www.eazytraining.fr

Services de sécurité & gestion de compte

Par Lahda Biassou Alphonsine

Lahda Biassou Alphonsine

Ingénieure cloud et formatrice a EAZYTraining

Plan

- **AWS KMS**
- **Secret Manager**
- **SSM Parameter Store**
- **CloudHSM**
- **AWS ACM**
- **Security Hub**
- **AWS Firewall Manager**
- **AWS WAF**
- **Amazon Detective**
- **AWS Inspector**

AWS Key Management Service (KMS)

- Chaque fois que vous entendez parler de "cryptage" pour un service AWS, il s'agit très probablement de KMS.
- Moyen simple de contrôler l'accès à vos données, AWS gère les clés pour nous.
- Entièrement intégré à IAM pour les autorisations
- Intégré de manière transparente dans :
  - Amazon EBS : chiffrement des volumes
  - Amazon S3 : chiffrement des objets côté serveur
  - Amazon Redshift : chiffrement des données
  - Amazon RDS : chiffrement des données- Amazon SSM : magasin de paramètres - Etc...
- Mais vous pouvez également utiliser le CLI / SDK

AWS Key Management Service (KMS)

- **Symétrique (clés AES-256)**
  - Première offre de KMS, clé de chiffrement unique utilisée pour le chiffrement et le déchiffrement.
  - Les services AWS intégrés à KMS utilisent les clés symétriques de KMS.
  - Nécessaires pour le chiffrement de l'enveloppe
  - Vous n'avez jamais accès à la clé KMS non chiffrée (vous devez appeler l'API KMS pour l'utiliser).

- **Asymétriques (paires de clés RSA et Elliptic Curve Cryptography (ECC))**
  - Paire de clés publique (chiffrement) et privée (déchiffrement)
  -Utilisée pour les opérations de cryptage/décryptage ou de signature/vérification.
  - La clé publique peut être téléchargée, mais vous ne pouvez pas accéder à la clé privée en clair.
  - Cas d'utilisation : chiffrement en dehors d'AWS par des utilisateurs qui ne peuvent pas appeler l'API KMS

AWS Key Management Service (KMS)

- **Clés gérées par le client ou Customer Managed Key (CMK)**
  - Création, gestion et utilisation, possibilité d'activation ou de désactivation
  - Possibilité de politique de rotation (nouvelle clé générée chaque année, ancienne clé conservée)
  - Possibilité d'ajouter une politique de clés (politique de ressources) et d'auditer dans CloudTrail
  - Utilisation pour le cryptage des enveloppes
- **Clés gérées par AWS**
  - Utilisées par un service AWS (aws/s3, aws/ebs, aws/redshift)
  - Gérées par AWS (rotation automatique tous les 1 an)
  - Voir la politique des clés et l'audit dans CloudTrail
- **Clés appartenant à AWS**
  - Créées et gérées par AWS, utilisées par certains services AWS pour protéger vos ressources.
  - Utilisées dans plusieurs comptes AWS, mais pas dans votre compte AWS
  - Vous ne pouvez pas les visualiser, les utiliser, les suivre ou les auditer.

AWS Key Management Service (KMS)

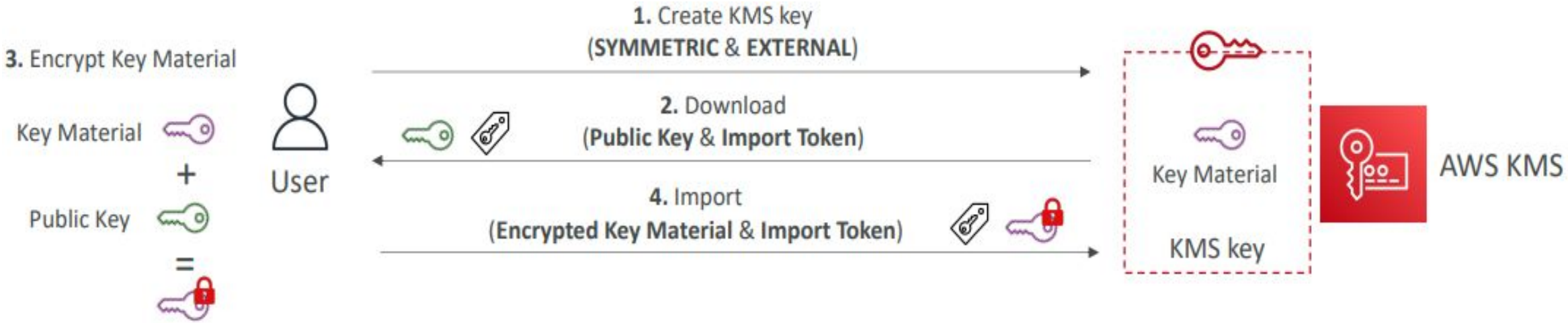
KMS Key	Customer Managed Key	AWS Managed Key	AWS Owned Key
Can view metadata?	✓	✓	✗
Can manage?	✓	✗	✗
Used only for my AWS account?	✓	✓	✗
Automatic Rotation	Optional (every 1 year)	Required (every 1 year)	Varies

AWS KMS Key Materials Origin

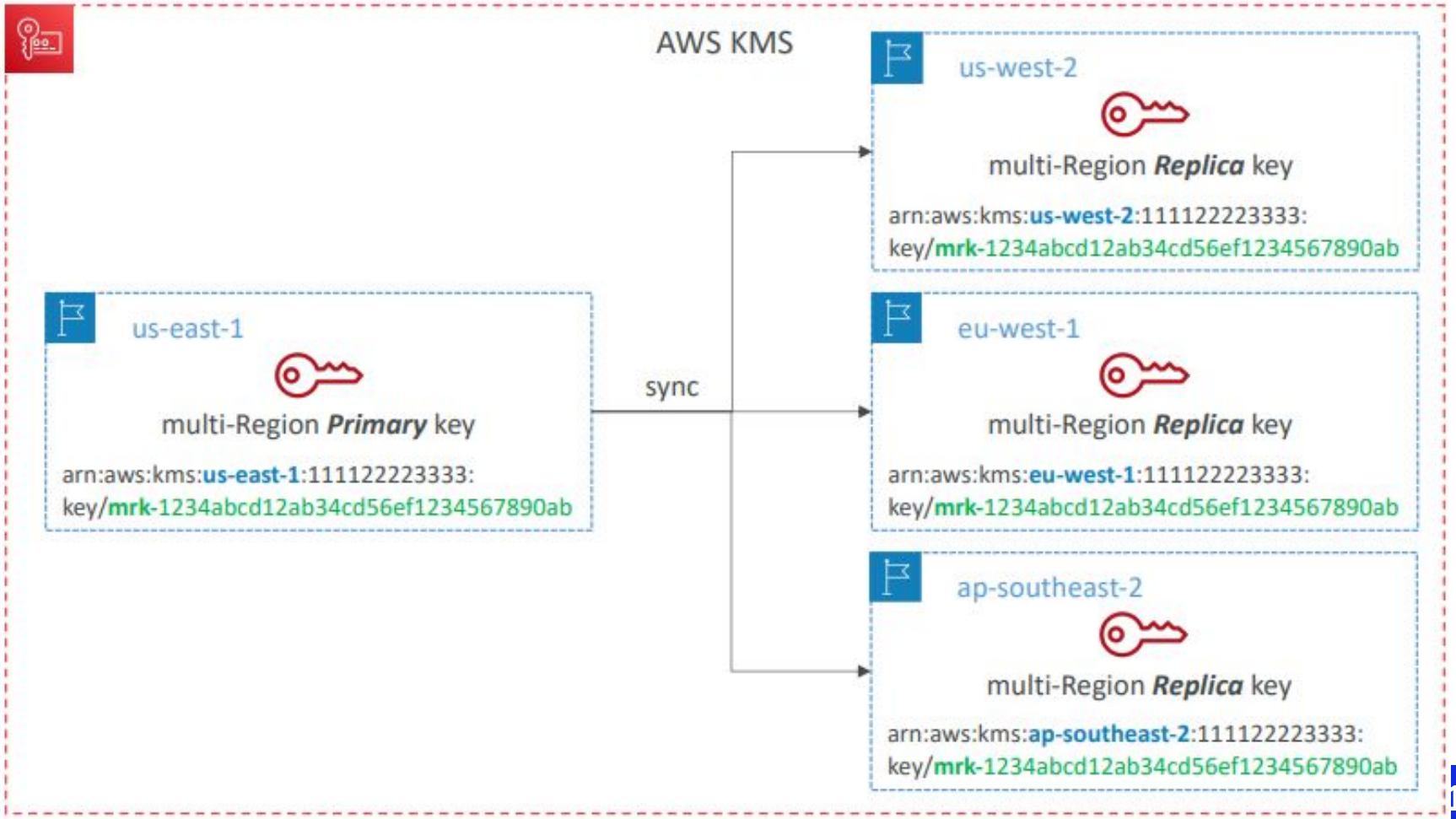
- Identifier les sources de matériels clés dans KMS Key
- Ne peut pas être changer après la création
- **KMS (AWS_KMS) –** default
  - AWS KMS crée et gère le matériel clé dans son propre stockage de clé
- **External (EXTERNAL)**
  - Vous importez le matériel clé dans KMS Key
  - Vous êtes responsable pour la sécuité et la gestion de ces matériels clé hors du compte AWS
- **Custom Key Store (AWS_CLOUDHSM)**
  - AWS KMS crée une clé matériel dans customm key store (CloudHSM Cluster)

