Mise en place de garde-corps et surveillance des systèmes présignés URLs

AWS Conseils prescriptifs

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Conseils prescriptifs: Mise en place de garde-corps et surveillance des systèmes présignés URLs

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques commerciales et la présentation commerciale d'Amazon ne peuvent pas être utilisées en relation avec un produit ou un service extérieur à Amazon, d'une manière susceptible d'entraîner une confusion chez les clients, ou d'une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d'Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Mise en place de garde-fous et surveillance des URL présignées

Ryan Baker, Amazon Web Services (AWS)

Juillet 2024 (historique du document)

La sécurité est une préoccupation essentielle pour toutes les entreprises et un pilier essentiel de l'AWS Well-Architected Framework. En tant qu'ingénieur en sécurité, vous souhaiterez mettre en place des garde-fous administratifs conformes aux exigences de contrôle de l'organisation. Dans le AWS Well-Architected Framework, les barrières de sécurité définissent les limites qui limitent l'activité.

Ce guide fournit des informations générales et les meilleures pratiques relatives à l'utilisation d'URL présignées, qui sont utilisées avec les objets Amazon Simple Storage Service (Amazon S3). Les URL présignées permettent aux utilisateurs ou aux applications ayant accès à des informations d'identification valides de générer des demandes qui sont signées à l'avance et acceptées jusqu'à une date d'expiration définie. Un cas d'utilisation courant des URL présignées consiste à étendre l'accès à des objets ou à des ressources en partageant ces demandes. Les demandes présignées partagées sont générées par des systèmes ou des utilisateurs autorisés à exécuter une demande spécifique, puis peuvent être envoyées à d'autres systèmes ou utilisateurs pour étendre la capacité d'exécuter cette même demande.

Dans ce guide, vous découvrirez :

- Les concepts des URL présignées
- Cas d'utilisation pour les URL présignées
- Rambardes recommandées et optionnelles
- Options de surveillance
- Exemples d' Services AWS utilisation d'URL présignées

Public visé

Ce guide est destiné aux architectes et aux ingénieurs de sécurité chargés d'implémenter les contrôles de sécurité dans le AWS Cloud.

Objectifs

En tant qu'ingénieur en sécurité, vous devez savoir comment les créateurs de solutions mettent en œuvre la sécurité et connaître le type d'accès dont disposent vos utilisateurs finaux. Ce guide couvre un type d'accès, les URL présignées, qui sont souvent utilisés avec Amazon S3. Les URL présignées fournissent aux constructeurs des options pour relier efficacement les mécanismes d'authentification.

Dans Amazon S3, les URL présignées représentent une catégorie unique de demandes. Les ingénieurs de sécurité peuvent surveiller et gérer ces demandes afin de s'assurer qu'elles ne sont utilisées que lorsque cela est approprié et nécessaire. L'objectif de ce guide est d'aider les ingénieurs de sécurité à fournir ce type de supervision de haut niveau.

Après avoir lu ce guide, vous devriez comprendre ce qu'est une URL présignée, à quel moment elle est généralement utilisée et quelles sont les motivations de son utilisation.

Prérequis

Si votre entreprise n'a pas défini de politique de sécurité, d'objectifs de contrôle ou de normes, comme décrit dans le guide Implémentation des contrôles de sécurité sur AWS, nous vous recommandons d'effectuer ces tâches de gouvernance avant de poursuivre ce guide.

Avant de commencer, vous devez également connaître les meilleures pratiques recommandées et facultatives en matière de contrôle et de surveillance. Pour plus d’informations, consultez :

- Politiques de contrôle des services (AWS Organizations documentation)
- Politiques relatives aux compartiments pour Amazon S3 (documentation Amazon S3)
- Journalisation des demandes avec journalisation des accès au serveur (documentation Amazon S3)
- Journalisation des appels d'API Amazon S3 à l'aide de AWS CloudTrail(documentation Amazon S3)

Vue d'ensemble des URL présignées

Une URL présignée est un type de requête HTTP reconnu par le service AWS Identity and Access Management (IAM). Ce qui différencie ce type de demande de toutes les autres AWS requêtes est le paramètre de requête X-Amz-Expires. Comme pour les autres demandes authentifiées, les demandes d'URL présignées incluent une signature. Pour les demandes d'URL présignées, cette signature est transmise dans`X-Amz-Signature`. La signature utilise les opérations cryptographiques Signature Version 4 pour coder tous les autres paramètres de demande.

> **Remarques**
>
> - La version 2 de Signature est actuellement en cours de dépréciation, mais elle est toujours prise en charge dans certains cas. Régions AWS Ce guide s'applique à la signature de Signature version 4.
> - Le service de réception peut traiter les en-têtes non signés, mais le support pour cette option est limité et ciblé, conformément aux meilleures pratiques. Sauf indication contraire, supposons que tous les en-têtes doivent être signés pour qu'une demande soit acceptée.

Le `X-Amz-Expires` paramètre permet de traiter une signature comme valide avec un écart plus important par rapport à la date et à l'heure codées. D'autres aspects de la validité des signatures sont toujours évalués. Les identifiants de signature, s'ils sont temporaires, ne doivent pas être expirés au moment du traitement de la signature. Les identifiants de signature doivent être attachés à un directeur IAM disposant des autorisations suffisantes au moment du traitement.

Les URL présignées sont un sous-ensemble des demandes présignées

Une URL présignée n'est pas la seule méthode pour signer une demande pour une date future. Amazon S3 prend également en charge les requêtes POST, qui sont également généralement présignées. Une signature POST présignée autorise les téléchargements conformes à une politique signée et dont la date d'expiration est intégrée à cette politique.

Les signatures des demandes peuvent être datées du futur, bien que cela soit rare. Tant que les informations d'identification sous-jacentes sont valides, l'algorithme de signature n'interdit pas les rencontres futures. Cependant, ces demandes ne peuvent pas être traitées avec succès avant leur période de validité, ce qui rend les rencontres futures peu pratiques pour la plupart des cas d'utilisation.

Que permet une demande présignée ?

Une demande présignée ne peut autoriser que les actions autorisées par les informations d'identification utilisées pour signer la demande. Si les informations d'identification refusent implicitement ou explicitement l'action spécifiée par la demande présignée, la demande présignée est refusée lors de son envoi. Cela s'applique aux éléments suivants :

- Politiques de session associées aux informations d'identification
- Politiques associées au principal associé aux informations d'identification
- Politiques relatives aux ressources qui affectent la session ou le principal
- Politiques de contrôle des services qui affectent la session ou le principal

Motivations motivant l'utilisation de demandes présignées

En tant qu'ingénieur en sécurité, vous devez savoir ce qui pousse les créateurs de solutions à utiliser des URL présignées. Comprendre ce qui est nécessaire et ce qui est facultatif vous aidera à communiquer avec les créateurs de solutions. Les motivations peuvent inclure les suivantes :

- Pour prendre en charge un mécanisme d'authentification non IAM tout en bénéficiant de l'évolutivité d'Amazon S3. L'une des principales motivations est de communiquer directement avec Amazon S3 afin de bénéficier de l'évolutivité intégrée fournie par ce service. Sans cette communication directe, une solution devrait prendre en charge la charge de retransmission des octets envoyés PutObjectet des GetObjectappels. En fonction de la charge totale, cette exigence ajoute des difficultés de mise à l'échelle qu'un concepteur de solutions pourrait vouloir éviter.

  D'autres moyens de communication directe avec Amazon S3, tels que l'utilisation d'informations d'identification temporaires dans AWS Security Token Service (AWS STS) ou de signatures Signature Version 4 en dehors des URL, peuvent ne pas être adaptés à votre cas d'utilisation. Amazon S3 identifie les utilisateurs à l'aide AWS d'informations d'identification, tandis que les demandes présignées supposent une identification par des mécanismes autres que AWS les informations d'identification. Il est possible de combler cette différence tout en maintenant la communication directe pour les données grâce à des demandes présignées.
- Pour bénéficier de la compréhension native des URL d'un navigateur. Les URL sont comprises par les navigateurs, alors que les AWS STS informations d'identification et les signatures de la version 4 de la signature ne le sont pas. Cela est avantageux lors de l'intégration à des solutions basées sur un navigateur. Les solutions alternatives nécessitent plus de code, utilisent davantage

de mémoire pour les fichiers volumineux et peuvent être traitées différemment par des extensions telles que les scanners de logiciels malveillants et de virus.

Comparaison avec les AWS STS informations d'identification temporaires

Les informations d'identification temporaires sont similaires aux demandes présignées. Ils expirent tous les deux, permettent de délimiter l'accès et sont couramment utilisés pour relier les informations d'identification non IAM à une utilisation nécessitant des informations d'identification AWS.

Vous pouvez limiter une AWS STS identification temporaire à un seul objet et à une seule action S3, mais cela peut entraîner des problèmes de dimensionnement car les AWS STS API ont des limites. (Pour plus d'informations, consultez l'article Comment puis-je résoudre les erreurs de limitation des API ou de « débit dépassé » pour IAM et sur AWS STS le site Web AWS Re:Post.) En outre, chaque identifiant généré nécessite un appel d' AWS STS API, ce qui ajoute de la latence et crée une nouvelle dépendance susceptible d'affecter la résilience. Un AWS STS identifiant temporaire a également un délai d'expiration minimum de 15 minutes, tandis qu'une demande présignée peut prendre en charge des durées plus courtes (60 secondes, c'est pratique dans les bonnes conditions).

