse.

CI/CD

Découvrez l'intégration continue et la livraison continue.

classification

Processus de catégorisation qui permet de générer des prédictions. Les modèles de ML pour les problèmes de classification prédisent une valeur discrète. Les valeurs discrètes se distinguent toujours les unes des autres. Par exemple, un modèle peut avoir besoin d'évaluer la présence ou non d'une voiture sur une image.

chiffrement côté client

Chiffrement des données en local, avant que le Service AWS cible ne les reçoive.

Centre d'excellence cloud (CCoE)

Une équipe multidisciplinaire qui dirige les efforts d'adoption du cloud au sein d'une organisation, notamment en développant les bonnes pratiques en matière de cloud, en mobilisant des ressources, en établissant des délais de migration et en guidant l'organisation dans le cadre de transformations à grande échelle. Pour plus d'informations, veuillez consulter les publications du CCoE sur le blog AWS Cloud Enterprise Strategy.

cloud computing

Technologie cloud généralement utilisée pour le stockage de données à distance et la gestion des appareils IoT. Le cloud computing est généralement associé à la technologie informatique de pointe.

modèle d'exploitation du cloud

Dans une organisation informatique, modèle d'exploitation utilisé pour créer, faire évoluer et optimiser un ou plusieurs environnements cloud. Pour plus d'informations, consultez la section Création de votre modèle d'exploitation cloud.

étapes d'adoption du cloud

Les quatre phases que les organisations traversent généralement lorsqu'elles migrent vers le Cloud AWS :

- Projet : exécution de quelques projets liés au cloud à des fins de preuve de concept et d'apprentissage
- Base : réaliser des investissements fondamentaux pour mettre à l'échelle l'adoption du cloud (par exemple, en créant une zone de destination, en définissant un CCoE ou en établissant un modèle opérationnel)
- Migration : migration d'applications individuelles
- Réinvention : optimisation des produits et services et innovation dans le cloud

Ces étapes ont été définies par Stephen Orban dans le billet de blog The Journey Toward Cloud-First & the Stages of Adoption sur le blog AWS Cloud Enterprise Strategy. Pour en savoir plus sur la façon dont elles sont liées à stratégie de migration AWS, veuillez consulter le guide de préparation à la migration.

CMDB

Consultez la base de données de gestion des configurations.

référentiel de code

Emplacement où le code source et d'autres ressources, comme la documentation, les exemples et les scripts, sont stockés et mis à jour par le biais de processus de contrôle de version. Les référentiels cloud courants incluent GitHub ouAWS CodeCommit. Chaque version du code est appelée branche. Dans une structure de microservice, chaque référentiel est consacré à une seule fonctionnalité. Un seul pipeline CI/CD peut utiliser plusieurs référentiels.

cache passif

Cache tampon vide, mal rempli ou contenant des données obsolètes ou non pertinentes. Cela affecte les performances, car l'instance de base de données doit lire à partir de la mémoire principale ou du disque, ce qui est plus lent que la lecture à partir du cache tampon.

données gelées

Données rarement consultées et généralement historiques. Lorsque vous interrogez ce type de données, les requêtes lentes sont généralement acceptables. Le transfert de ces données vers des niveaux ou classes de stockage moins performants et moins coûteux peut réduire les coûts.

vision par ordinateur

Domaine de l'IA utilisé par les machines pour identifier des personnes, des lieux et des objets sur des images avec une précision égale ou supérieure à celle de l'être humain. Souvent conçu à partir de modèles d'apprentissage profond, il automatise l'extraction, l'analyse, la classification et la compréhension des informations utiles à partir d'une seule image ou d'une séquence d'images.

base de données de gestion des configurations (CMDB)

Référentiel qui stocke et gère les informations relatives à une base de données et à son environnement informatique, y compris les composants matériels et logiciels ainsi que leurs configurations. Vous utilisez généralement les données d'une CMDB lors de la phase de découverte et d'analyse du portefeuille de la migration.

pack de conformité

Une collection de règles AWS Config et d'actions correctives que vous pouvez mettre en place pour personnaliser vos contrôles de conformité et de sécurité. Vous pouvez déployer un pack de conformité en tant qu'entité unique dans un Compte AWS et une région, ou au sein d'une organisation, à l'aide d'un modèle YAML. Pour plus d'informations, veuillez consulter Conformance packs dans la documentation AWS Config.

intégration continue et livraison continue (CI/CD)

Processus d'automatisation des étapes source, de génération, de test, intermédiaire et de production du processus de publication du logiciel. CI/CD est communément décrit comme un pipeline. CI/CD peut vous aider à automatiser les processus, à améliorer la productivité, à améliorer la qualité du code et à accélérer les livraisons. Pour plus d'informations, veuillez consulter Avantages de la livraison continue. CD peut également signifier déploiement continu. Pour plus d'informations, veuillez consulter Livraison continue et déploiement continu.

D

données au repos

Données stationnaires dans votre réseau, telles que les données stockées.

classification des données

Processus permettant d'identifier et de catégoriser les données de votre réseau en fonction de leur sévérité et de leur sensibilité. Il s'agit d'un élément essentiel de toute stratégie de gestion des risques de cybersécurité, car il vous aide à déterminer les contrôles de protection et de conservation appropriés pour les données. La classification des données est une composante du pilier de sécurité du cadre AWS Well-Architected. Pour plus d'informations, veuillez consulter Classification des données.

dérive des données

Une variation significative entre les données de production et les données utilisées pour entraîner un modèle ML, ou une modification significative des données d'entrée au fil du temps. La dérive des données peut réduire la qualité, la précision et l'équité globales des prédictions des modèles ML.

données en transit

Données qui circulent activement sur votre réseau, par exemple entre les ressources du réseau.

minimisation des données

Le principe de collecte et de traitement des seules données strictement nécessaires. La pratique de la minimisation des données AWS Cloud peut réduire les risques liés à la confidentialité, les coûts et l'empreinte carbone de vos analyses.

périmètre de données

Ensemble de garde-fous préventifs dans votre AWS environnement qui permettent de garantir que seules les identités fiables accèdent aux ressources fiables des réseaux attendus. Pour plus d'informations, voir Création d'un périmètre de données sur AWS.

prétraitement des données

Pour transformer les données brutes en un format facile à analyser par votre modèle de ML. Le prétraitement des données peut impliquer la suppression de certaines colonnes ou lignes et le traitement des valeurs manquantes, incohérentes ou en double.

provenance des données

Le processus de suivi de l'origine et de l'historique des données tout au long de leur cycle de vie, par exemple la manière dont les données ont été générées, transmises et stockées.

sujet des données

Personne dont les données sont collectées et traitées.

entrepôt de données

Un système de gestion des données qui prend en charge les informations commerciales, telles que les analyses. Les entrepôts de données contiennent généralement de grandes quantités de données historiques et sont généralement utilisés pour les requêtes et les analyses.

langage de définition de base de données (DDL)

Instructions ou commandes permettant de créer ou de modifier la structure des tables et des objets dans une base de données.

langage de manipulation de base de données (DML)

Instructions ou commandes permettant de modifier (insérer, mettre à jour et supprimer) des informations dans une base de données.