KMS Key Source- externe

- Importer votre matériel clé dans KMS Key, Bring Your Own Key (BYOK)
- Vous êtes responsable pour la sécurité du material's Key, la disponibilité hors de AWS
- Doit être 256-bit **Symmetric** key (Asymmetrc is NOT supported)
- Ne peut pas être utilisé avec Custom Key store (CloudHSM)
- Rotation manuelle de votre KMS Key (Automatic Key Rotation n'est pas supporté)



KMS Multi-Region : Examen



KMS -Region key

- Un ensemble de clés KMS identiques dans différentes régions AWS qui peuvent être utilisées de manière interchangeable (~ même clé KMS dans plusieurs régions). interchangeables (~ même clé KMS dans plusieurs régions).
- Cryptage dans une région et décryptage dans d'autres régions (pas besoin de recryptage ou d'appels API interrégionaux) ou d'effectuer des appels API interrégionaux)
- Les clés multi régions ont le même ID de clé, le même matériau de clé, la même rotation automatique, ...
- Les KMS Multi-Régions ne sont PAS globaux (Primaire + Répliques)
- Chaque clé Multi-Région est gérée indépendamment
- Il n'y a qu'une seule clé primaire à la fois, mais les répliques peuvent devenir leur propre clé primaire.
- **Cas d'utilisation :** Reprise après sinistre, gestion globale des données (par exemple, DynamoDB Tables globales), applications actives qui couvrent plusieurs régions, Applications de signature distribuée,…)

Plan

- AWS KMS
- **Secret Manager**
- **SSM Parameter Store**
- **CloudHSM**
- **AWS ACM**
- **Security Hub**
- **AWS Firewall Manager**
- **AWS WAF**
- **Amazon Detective**
- **AWS Inspector**

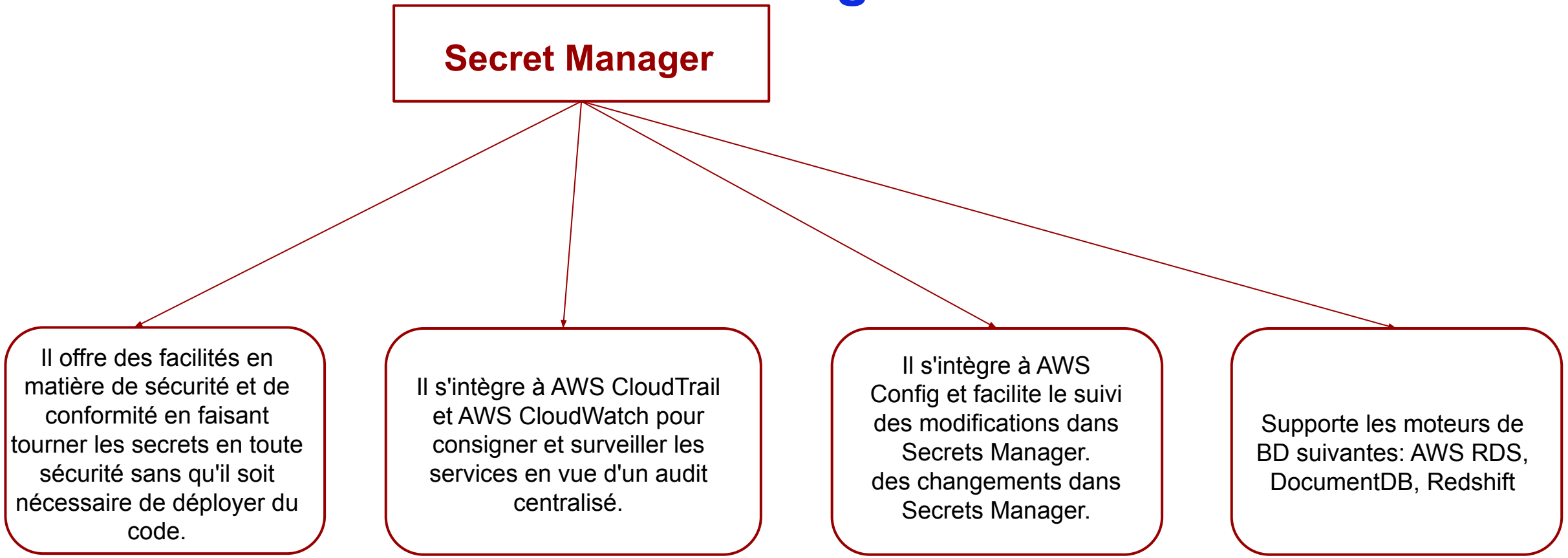
Secret Manager

Secret Manager

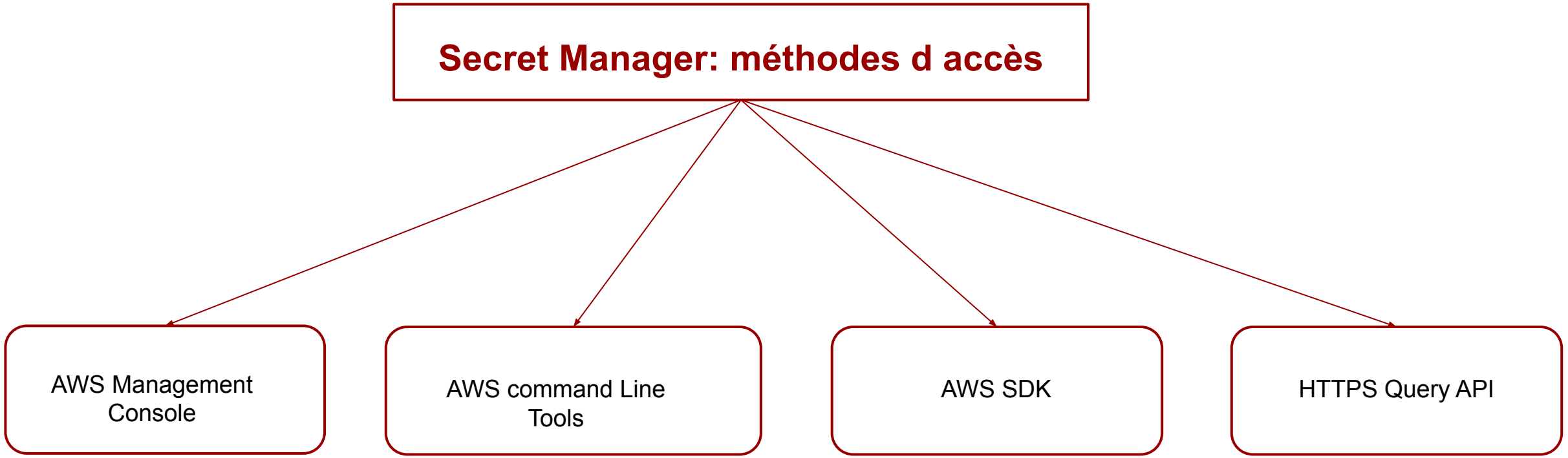
AWS Secrets Manager est un service qui empêche que les d'être codées en dur dans le code source.