Comparaison avec les solutions basées uniquement sur les signatures

Le seul élément intrinsèquement secret d'une demande présignée est sa signature Signature Version 4. Si un client connaît les autres détails d'une demande et reçoit une signature valide correspondant à ces détails, il peut envoyer une demande valide. Sans signature valide, ce n'est pas possible.

Les URL présignées et les solutions utilisant uniquement des signatures sont cryptographiquement similaires. Cependant, les solutions basées uniquement sur les signatures présentent des avantages pratiques tels que la possibilité d'utiliser un en-tête HTTP au lieu d'un paramètre de chaîne de requête pour transmettre la signature (voir la section Journalisation des interactions et des mesures d'atténuation). Les administrateurs doivent également tenir compte du fait que les chaînes de requête sont généralement traitées comme des métadonnées, alors que les en-têtes sont moins souvent traités comme tels.

D'autre part, les AWS SDK fournissent moins de support pour la génération et l'utilisation directes de signatures. La création d'une solution basée uniquement sur les signatures nécessite davantage de code personnalisé. D'un point de vue pratique, l'utilisation de bibliothèques plutôt que de code personnalisé pour des raisons de sécurité est une bonne pratique générale. Le code des solutions utilisant uniquement des signatures doit donc faire l'objet d'une attention particulière.

Les solutions utilisant uniquement des signatures n'utilisent pas la chaîne de `X-Amz-Expires` requête et ne fournissent aucune période de validité explicite. IAM gère les périodes de validité implicites des signatures qui n'ont pas de date d'expiration explicite. Ces périodes implicites ne sont pas publiées. Ils ne changent généralement pas, mais ils sont gérés dans un souci de sécurité. Vous ne devez donc pas vous fier aux périodes de validité. Il y a un compromis entre le contrôle explicite de la date d'expiration et la gestion de l'expiration par IAM.

En tant qu'administrateur, vous préférerez peut-être une solution basée uniquement sur les signatures. Cependant, d'un point de vue pratique, vous devrez soutenir les solutions telles qu'elles ont été conçues.

Identifier les demandes présignées

Identification des demandes utilisant une URL présignée

Amazon S3 fournit deux mécanismes intégrés pour surveiller l'utilisation au niveau de la demande : les journaux d'accès au serveur Amazon S3 et les événements AWS CloudTrail liés aux données. Les deux mécanismes peuvent identifier l'utilisation des URL présignées.

Pour filtrer les journaux en fonction de l'utilisation des URL présignées, vous pouvez utiliser le type d'authentification. Pour les journaux d'accès au serveur, examinez le champ Type d'authentification, généralement nommé authtype lorsqu'il est défini dans une table Amazon Athena. Pour CloudTrail, examinez AuthenticationMethod`additionalEventData`sur le terrain. Dans les deux cas, la valeur du champ pour les demandes utilisant des URL présignées est`QueryString`, alors que c'`AuthHeader`est la valeur pour la plupart des autres demandes.

`QueryString`l'utilisation n'est pas toujours associée aux URL présignées. Pour limiter votre recherche à l'utilisation d'URL présignées uniquement, recherchez les demandes contenant le paramètre `X-Amz-Expires` de chaîne de requête. Pour les journaux d'accès au serveur, examinez Request-URI et recherchez les demandes dont la chaîne de requête contient un `X-Amz-Expires` paramètre. Pour CloudTrail, examinez l'`requestParameters`élément pour un `X-Amz-Expires` élément.

```
{"Records": [{…, "requestParameters": {…, "X-Amz-Expires": "300"}}, …]}
```

La requête Athena suivante applique ce filtre :

```
SELECT * FROM {athena-table} WHERE
  authtype = 'QueryString' AND
  request_uri LIKE '%X-Amz-Expires=%';
```

Pour AWS CloudTrail Lake, la requête suivante applique ce filtre :

```
SELECT * FROM {data-store-event-id} WHERE
  additionalEventData['AuthenticationMethod'] = 'QueryString' AND
  requestParameters['X-Amz-Expires'] IS NOT NULL
```

Identifier d'autres types de demandes présignées

La requête POST possède également un type d'authentification unique`HtmlForm`, dans les journaux d'accès au serveur Amazon S3 et CloudTrail. Ce type d'authentification étant moins courant, il est possible que vous ne trouviez pas ces demandes dans votre environnement.

La requête Athena suivante applique le filtre pour : `HtmlForm`

```
SELECT * FROM {athena-table} WHERE
  authtype = 'HtmlForm';
```

Pour CloudTrail Lake, la requête suivante applique le filtre :

```
SELECT * FROM {data-store-event-id} WHERE
  additionalEventData['AuthenticationMethod'] = 'HtmlForm'
```

Identification des modèles de demandes

Vous pouvez trouver des demandes présignées en utilisant les techniques décrites dans la section précédente. Toutefois, pour rendre ces données utiles, vous devez trouver des modèles. Les `TOP 10` résultats simples de votre requête peuvent fournir un aperçu, mais si cela ne suffit pas, utilisez les options de regroupement du tableau suivant.

Option de regroupement	Journaux d'accès au serveur	CloudTraillac	Description
Agent utilisateur	`GROUP BY useragent`	`GROUP BY userAgent`	Cette option de regroupement vous permet de trouver la source et le but des demandes. L'agent utilisateur est fourni par l'utilisateur et n'est pas fiable en tant que mécanisme d'authentification ou d'autorisation. Cependant

Option de regroupement	Journaux d'accès au serveur	CloudTraillac	Description
			, cela peut révéler beaucoup de choses si vous recherchez des modèles, car la plupart des clients utilisent une chaîne unique qui est au moins partiellement lisible par l'homme.

Option de regroupement	Journaux d'accès au serveur	CloudTraillac	Description
Demandeur	`GROUP BY requester`	`GROUP BY userIdentity['arn']`	Cette option de regroupement permet de trouver les principaux IAM qui ont signé les demandes. Si votre objectif est de bloquer ces demandes ou de créer une exception pour les demandes existantes, ces requêtes fournissent suffisamment d'informations à cette fin. Lorsque vous utilisez des rôles conformément aux meilleures pratiques IAM, le propriétaire du rôle est clairement identifié, et vous pouvez utiliser ces informations pour en savoir plus.

Option de regroupement	Journaux d'accès au serveur	CloudTraillac	Description
Adresse IP source	`GROUP BY remoteip`	`GROUP BY sourceIPAddress`	Cette option est groupée en fonction du dernier saut de traduction réseau avant d'atteindre Amazon S3. • Si le trafic passe par une passerelle NAT, il s'agira de l'adresse de la passerelle NAT. • Si le trafic passe par une passerelle Internet, il s'agira de l'adresse IP publique qui a envoyé le trafic vers la passerelle Internet. • Si le trafic provient de l'extérieur AWS, il s'agira de l'adresse Internet publique associée à l'origine. • S'il passe par un point de terminaison de cloud privé

Option de regroupement	Journaux d'accès au serveur	CloudTraillac	Description
			virtuel (VPC) de passerelle, il s'agira de l'adresse IP de l'instance dans le VPC. • S'il passe par une interface virtuelle publique (VIF), il s'agira de l'adresse IP locale du demandeur ou de tout intermédiaire tel qu'un serveur proxy ou un pare-feu qui n'expose que son adresse IP. • S'il passe par un point de terminaison VPC d'interface, il peut s'agir de l'adresse IP d'une instance du VPC. Il peut également s'agir d'une adresse IP provenant d'un autre VPC ou d'un réseau sur site. Comme pour les VIF publiques, il peut s'agir de l'adresse IP de

Option de regroupement	Journaux d'accès au serveur	CloudTraillac	Description
			n'importe quel intermédiaire. Ces données sont utiles si votre objectif est d'imposer des contrôles réseau. Vous devrez peut-être combiner cette option avec des données telles que `endpoint` (pour les journaux d'accès au serveur) ou `vpcEndpointId` (pour CloudTrail Lake) pour clarifier la source, car différents réseaux peuvent dupliquer des adresses IP privées.
Nom du compartiment S3	`GROUP BY bucket_name`	`GROUP BY requestParameters['bucketName']`	Cette option de regroupement permet de trouver les compartiments ayant reçu des demandes. Cela vous permet d'identifier le besoin d'exceptions.

Bonnes pratiques d'utilisation des demandes présignées

Cette section décrit les meilleures pratiques d'utilisation des demandes présignées qu'un ingénieur en sécurité doit prendre en compte. Les directives incluent :

- Les meilleures pratiques fondamentales, qui sont des pratiques que chaque organisation devrait suivre.
- Des garde-fous supplémentaires, pratiques que vous devriez envisager, mais que vous pourriez décider de mettre en œuvre partiellement ou avec des exceptions. Ils visent à fournir un contrôle et une défense supplémentaires en profondeur, mais doivent être mis en balance avec la complexité globale.
- Enregistrement des interactions, qui peuvent résulter d'appareils ou de services relevant de votre responsabilité ou de celle de votre client dans le cadre du modèle de responsabilité partagée. Cette section inclut des précautions visant à limiter les informations accessibles par le biais des journaux.

Bonnes pratiques fondamentales

Les meilleures pratiques générales qui constituent des contrôles efficaces pour les autres demandes d' AWS API s'appliquent également aux demandes présignées. Cette section passe en revue deux des pratiques les plus pertinentes : le moindre privilège et les périmètres de données. Ces pratiques créent une profondeur de contrôle que d'autres pratiques étendent.

Appliquer le principe du moindre privilège

La première étape pour limiter l'utilisation des demandes présignées consiste à limiter l'accès à Amazon S3 en général. Une URL présignée ne peut pas fournir d'accès à des ressources qui n'ont pas été accordées au principal qui a généré la signature de l'URL présignée. Il ne peut pas non plus donner accès à une ressource d'une manière qui n'a pas été accordée à ce mandant. En tant que tel, l'application des meilleures pratiques pour accorder le moins de privilèges à ces principaux constitue un garde-fou efficace.