DDL

Voir langage de définition de base de données.

ensemble profond

Sert à combiner plusieurs modèles de deep learning à des fins de prédiction. Vous pouvez utiliser des ensembles profonds pour obtenir une prévision plus précise ou pour estimer l'incertitude des prédictions.

deep learning

Un sous-champ de ML qui utilise plusieurs couches de réseaux neuronaux artificiels pour identifier le mappage entre les données d'entrée et les variables cibles d'intérêt.

defense-in-depth

Approche de la sécurité de l'information dans laquelle une série de mécanismes et de contrôles de sécurité sont judicieusement répartis sur l'ensemble d'un réseau informatique afin de protéger la confidentialité, l'intégrité et la disponibilité du réseau et des données qu'il contient. Lorsque vous adoptez cette stratégie sur AWS, vous ajoutez plusieurs contrôles à différentes couches de

la structure AWS Organizations afin de protéger les ressources. Par exemple, une defense-in-depth approche peut combiner l'authentification multifactorielle, la segmentation du réseau et le chiffrement.

administrateur délégué

Dans AWS Organizations, un service compatible peut enregistrer un compte membre AWS pour administrer les comptes de l'organisation et gérer les autorisations pour ce service. Ce compte est appelé administrateur délégué pour ce service. Pour plus d'informations et une liste des services compatibles, veuillez consulter la rubrique Services qui fonctionnent avec AWS Organizations dans la documentation AWS Organizations.

déploiement

Processus de mise à disposition d'une application, de nouvelles fonctionnalités ou de corrections de code dans l'environnement cible. Le déploiement implique la mise en œuvre de modifications dans une base de code, puis la génération et l'exécution de cette base de code dans les environnements de l'application.

environnement de développement

Voir environnement.

contrôle de détection

Contrôle de sécurité conçu pour détecter, journaliser et alerter après la survenue d'un événement. Ces contrôles constituent une deuxième ligne de défense et vous alertent en cas d'événements de sécurité qui ont contourné les contrôles préventifs en place. Pour plus d'informations, veuillez consulter la rubrique Contrôles de détection dans Implementing security controls on AWS.

cartographie de la chaîne de valeur du développement (DVSM)

Processus utilisé pour identifier et hiérarchiser les contraintes qui nuisent à la rapidité et à la qualité du cycle de vie du développement logiciel. DVSM étend le processus de cartographie de la chaîne de valeur initialement conçu pour les pratiques de production allégée. Il met l'accent sur les étapes et les équipes nécessaires pour créer et transférer de la valeur tout au long du processus de développement logiciel.

jumeau numérique

Représentation virtuelle d'un système réel, tel qu'un bâtiment, une usine, un équipement industriel ou une ligne de production. Les jumeaux numériques prennent en charge la maintenance prédictive, la surveillance à distance et l'optimisation de la production.

tableau des dimensions

Dans un schéma en étoile, table plus petite contenant les attributs de données relatifs aux données quantitatives d'une table de faits. Les attributs des tables de dimensions sont généralement des champs de texte ou des nombres discrets qui se comportent comme du texte. Ces attributs sont couramment utilisés pour la contrainte des requêtes, le filtrage et l'étiquetage des ensembles de résultats.

catastrophe

Un événement qui empêche une charge de travail ou un système d'atteindre ses objectifs commerciaux sur son site de déploiement principal. Ces événements peuvent être des catastrophes naturelles, des défaillances techniques ou le résultat d'actions humaines, telles qu'une mauvaise configuration involontaire ou une attaque de logiciel malveillant.

reprise après sinistre (DR)

La stratégie et le processus que vous utilisez pour minimiser les temps d'arrêt et les pertes de données causés par un sinistre. Pour plus d'informations, consultez Disaster Recovery of Workloads on AWS : Recovery in the Cloud in the AWS Well-Architected Framework.

DML

Voir langage de manipulation de base de données.

conception axée sur le domaine

Approche visant à développer un système logiciel complexe en connectant ses composants à des domaines évolutifs, ou objectifs métier essentiels, que sert chaque composant. Ce concept a été introduit par Eric Evans dans son ouvrage Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston : Addison-Wesley Professional, 2003). Pour plus d'informations sur l'utilisation du design piloté par domaine avec le modèle de figuier étrangleur, veuillez consulter Modernizing legacy Microsoft ASP.NET (ASMX) web services incrementally by using containers and Amazon API Gateway.

DR

Voir reprise après sinistre.

détection de dérive

Suivi des écarts par rapport à une configuration de référence. Par exemple, vous pouvez l'utiliser AWS CloudFormation pour détecter la dérive des ressources du système ou AWS Control Tower pour détecter les modifications de votre zone d'atterrissage susceptibles d'affecter le respect des exigences de gouvernance.

DVSM

Voir la cartographie de la chaîne de valeur du développement.

E

EDA

Voir analyse exploratoire des données.

informatique de périphérie

Technologie qui augmente la puissance de calcul des appareils intelligents en périphérie d'un réseau IoT. Comparé au cloud computing, l'informatique de pointe peut réduire la latence des communications et améliorer le temps de réponse.

chiffrement

Processus informatique qui transforme des données en texte clair, lisibles par l'homme, en texte chiffré.

clé de chiffrement

Chaîne cryptographique de bits aléatoires générée par un algorithme cryptographique. La longueur des clés peut varier, et chaque clé est conçue pour être imprévisible et unique.

endianisme

Ordre selon lequel les octets sont stockés dans la mémoire de l'ordinateur. Les systèmes de poids fort stockent d'abord l'octet le plus significatif. Les systèmes de poids faible stockent d'abord l'octet le moins significatif.

point de terminaison

Voir point de terminaison de service.

service de point de terminaison

Service que vous pouvez héberger sur un cloud privé virtuel (VPC) pour le partager avec d'autres utilisateurs. Vous pouvez créer un service de point de terminaison avec AWS PrivateLink et accorder des autorisations à d'autres Comptes AWS ou aux principaux AWS Identity and Access Management (IAM). Ces comptes ou principaux peuvent se connecter à votre service de point de terminaison de manière privée en créant des points de terminaison d'un VPC d'interface. Pour plus d'informations, veuillez consulter Création d'un service de point de terminaison dans la documentation Amazon Virtual Private Cloud (Amazon VPC).

chiffrement d'enveloppe

Processus de chiffrement d'une clé de chiffrement à l'aide d'une autre clé de chiffrement. Pour plus d'informations, veuillez consulter la rubrique Envelope encryption dans la documentation AWS Key Management Service (AWS KMS).

environment

Instance d'une application en cours d'exécution. Les types d'environnement les plus courants dans le cloud computing sont les suivants :

- Environnement de développement : instance d'une application en cours d'exécution à laquelle seule l'équipe principale chargée de la maintenance de l'application peut accéder. Les environnements de développement sont utilisés pour tester les modifications avant de les promouvoir dans les environnements supérieurs. Ce type d'environnement est parfois appelé environnement de test.
- Environnements inférieurs : tous les environnements de développement d'une application, tels que ceux utilisés pour les générations et les tests initiaux.
- Environnement de production : instance d'une application en cours d'exécution à laquelle les utilisateurs finaux peuvent accéder. Dans un pipeline CI/CD, l'environnement de production est le dernier environnement de déploiement.
- Environnements supérieurs : tous les environnements accessibles aux utilisateurs autres que l'équipe de développement principale. Ils peuvent inclure un environnement de production, des environnements de préproduction et des environnements pour les tests d'acceptation par les utilisateurs.

épopée

Dans les méthodologies agiles, catégories fonctionnelles qui aident à organiser et à prioriser votre travail. Les épopées fournissent une description détaillée des exigences et des tâches d'implémentation. Par exemple, les épopées AWS CAF en matière de sécurité comprennent la gestion des identités et des accès, les contrôles de détection, la sécurité de l'infrastructure, la protection des données et la réponse aux incidents. Pour plus d'informations sur les épopées dans la stratégie de migration AWS, veuillez consulter le guide d'implémentation du programme.

analyse exploratoire des données (EDA)

Processus d'analyse d'un jeu de données pour comprendre ses principales caractéristiques. Vous collectez ou agrégez des données, puis vous effectuez des enquêtes initiales pour trouver des modèles, détecter des anomalies et vérifier les hypothèses. L'EDA est réalisée en calculant des statistiques récapitulatives et en créant des visualisations de données.