- Assure le cryptage en transit du secret entre AWS et le système de récupération du secret. AWS.
- Rotation des informations d'identification pour les services AWS à l'aide de la fonction Lambda qui demande à Secrets Manager d'interagir avec le service ou la base de données.
- Enregistre la valeur secrète cryptée dans le champ SecretString ou SecretBinary.
- Utilise des composants clients open-source pour mettre en cache les secrets et les met à jour lorsqu'une rotation est nécessaire.

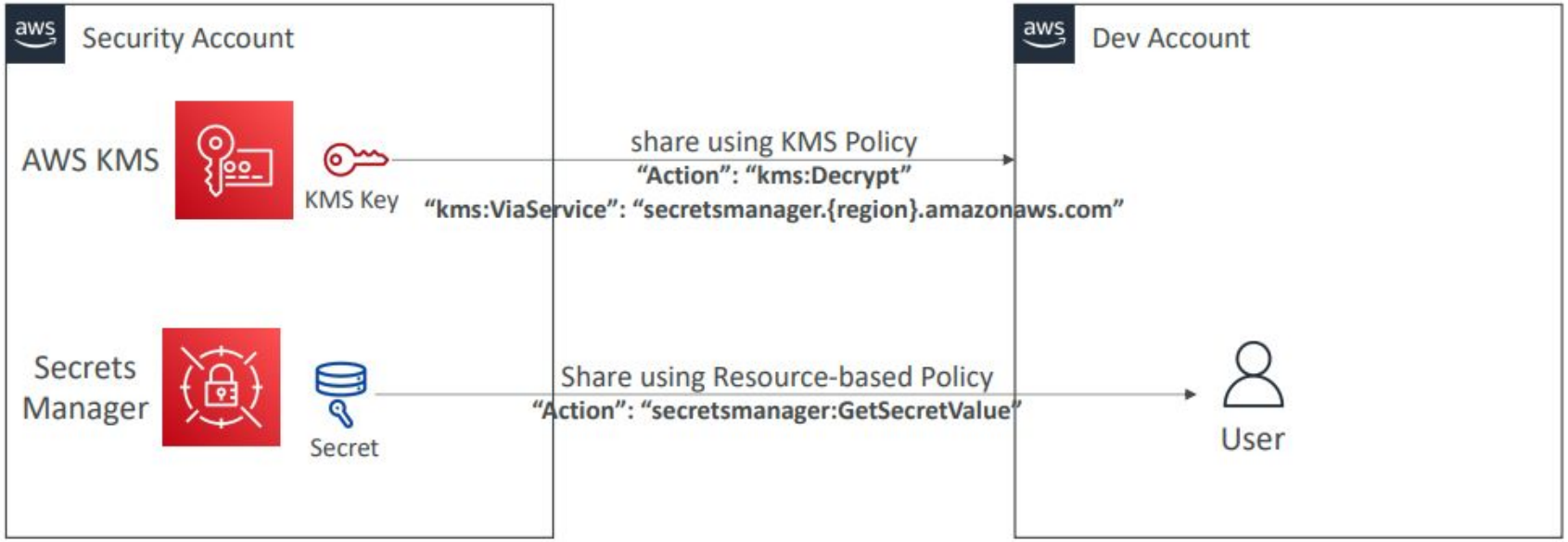
Secret Manager



AWS Secret Manager



AWS Secret Manager -partage entre les comptes

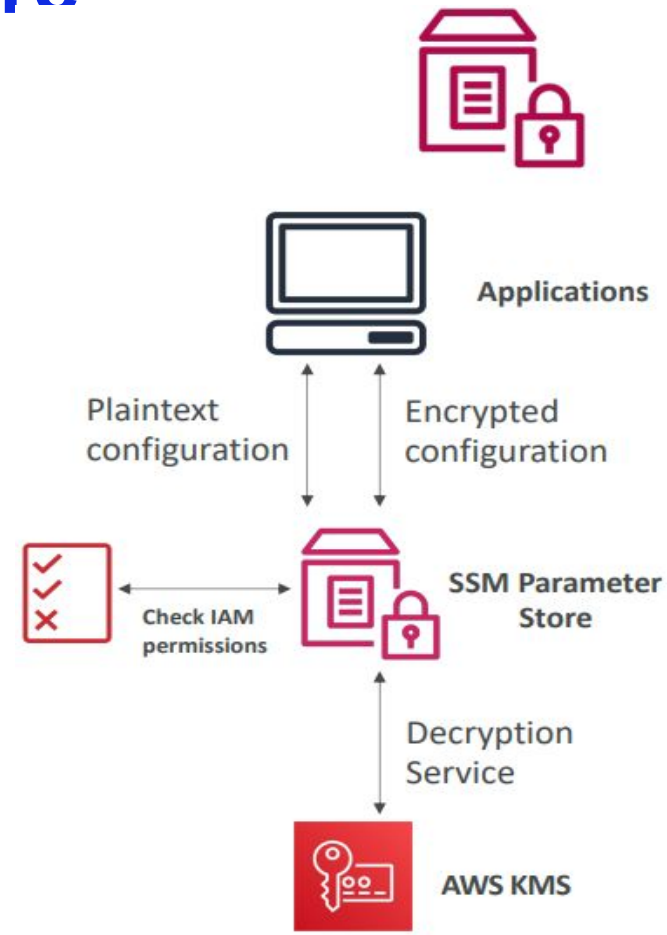


Plan

- AWS KMS
- Secret Manager
- SSM Parameter Store
- CloudHSM
- AWS ACM
- Security Hub
- AWS Firewall Manager
- AWS WAF
- Amazon Detective
- AWS Inspector

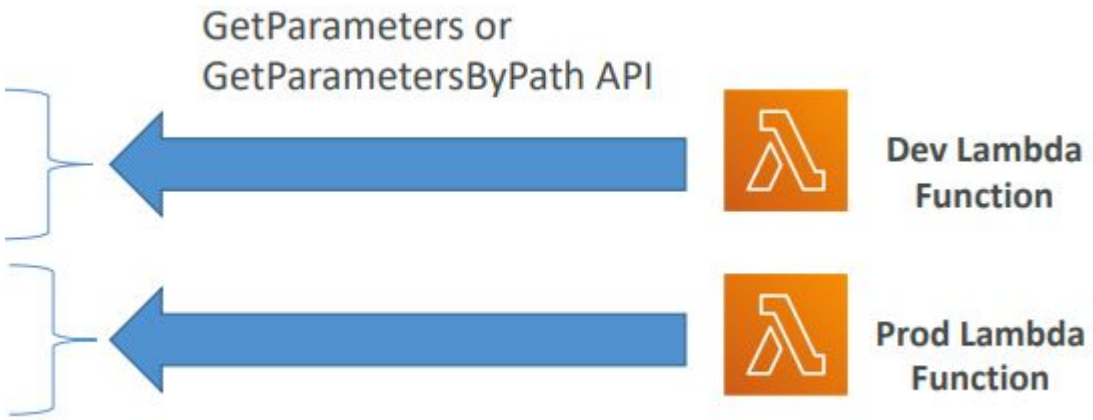
SSM Parameter Store

- Stockage sécurisé de la configuration et des secrets- Cryptage transparent en option à l'aide de KMS
- SDK sans serveur, évolutif, durable et facile à utiliser
- Suivi des versions des configurations / secrets
- Sécurité par IAM
- Notifications avec Amazon EventBridge Intégration avec CloudFormation