Le processus de création d'une URL présignée est une opération algorithmique basée sur une norme publiée (Signature Version 4) pour la génération de signatures. Il n'est donc pas possible de limiter la génération de présignés URLs. Toutefois, pour être pertinente, une URL présignée doit être valide et fournir un accès aux ressources. La validité d'une URL présignée constitue donc également un garde-fou efficace.

Pour plus d'informations sur le moindre privilège, voir Accorder l'accès au moindre privilège dans le pilier Sécurité du AWS Well-Architected Framework.

Implémenter un périmètre de données

L'extension du moindre privilège consiste à maintenir un périmètre de données conforme aux besoins de votre entreprise. Les présignés URLs sont compatibles avec les périmètres de données. Comme pour les autres demandes, la validité d'une demande d'URL présignée est évaluée au moment de la demande. Si les propriétés du réseau, de la ressource, de la session de rôle et du principal changent, elles sont évaluées au moment et en utilisant la méthode par laquelle une demande est reçue.

Supposons, par exemple, qu'un service exécuté dans un conteneur Amazon Elastic Kubernetes Service (Amazon EKS) signe une demande. La demande est ensuite envoyée depuis le système informatique personnel d'un utilisateur connecté à Internet. Dans ce cas, la SourceIp condition aws : évalue l'adresse IP publique visible de la demande depuis le système personnel de l'utilisateur, et non l'adresse IP du service dans le conteneur Amazon EKS.

De même, si les balises du principal ou de la ressource changent avant l'envoi de la demande, les valeurs mises à jour, et non les valeurs d'origine, s'appliqueront à la demande via les conditions aws : PrincipalTag /tag-key et aws : ResourceTag /tag-key.

Rambardes supplémentaires

Lorsque les demandes présignées sont utilisées de manière appropriée par les créateurs de solutions et les utilisateurs, elles fournissent un mécanisme sécurisé permettant aux utilisateurs d'accéder aux données. En outre, la possibilité de générer des demandes présignées ne fournit pas aux donneurs d'ordre un accès qu'ils n'avaient pas déjà.

Dans ce contexte, des contrôles supplémentaires sont-ils nécessaires ? La justification des contrôles supplémentaires ne repose pas sur la nécessité de refuser l'accès, mais sur la capacité de surveiller, d'approuver l'utilisation et de fixer des limites, et de réduire les risques d'erreurs des utilisateurs. De cette façon, vous pouvez contribuer à garantir que l'utilisation est appropriée et nécessaire.

Les rambardes suivantes vous aideront à atteindre cet objectif. Avant d'activer ces contrôles, vous souhaiterez peut-être déterminer l'utilisation existante en identifiant les demandes présignées. Cette identification vous aide à vous préparer à l'impact du garde-corps sur l'utilisation existante ou à planifier des exceptions si nécessaire.

Rambarde pour S3 : SignatureAge

L'une des caractéristiques déterminantes des demandes présignées est qu'elles décrivent un délai d'expiration. La signature de la demande contient une date. Cette date est transmise sous forme de paramètre de chaîne de `X-Amz-Date` requête pour un POST présigné URLs, et sous forme de date ou d' x-amz-dateen-tête pour un POST présigné.

Amazon S3 fournit une clé de condition, s3:SignatureAge, que vous pouvez utiliser pour limiter le délai maximum entre la date de signature et l'expiration effective de la demande. Cette condition ne peut jamais augmenter la durée de validité, mais elle peut la réduire.

Dans la politique suivante, la clé de `s3:signatureAge` condition limite les demandes présignées à 15 minutes de validité. Les exemples suivants utilisent tous 15 minutes pour limiter la validité à une période similaire à celle prise en charge par la signature standard.

La deuxième déclaration de la politique refuse tout accès à Signature Version 2. Cette version du protocole de signature est obsolète, mais elle est toujours prise en charge dans certains d'entre eux. Régions AWS Nous vous recommandons de le bloquer explicitement avant qu'il ne soit totalement obsolète.

Vous pouvez appliquer la politique suivante en tant que politique AWS Organizations de contrôle des services (SCP). Les utilisateurs peuvent toujours utiliser des demandes présignées et déployer des solutions qui dépendent de ces demandes, à condition que le délai entre la génération des signatures et leur utilisation soit inférieur à 15 minutes. Selon l'implémentation, cette limitation peut n'avoir aucun impact, rendre la solution inutilisable ou provoquer des échecs occasionnels qui peuvent être réessayés.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPresignedOver15Minutes",
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        }
      }
```

```
    },
    {
      "Sid": "DenySignatureVersion2",
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
           "s3:signatureversion": "AWS"
        }
      }
    }
  ]
}
```

Exceptions

Si une solution nécessite un délai plus long avant son expiration et est donc affectée par la politique précédente, nous vous recommandons de fournir une méthode pour approuver les exceptions. Pour éviter d'énumérer les exceptions dans un SCP, utilisez aws : PrincipalTag, comme dans la politique suivante, pour gérer les exceptions de manière évolutive. D'autres AWS exemples, tels que les exemples de politique de périmètre des données AWS, utilisent cette stratégie.

Si vous implémentez une politique d'exception en utilisant`aws:PrincipalTag`, vous devez contrôler l'accès aux balises de configuration sur les principes. Les balises de ce type peuvent provenir directement des principaux et peuvent être contrôlées par un SCP, comme dans cet exemple de contrôle des valeurs de balise pouvant être définies. Une balise de ce type peut également provenir de balises de session, définies par un fournisseur d'identité (IdP) ou lors de l'utilisation. AWS STS Le contrôle de l'accès à `aws:PrincipalTag` est un sujet complexe. Toutefois, une organisation expérimentée dans l'utilisation du contrôle d'accès basé sur les attributs (ABAC) aura l'expérience et les contrôles nécessaires pour permettre une utilisation appropriée `aws:PrincipalTag` pour ce cas d'utilisation.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPresignedOver15Minutes",
      "Effect": "Deny",
      "Action": "s3:*",
```

```
      "Resource": "*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
--- Example exception ---
        "StringNotEquals": {
          "aws:PrincipalTag/long-presigned-allowed": "true"
        }
--- Example exception end ---
      }
    }
  ]
}
```

Politiques de compartiment

Vous pouvez appliquer des politiques de compartiment à tous les compartiments ou à certains d'entre eux en utilisant une politique, comme dans l'exemple suivant. Contrairement à un SCP, une politique de compartiment cible également l'utilisation principale du service. L'annexe A ne documente aucune utilisation prévue du principal service des demandes présignées, mais si vous souhaitez mettre en œuvre un contrôle afin de prouver cette limite, la politique suivante vous fournira ce contrôle. De plus, contrairement à un SCP, une politique de compartiment peut s'appliquer aux principaux de votre compte de gestion. Les exceptions basées sur ABAC fonctionnent dans les politiques de compartiment de la même manière qu'un SCP.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPresignedOver15Minutes",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::{bucket-name}/*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
--- Example exception ---
        "StringNotEquals": {
```

```
          "aws:PrincipalTag/long-presigned-allowed": "true"
        }
--- Example exception end ---
      }
    }
  ]
}
```

Rambarde pour S3:AuthType

Le présigné URLs utilise l'authentification par chaîne de requête, et le présigné utilise POSTs toujours l'authentification POST. Amazon S3 prend en charge le refus des demandes en fonction du type d'authentification via la clé de condition s3:AuthType. `REST-QUERY-STRING`est la `s3:authType` valeur des chaînes de requête et `POST` la `s3:authType` valeur de POST.

Vous pouvez appliquer la politique suivante en tant que SCP. La politique permet `s3:authType` d'autoriser uniquement l'authentification basée sur les en-têtes. Il configure également une méthode pour fournir des exceptions à des utilisateurs ou à des rôles individuels.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonHeaderAuth",
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "s3:authType": "REST-HEADER",
          "aws:PrincipalTag/non-header-auth-allowed": "true"
        }
      }
    }
  ]
}
```

Le refus des demandes en fonction du type d'authentification affecte toute solution ou fonctionnalité utilisant le type d'authentification refusé. Par exemple, le refus `REST-QUERY-STRING` empêche les utilisateurs d'effectuer des chargements ou des téléchargements depuis la console Amazon S3. Si

vous souhaitez que les utilisateurs utilisent la console Amazon S3, n'utilisez pas ce garde-fou et ne faites pas d'exception pour les utilisateurs. D'autre part, si vous ne souhaitez pas que les utilisateurs utilisent la console Amazon S3, vous pouvez refuser l'accès `REST-QUERY-STRING` aux utilisateurs.

Peut-être refusez-vous déjà aux utilisateurs l'accès direct aux ressources Amazon S3. Dans ce cas, un garde-fou pour le type d'authentification est redondant. Cependant, une instruction de `s3:authType` refus est defense-in-depth utile car les implémentations visant à refuser l'accès direct couvrent généralement de nombreuses instructions de contrôle, certaines avec des exceptions.

Les rôles utilisés pour les charges de travail n'ont généralement pas besoin d'accéder à une chaîne de requête ou `POST` d'authentification. Les exceptions sont les rôles qui prennent en charge les services conçus pour utiliser des demandes présignées. Vous pouvez créer des exceptions spécifiques pour ces rôles.