F

tableau des faits

La table centrale dans un schéma en étoile. Il stocke des données quantitatives sur les opérations commerciales. Généralement, une table de faits contient deux types de colonnes : celles qui contiennent des mesures et celles qui contiennent une clé étrangère pour une table de dimensions.

échouer rapidement

Une philosophie qui utilise des tests fréquents et progressifs pour réduire le cycle de vie du développement. C'est un élément essentiel d'une approche agile.

limite d'isolation des défauts

Dans leAWS Cloud, une limite telle qu'une zone de disponibilitéRégion AWS, un plan de contrôle ou un plan de données qui limite l'effet d'une panne et contribue à améliorer la résilience des charges de travail. Pour plus d'informations, consultez la section Limites d'isolation des AWS pannes.

branche de fonctionnalités

Voir succursale.

fonctionnalités

Les données d'entrée que vous utilisez pour faire une prédiction. Par exemple, dans un contexte de fabrication, les fonctionnalités peuvent être des images capturées périodiquement à partir de la ligne de fabrication.

importance des fonctionnalités

Le niveau d'importance d'une fonctionnalité pour les prédictions d'un modèle. Il s'exprime généralement sous la forme d'un score numérique qui peut être calculé à l'aide de différentes techniques, telles que la méthode Shapley Additive Explanations (SHAP) et les gradients intégrés. Pour plus d'informations, voir Interprétabilité du modèle d'apprentissage automatique avec : AWS.

transformation de fonctionnalité

Optimiser les données pour le processus de ML, notamment en enrichissant les données avec des sources supplémentaires, en mettant à l'échelle les valeurs ou en extrayant plusieurs ensembles d'informations à partir d'un seul champ de données. Cela permet au modèle de ML de tirer parti des données. Par exemple, si vous décomposez la date « 2021-05-27 00:15:37 » en

« 2021 », « mai », « jeudi » et « 15 », vous pouvez aider l'algorithme d'apprentissage à apprendre des modèles nuancés associés à différents composants de données.

FGAC

Découvrez le contrôle d'accès détaillé.

contrôle d'accès détaillé (FGAC)

Utilisation de plusieurs conditions pour autoriser ou refuser une demande d'accès.

migration instantanée (flash-cut)

Méthode de migration de base de données qui utilise la réplication continue des données par le biais de la capture des données de modification afin de migrer les données dans les plus brefs délais, au lieu d'utiliser une approche progressive. L'objectif est de réduire au maximum les temps d'arrêt.

G

blocage géographique

Voir les restrictions géographiques.

restrictions géographiques (blocage géographique)

Sur Amazon CloudFront, option permettant d'empêcher les utilisateurs de certains pays d'accéder aux distributions de contenu. Vous pouvez utiliser une liste d'autorisation ou une liste de blocage pour spécifier les pays approuvés et interdits. Pour plus d'informations, consultez la section Restreindre la distribution géographique de votre contenu dans la CloudFront documentation.

Flux de travail Gitflow

Approche dans laquelle les environnements inférieurs et supérieurs utilisent différentes branches dans un référentiel de code source. Le flux de travail Gitflow est considéré comme existant, et le flux de travail basé sur les troncs est l'approche moderne préférée.

stratégie inédite

L'absence d'infrastructures existantes dans un nouvel environnement. Lorsque vous adoptez une stratégie inédite pour une architecture système, vous pouvez sélectionner toutes les nouvelles technologies sans restriction de compatibilité avec l'infrastructure existante, également appelée brownfield. Si vous étendez l'infrastructure existante, vous pouvez combiner des politiques brownfield (existantes) et greenfield (inédites).

barrière de protection

Règle de haut niveau qui permet de régir les ressources, les politiques et la conformité au sein des unités d'organisation (UO). Les barrières de protection préventives appliquent des politiques pour garantir l'alignement sur les normes de conformité. Elles sont mises en œuvre à l'aide de politiques de contrôle des services et de limites des autorisations IAM. Les barrières de protection de détection détectent les violations des politiques et les problèmes de conformité, et génèrent des alertes pour y remédier. Ils sont implémentés à l'aide d'Amazon AWS Config AWS Security Hub GuardDutyAWS Trusted Advisor, d'Amazon Inspector et de AWS Lambda contrôles personnalisés.

H

HA

Découvrez la haute disponibilité.

migration de base de données hétérogène

Migration de votre base de données source vers une base de données cible qui utilise un moteur de base de données différent (par exemple, Oracle vers Amazon Aurora). La migration hétérogène fait généralement partie d'un effort de réarchitecture, et la conversion du schéma peut s'avérer une tâche complexe. AWS propose AWS SCT qui facilite les conversions de schémas.

haute disponibilité (HA)

Capacité d'une charge de travail à fonctionner en continu, sans intervention, en cas de difficultés ou de catastrophes. Les systèmes HA sont conçus pour basculer automatiquement, fournir constamment des performances de haute qualité et gérer différentes charges et défaillances avec un impact minimal sur les performances.

modernisation des historiens

Approche utilisée pour moderniser et mettre à niveau les systèmes de technologie opérationnelle (OT) afin de mieux répondre aux besoins de l'industrie manufacturière. Un historien est un type de base de données utilisé pour collecter et stocker des données provenant de diverses sources dans une usine.

migration de base de données homogène

Migration de votre base de données source vers une base de données cible qui partage le même moteur de base de données (par exemple, Microsoft SQL Server vers Amazon RDS

for SQL Server). La migration homogène s'inscrit généralement dans le cadre d'un effort de réhébergement ou de replateforme. Vous pouvez utiliser les utilitaires de base de données natifs pour migrer le schéma.

données chaudes

Données fréquemment consultées, telles que les données en temps réel ou les données translationnelles récentes. Ces données nécessitent généralement un niveau ou une classe de stockage à hautes performances pour fournir des réponses rapides aux requêtes.

correctif

Solution d'urgence à un problème critique dans un environnement de production. En raison de son urgence, un correctif est généralement créé en dehors du flux de travail de DevOps publication habituel.

période de soins intensifs

Immédiatement après le basculement, période pendant laquelle une équipe de migration gère et surveille les applications migrées dans le cloud afin de résoudre les problèmes éventuels. En règle générale, cette période dure de 1 à 4 jours. À la fin de la période de soins intensifs, l'équipe de migration transfère généralement la responsabilité des applications à l'équipe des opérations cloud.

I

IaC

Considérez l'infrastructure comme un code.

politique basée sur l'identité

Politique attachée à un ou plusieurs principaux IAM qui définit leurs autorisations au sein de l'environnement AWS Cloud.

application inactive

Application dont l'utilisation moyenne du processeur et de la mémoire se situe entre 5 et 20 % sur une période de 90 jours. Dans un projet de migration, il est courant de retirer ces applications ou de les retenir sur site.

IIoT

Voir Internet industriel des objets.

infrastructure immuable

Modèle qui déploie une nouvelle infrastructure pour les charges de travail de production au lieu de mettre à jour, d'appliquer des correctifs ou de modifier l'infrastructure existante. Les infrastructures immuables sont intrinsèquement plus cohérentes, fiables et prévisibles que les infrastructures mutables. Pour plus d'informations, consultez les meilleures pratiques de déploiement à l'aide d'une infrastructure immuable dans le AWS Well-Architected Framework.