SSM Parameter Store -hiérarchie

- /mon-département/
  - mon-app/
    - dev/
      - db-url
      - db-password
    - prod/
      - db-url
      - db-password
  - other-app/



- /autre-département/
- /aws/reference/secretsmanager/secret_ID_in_Secrets_Manager
- /aws/service/ami-amazon-linux-latest/amaz2-ami-hvm-x86_64-gp2 (public)

SSM Parameter Store - Standard and Advanced tiers

	Standard	Advanced
Total number of parameters allowed (per AWS account and Region)	10,000	100,000
Maximum size of a parameter value	4 KB	8 KB
Parameter policies available	No	Yes
Cost	No additional charge	Charges apply
Storage Pricing	Free	$0.05 per advanced parameter per month

SSM Parameter Store - parameter policies

- Permet d'assigner un TTL à un paramètre (date d'expiration) pour forcer la mise à jour ou la suppression de données sensibles telles que les mots de passe.
- Possibilité d'assigner plusieurs politiques à la fois

Expiration (to delete a parameter)

```
{
    "Type":"Expiration",
    "Version":"1.0",
    "Attributes":{
        "Timestamp":"2020-12-02T21:34:33.000Z"
    }
}
```

ExpirationNotification (EventBridge)

```
{
    "Type":"ExpirationNotification",
    "Version":"1.0",
    "Attributes":{
        "Before":"15",
        "Unit":"Days"
    }
}
```

NoChangeNotification (EventBridge)

```
{
    "Type":"NoChangeNotification",
    "Version":"1.0",
    "Attributes":{
        "After":"20",
        "Unit":"Days"
    }
}
```

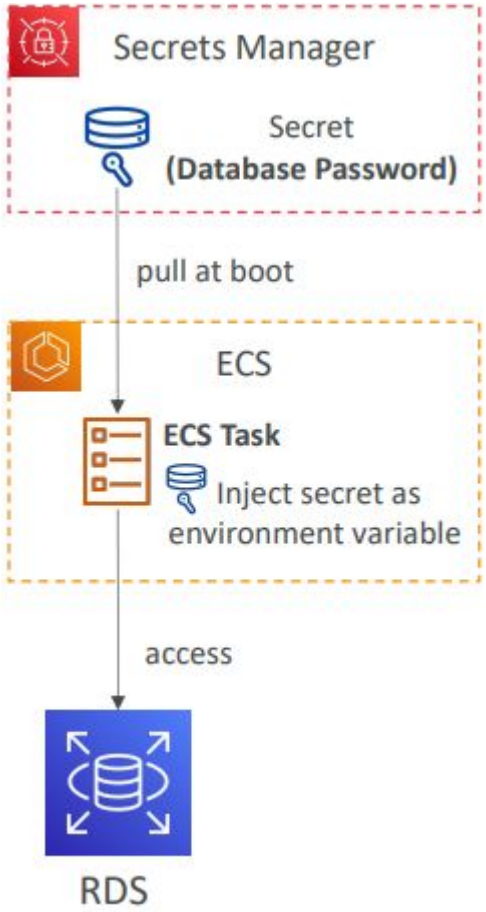
SSM Parameter Store - advanced parameter policies

- Destiné à stocker des secrets (par exemple, des mots de passe, des clés API, ...)

- Possibilité de forcer la rotation des secrets tous les X jours
  - Automatiser la génération des secrets lors de la rotation (utilise Lambda)
    - Supporte nativement Amazon RDS (tous les moteurs de base de données supportés), Redshift, DocumentDB
    - Prise en charge d'autres bases de données et services (fonction Lambda personnalisée)

- Contrôle de l'accès aux secrets à l'aide d'une politique basée sur les ressources

- Intégration avec d'autres services AWS pour extraire nativement les secrets de Secrets Manager nativement les secrets de Secrets Manager : CloudFormation, CodeBuild, ECS, EMR, Fargate, EKS, Parameter Store

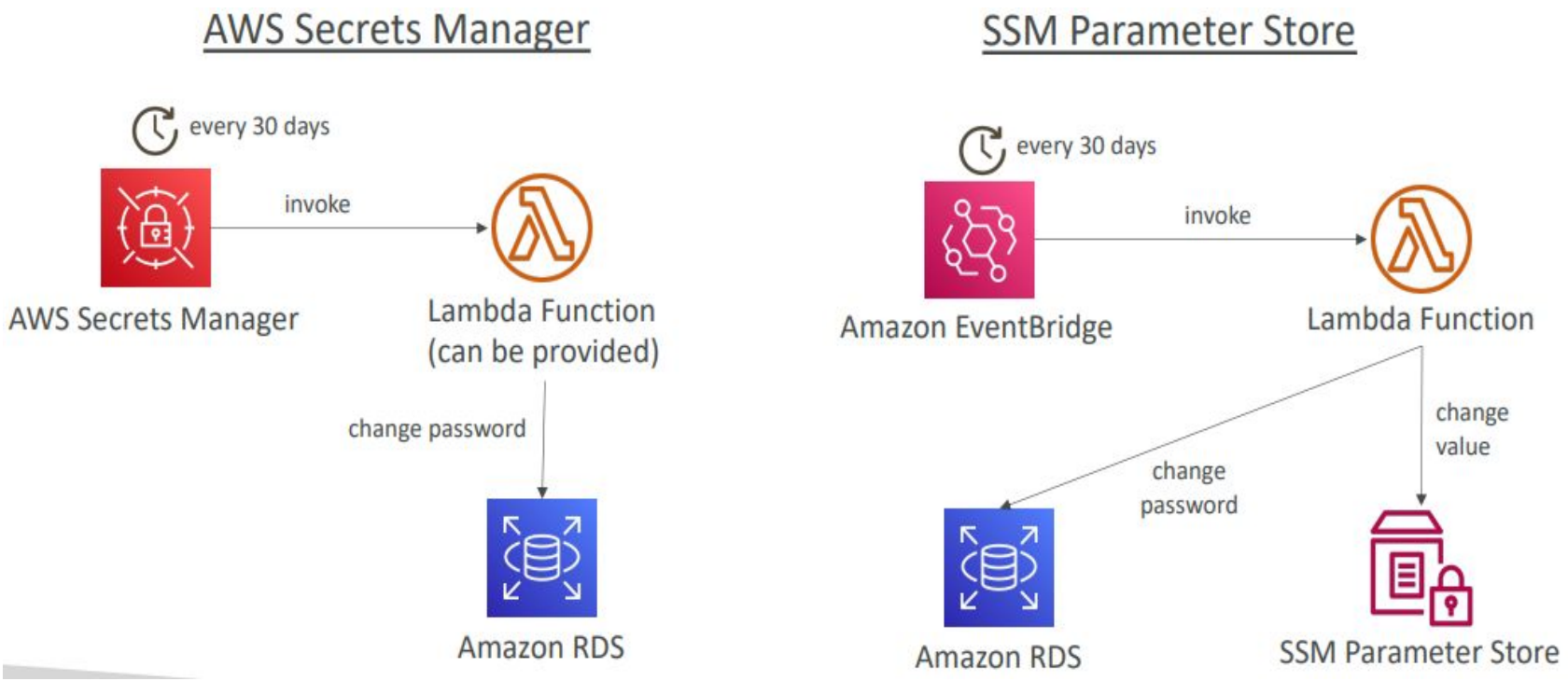


SSM parameter Store vs Secrets manager

- **Gestionnaire de secrets ($$$) :**
  - Rotation automatique des secrets avec AWS Lambda
  - La fonction Lambda est fournie pour RDS, Redshift, DocumentDB
  - Le cryptage KMS est obligatoire
  - Intégration possible avec CloudFormation