Vous pouvez également appliquer une politique de compartiment à tous les compartiments ou à certains d'entre eux en utilisant une stratégie telle que la suivante :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonHeaderAuth",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::{bucket-name}/*",
      "Condition": {
        "StringNotEquals": {
          "s3:authType": "REST-HEADER",
          "aws:PrincipalTag/non-header-auth-allowed": "true"
        }
      }
    }
  ]
}
```

Cette politique de compartiment a pour effet de refuser l'utilisation de CopyObjectet UploadPartCopy APIs pour effectuer des copies entre régions. Amazon S3 Replication n'est pas affectée car elle ne repose pas sur ces éléments APIs.

Si vous souhaitez utiliser une politique de compartiment telle que la politique précédente tout en prenant en charge l'interrégion CopyObjectou UploadPartCopyl'API, ajoutez une condition `aws:ViaAWSService` similaire à la suivante :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonHeaderAuth",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::{bucket-name}/*",
      "Condition": {
        "StringNotEquals": {
          "s3:authType": "REST-HEADER",
          "aws:PrincipalTag/non-header-auth-allowed": "true"
        },
        "Bool": {
          "aws:ViaAWSService": "false"
        },
      }
    }
  ]
}
```

Combinaison de garde-corps présignés et d'exceptions à d'autres garde-corps

Si vous ne prévoyez pas d'appliquer de garde-fou de manière générale à vos utilisateurs et à vos rôles, vous souhaiterez peut-être l'appliquer aux exceptions des autres barrières de sécurité courantes, afin que ces exceptions ne prennent pas en charge les demandes présignées.

Si vous avez des restrictions réseau mais que vous autorisez des exceptions pour des partenaires externes ou des cas d'utilisation particuliers, vous devez bloquer la chaîne de requête ou `POST` l'authentification lorsque ces exceptions sont appliquées, sauf si elles sont spécifiquement identifiées comme étant obligatoires.

Limitations de S3 : SignatureAge

Les administrateurs trouveront utile de mieux comprendre les implications des`s3:signatureAge`. Chaque demande signée inclut`X-Amz-Date`, qui doit indiquer l'heure actuelle. Cette valeur est renseignée par le client et le signataire de la demande. AWS rejette les demandes dont les heures sont considérées comme non valides. Cependant, un signataire peut générer des signatures à l'avance pour une date future. Amazon S3 rejette les demandes qui spécifient une date future si elles sont envoyées trop longtemps à l'avance. Toutefois, si la demande n'est envoyée qu'au moment de la connexion à la signature, celle-ci peut être générée plus tôt et envoyée ultérieurement.

`s3:signatureAge`limite l'âge maximum d'`X-Amz-Date`une signature uniquement pour les demandes présignées. Les demandes dont l'âge est supérieur à l'âge spécifié sont refusées, même si leur date d'expiration `X-Amz-Expires` ou si une `POST` politique les aurait déclarées valides. `s3:signatureAge`ne modifie pas la période de validité pour les demandes qui n'incluent pas d'expiration explicite. Il ne contrôle pas non plus la valeur de `X-Amz-Date` ce qu'un client utilise pour une signature.

Si l'horloge système est incorrecte ou si un client reporte intentionnellement ses demandes, l'heure de signature peut ne pas correspondre à l'heure à laquelle la signature a été générée. Cela limite la mesure dans laquelle les solutions `s3:signatureAge` peuvent être contrôlées. Une solution qui utilise l'heure actuelle à laquelle elle génère des signatures est limitée comme prévu : les signatures restent valides pendant le nombre de millisecondes spécifié dans. `s3:signatureAge` Une solution qui n'utilise pas l'heure actuelle aura des limites différentes. L'une des restrictions est que les informations d'identification utilisées pour signer la signature doivent toujours être valides. En tant qu'administrateur, vous pouvez contrôler la validité maximale des informations d'identification temporaires émises. Vous pouvez autoriser la validité des informations d'identification jusqu'à 36 heures ou limiter leur validité à 15 minutes. L'expiration des informations d'identification temporaires ne dépend pas de la valeur de`X-Amz-Date`.

Les informations d'identification permanentes ne sont pas soumises à cette restriction. Il est recommandé d'utiliser uniquement des informations d'identification temporaires, et vous pouvez révoquer explicitement toute identification permanente, ce qui invaliderait également toute signature basée sur cette identification.

Bien qu'il `s3:signatureAge` soit mesuré en millisecondes, il n'est pas pratique de le régler à moins de 60 secondes, même si votre horloge est bien synchronisée et que vous utilisez une faible latence. Les paramètres inférieurs à 60 secondes risquent de rejeter des demandes valides. Si vous vous attendez à des retards entre la génération des signatures et l'envoi de la demande, ou

à des problèmes de synchronisation des horloges, vous devez en tenir compte dans votre gestion des`s3:signatureAge`.

Cibler les seaux à grande échelle

SCPs peut être utilisé `aws:PrincipalTag` pour faire des exceptions pour les utilisateurs. Vous ne pouvez pas utiliser de balises sur un bucket pour contrôler l'accès par ce biais `aws:ResourceTag` : seules les balises d'objet sont utilisées pour le contrôle d'accès. Il n'est généralement pas évolutif d'ajouter une balise à chaque objet auquel vous souhaitez appliquer ce contrôle.

Une solution adaptée à de nombreux cas d'utilisation consiste à appliquer la politique et l'exception au niveau du compte, soit en modifiant les comptes auxquels le SCP s'applique, soit en utilisant aws : ResourceAccount, aws : ResourceOrgPaths ou aws : ResourceOrg ID. Par exemple, un SCP peut être appliqué à un ensemble de comptes de production.

Une autre solution consiste à utiliser une AWS Config règle personnalisée pour implémenter un contrôle de détection ou un contrôle réactif. L'objectif serait que chaque compartiment contienne une politique de compartiment avec le garde-corps approprié. En plus de tester le contenu d'une politique de compartiment, la AWS Config règle personnalisée peut récupérer les balises du compartiment et exclure le compartiment de la règle si le compartiment est étiqueté avec une valeur spécifique. Si cette règle échoue à son contrôle de conformité, elle peut soit marquer le compartiment comme non conforme, soit invoquer une correction pour ajouter le garde-fou à la politique du compartiment.

> **Note**
>
> Vous ne pouvez pas restreindre le contenu des balises des demandes à PutBucketTagging. Pour garder le contrôle sur la façon dont un bucket est étiqueté, vous devez limiter l'accès à `PutBucketTagging` et DeleteBucketTagging.

Enregistrement des interactions et mesures d'atténuation

Une URL présignée contient une signature et peut être utilisée, pendant la période précédant son expiration, pour effectuer l'opération d'API spécifique pour laquelle elle a été signée. Il doit être traité comme un identifiant d'accès temporaire. La signature doit rester confidentielle uniquement pour les parties qui ont besoin de la connaître. Dans la plupart des environnements, il s'agit du client qui envoie la demande et du serveur qui la reçoit. L'envoi de la signature dans le cadre d'une session

HTTPS directe conserve son caractère privé, car seul un participant à la session HTTPS a une visibilité sur l'URI qui transmet la signature.

Dans le cas d'une signature présignée URLs, la signature est transmise en tant que paramètre de chaîne de `X-Amz-Signature` requête. Les paramètres de chaîne de requête font partie d'un URI. Le risque est que les clients puissent enregistrer l'URI et la signature avec celui-ci. Les clients ont accès à l'intégralité de la requête HTTP et peuvent enregistrer n'importe quelle partie de la demande, des données et des en-têtes (y compris les en-têtes d'authentification). Cependant, cela est par convention moins courant. La journalisation des URI est plus courante et est requise dans des cas tels que la journalisation des accès. Les clients doivent utiliser la rédaction ou le masquage pour supprimer la signature avant de se connecter. URIs

Dans certains environnements, les utilisateurs autorisent les intermédiaires (proxies) à obtenir de la visibilité sur leurs sessions HTTPS. L'activation des proxys nécessite un niveau élevé d'accès privilégié aux systèmes clients, car ils nécessitent une configuration et des certificats fiables. L'installation de la configuration du proxy et de certificats sécurisés, dans le contexte local de l'environnement intermédiaire du client, permet un niveau de privilège très élevé. C'est pourquoi l'accès à ces intermédiaires doit être étroitement contrôlé.

Le but d'un intermédiaire est généralement de bloquer les sorties indésirables et de suivre les autres sorties. Il est donc courant que ces intermédiaires enregistrent les demandes. Bien que les intermédiaires puissent, comme les clients, enregistrer le contenu, les en-têtes et les données (qui sont tous très sensibles), il est plus courant qu'ils enregistrent URIs, comme ceux qui incluent le paramètre de chaîne de `X-Amz-Signature` requête.

Atténuations

Nous recommandons que la journalisation des URI supprime le paramètre de la chaîne de `X-Amz-Signature` requête, supprime l'intégralité de la chaîne de requête ou traite les informations de manière hautement confidentielle, comme dans le cas d'un accès direct au serveur intermédiaire. Bien que ces protections soient fortement recommandées, le fait que l' URLs expiration soit présignée atténue les risques d'exposition aux logs, à condition que l'exposition soit retardée suffisamment longtemps pour que les signatures expirent.

Amazon S3 voit également les signatures et doit les gérer de manière appropriée. Les journaux d'accès au serveur Amazon S3 incluent l'URI de la demande, mais le biffent`X-Amz-Signature`, comme recommandé. Il en va de même lorsque CloudTrail des événements de données sont

enregistrés pour Amazon S3. Vous pouvez configurer Amazon CloudWatch Logs pour masquer les données à l'aide d'identifiants de données personnalisés.