VPC entrant (d'entrée)

Dans une architecture à comptes multiples AWS, VPC qui accepte, inspecte et achemine les connexions réseau depuis l'extérieur d'une application. L'architecture de référence de sécurité AWS recommande de configurer votre compte réseau avec des VPC entrants, sortants et d'inspection afin de protéger l'interface bidirectionnelle entre votre application et Internet en général.

migration incrémentielle

Stratégie de basculement dans le cadre de laquelle vous migrez votre application par petites parties au lieu d'effectuer un basculement complet unique. Par exemple, il se peut que vous ne transfériez que quelques microservices ou utilisateurs vers le nouveau système dans un premier temps. Après avoir vérifié que tout fonctionne correctement, vous pouvez transférer progressivement des microservices ou des utilisateurs supplémentaires jusqu'à ce que vous puissiez mettre hors service votre système hérité. Cette stratégie réduit les risques associés aux migrations de grande ampleur.

infrastructure

Ensemble des ressources et des actifs contenus dans l'environnement d'une application.

infrastructure en tant que code (IaC)

Processus de mise en service et de gestion de l'infrastructure d'une application via un ensemble de fichiers de configuration. IaC est conçue pour vous aider à centraliser la gestion de l'infrastructure, à normaliser les ressources et à mettre à l'échelle rapidement afin que les nouveaux environnements soient reproductibles, fiables et cohérents.

internet industriel des objets (IIoT)

L'utilisation de capteurs et d'appareils connectés à Internet dans les secteurs industriels tels que la fabrication, l'énergie, l'automobile, les soins de santé, les sciences de la vie et l'agriculture. Pour plus d'informations, veuillez consulter Building an industrial Internet of Things (IIoT) digital transformation strategy.

VPC d'inspection

Dans une architecture AWS à comptes multiples, VPC centralisé qui gère les inspections du trafic réseau entre des VPC (dans des Régions AWS identiques ou différentes), Internet et les réseaux sur site. L'architecture de référence de sécurité AWS recommande de configurer votre compte réseau avec des VPC entrants, sortants et d'inspection afin de protéger l'interface bidirectionnelle entre votre application et Internet en général.

Internet des objets (IoT)

Réseau d'objets physiques connectés dotés de capteurs ou de processeurs intégrés qui communiquent avec d'autres appareils et systèmes via Internet ou via un réseau de communication local. Pour plus d'informations, veuillez consulter la section Qu'est-ce que l'IoT ?.

interprétabilité

Caractéristique d'un modèle de machine learning qui décrit dans quelle mesure un être humain peut comprendre comment les prédictions du modèle dépendent de ses entrées. Pour plus d'informations, veuillez consulter Machine learning model interpretability with AWS.

IoT

Voir Internet des objets.

Bibliothèque d'informations informatiques (ITIL)

Ensemble de bonnes pratiques pour proposer des services informatiques et les aligner sur les exigences métier. L'ITIL constitue la base de l'ITSM.

gestion des services informatiques (ITSM)

Activités associées à la conception, à la mise en œuvre, à la gestion et à la prise en charge de services informatiques d'une organisation. Pour plus d'informations sur l'intégration des opérations cloud aux outils ITSM, veuillez consulter le guide d'intégration des opérations.

ITIL

Consultez la bibliothèque d'informations informatiques.

ITSM

Voir Gestion des services informatiques.

L

contrôle d'accès basé sur des étiquettes (LBAC)

Une implémentation du contrôle d'accès obligatoire (MAC) dans laquelle une valeur d'étiquette de sécurité est explicitement attribuée aux utilisateurs et aux données elles-mêmes. L'intersection entre l'étiquette de sécurité utilisateur et l'étiquette de sécurité des données détermine les lignes et les colonnes visibles par l'utilisateur.

zone de destination

Une zone de destination est un environnement AWS à comptes multiples Well-Architected évolutif et sécurisé. Il s'agit d'un point de départ à partir duquel vos entreprises peuvent rapidement lancer et déployer des charges de travail et des applications en toute confiance dans leur environnement de sécurité et d'infrastructure. Pour plus d'informations sur les zones de destination, veuillez consulter Setting up a secure and scalable multi-account AWS environment.

migration de grande envergure

Migration de 300 serveurs ou plus.

LBAC

Voir contrôle d'accès basé sur des étiquettes.

principe de moindre privilège

Bonne pratique de sécurité qui consiste à accorder les autorisations minimales nécessaires à l'exécution d'une tâche. Pour plus d'informations, veuillez consulter la rubrique Accorder les autorisations de moindre privilège dans la documentation IAM.

lift and shift

Voir 7 Rs.

système de poids faible

Système qui stocke d'abord l'octet le moins significatif. Voir aussi endianité.

environnements inférieurs

Voir environnement.

M

machine learning (ML)

Type d'intelligence artificielle qui utilise des algorithmes et des techniques pour la reconnaissance et l'apprentissage de modèles. Le ML analyse et apprend à partir de données enregistrées, telles que les données de l'Internet des objets (IoT), pour générer un modèle statistique basé sur des modèles. Pour plus d'informations, veuillez consulter Machine Learning.

branche principale

Voir succursale.

services gérés

Services AWSpour lequel AWS fonctionnent la couche d'infrastructure, le système d'exploitation et les plateformes, et vous accédez aux points de terminaison pour stocker et récupérer des données. Amazon Simple Storage Service (Amazon S3) et Amazon DynamoDB sont des exemples de services gérés. Ils sont également connus sous le nom de services abstraits.

MAP

Voir Migration Acceleration Program.

mécanisme

Processus complet au cours duquel vous créez un outil, favorisez son adoption, puis inspectez les résultats afin de procéder aux ajustements nécessaires. Un mécanisme est un cycle qui se renforce et s'améliore au fur et à mesure de son fonctionnement. Pour plus d'informations, voir Création de mécanismes dans le cadre AWS Well-Architected.

compte membre

Tous les Comptes AWS autres que le compte de gestion qui font partie d'une organisation dans AWS Organizations. Un compte ne peut être membre que d'une seule organisation à la fois.

microservice

Petit service indépendant qui communique via des API bien définies et qui est généralement détenu par de petites équipes autonomes. Par exemple, un système d'assurance peut inclure des microservices qui mappent à des capacités métier, telles que les ventes ou le marketing, ou à des sous-domaines, tels que les achats, les réclamations ou l'analytique. Les avantages des microservices incluent l'agilité, la flexibilité de la mise à l'échelle, la facilité de déploiement,

la réutilisation du code et la résilience. Pour plus d'informations, veuillez consulter Integrating microservices by using AWS serverless services.

architecture de microservices

Approche de création d'une application avec des composants indépendants qui exécutent chaque processus d'application en tant que microservice. Ces microservices communiquent via une interface bien définie à l'aide d'API légères. Chaque microservice de cette architecture peut être mis à jour, déployé et mis à l'échelle pour répondre à la demande de fonctions spécifiques d'une application. Pour plus d'informations, veuillez consulter Implémentation de microservices sur AWS.