- **SSM Parameter Store ($) :**
  - API simple
  - Pas de rotation des secrets (possibilité d'activer la rotation à l'aide d'une fonction Lambda déclenchée par EventBridge)
  - Le chiffrement KMS est facultatif- Peut s'intégrer à CloudFormation
  - Peut extraire un secret de Secrets Manager à l'aide de l'API SSM Parameter Store

SSM parameter Store vs Secrets manager



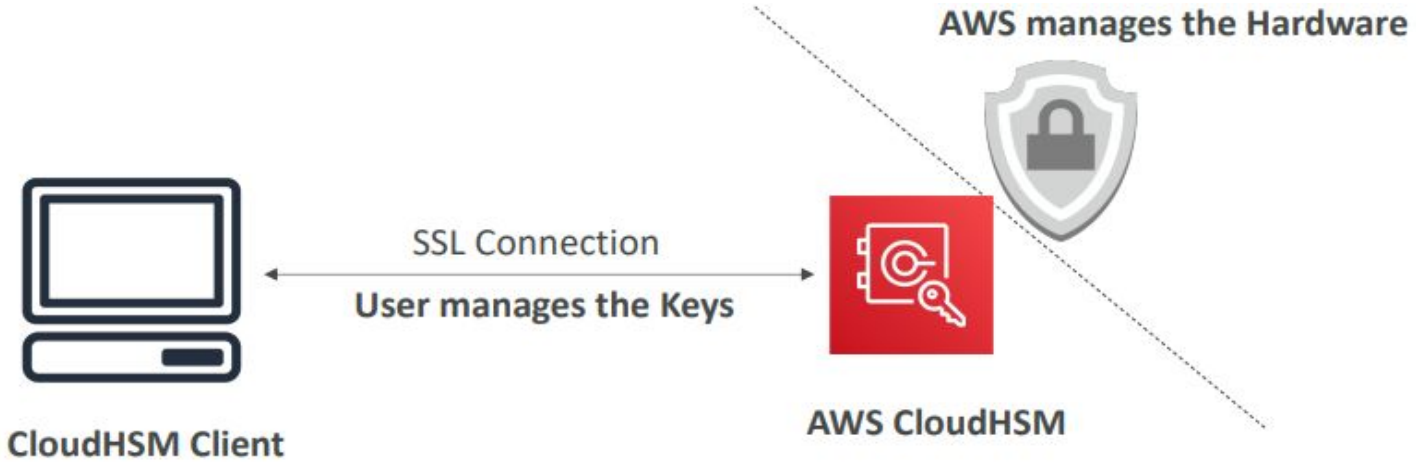
Plan

- AWS KMS
- Secret Manager
- SSM Parameter Store
- CloudHSM
- AWS ACM
- Security Hub
- AWS Firewall Manager
- AWS WAF
- Amazon Detective
- AWS Inspector

AWS CloudHSM

- KMS => AWS gère le logiciel de cryptage
- CloudHSM => AWS fournit le matériel de cryptage
- Matériel dédié (HSM = Hardware Security Module)
- Vous gérez entièrement vos propres clés de chiffrement (pas AWS).
- Le dispositif HSM est inviolable et conforme à la norme FIPS 140-2 de niveau 3.
- Prise en charge du cryptage symétrique et asymétrique (clés SSL/TLS)
- Pas de version gratuite disponible
- Nécessité d'utiliser le logiciel client CloudHSM
- Redshift prend en charge CloudHSM pour le chiffrement des bases de données et la gestion des clés.
- Bonne option à utiliser avec le cryptage SSE-C

AWS CloudHSM -diagram



IAM permissions:

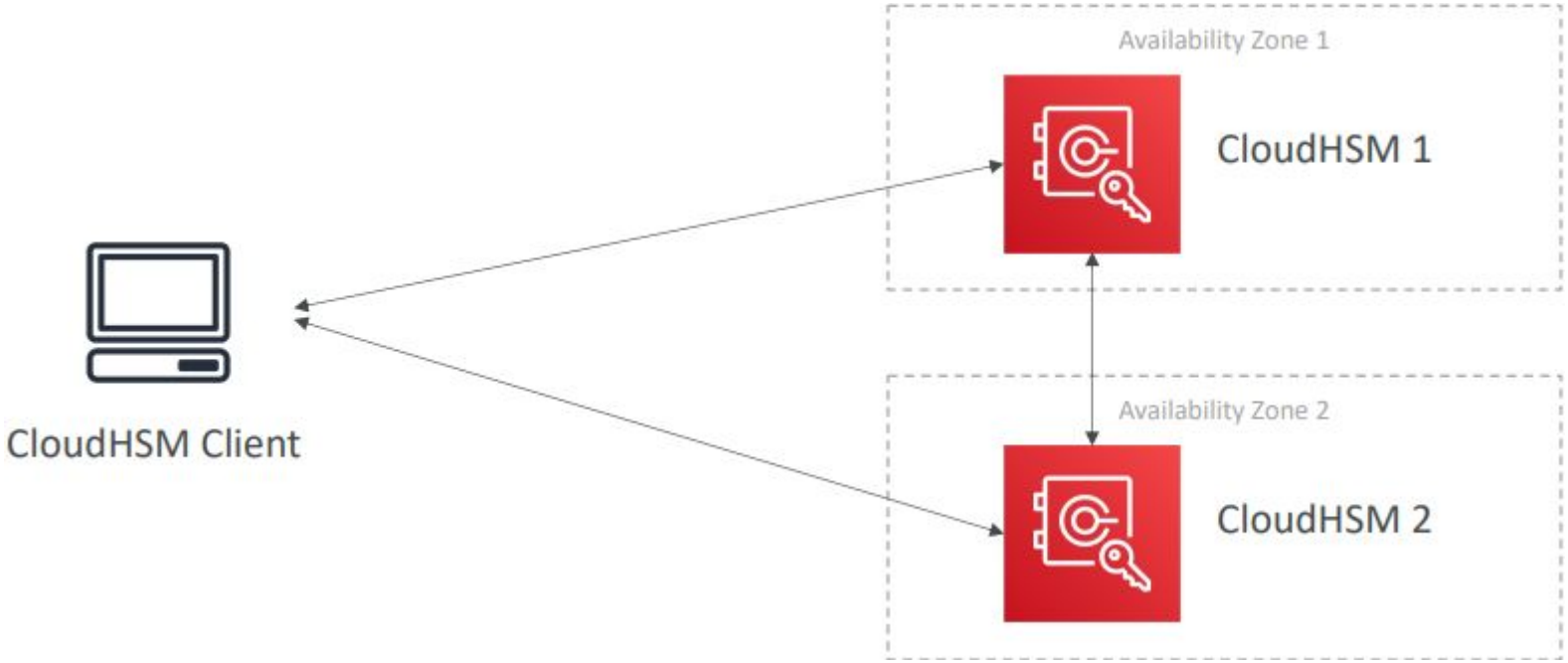
- CRUD an HSM Cluster

CloudHSM Software:

- Manage the Keys
- Manage the Users

CloudHSM -Haute disponibilité

- Les clusters CloudHSM sont répartis sur Multi AZ (HA)
- Excellent pour la disponibilité et la durabilité