L'expression régulière suivante correspond à `X-Amz-Signature` celle qui apparaît dans un URI :

```
X-Amz-Signature=[a-f0-9]{64}
```

L'expression régulière suivante ajoute des modèles de regroupement pour identifier plus spécifiquement le texte à remplacer :

```
(?:X-Amz-Signature=)([a-f0-9]{64})
```

Si vous avez une entrée du journal d'accès telle que la suivante :

```
X-Amz-Signature=733255ef022bec3f2a8701cd61d4b371f3f28c9f193a1f02279211d48d5193d7
```

La première expression régulière traduit l'entrée du journal d'accès en :

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

La deuxième expression régulière, sur les systèmes qui prennent en charge les groupes non capturants, traduit l'entrée du journal d'accès en :

```
X-Amz-Signature=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

FAQ

Une demande présignée peut-elle être utilisée plusieurs fois ? Est-ce un risque de sécurité ?

Oui, une signature figurant dans une demande présignée peut être utilisée plusieurs fois. La question de savoir s'il s'agit d'un risque de sécurité est une question contextuelle. D'autres méthodes d'accès aux services AWS autorisent également la répétition. Un utilisateur ou une charge de travail disposant AWS d'informations d'identification peut envoyer de nombreuses demandes Services AWS, et chacune de ces demandes peut être dupliquée.

Si votre cas d'utilisation ne nécessite qu'une seule exécution, vous devez mettre en œuvre d'autres mécanismes pour appliquer l'usage unique. L'usage unique n'est pas une fonctionnalité des demandes présignées. En tant qu'ingénieur en sécurité, vous devez examiner les cas d'utilisation et les implémentations, mais dans de nombreux cas, une utilisation multiple convient à une utilisation acceptable.

Une autre personne que l'utilisateur prévu peut-elle utiliser une demande présignée ?

La signature d'une demande présignée peut être envoyée par toute personne en possession de cette signature. Il ne sera accepté que s'il passe d'autres formes de validation, telles que les contrôles du périmètre des données. Si la signature a expiré, si les informations d'identification ont expiré ou si les informations de signature n'ont pas accès aux ressources demandées, la demande sera refusée.

Il en va de même pour les autres méthodes d'authentification avec Services AWS. Les informations d'identification partagées de manière inappropriée autorisent un accès inapproprié. La meilleure pratique de base consiste à partager les informations d'identification et les signatures uniquement avec le public cible. Si vous ne pouvez pas faire confiance à votre public cible pour protéger les données privées et ne pas les partager avec d'autres, cela compromettra toute forme d'authentification.

Un utilisateur autorisé peut-il utiliser une demande présignée pour exfiltrer des données ?

La sécurisation des données nécessite des mesures énergiques. Permettre l'accès aux fins prévues tout en maintenant un périmètre de données nécessite une approche globale. L'accès au moindre privilège, le contrôle du périmètre des données et l'utilisation d'identifiants d'accès temporaires uniquement sont les meilleures pratiques générales applicables à la sécurisation des données. L'utilisation appropriée de ces contrôles limite également la capacité des utilisateurs à effectuer des actions par le biais des demandes présignées qu'ils génèrent.

Cela est dû au fait que l'accès fourni par une demande présignée est un sous-ensemble de l'accès accordé aux informations d'identification utilisées pour signer la demande. Dans ce contexte, les meilleures pratiques applicables à l'accès aux données s'appliquent généralement aux demandes présignées, mais les demandes présignées ne créent aucun nouvel accès aux données.

- L'expiration maximale est limitée à l'expiration des informations de signature. Si les informations de signature sont révoquées, les signatures basées sur les informations d'identification ne sont plus valides.
- Si les autorisations accordées au principal IAM associées aux informations d'identification de signature n'incluent pas l'exécution de l'action associée à la demande présignée, l'appel d'une demande présignée entraîne une réponse « accès refusé ». La réponse dépend de l'état actuel des autorisations au moment de l'invocation, qui n'a aucun rapport avec le moment où la signature de la demande présignée a été générée.
- Les propriétés du principal sont évaluées en fonction du principal associé aux informations de signature.
- Les propriétés d'une session de rôle sont évaluées en fonction de la session de rôle associée aux informations d'identification de signature.
- Les propriétés du réseau sont évaluées en fonction de la façon dont la demande a été reçue, comme pour les demandes normales.

Dans ce contexte, l'examen des risques associés aux demandes présignées est limité aux domaines dans lesquels elles sont signées avec des informations d'identification différentes de celles de l'utilisateur et fournissent un accès qui ne faisait pas partie du principal de l'utilisateur. Cet examen doit être appliqué à la conception du service, à la charge de travail ou à la solution qui génère des signatures au nom d'un utilisateur, plutôt qu'à la capacité de demande présignée elle-même.

Puis-je refuser l'accès à partir d'une URL présignée si je pense qu'elle a été partagée de manière non autorisée ?

Oui. Cela nécessite d'invalider les informations d'identification avec lesquelles l'URL a été signée. Il existe plusieurs moyens d'y parvenir :

- Supprimez les autorisations du principal IAM auquel appartiennent les informations d'identification. Si ce principal IAM n'a plus accès à la ressource et à l'opération pour lesquelles l'URL est signée, l'URL ne peut pas exécuter cette opération. Cela affecte toutes les utilisations correspondantes provenant de ce principal IAM.
- Si les informations d'identification utilisées pour signer l'URL sont des AWS STS informations d'identification temporaires, vous pouvez révoquer les autorisations de session pour les informations d'identification temporaires émises avant une heure précise pour le principal IAM. Selon le cas d'utilisation, d'autres sessions valides peuvent être invalidées avant leur date d'expiration normale, mais les nouvelles sessions ne seront pas affectées. La révocation des autorisations de session invalide également toutes les URL signées à l'aide des informations d'identification associées à ces sessions, mais les nouvelles URL associées aux nouvelles sessions ne seront pas affectées.
- Si les informations d'identification utilisées pour signer l'URL sont des informations d'identification permanentes, désactivez la clé d'accès. Cela affecte toutes les utilisations liées à ces informations d'identification.

Ressources

Documentation Amazon S3

- Authentification des demandes (AWS Signature version 4)
- Authentification des demandes : utilisation des paramètres de requête (AWS Signature version 4)
- Authentification des demandes : téléchargements depuis un navigateur à l'aide de POST (AWS Signature Version 4)
- Clés de politique spécifiques à l'authentification Amazon S3 Signature version 4
- Utilisation d'URL présignées

Autres références

- Création d'un périmètre de données sur AWS (AWS livre blanc)
- SEC03-BP02 Accorder le moindre privilège d'accès (cadre AWS bien conçu, pilier de sécurité)
- SEC03-BP05 Définissez des barrières d'autorisation pour votre organisation (AWS Well Architected Framework, Security Pilier)

Annexe A : Comment Services AWS utiliser le présigné URLs

Cette annexe fournit des informations Services AWS et des fonctionnalités relatives à l'utilisation de la présignatureURLs. Ces informations ont deux objectifs :

- Fournir aux ingénieurs de sécurité qui mettent en œuvre des contrôles des informations sur les impacts possibles de ces contrôles.
- Sensibiliser aux situations dans lesquelles ce risque peut être pertinent pour la URL journalisation des interactions.

> **Important**
>
> Cette annexe ne fournit pas une liste complète des présignés Services AWS URLs ni leur utilisation. Il ne couvre pas non plus les solutions personnalisées ou tierces.

Console Amazon S3

Principal : utilisateur de la console

Expiration par défaut : 5 minutes

> **Exclusion de responsabilité**
>
> Cette section décrit le comportement actuel de la console Amazon S3. AWS les comportements de la console peuvent être modifiés sans préavis.

La console Amazon S3 prend en charge le téléchargement et le chargement d'objets. Les téléchargements utilisent un présigné URL dont le délai d'expiration est de 300 secondes (5 minutes). Le URL est généré par une demande adressée à`https://<bucket-region>.console.aws.amazon.com/s3/batchOpsServlet-proxy`.

Cette demande est lancée lorsque l'utilisateur clique sur un bouton de téléchargement, de sorte qu'elle URL n'est pas générée à l'avance ou envoyée au client tant que la demande explicite de téléchargement ne se produit pas.

Les téléchargements sont similaires, sauf que la console envoie deux demandes : en `OPTIONS` tant que CORS contrôle avant le vol, et. `PUT` Les deux demandes utilisent la même signature.

Les informations d'identification utilisées pour la signature sont des informations d'identification temporaires associées à l'utilisateur actuellement connecté. Les détails relatifs à la méthode d'obtention de ces informations d'identification temporaires ne sont pas inclus dans ce guide.

Amazon S3 Object Lambda

Principal : appelant du point d'accès

Expiration par défaut : 61 secondes

Amazon S3 Object Lambda utilise des AWS Lambda fonctions pour traiter et transformer automatiquement les données lorsqu'elles sont extraites d'Amazon S3. Lorsque S3 Object Lambda invoque une fonction, celle-ci reçoit un présigné URL (`inputS3Url`) qu'elle peut utiliser pour télécharger l'objet d'origine depuis le point d'accès compatible.

Ils URLs sont présignés pour le point d'accès Amazon S3 compatible, qui est fourni lorsque vous configurez S3 Object Lambda. (Ce n'est pas la même chose que le point d'accès Object Lambda.) Au lieu d'utiliser un rôle lié à la fonction Lambda, celui-ci URL est signé en utilisant l'identité de l'appelant d'origine, et les autorisations de cet utilisateur s'appliqueront lors de l'utilisation duURL. S'il y a des en-têtes signés dans leURL, la fonction Lambda doit inclure ces en-têtes dans l'appel à Amazon S3.

Le présigné renvoyé URL a un délai d'expiration de 61 secondes (une seconde de plus que la durée maximale d'une fonction Lambda d'un objet S3). Le produit ne URL peut être utilisé qu'avec le point d'accès compatible. L'appelant du point d'accès S3 Object Lambda doit avoir accès à ce point d'accès. Vous pouvez limiter cet accès au contexte de S3 Object Lambda en utilisant la condition. `"aws:CalledVia": ["s3-object-lambda.amazonaws.com"]` Lorsque cette condition est attachée à un point d'accès ou à un bucket de support, un utilisateur ne peut pas accéder directement au point d'accès ou au bucket de support.

L'avantage de cette approche est qu'il n'est pas nécessaire d'accorder à la fonction Lambda l'accès à votre compartiment ou point d'accès S3. Le rôle associé à la fonction Lambda aura besoin d'autorisations pour WriteGetObjectResponse, mais pas d'autorisations pour. GetObject