Programme d'accélération des migrations (MAP)

Programme AWS qui fournit un support de conseil, des formations et des services pour aider les entreprises à générer une base opérationnelle solide pour passer au cloud et pour aider à compenser le coût initial des migrations. MAP inclut une méthodologie de migration pour exécuter les migrations héritées de manière méthodique, ainsi qu'un ensemble d'outils pour automatiser et accélérer les scénarios de migration courants.

migration à grande échelle

Processus consistant à transférer la majeure partie du portefeuille d'applications vers le cloud par vagues, un plus grand nombre d'applications étant déplacées plus rapidement à chaque vague. Cette phase utilise les bonnes pratiques et les enseignements tirés des phases précédentes pour implémenter une usine de migration d'équipes, d'outils et de processus en vue de rationaliser la migration des charges de travail grâce à l'automatisation et à la livraison agile. Il s'agit de la troisième phase de la stratégie de migration AWS.

usine de migration

Équipes interfonctionnelles qui rationalisent la migration des charges de travail grâce à des approches automatisées et agiles. Les équipes de Migration Factory comprennent généralement les opérations, les analystes commerciaux et les propriétaires, les ingénieurs de migration, les développeurs et les DevOps professionnels travaillant dans le cadre de sprints. Entre 20 et 50 % du portefeuille d'applications d'entreprise est constitué de modèles répétés qui peuvent être optimisés par une approche d'usine. Pour plus d'informations, veuillez consulter la rubrique discussion of migration factories et le guide Cloud Migration Factory dans cet ensemble de contenus.

métadonnées de migration

Informations relatives à l'application et au serveur nécessaires pour finaliser la migration. Chaque modèle de migration nécessite un ensemble de métadonnées de migration différent. Les exemples de métadonnées de migration incluent le sous-réseau cible, le groupe de sécurité et le compte AWS.

modèle de migration

Tâche de migration reproductible qui détaille la stratégie de migration, la destination de la migration et l'application ou le service de migration utilisé. Exemple : réhéberger la migration vers Amazon EC2 avec AWS Application Migration Service.

Évaluation du portefeuille de migration (MPA)

Outil en ligne qui fournit des informations pour valider l'analyse de rentabilisation en faveur de la migration vers le Cloud AWS. La MPA propose une évaluation détaillée du portefeuille (dimensionnement approprié des serveurs, tarification, comparaison du coût total de possession, analyse des coûts de migration), ainsi que la planification de la migration (analyse et collecte des données d'applications, regroupement des applications, priorisation des migrations et planification des vagues). L'outil MPA (connexion requise) est mis gratuitement à la disposition de tous les consultants AWS et consultants partenaires APN.

Évaluation de la préparation à la migration (MRA)

Processus qui consiste à obtenir des informations sur l'état de préparation au cloud d'une entreprise, à identifier les forces et les faiblesses, ainsi qu'à élaborer un plan d'action pour combler les lacunes identifiées, à l'aide d'AWS CAF. Pour plus d'informations, veuillez consulter le guide de préparation à la migration. La MRA est la première phase de la stratégie de migration AWS.

stratégie de migration

Approche utilisée pour migrer une charge de travail vers le Cloud AWS. Pour plus d'informations, reportez-vous aux 7 R de ce glossaire et à Mobiliser votre organisation pour accélérer les migrations à grande échelle.

ML

Voir apprentissage automatique.

MPA

Voir Évaluation du portefeuille de migration.

modernisation

Transformation d'une application obsolète (héritée ou monolithique) et de son infrastructure en un système agile, élastique et hautement disponible dans le cloud afin de réduire les coûts, de gagner en efficacité et de tirer parti des innovations. Pour plus d'informations, veuillez consulter Strategy for modernizing applications in the AWS Cloud.

évaluation de la préparation à la modernisation

Évaluation qui permet de déterminer si les applications d'une organisation sont prêtes à être modernisées, d'identifier les avantages, les risques et les dépendances, et qui détermine dans quelle mesure l'organisation peut prendre en charge l'état futur de ces applications. Le résultat de l'évaluation est un plan de l'architecture cible, une feuille de route détaillant les phases de développement et les étapes du processus de modernisation, ainsi qu'un plan d'action pour combler les lacunes identifiées. Pour plus d'informations, veuillez consulter Evaluating modernization readiness for applications in the AWS Cloud.

applications monolithiques (monolithes)

Applications qui s'exécutent en tant que service unique avec des processus étroitement couplés. Les applications monolithiques ont plusieurs inconvénients. Si une fonctionnalité de l'application connaît un pic de demande, l'architecture entière doit être mise à l'échelle. L'ajout ou l'amélioration des fonctionnalités d'une application monolithique devient également plus complexe lorsque la base de code s'élargit. Pour résoudre ces problèmes, vous pouvez utiliser une architecture de microservices. Pour plus d'informations, veuillez consulter Decomposing monoliths into microservices.

classification multi-classes

Processus qui permet de générer des prédictions pour plusieurs classes (prédiction d'un résultat parmi plus de deux). Par exemple, un modèle de ML peut demander « Ce produit est-il un livre, une voiture ou un téléphone ? » ou « Quelle catégorie de produits intéresse le plus ce client ? ».

infrastructure mutable

Modèle qui met à jour et modifie l'infrastructure existante pour les charges de travail de production. Pour améliorer la cohérence, la fiabilité et la prévisibilité, le AWS Well-Architected Framework recommande l'utilisation d'une infrastructure immuable comme meilleure pratique.

O

OAC

Voir Contrôle d'accès à l'origine.

OAI

Voir l'identité d'accès à l'origine.

OCM

Voir gestion du changement organisationnel.

migration hors ligne

Méthode de migration dans laquelle la charge de travail source est supprimée au cours du processus de migration. Cette méthode implique un temps d'arrêt prolongé et est généralement utilisée pour de petites charges de travail non critiques.

OI

Voir Intégration des opérations.

OLA

Voir l'accord au niveau opérationnel.

migration en ligne

Méthode de migration dans laquelle la charge de travail source est copiée sur le système cible sans être mise hors ligne. Les applications connectées à la charge de travail peuvent continuer à fonctionner pendant la migration. Cette méthode implique un temps d'arrêt nul ou minimal et est généralement utilisée pour les charges de travail de production critiques.

accord au niveau opérationnel (OLA)

Accord qui précise ce que les groupes informatiques fonctionnels s'engagent à fournir les uns aux autres, afin de prendre en charge un contrat de niveau de service (SLA).

examen de l'état de préparation opérationnelle (ORR)

Une liste de questions et de bonnes pratiques associées qui vous aident à comprendre, à évaluer, à prévenir ou à réduire l'ampleur des incidents et des défaillances possibles. Pour plus d'informations, voir Operational Readiness Reviews (ORR) dans le AWS Well-Architected Framework.

intégration des opérations (OI)

Processus de modernisation des opérations dans le cloud, qui implique la planification de la préparation, l'automatisation et l'intégration. Pour en savoir plus, veuillez consulter le guide d'intégration des opérations.

journal de suivi d'organisation

Journal de suivi créé par AWS CloudTrail qui journalise tous les événements pour tous les Comptes AWS dans une organisation dans AWS Organizations. Ce journal de suivi est créé dans chaque Compte AWS qui fait partie de l'organisation et suit l'activité de chaque compte. Pour plus d'informations, consultez la section Création d'un suivi pour une organisation dans la CloudTrail documentation.

gestion du changement organisationnel (OCM)

Cadre pour gérer les transformations métier majeures et perturbatrices du point de vue des personnes, de la culture et du leadership. L'OCM aide les organisations à se préparer et à effectuer la transition vers de nouveaux systèmes et de nouvelles politiques en accélérant l'adoption des changements, en abordant les problèmes de transition et en favorisant des changements culturels et organisationnels. Dans la stratégie de migration AWS, ce cadre s'appelle accélération des personnes, en raison de la rapidité du changement requise dans les projets d'adoption du cloud. Pour plus d'informations, veuillez consulter le guide OCM.

contrôle d'accès d'origine (OAC)

Dans CloudFront, une option améliorée pour restreindre l'accès afin de sécuriser votre contenu Amazon Simple Storage Service (Amazon S3). OAC prend en charge tous les compartiments S3 dans toutes les Régions AWS, le chiffrement côté serveur avec AWS KMS (SSE-KMS), ainsi que les demandes `PUT` et `DELETE` dynamiques adressées au compartiment S3.

identité d'accès d'origine (OAI)

Dans CloudFront, une option permettant de restreindre l'accès afin de sécuriser votre contenu Amazon S3. Lorsque vous utilisez OAI, il CloudFront crée un principal auprès duquel Amazon S3 peut s'authentifier. Les principaux authentifiés ne peuvent accéder au contenu d'un compartiment S3 que par le biais d'une distribution spécifique CloudFront . Voir également OAC, qui fournit un contrôle d'accès plus précis et amélioré.