CloudHSM VS KMS

Feature	AWS KMS	AWS CloudHSM
Tenancy	Multi-Tenant	Single-Tenant
Standard	FIPS 140-2 Level 2	FIPS 140-2 Level 3
Master Keys	• AWS Owned Keys • AWS Managed Keys • Customer Managed KMS Keys	Customer Managed CMK
Key Types	• Symmetric • Asymmetric • Digital Signing	• Symmetric • Asymmetric • Digital Signing & Hashing
Key Accessibility	Accessible in multiple AWS regions KMS Key Replication	• Deployed and managed in a VPC • Can be shared across VPCs (VPC Peering)
Cryptographic Acceleration	None	• SSL/TLS Acceleration • Oracle TDE Acceleration
Access & Authentication	AWS IAM	You create users and manage their permissions

CloudHSM VS KMS

Feature	AWS KMS	AWS CloudHSM
High Availability	AWS Managed Service	Add multiple HSMs over different AZs
Audit Capability	• CloudTrail • CloudWatch	• CloudTrail • CloudWatch • MFA support
Free Tier	Yes	No

Plan

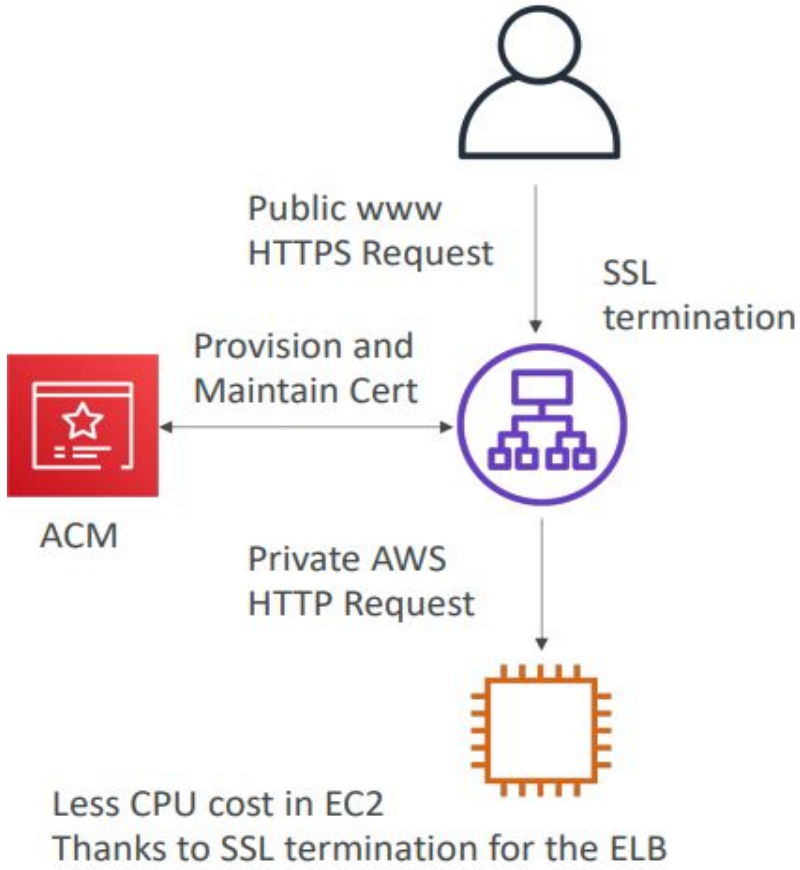
- AWS KMS
- Secret Manager
- SSM Parameter Store
- CloudHSM
- AWS ACM
- Security Hub
- AWS Firewall Manager
- AWS WAF
- Amazon Detective
- AWS Inspector

AWS certificate Manager -ACM

- Pour héberger des certificats SSL publics dans AWS, vous pouvez
  - acheter vos propres certificats et les télécharger à l'aide du CLI
  - Demander à ACM de provisionner et de renouveler les certificats publics pour vous (gratuitement)

- ACM charge les certificats SSL sur les intégrations suivantes intégrations suivantes :
  - Équilibreurs de charge (y compris ceux créés par EB)
  - Distributions CloudFront- APIs sur les passerelles API

- Les certificats SSL sont généralement difficiles à gérer manuellement. manuellement, c'est pourquoi ACM est un excellent levier pour votre Infrastructure AWS!



AWS certificate Manager -ACM

- Possibilité de créer des certificats publics
  - Doit vérifier le DNS public
  - Doit être émis par une autorité de certification publique de confiance (CA)

- Possibilité de créer des certificats privés
  - Pour vos applications internes
  - Vous créez votre propre AC privée
  - Vos applications doivent faire confiance à votre AC privée

- Renouvellement du certificat :
  - Automatiquement si généré provisionné par ACM
  - Tout certificat téléchargé manuellement doit être renouvelé manuellement et rechargé.

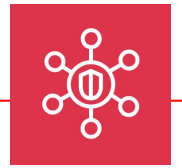
- ACM est un service régional
  - Pour l'utiliser avec une application globale (plusieurs ALB par exemple), vous devez émettre un certificat SSL dans chaque région où votre application est déployée.
  - Vous ne pouvez pas copier les certificats d'une région à l'autre.

Plan

- AWS KMS
- Secret Manager
- SSM Parameter Store
- CloudHSM
- AWS ACM
- Security Hub
- AWS Firewall Manager
- AWS WAF
- Amazon Detective
- AWS Inspector

AWS security Hub

AWS security Hub



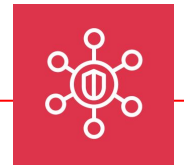
AWS Security Hub est un service qui offre des aspects de sécurité pour protéger l'environnement en utilisant les meilleures pratiques de l'industrie.

Il recueille les résultats ou les alertes de plusieurs comptes AWS. Ensuite, il analyse les tendances en matière de sécurité et identifie les problèmes
les plus prioritaires.

AWS Security Hub permet d'agréger, d'organiser et de hiérarchiser les alertes de sécurité ou les découvertes provenant de plusieurs systèmes AWS.

Il vérifie automatiquement l'état de conformité à l'aide du CIS AWS Foundations Benchmark.

AWS security Hub



AWS Security Hub est un service qui offre des aspects de sécurité pour protéger l'environnement en utilisant les meilleures pratiques de l'industrie.

Il vérifie automatiquement le statut de conformité à l'aide de la Foundations Benchmark du CIS.

Les alertes de sécurité ou les constatations peuvent être examinées à l'aide d'Amazon Detective ou Amazon CloudWatch Event rules.

Il recueille les données des services AWS dans tous les comptes et réduit la nécessité d'une conversion de données fastidieuse qui prend du temps.

AWS Security Hub

AWS security Hub

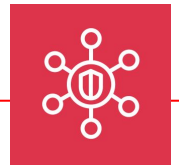
AWS Security Hub aide la norme de sécurité des données de l'industrie des cartes de paiement (Payment Card Industry Data (PCI DSS) et le Center for Internet Security (CIS) avec un ensemble de meilleures pratiques de configuration de la sécurité pour AWS.