Lorsque S3 Object Lambda génère une version présignéeURLs, il n'ajoute aucune restriction réseau, de sorte que a URL peut être utilisé en dehors de la fonction Lambda. Cependant, toutes les restrictions imposées à l'appelant de S3 Object Lambda s'appliquent toujours. Par exemple, si votre fonction Lambda s'exécute dans un VPC et que vous limitez l'appelant à utiliser un VPC point de terminaison, toute personne en possession du présigné URL devra être en mesure de l'envoyer via ce point de terminaison. VPC Cette restriction s'applique également à SourceIpet VpcSourceIp.

> **Note**
>
> Pour utiliser une fonction Lambda d'un objet S3 dans unVPC, VPC il faut disposer d'une route vers les points de terminaison S3 publics à appeler. WriteGetObjectResponse Cela n'indique pas que les exigences relatives à l'utilisation d'un VPC point de terminaison ne s'appliqueraient pas aux demandes de récupération de données depuis le compartiment.

AWS Lambda Interrégional CopyObject

Principal :AWS interne

Expiration par défaut : 3600 secondes

Lorsque vous utilisez le CopyObjectou UploadPartCopyAPIpour copier Régions AWS, Amazon S3 utilise le présigné URLs en interne. Ils APIs peuvent être appelés directement depuis SDKs ou depuis les AWS CLI commandes `aws s3api copy-object` et`aws s3api upload-part`. Ils APIs ne sont pas utilisés pour la réplication Amazon S3, mais ils sont utilisés par les `aws s3 sync` commandes AWS CLI `aws s3 cp` et lorsque la source et la destination sont des compartiments S3. Ils sont également pris en charge par `TransferManager` des implémentations dans divers AWS SDKs domaines.

AWS Lambda GetFunction

Principal : AWS interne

Expiration par défaut : 10 minutes

AWS Lambda stocke la version utilisateur dans un compartiment S3 appartenant à l'équipe Lambda, avant de générer les actifs déployés sur des conteneurs Lambda. Lorsque vous souhaitez accéder au code de votre fonction, vous appelez le GetFunctionAPI. Cela API répond par `Code.Location`

un message présigné URL valide pendant 10 minutes (ce délai d'expiration correspond au comportement actuel et non à un contrat publié). Si vous ne voulez pas le code, vous pouvez utiliser une combinaison de GetFunctionConfigurationGetFunctionConcurrency, et ListTagspour récupérer les autres données renvoyées par`GetFunction`.

Le document renvoyé URL n'est pas signé avec les informations d'identification de l'utilisateur actuellement connecté, mais au nom de l'utilisateur par Lambda. Pour cette raison, les clés de condition (telles que`aws:SourceIP`) appliquées à l'utilisateur actuellement connecté ou aux informations d'identification de session temporaires de l'utilisateur ne s'appliquent pas aux clés généréesURL. Cela est vrai que les clés de condition soient appliquées GetFunctionuniquement ou qu'elles soient appliquées à toutes les AWS API utilisations de l'utilisateur ou de la session.

La console Lambda utilise également GetFunctionet renvoie le présigné URL qu'elle renvoie. La console utilise les informations d'identification temporaires associées à l'utilisateur actuellement connecté pour appeler GetFunction. Les détails relatifs à l'obtention de ces informations d'identification temporaires ne sont pas couverts par ce document.

Amazon ECR

Principal : AWS interne

Expiration par défaut : 1 heure

Amazon Elastic Container Registry (AmazonECR) fournit le GetDownloadUrlForLayerAPI, qui renvoie un présigné URL valide pendant une heure et prend en charge le téléchargement d'une seule couche à partir d'une ECR image Amazon. Cependant, cette opération est utilisée par le ECR proxy Amazon et n'est généralement pas utilisée par les utilisateurs pour extraire et envoyer des images.

Amazon Redshift Spectrum

Principal : Rôle CREATEEXTERNALSCHEMAtransmis `IAM_ROLE`

Expiration par défaut : 1 heure

Amazon Redshift Spectrum utilise le URLs présigné en interne et interdit les restrictions sur la combinaison du compartiment et du rôle Amazon Redshift qui limiteraient le présigné. URLs Vous pouvez utiliser une `s3:signatureAge` valeur de 16 minutes, mais les valeurs très faibles ne sont pas fiables. La valeur minimale que vous pouvez utiliser dépend du moment et de la taille de votre

requête. Bien qu'une valeur inférieure à 16 minutes fonctionne pour de nombreux scénarios, elle doit être testée. Le rôle peut et doit être limité à l'utilisation exclusive de Redshift Spectrum, qui ne divulgue pas ce URLs qu'il génère, atténuant ainsi la justification typique des valeurs d'expiration inférieures.

Amazon SageMaker AI Studio

Amazon SageMaker AI Studio prend en charge deux API actions : CreatePresignedDomainUrlet CreatePresignedNotebookInstanceUrl. Toutefois, ils APIs ne sont pas liés à la URL fonctionnalité présignée de Signature Version 4. Ils APIs créent un URL qui utilise un `authToken` paramètre, mais ils ne prennent en charge aucun des paramètres de requête standard de Signature Version 4.

`authToken`est un mécanisme différent mais présente des similitudes avec le pré-signéURLs. Il est envoyé sous forme de paramètre de chaîne de requête et prend en charge un délai d'expiration de 5 minutes.

SageMaker L'IA prend en charge les restrictions du réseau. Si vous limitez l'`sagemaker:CreatePresignedDomainUrl`action, celle-ci s'applique à la fois à l'appel CreatePresignedDomainUrlet à l'utilisation du code généréURL. Si a URL est généré à partir d'un réseau valide puis envoyé par un réseau non valide, l'APIappel pour générer le URL succès, mais la demande qui l'URLenvoie échoue. Il en va de CreatePresignedNotebookInstanceUrlmême pour l'`sagemaker:CreatePresignedNotebookInstanceUrl`action.

Pour plus d'informations, consultez la documentation sur l'SageMaker IA.

Annexe B : Incidence des contrôles relatifs aux URL présignées Services AWS

Cette annexe décrit les interactions entre les URL Services AWS qui utilisent des URL présignées, comme décrit dans l'annexe A, et les contrôles décrits plus haut dans ce guide.

Rambarde pour S3 : SignatureAge

La console Amazon S3 n'est pas perturbée par l'expiration maximale de 5 minutes définie par la clé de `s3:signatureAge` condition. La console Amazon S3 génère des URL présignées lorsque vous cliquez sur le bouton Télécharger et applique son propre délai d'expiration de 5 minutes. Une durée maximale inférieure à 2 minutes peut créer des défaillances aléatoires en fonction de la synchronisation de l'horloge et des latences.

Amazon S3 Object Lambda utilise un délai d'expiration de 61 secondes. Par conséquent, le fait de définir des conditions sur une `s3:signatureAge` valeur de 61 secondes ou plus ne provoquera aucune interruption. Des durées plus courtes peuvent être moins fiables et provoquer des pannes intermittentes.

Amazon S3 Cross-region CopyObjectn'est pas perturbé par une expiration maximale de 5 minutes. Cependant, des durées plus courtes peuvent créer des défaillances aléatoires en fonction de la synchronisation des horloges et des latences.

In AWS Lambda, GetFunctionfournit une URL vers des objets extérieurs au compte client, de sorte que les politiques du client n'affectent pas les URL générées.

Amazon Redshift Spectrum a été testé avec `s3:signatureAge` une condition de 16 minutes. Cependant, des durées plus courtes peuvent entraîner des perturbations.

Garde-corps pour S3:AuthType lorsque les restrictions du réseau ne sont pas utilisées

La console Amazon S3 est généralement affectée par le `s3:authType` garde-corps. La console est acheminée vers Amazon S3 en fonction de la configuration du réseau local. Si le réseau local est acheminé vers Amazon S3 conformément aux restrictions du réseau, la console Amazon S3

fonctionnera toujours. Toutefois, s'il est acheminé via un proxy ou via Internet public d'une manière non autorisée, son utilisation sera bloquée. Cependant, le blocage de l'utilisation est probablement l'objectif de cette politique.

Amazon S3 Object Lambda est affecté si la fonction Lambda n'est pas connectée à un VPC approprié. Dans cette configuration, le VPC doit disposer d'une passerelle NAT, non pas pour accéder au compartiment S3, mais pour appeler. WriteGetObjectResponse

Amazon S3 Interregion CopyObjectest perturbé si ce garde-fou est appliqué à une politique de compartiment sans l'exception recommandée concernant le moment où elle **`aws:viaAWSService`** est vraie.

Amazon Redshift Spectrum est affecté par `s3:authType` le garde-corps sauf si un routage VPC amélioré est utilisé. À l'heure actuelle, Redshift Spectrum prend en charge le routage VPC amélioré uniquement avec les clusters sans serveur, et non avec les clusters provisionnés.

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
Publication initiale	—	23 juillet 2024

AWS Glossaire des directives prescriptives

Les termes suivants sont couramment utilisés dans les stratégies, les guides et les modèles fournis par les directives AWS prescriptives. 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 l'édition compatible avec Amazon Aurora 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) pour Oracle dans le. AWS Cloud
- 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 locale vers Oracle sur une EC2 instance du AWS Cloud.
- 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. Vous migrez des serveurs d'une plateforme sur site vers un service cloud pour la même plateforme. Exemple : migrer une Microsoft Hyper-V application vers 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 son AIOps utilisation dans la stratégie de AWS migration, consultez 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, consultez ABAC pour 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

Un emplacement distinct au sein d'un Région AWS réseau isolé des défaillances dans d'autres zones de disponibilité et fournissant une connectivité réseau peu coûteuse et à faible latence aux autres zones de disponibilité de la même région.

AWS Cadre d'adoption du cloud (AWS CAF)

Un cadre de directives et de meilleures pratiques visant AWS à aider les entreprises à élaborer un plan efficace pour réussir leur migration vers le cloud. AWS La CAF organise ses conseils en six domaines prioritaires appelés perspectives : les affaires, les personnes, la gouvernance, les plateformes, 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, la 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 Cadre de qualification de la charge de travail (AWS WQF)

Outil qui évalue les charges de travail liées à la migration des bases de données, recommande des stratégies de migration et fournit des estimations de travail. AWS Le 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

mauvais bot

Un bot destiné à perturber ou à nuire à des individus ou à des organisations.

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.

déploiement bleu/vert

Stratégie de déploiement dans laquelle vous créez deux environnements distincts mais identiques. Vous exécutez la version actuelle de l'application dans un environnement (bleu) et la nouvelle version de l'application dans l'autre environnement (vert). Cette stratégie vous permet de revenir rapidement en arrière avec un impact minimal.