OU

Voir l'examen de l'état de préparation opérationnelle.

VPC sortant (de sortie)

Dans une architecture AWS à comptes multiples, VPC qui gère les connexions réseau initiées depuis une application. L'architecture de référence de sécurité AWS recommande de configurer votre compte réseau avec des VPC entrants, sortants et d'inspection afin de protéger l'interface bidirectionnelle entre votre application et Internet en général.

P

limite des autorisations

Politique de gestion IAM attachée aux principaux IAM pour définir les autorisations maximales que peut avoir l'utilisateur ou le rôle. Pour plus d'informations, veuillez consulter la rubrique Limites des autorisations dans la documentation IAM.

informations personnelles identifiables (PII)

Informations qui, lorsqu'elles sont consultées directement ou associées à d'autres données connexes, peuvent être utilisées pour déduire raisonnablement l'identité d'une personne. Les exemples d'informations personnelles incluent les noms, les adresses et les informations de contact.

PII

Voir les informations personnelles identifiables.

manuel stratégique

Ensemble d'étapes prédéfinies qui capturent le travail associé aux migrations, comme la fourniture de fonctions d'opérations de base dans le cloud. Un manuel stratégique peut revêtir la forme de scripts, de runbooks automatisés ou d'un résumé des processus ou des étapes nécessaires au fonctionnement de votre environnement modernisé.

politique

Objet capable de définir les autorisations (voir la politique basée sur l'identité), de spécifier les conditions d'accès (voir la politique basée sur les ressources) ou de définir les autorisations maximales pour tous les comptes d'une organisation dans AWS Organizations (voir la politique de contrôle des services).

persistance polyglotte

Choix indépendant de la technologie de stockage de données d'un microservice en fonction des modèles d'accès aux données et d'autres exigences. Si vos microservices utilisent la même technologie de stockage de données, ils peuvent rencontrer des difficultés d'implémentation ou présenter des performances médiocres. Les microservices sont plus faciles à mettre en œuvre, atteignent de meilleures performances, ainsi qu'une meilleure capacité de mise à l'échelle s'ils utilisent l'entrepôt de données le mieux adapté à leurs besoins. Pour plus d'informations, veuillez consulter Enabling data persistence in microservices.

évaluation du portefeuille

Processus de découverte, d'analyse et de priorisation du portefeuille d'applications afin de planifier la migration. Pour plus d'informations, veuillez consulter Evaluating migration readiness.

predicate

Une condition de requête qui renvoie `true` ou`false`, généralement située dans une `WHERE` clause.

prédicat pushdown

Technique d'optimisation des requêtes de base de données qui filtre les données de la requête avant le transfert. Cela réduit la quantité de données qui doivent être extraites et traitées à partir de la base de données relationnelle et améliore les performances des requêtes.

contrôle préventif

Contrôle de sécurité conçu pour empêcher qu'un événement ne se produise. Ces contrôles constituent une première ligne de défense pour empêcher tout accès non autorisé ou toute modification indésirable de votre réseau. Pour plus d'informations, veuillez consulter Preventative controls dans Implementing security controls on AWS.

principal

Une entité d'AWS qui peut exécuter des actions et accéder à des ressources. Cette entité est généralement un utilisateur root pour un Compte AWS, un rôle IAM ou un utilisateur. Pour plus d'informations, veuillez consulter la rubrique Principal dans Termes et concepts relatifs aux rôles, dans la documentation IAM.

Confidentialité dès la conception

Une approche de l'ingénierie des systèmes qui prend en compte la confidentialité tout au long du processus d'ingénierie.

zones hébergées privées

Conteneur qui contient des informations concernant la façon dont vous souhaitez qu'Amazon Route 53 réponde aux requêtes DNS pour un domaine et ses sous-domaines dans un ou plusieurs VPC. Pour plus d'informations, veuillez consulter Working with private hosted zones dans la documentation Route 53.

contrôle proactif

Contrôle de sécurité conçu pour empêcher le déploiement de ressources non conformes. Ces contrôles analysent les ressources avant qu'elles ne soient provisionnées. Si la ressource n'est pas conforme au contrôle, elle n'est pas provisionnée. Pour plus d'informations, consultez le guide de référence sur les contrôles dans la AWS Control Tower documentation et consultez la section Contrôles proactifs dans Implémentation des contrôles de sécurité sur AWS.

environnement de production

Voir environnement.

pseudonymisation

Processus de remplacement des identifiants personnels dans un ensemble de données par des valeurs fictives. La pseudonymisation peut contribuer à protéger la vie privée. Les données pseudonymisées sont toujours considérées comme des données personnelles.

Q

plan de requête

Série d'étapes, telles que des instructions, utilisées pour accéder aux données d'un système de base de données relationnelle SQL.

régression du plan de requêtes

Le cas où un optimiseur de service de base de données choisit un plan moins optimal qu'avant une modification donnée de l'environnement de base de données. Cela peut être dû à des changements en termes de statistiques, de contraintes, de paramètres d'environnement, de liaisons de paramètres de requêtes et de mises à jour du moteur de base de données.

R

Matrice RACI

Voir responsable, responsable, consulté, informé (RACI).

rançongiciel

Logiciel malveillant conçu pour bloquer l'accès à un système informatique ou à des données jusqu'à ce qu'un paiement soit effectué.

Matrice RASCI

Voir responsable, responsable, consulté, informé (RACI).

RCAC

Voir contrôle d'accès aux lignes et aux colonnes.

réplica en lecture

Copie d'une base de données utilisée en lecture seule. Vous pouvez acheminer les requêtes vers le réplica de lecture pour réduire la charge sur votre base de données principale.

réarchitecte

Voir 7 Rs.

objectif de point de récupération (RPO)

Durée maximale acceptable depuis le dernier point de récupération des données. Cela permet de déterminer ce qui est considéré comme une perte de données acceptable entre le dernier point de restauration et l'interruption du service.

objectif de temps de récupération (RTO)

Le délai maximum acceptable entre l'interruption du service et le rétablissement du service.

refactoriser

Voir 7 Rs.