L'activation (ou la désactivation) peut se faire rapidement par AWS Security Hub par l'intermédiaire de :

- AWS Management Console
- AWS CLI
- En utilisant des outils d'infrastructure en tant que code -- Terraform

AWS Security Hub

AWS security Hub

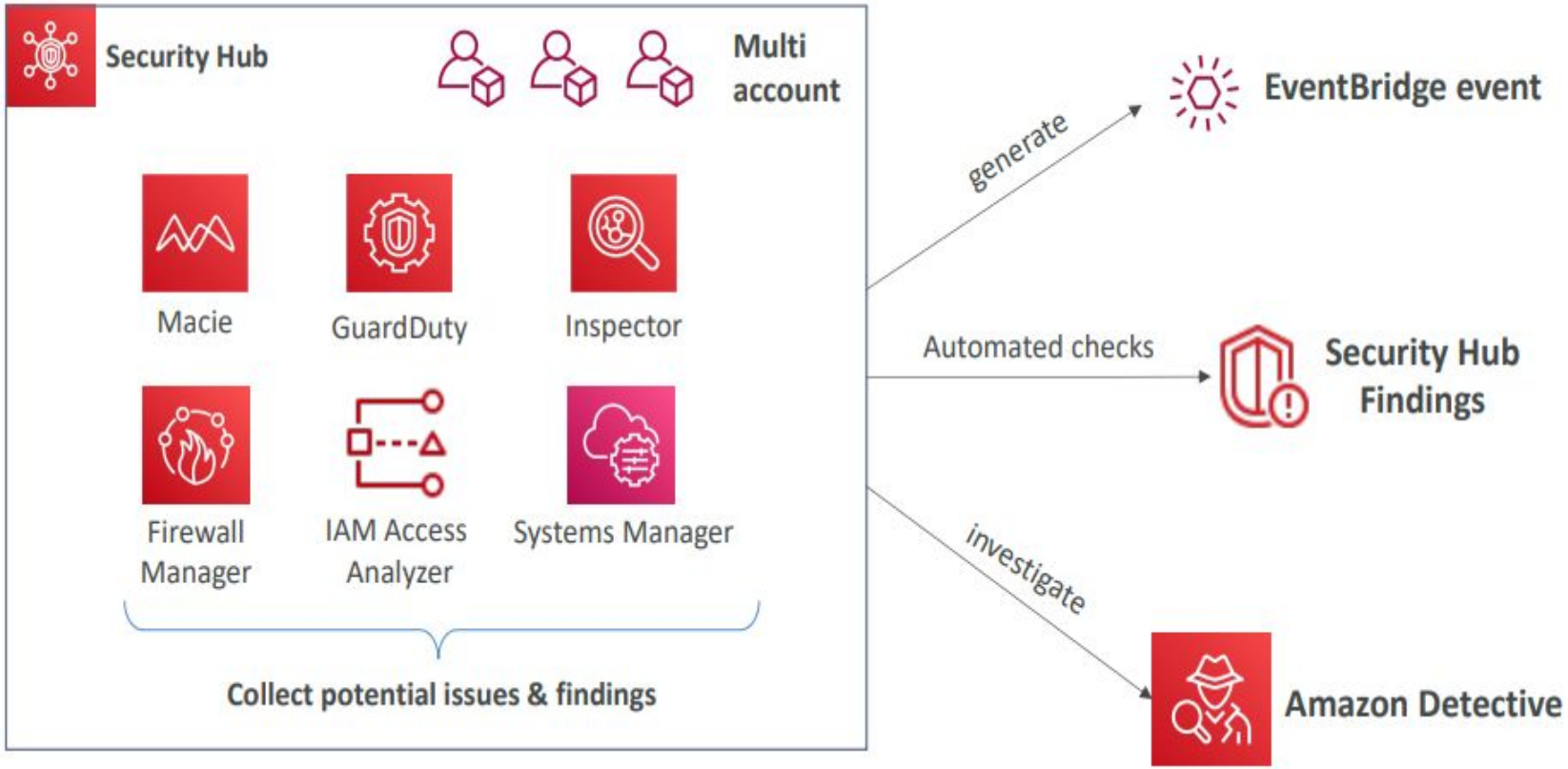


AWS Security Hub est un service qui offre des aspects de sécurité pour protéger l'environnement en utilisant les meilleures pratiques de l'industrie.

Il utilise des tableaux de bord intégrés pour montrer l'état actuel de la sécurité et de la conformité.

Les frais ne sont appliqués que pour la région en cours, et non pour toutes les régions dans lesquelles le Security Hub est activé

AWS Security Hub



Plan

- AWS KMS
- Secret Manager
- SSM Parameter Store
- CloudHSM
- AWS ACM
- Security Hub
- AWS Firewall Manager
- AWS WAF
- Amazon Detective
- AWS Inspector

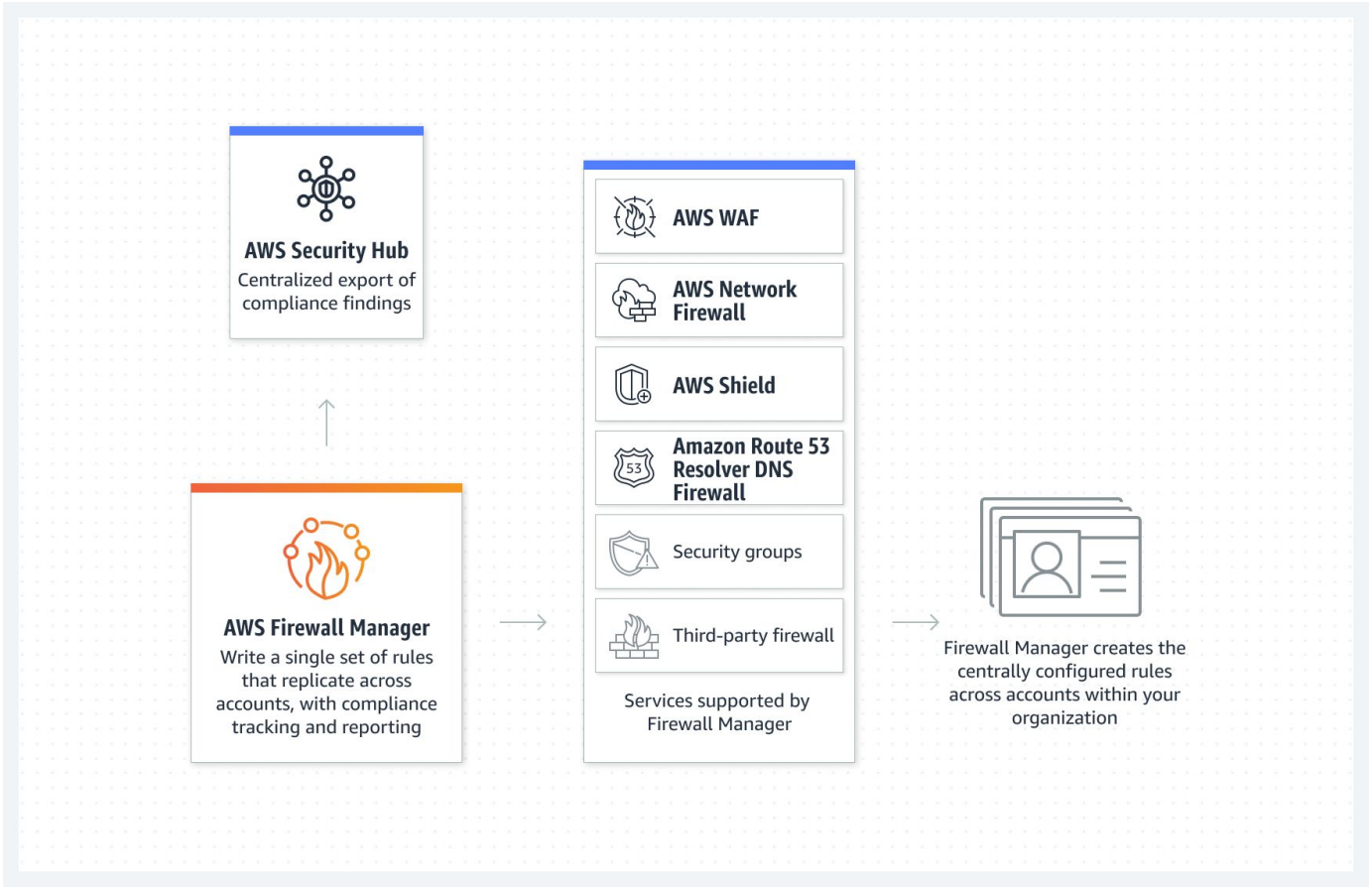
AWS Firewall Manager

AWS Firewall Manager

Configurer et gérer de manière centralisée les règles de pare-feu sur vos comptes

- Utilisez un compte administrateur central pour gérer les règles de pare-feu sur plusieurs comptes AWS.
- Déployez des règles gérées, telles que des règles WAF préconfigurées sur vos applications, sur l'ensemble des comptes
- Appliquez automatiquement vos politiques de sécurité définies sur les ressources existantes et nouvellement créées.
- Déployez de manière centralisée des règles de groupe de sécurité de base pour protéger vos clouds privés virtuels (VPC).