bot

Application logicielle qui exécute des tâches automatisées sur Internet et simule l'activité ou l'interaction humaine. Certains robots sont utiles ou bénéfiques, comme les robots d'exploration Web qui indexent des informations sur Internet. D'autres robots, appelés « bots malveillants », sont destinés à perturber ou à nuire à des individus ou à des organisations.

botnet

Réseaux de robots infectés par des logiciels malveillants et contrôlés par une seule entité, connue sous le nom d'herder ou d'opérateur de bots. Les botnets sont le mécanisme le plus connu pour faire évoluer les bots et leur impact.

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-Architected AWS .

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.

déploiement de Canary

Diffusion lente et progressive d'une version pour les utilisateurs finaux. Lorsque vous êtes sûr, vous déployez la nouvelle version et remplacez la version actuelle dans son intégralité.

CCo E

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 localement, avant que la cible ne les Service AWS reçoive.

Centre d'excellence du 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, consultez les CCoarticles électroniques du blog sur la stratégie AWS Cloud d'entreprise.

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 entreprises traversent généralement lorsqu'elles migrent vers AWS Cloud :

- Projet : exécution de quelques projets liés au cloud à des fins de preuve de concept et d'apprentissage
- Base : réaliser des investissements fondamentaux pour accélérer votre adoption du cloud (par exemple, créer une zone de landing zone, définir un CCo E, établir 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 publié sur le blog AWS Cloud Enterprise Strategy. Pour plus d'informations sur leur lien avec la stratégie de AWS migration, consultez le guide de préparation à la migration.

CMDB

Voir base de données de gestion de configuration.

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 ouBitbucket Cloud. 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 (CV)

Domaine de l'IA qui utilise l'apprentissage automatique pour analyser et extraire des informations à partir de formats visuels tels que des images numériques et des vidéos. Par exemple, Amazon SageMaker AI fournit des algorithmes de traitement d'image pour les CV.

dérive de configuration

Pour une charge de travail, une modification de configuration par rapport à l'état attendu. Cela peut entraîner une non-conformité de la charge de travail, et cela est généralement progressif et involontaire.

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

Ensemble de AWS Config règles et d'actions correctives que vous pouvez assembler pour personnaliser vos contrôles de conformité et de sécurité. Vous pouvez déployer un pack de conformité en tant qu'entité unique dans une région Compte AWS et, ou au sein d'une organisation, à l'aide d'un modèle YAML. Pour plus d'informations, consultez la section Packs de conformité dans la AWS Config documentation.

intégration continue et livraison continue (CI/CD)

Processus d'automatisation des étapes de source, de construction, de test, de préparation et de production du processus de publication du logiciel. CI/CD is commonly described as a pipeline. CI/CDpeut 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.

CV

Voir vision par ordinateur.

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 AWS Well-Architected Framework. 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.

maillage de données

Un cadre architectural qui fournit une propriété des données distribuée et décentralisée avec une gestion et une gouvernance centralisées.

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 des 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 AWS, vous ajoutez plusieurs contrôles à différentes couches de

la AWS Organizations structure afin de sécuriser 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 AWS membre 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.

EDI

Voir échange de données informatisé.

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.

échange de données informatisé (EDI)

L'échange automatique de documents commerciaux entre les organisations. Pour plus d'informations, voir Qu'est-ce que l'échange de données informatisé ?

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 à AWS Identity and Access Management (IAM) principaux. 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).

planification des ressources d'entreprise (ERP)

Système qui automatise et gère les principaux processus métier (tels que la comptabilité, le MES et la gestion de projet) pour une entreprise.

chiffrement d'enveloppe

Processus de chiffrement d'une clé de chiffrement à l'aide d'une autre clé de chiffrement. Pour plus d'informations, consultez la section Chiffrement des enveloppes 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 points forts de la AWS CAF en matière de sécurité incluent la gestion des identités et des accès, les contrôles de détection, la sécurité des infrastructures, 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.

ERP

Voir Planification des ressources d'entreprise.

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 le AWS Cloud, une limite telle qu'une zone de disponibilité Région 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.

invitation en quelques coups

Fournir à un LLM un petit nombre d'exemples illustrant la tâche et le résultat souhaité avant de lui demander d'effectuer une tâche similaire. Cette technique est une application de l'apprentissage contextuel, dans le cadre de laquelle les modèles apprennent à partir d'exemples (prises de vue) intégrés dans des instructions. Les instructions en quelques étapes peuvent être efficaces pour les tâches qui nécessitent un formatage, un raisonnement ou des connaissances de domaine spécifiques. Voir également l'invite Zero-Shot.

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.

FM

Voir le modèle de fondation.

modèle de fondation (FM)

Un vaste réseau neuronal d'apprentissage profond qui s'est entraîné sur d'énormes ensembles de données généralisées et non étiquetées. FMs sont capables d'effectuer une grande variété de tâches générales, telles que comprendre le langage, générer du texte et des images et converser en langage naturel. Pour plus d'informations, voir Que sont les modèles de base ?

G

IA générative

Sous-ensemble de modèles d'IA qui ont été entraînés sur de grandes quantités de données et qui peuvent utiliser une simple invite textuelle pour créer de nouveaux contenus et artefacts, tels que des images, des vidéos, du texte et du son. Pour plus d'informations, consultez Qu'est-ce que l'IA générative.

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.

image dorée

Un instantané d'un système ou d'un logiciel utilisé comme modèle pour déployer de nouvelles instances de ce système ou logiciel. Par exemple, dans le secteur de la fabrication, une image dorée peut être utilisée pour fournir des logiciels sur plusieurs appareils et contribue à améliorer la vitesse, l'évolutivité et la productivité des opérations de fabrication des appareils.

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 organisationnelles (OUs). 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 GuardDuty AWS 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.

données de rétention

Partie de données historiques étiquetées qui n'est pas divulguée dans un ensemble de données utilisé pour entraîner un modèle d'apprentissage automatique. Vous pouvez utiliser les données de blocage pour évaluer les performances du modèle en comparant les prévisions du modèle aux données de blocage.

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' AWS Cloud environnement.

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.

IIo T

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 AWS multi-comptes, un VPC qui accepte, inspecte et achemine les connexions réseau depuis l'extérieur d'une application. L'architecture AWS de référence de sécurité recommande de configurer votre compte réseau avec les fonctions entrantes, sortantes

et d'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et l'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.

Industry 4.0

Terme introduit par Klaus Schwab en 2016 pour désigner la modernisation des processus de fabrication grâce aux avancées en matière de connectivité, de données en temps réel, d'automatisation, d'analyse et d'IA/ML.

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, voir Élaboration d'une stratégie de transformation numérique de l'Internet des objets (IIoT) industriel.

VPC d'inspection

Dans une architecture AWS multi-comptes, un VPC centralisé qui gère les inspections du trafic réseau VPCs entre (identique ou Régions AWS différent), Internet et les réseaux locaux. L'architecture AWS de référence de sécurité recommande de configurer votre compte réseau

avec les fonctions entrantes, sortantes et d'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et l'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, voir Interprétabilité du modèle d'apprentissage automatique avec 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 d'atterrissage est un AWS environnement multi-comptes bien conçu, 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.

grand modèle de langage (LLM)

Un modèle d'intelligence artificielle basé sur le deep learning qui est préentraîné sur une grande quantité de données. Un LLM peut effectuer plusieurs tâches, telles que répondre à des questions, résumer des documents, traduire du texte dans d'autres langues et compléter des phrases. Pour plus d'informations, voir Que sont LLMs.

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.

LLM

Voir le grand modèle de langage.

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.

malware

Logiciel conçu pour compromettre la sécurité ou la confidentialité de l'ordinateur. Les logiciels malveillants peuvent perturber les systèmes informatiques, divulguer des informations sensibles ou obtenir un accès non autorisé. Parmi les malwares, on peut citer les virus, les vers, les rançongiciels, les chevaux de Troie, les logiciels espions et les enregistreurs de frappe.

services gérés

Services AWS pour 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.

système d'exécution de la fabrication (MES)

Un système logiciel pour le suivi, la surveillance, la documentation et le contrôle des processus de production qui convertissent les matières premières en produits finis dans l'atelier.

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, à l' Comptes AWS exception du 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.

MAILLES

Voir le système d'exécution de la fabrication.

Transport télémétrique en file d'attente de messages (MQTT)

Protocole de communication léger machine-to-machine (M2M), basé sur le modèle de publication/d'abonnement, pour les appareils IoT aux ressources limitées.

microservice

Un petit service indépendant qui communique via un réseau bien défini APIs 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, consultez la section Intégration de microservices à l'aide de services AWS sans serveur.