Région

Ensemble de ressources AWS dans une zone géographique. Chaque Région AWS est isolée et indépendante des autres pour assurer la tolérance aux pannes, la stabilité et la résilience. Pour plus d'informations, veuillez consulter Managing Régions AWS dans Références générales AWS.

régression

Technique de ML qui prédit une valeur numérique. Par exemple, pour résoudre le problème « Quel sera le prix de vente de cette maison ? », un modèle de ML pourrait utiliser un modèle de régression linéaire pour prédire le prix de vente d'une maison sur la base de faits connus à son sujet (par exemple, la superficie en mètres carrés).

réhéberger

Voir 7 Rs.

version

Dans un processus de déploiement, action visant à promouvoir les modifications apportées à un environnement de production.

déplacer

Voir 7 Rs.

replateforme

Voir 7 Rs.

rachat

Voir 7 Rs.

politique basée sur les ressources

Politique attachée à une ressource, comme un compartiment Amazon S3, un point de terminaison ou une clé de chiffrement. Ce type de politique précise les principaux auxquels l'accès est autorisé, les actions prises en charge et toutes les autres conditions qui doivent être remplies.

matrice responsable, redevable, consulté et informé (RACI)

Une matrice qui définit les rôles et les responsabilités de toutes les parties impliquées dans les activités de migration et les opérations cloud. Le nom de la matrice est dérivé des types de responsabilité définis dans la matrice : responsable (R), responsable (A), consulté (C) et informé (I). Le type de support (S) est facultatif. Si vous incluez le support, la matrice est appelée matrice RASCI, et si vous l'excluez, elle est appelée matrice RACI.

contrôle réactif

Contrôle de sécurité conçu pour permettre de remédier aux événements indésirables ou aux écarts par rapport à votre référence de sécurité. Pour plus d'informations, veuillez consulter la rubrique Responsive controls dans Implementing security controls on AWS.

retain

Voir 7 Rs.

se retirer

Voir 7 Rs.

rotation

Processus de mise à jour périodique d'un secret pour empêcher un attaquant d'accéder aux informations d'identification.

contrôle d'accès aux lignes et aux colonnes (RCAC)

Utilisation d'expressions SQL simples et flexibles dotées de règles d'accès définies. Le RCAC comprend des autorisations de ligne et des masques de colonnes.

RPO

Voir l'objectif du point de récupération.

RTO

Voir l'objectif relatif au temps de rétablissement.

runbook

Ensemble de procédures manuelles ou automatisées nécessaires à l'exécution d'une tâche spécifique. Elles visent généralement à rationaliser les opérations ou les procédures répétitives présentant des taux d'erreur élevés.

S

SAML 2.0

Un standard ouvert utilisé par de nombreux fournisseurs d'identité (IdPs). Cette fonctionnalité active l'authentification unique (SSO) fédérée, permettant aux utilisateurs de se connecter à AWS Management Console ou d'appeler les opérations d'API AWS sans qu'il soit nécessaire de créer un utilisateur dans IAM pour chaque membre de l'organisation. Pour plus d'informations sur la fédération SAML 2.0, veuillez consulter À propos de la fédération SAML 2.0 dans la documentation IAM.

SCP

Voir la politique de contrôle des services.

secret

Dans AWS Secrets Manager des informations confidentielles ou restreintes, telles qu'un mot de passe ou des informations d'identification utilisateur, que vous stockez sous forme cryptée. Il comprend la valeur secrète et ses métadonnées. La valeur secrète peut être binaire, une chaîne unique ou plusieurs chaînes. Pour plus d'informations, consultez la section Secret dans la documentation de Secrets Manager.

contrôle de sécurité

Barrière de protection technique ou administrative qui empêche, détecte ou réduit la capacité d'un assaillant d'exploiter une vulnérabilité de sécurité. Il existe quatre principaux types de contrôles de sécurité : préventifs, détectifs, réactifs et proactifs.

renforcement de la sécurité

Processus qui consiste à réduire la surface d'attaque pour la rendre plus résistante aux attaques. Cela peut inclure des actions telles que la suppression de ressources qui ne sont plus requises, la mise en œuvre des bonnes pratiques de sécurité consistant à accorder le moindre privilège ou la désactivation de fonctionnalités inutiles dans les fichiers de configuration.

système de gestion des informations et des événements de sécurité (SIEM)

Outils et services qui associent les systèmes de gestion des informations de sécurité (SIM) et de gestion des événements de sécurité (SEM). Un système SIEM collecte, surveille et analyse les données provenant de serveurs, de réseaux, d'appareils et d'autres sources afin de détecter les menaces et les failles de sécurité, mais aussi de générer des alertes.

automatisation des réponses de sécurité

Action prédéfinie et programmée conçue pour répondre automatiquement à un événement de sécurité ou y remédier. Ces automatisations servent de contrôles de sécurité détectifs ou réactifs qui vous aident à mettre en œuvre les meilleures pratiques AWS de sécurité. Parmi les actions de réponse automatique, citons la modification d'un groupe de sécurité VPC, l'application de correctifs à une instance Amazon EC2 ou la rotation des informations d'identification.

chiffrement côté serveur

Chiffrement des données à destination, par le Service AWS qui les reçoit.

Politique de contrôle des services (SCP)

Politique qui propose un contrôle centralisé des autorisations pour tous les comptes d'une organisation dans AWS Organizations. Les SCP définissent des barrières de protection ou des

limites aux actions qu'un administrateur peut déléguer à des utilisateurs ou à des rôles. Vous pouvez utiliser les SCP comme listes d'autorisation ou de refus, pour indiquer les services ou les actions autorisés ou interdits. Pour plus d'informations, veuillez consulter la rubrique Politiques de contrôle de service dans la documentation AWS Organizations.

point de terminaison du service

URL du point d'entrée pour un Service AWS. Pour vous connecter par programmation au service cible, vous pouvez utiliser un point de terminaison. Pour plus d'informations, veuillez consulter la rubrique Service AWS endpoints dans Références générales AWS.

contrat de niveau de service (SLA)

Accord qui précise ce qu'une équipe informatique promet de fournir à ses clients, comme le temps de disponibilité et les performances des services.

indicateur de niveau de service (SLI)

Mesure d'un aspect des performances d'un service, tel que son taux d'erreur, sa disponibilité ou son débit.

objectif de niveau de service (SLO)

Mesure cible qui représente l'état d'un service, tel que mesuré par un indicateur de niveau de service.

modèle de responsabilité partagée

Modèle décrivant la responsabilité que vous partagez avec AWS pour la conformité et la sécurité du cloud. AWS est responsable de la sécurité du cloud, tandis que vous êtes responsable de la sécurité dans le cloud. Pour de plus amples informations, veuillez consulter Modèle de responsabilité partagée.

SIEM

Consultez les informations de sécurité et le système de gestion des événements.

point de défaillance unique (SPOF)

Défaillance d'un seul composant critique d'une application susceptible de perturber le système.

SLA

Voir le contrat de niveau de service.

SLI

Voir l'indicateur de niveau de service.

SLO

Voir l'objectif de niveau de service.

split-and-seed modèle

Modèle permettant de mettre à l'échelle et d'accélérer les projets de modernisation. Au fur et à mesure que les nouvelles fonctionnalités et les nouvelles versions de produits sont définies, l'équipe principale se divise pour créer des équipes de produit. Cela permet de mettre à l'échelle les capacités et les services de votre organisation, d'améliorer la productivité des développeurs et de favoriser une innovation rapide. Pour plus d'informations, consultez la section Approche progressive de la modernisation des applications dans le. AWS Cloud

SPOF

Voir point de défaillance unique.

schéma en étoile

Structure organisationnelle de base de données qui utilise une grande table de faits pour stocker les données transactionnelles ou mesurées et utilise une ou plusieurs tables dimensionnelles plus petites pour stocker les attributs des données. Cette structure est conçue pour être utilisée dans un entrepôt de données ou à des fins de business intelligence.

modèle de figuier étrangleur

Approche de modernisation des systèmes monolithiques en réécrivant et en remplaçant progressivement les fonctionnalités du système jusqu'à ce que le système hérité puisse être mis hors service. Ce modèle utilise l'analogie d'un figuier de vigne qui se développe dans un arbre existant et qui finit par supplanter son hôte. Le schéma a été présenté par Martin Fowler comme un moyen de gérer les risques lors de la réécriture de systèmes monolithiques. Pour obtenir un exemple d'application de ce modèle, veuillez consulter Modernizing legacy Microsoft ASP.NET (ASMX) web services incrementally by using containers and Amazon API Gateway.

sous-réseau

Plage d'adresses IP dans votre VPC. Un sous-réseau doit se trouver dans une seule zone de disponibilité.

chiffrement symétrique

Algorithme de chiffrement qui utilise la même clé pour chiffrer et déchiffrer les données.

tests synthétiques

Tester un système de manière à simuler les interactions des utilisateurs afin de détecter les problèmes potentiels ou de surveiller les performances. Vous pouvez utiliser Amazon CloudWatch Synthetics pour créer ces tests.