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 en utilisant Lightweight. APIs 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, consultez la section Implémentation de microservices sur AWS.

Programme d'accélération des migrations (MAP)

Un AWS programme qui fournit un support de conseil, des formations et des services pour aider les entreprises à établir 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 des responsables des opérations, des analystes commerciaux et des propriétaires, des ingénieurs de migration, des développeurs et DevOps des 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 AWS compte.

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 : réorganisez la migration vers Amazon EC2 avec le service de migration AWS d'applications.

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. AWS Cloud 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 disponible gratuitement pour tous les AWS consultants et consultants APN Partner.

Évaluation de la préparation à la migration (MRA)

Processus qui consiste à obtenir des informations sur l'état de préparation d'une organisation au cloud, à identifier les forces et les faiblesses et à élaborer un plan d'action pour combler les lacunes identifiées, à l'aide du 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

L'approche utilisée pour migrer une charge de travail vers le AWS Cloud. 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.

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, consultez la section Stratégie de modernisation des applications dans le 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, consultez la section Évaluation de l'état de préparation à la modernisation des applications dans le 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.

MPA

Voir Évaluation du portefeuille de migration.

MQTT

Voir Message Queuing Telemetry Transport.

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.

OPC-UA

Voir Open Process Communications - Architecture unifiée.

Communications par processus ouvert - Architecture unifiée (OPC-UA)

Un protocole de communication machine-to-machine (M2M) pour l'automatisation industrielle. L'OPC-UA fournit une norme d'interopérabilité avec des schémas de cryptage, d'authentification et d'autorisation des données.

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, évaluer, prévenir ou réduire l'ampleur des incidents et des défaillances possibles. Pour plus d'informations, voir Operational Readiness Reviews (ORR) dans le AWS Well-Architected Framework.

technologie opérationnelle (OT)

Systèmes matériels et logiciels qui fonctionnent avec l'environnement physique pour contrôler les opérations, les équipements et les infrastructures industriels. Dans le secteur manufacturier, l'intégration des systèmes OT et des technologies de l'information (IT) est au cœur des transformations de l'industrie 4.0.

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

Un parcours créé par AWS CloudTrail qui enregistre tous les événements pour tous les membres Comptes AWS d'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 AWS migration, ce cadre est appelé accélération du personnel, 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). L'OAC prend en charge tous les compartiments S3 dans leur ensemble Régions AWS, le chiffrement côté serveur avec AWS KMS (SSE-KMS) et les requêtes dynamiques `PUT` adressées au compartiment S3. `DELETE`

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.

ORR

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

DE

Voir technologie opérationnelle.

VPC sortant (de sortie)

Dans une architecture AWS multi-comptes, un VPC qui gère les connexions réseau initiées depuis une application. L'architecture AWS de référence de sécurité recommande de configurer votre compte réseau avec les fonctions entrantes, sortantes et d'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et l'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.

PLC

Voir contrôleur logique programmable.

PLM

Consultez la section Gestion du cycle de vie des produits.

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

Entité capable d'effectuer AWS des actions et d'accéder à des ressources. Cette entité est généralement un utilisateur root pour un Compte AWS 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 d'ingénierie système qui prend en compte la confidentialité tout au long du processus de développement.

zones hébergées privées

Conteneur contenant des informations sur la manière dont vous souhaitez qu'Amazon Route 53 réponde aux requêtes DNS pour un domaine et ses sous-domaines au sein d'un ou de plusieurs

VPCs domaines. 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.

gestion du cycle de vie des produits (PLM)

Gestion des données et des processus d'un produit tout au long de son cycle de vie, depuis la conception, le développement et le lancement, en passant par la croissance et la maturité, jusqu'au déclin et au retrait.

environnement de production

Voir environnement.

contrôleur logique programmable (PLC)

Dans le secteur manufacturier, un ordinateur hautement fiable et adaptable qui surveille les machines et automatise les processus de fabrication.

chaînage rapide

Utiliser le résultat d'une invite LLM comme entrée pour l'invite suivante afin de générer de meilleures réponses. Cette technique est utilisée pour décomposer une tâche complexe en sous-tâches ou pour affiner ou développer de manière itérative une réponse préliminaire. Cela permet d'améliorer la précision et la pertinence des réponses d'un modèle et permet d'obtenir des résultats plus précis et personnalisés.

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.

publish/subscribe (pub/sub)

Modèle qui permet des communications asynchrones entre les microservices afin d'améliorer l'évolutivité et la réactivité. Par exemple, dans un MES basé sur des microservices, un microservice peut publier des messages d'événements sur un canal auquel d'autres microservices

peuvent s'abonner. Le système peut ajouter de nouveaux microservices sans modifier le service de publication.

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).

CHIFFON

Voir Retrieval Augmented Generation.

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. Il détermine ce qui est considéré comme étant une perte de données acceptable entre le dernier point de reprise 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

Un ensemble de AWS ressources dans une zone géographique. Chacun Région AWS est isolé et indépendant des autres pour garantir tolérance aux pannes, stabilité et résilience. Pour plus d'informations, voir Spécifier ce que Régions AWS votre compte peut utiliser.

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.

résilience

La capacité d'une application à résister aux perturbations ou à s'en remettre. La haute disponibilité et la reprise après sinistre sont des considérations courantes lors de la planification de la résilience dans le AWS Cloud. Pour plus d'informations, consultez la section AWS Cloud Résilience.

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.

Génération augmentée de récupération (RAG)

Technologie d'IA générative dans laquelle un LLM fait référence à une source de données faisant autorité qui se trouve en dehors de ses sources de données de formation avant de générer une

réponse. Par exemple, un modèle RAG peut effectuer une recherche sémantique dans la base de connaissances ou dans les données personnalisées d'une organisation. Pour plus d'informations, voir Qu'est-ce que RAG ?

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 permet l'authentification unique fédérée (SSO), afin que les utilisateurs puissent se connecter AWS Management Console ou appeler les opérations de l' AWS API sans que vous ayez à créer un utilisateur dans IAM pour tous les membres de votre 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.

SCADA

Voir Contrôle de supervision et acquisition de données.

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, voir Que contient le secret d'un Secrets Manager ? dans la documentation de Secrets Manager.

sécurité dès la conception

Une approche d'ingénierie système qui prend en compte la sécurité tout au long du processus de développement.

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 EC2 instance Amazon ou la rotation des informations d'identification.

chiffrement côté serveur

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

Politique de contrôle des services (SCP)

Politique qui fournit un contrôle centralisé des autorisations pour tous les comptes d'une organisation dans AWS Organizations. SCPs définissez des garde-fous ou des limites aux actions qu'un administrateur peut déléguer à des utilisateurs ou à des rôles. Vous pouvez les utiliser SCPs comme listes d'autorisation ou de refus pour spécifier les services ou les actions autorisés ou interdits. Pour plus d'informations, consultez la section Politiques de contrôle des services dans la AWS Organizations documentation.

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

Un modèle décrivant la responsabilité que vous partagez en matière AWS de sécurité et de conformité dans le cloud. AWS est responsable de la sécurité du cloud, alors 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.

contrôle de supervision et acquisition de données (SCADA)

Dans le secteur manufacturier, un système qui utilise du matériel et des logiciels pour surveiller les actifs physiques et les opérations de production.

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.

invite du système

Technique permettant de fournir un contexte, des instructions ou des directives à un LLM afin d'orienter son comportement. Les instructions du système aident à définir le contexte et à établir des règles pour les interactions avec les utilisateurs.

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

Un hub de transit réseau que vous pouvez utiliser pour interconnecter vos réseaux VPCs et ceux sur site. Pour plus d'informations, voir Qu'est-ce qu'une passerelle de transit dans la AWS Transit Gateway documentation.

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

Accorder des autorisations à un service que vous spécifiez pour effectuer des tâches au sein de votre organisation 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, consultez la section Utilisation AWS Organizations avec d'autres AWS services dans la AWS Organizations documentation.

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

Une connexion entre deux VPCs qui vous permet d'acheminer le trafic en utilisant des 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

Voir le cadre AWS de qualification de la charge de travail.

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.

invite Zero-Shot

Fournir à un LLM des instructions pour effectuer une tâche, mais aucun exemple (plans) pouvant aider à la guider. Le LLM doit utiliser ses connaissances pré-entraînées pour gérer la tâche. L'efficacité de l'invite zéro dépend de la complexité de la tâche et de la qualité de l'invite. Voir également les instructions en quelques clics.

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.