T

balises

Des paires clé-valeur qui agissent comme des métadonnées pour organiser vos AWS ressources. Les balises peuvent vous aider à gérer, identifier, organiser, rechercher et filtrer des ressources. Pour plus d'informations, veuillez consulter la rubrique Balisage de vos AWS ressources.

variable cible

La valeur que vous essayez de prédire dans le cadre du ML supervisé. Elle est également qualifiée de variable de résultat. Par exemple, dans un environnement de fabrication, la variable cible peut être un défaut du produit.

liste de tâches

Outil utilisé pour suivre les progrès dans un runbook. Liste de tâches qui contient une vue d'ensemble du runbook et une liste des tâches générales à effectuer. Pour chaque tâche générale, elle inclut le temps estimé nécessaire, le propriétaire et l'avancement.

environnement de test

Voir environnement.

entraînement

Pour fournir des données à partir desquelles votre modèle de ML peut apprendre. Les données d'entraînement doivent contenir la bonne réponse. L'algorithme d'apprentissage identifie des modèles dans les données d'entraînement, qui mettent en correspondance les attributs des données d'entrée avec la cible (la réponse que vous souhaitez prédire). Il fournit un modèle de ML qui capture ces modèles. Vous pouvez alors utiliser le modèle de ML pour obtenir des prédictions sur de nouvelles données pour lesquelles vous ne connaissez pas la cible.

passerelle de transit

Hub de transit de réseau que vous pouvez utiliser pour relier vos VPC et vos réseaux sur site. Pour plus d'informations, veuillez consulter la rubrique Qu'est-ce qu'une passerelle de transit ? dans la documentation AWS Transit Gateway.

flux de travail basé sur jonction

Approche selon laquelle les développeurs génèrent et testent des fonctionnalités localement dans une branche de fonctionnalités, puis fusionnent ces modifications dans la branche principale. La branche principale est ensuite intégrée aux environnements de développement, de préproduction et de production, de manière séquentielle.

accès sécurisé

Octroi d'autorisations à un service que vous spécifiez pour effectuer des tâches au sein de votre organisation dans AWS Organizations et dans ses comptes en votre nom. Le service de confiance crée un rôle lié au service dans chaque compte, lorsque ce rôle est nécessaire, pour effectuer des tâches de gestion à votre place. Pour plus d'informations, veuillez consulter la rubrique Utilisation d'AWS Organizations avec d'autres services AWS dans la documentation AWS Organizations.

réglage

Pour modifier certains aspects de votre processus d'entraînement afin d'améliorer la précision du modèle de ML. Par exemple, vous pouvez entraîner le modèle de ML en générant un ensemble d'étiquetage, en ajoutant des étiquettes, puis en répétant ces étapes plusieurs fois avec différents paramètres pour optimiser le modèle.

équipe de deux pizzas

Une petite DevOps équipe que vous pouvez nourrir avec deux pizzas. Une équipe de deux pizzas garantit les meilleures opportunités de collaboration possible dans le développement de logiciels.

U

incertitude

Un concept qui fait référence à des informations imprécises, incomplètes ou inconnues susceptibles de compromettre la fiabilité des modèles de ML prédictifs. Il existe deux types d'incertitude : l'incertitude épistémique est causée par des données limitées et incomplètes, alors que l'incertitude aléatoire est causée par le bruit et le caractère aléatoire inhérents aux données.

Pour plus d'informations, veuillez consulter le guide Quantifying uncertainty in deep learning systems.

tâches indifférenciées

Également connu sous le nom de « levage de charges lourdes », ce travail est nécessaire pour créer et exploiter une application, mais qui n'apporte pas de valeur directe à l'utilisateur final ni d'avantage concurrentiel. Les exemples de tâches indifférenciées incluent l'approvisionnement, la maintenance et la planification des capacités.

environnements supérieurs

Voir environnement.

V

mise à vide

Opération de maintenance de base de données qui implique un nettoyage après des mises à jour incrémentielles afin de récupérer de l'espace de stockage et d'améliorer les performances.

contrôle de version

Processus et outils permettant de suivre les modifications, telles que les modifications apportées au code source dans un référentiel.

Appairage de VPC

Connexion entre deux VPC qui vous permet d'acheminer le trafic à l'aide d'adresses IP privées. Pour plus d'informations, veuillez consulter la rubrique Qu'est-ce que l'appairage de VPC ? dans la documentation Amazon VPC.

vulnérabilités

Défaut logiciel ou matériel qui compromet la sécurité du système.

W

cache actif

Cache tampon qui contient les données actuelles et pertinentes fréquemment consultées. L'instance de base de données peut lire à partir du cache tampon, ce qui est plus rapide que la lecture à partir de la mémoire principale ou du disque.

données chaudes

Données rarement consultées. Lorsque vous interrogez ce type de données, des requêtes modérément lentes sont généralement acceptables.

fonction de fenêtre

Fonction SQL qui effectue un calcul sur un groupe de lignes liées d'une manière ou d'une autre à l'enregistrement en cours. Les fonctions de fenêtre sont utiles pour traiter des tâches, telles que le calcul d'une moyenne mobile ou l'accès à la valeur des lignes en fonction de la position relative de la ligne en cours.

charge de travail

Ensemble de ressources et de code qui fournit une valeur métier, par exemple une application destinée au client ou un processus de backend.

flux de travail

Groupes fonctionnels d'un projet de migration chargés d'un ensemble de tâches spécifique. Chaque flux de travail est indépendant, mais prend en charge les autres flux de travail du projet. Par exemple, le flux de travail du portefeuille est chargé de prioriser les applications, de planifier les vagues et de collecter les métadonnées de migration. Le flux de travail du portefeuille fournit ces actifs au flux de travail de migration, qui migre ensuite les serveurs et les applications.

VER

Voir écrire une fois, lire plusieurs.

WQF

Consultez le cadre de qualification des charges de travail AWS.

écrire une fois, lire plusieurs (WORM)

Modèle de stockage qui écrit les données une seule fois et empêche leur suppression ou leur modification. Les utilisateurs autorisés peuvent lire les données autant de fois que nécessaire, mais ils ne peuvent pas les modifier. Cette infrastructure de stockage de données est considérée comme immuable.

Z

exploit Zero-Day

Une attaque, généralement un logiciel malveillant, qui tire parti d'une vulnérabilité de type « jour zéro ».

vulnérabilité « jour zéro »

Une faille ou une vulnérabilité non atténuée dans un système de production. Les acteurs malveillants peuvent utiliser ce type de vulnérabilité pour attaquer le système. Les développeurs prennent souvent conscience de la vulnérabilité à la suite de l'attaque.

application zombie

Application dont l'utilisation moyenne du processeur et de la mémoire est inférieure à 5 %. Dans un projet de migration, il est courant de retirer ces applications.

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.