AWS Firewall Manager



AWS Firewall Manager -cas d usage

- Protéger les applications hébergées sur des instances EC2
- Déployer des outils à grande échelle pour protéger les données
- Auditer les ressources en continu

AWS Firewall Manager -avantages

- Permet de protéger les ressources entre comptes
- Permet de protéger toutes les ressources d'un type particulier, telles que toutes les CloudFront distributions Amazon
- Permet de protéger toutes les ressources avec des balises spécifiques
- Ajoute automatiquement la protection aux ressources qui sont ajoutées à votre compte

AWS Firewall Manager -avantages

- Permet d'abonner tous les comptes membres d'une organisation AWS Organizations à AWS Shield Advanced, et abonne automatiquement les nouveaux comptes concernés qui rejoignent l'organisation
- Permet d'appliquer des règles de groupe de sécurité à tous les comptes membres ou sous-ensembles spécifiques de comptes d'une organisation AWS Organizations et applique automatiquement les règles aux nouveaux comptes concernés qui rejoignent l'organisation
- Vous permet d'utiliser vos propres règles ou d'acheter des règles gérées à partir de AWS Marketplace

Plan

- AWS KMS
- Secret Manager
- SSM Parameter Store
- CloudHSM
- AWS ACM
- Security Hub
- AWS Firewall Manager
- AWS WAF
- Amazon Detective
- AWS Inspector

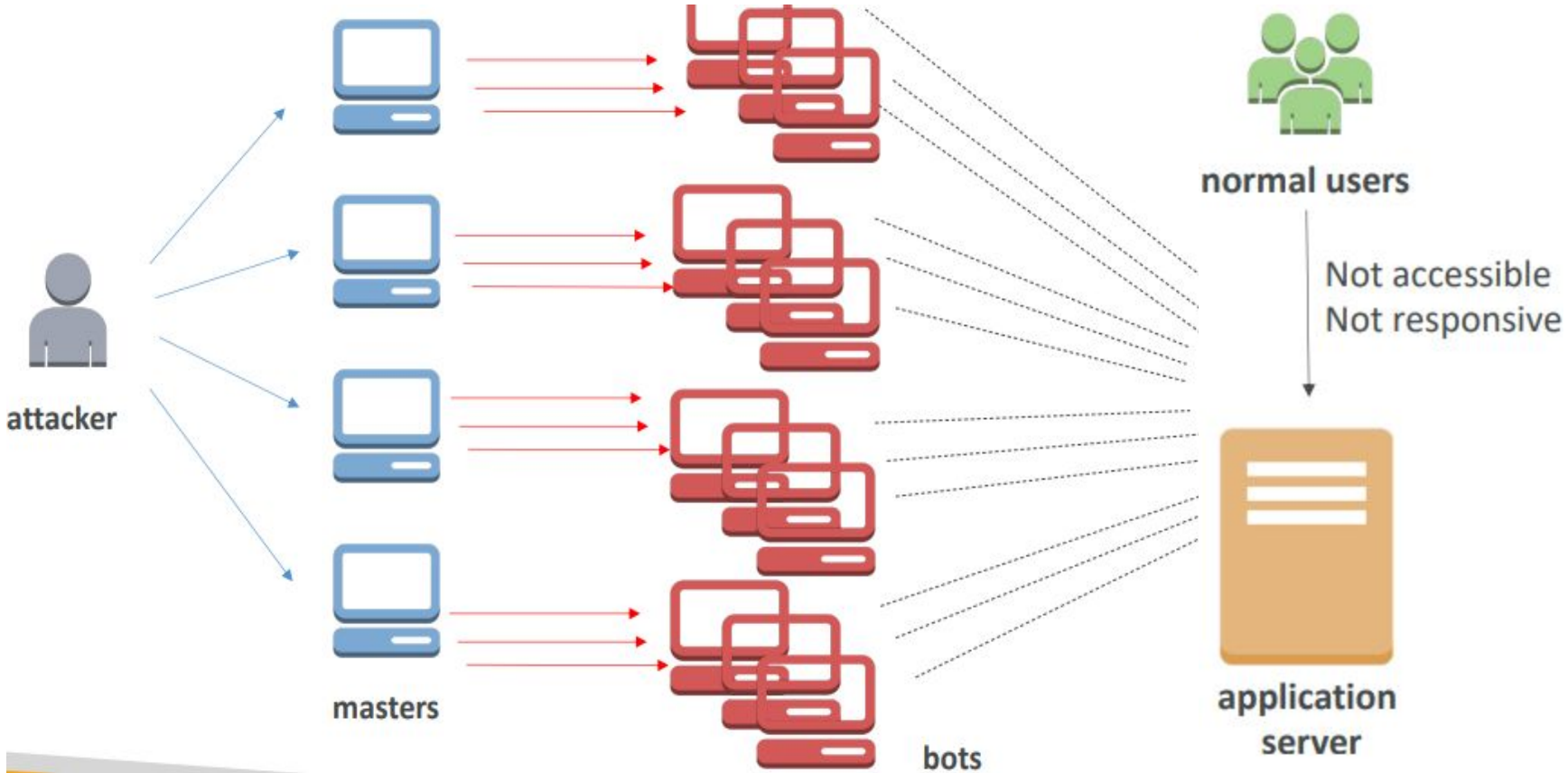
AWS Web Application Firewall (WAF)

- Protège vos applications web contre les exploits web courants (couche 7)
- Déploiement sur l'équilibreur de charge d'application (règles localisées)
- Déploiement sur API Gateway (règles exécutées au niveau régional ou périphérique)
- Déploiement sur CloudFront (règles globales sur les sites périphériques)
  - Utilisé en amont d'autres solutions : CLB, instances EC2, origines personnalisées, sites web S3
- Déploiement sur AppSync (protection de vos API GraphQL)
- Le WAF n'est pas destiné à la protection contre les attaques DDoS
- Définir des ACL Web (liste de contrôle d'accès Web) :
  - Les règles peuvent inclure des adresses IP, des en-têtes HTTP, des corps HTTP ou des chaînes URI.
  - Protège contre les attaques courantes - injection SQL et Cross-Site Scripting(XSS)
  - Contraintes de taille, correspondance géographique
  - Règles basées sur le taux (pour compter les occurrences d'événements)
- Actions des règles : Compter | Autoriser | Bloquer | CAPTCHA

AWS WAF -Managed rules

- Bibliothèque de plus de 190 règles gérées
- Règles prêtes à l'emploi gérées par AWS et les vendeurs d'AWS Marketplace
- **Groupes de règles de base** - protection générale contre les menaces courantes- AWSManagedRulesCommonRuleSet, AWSManagedRulesAdminProtectionRuleSet, ...
- **Groupes de règles spécifiques aux cas d'utilisation -**protection pour de nombreux cas d'utilisation de l'AWS WAF
  - AWSManagedRulesSQLiRuleSet, AWSManagedRulesWindowsRuleSet, AWSManagedRulesPHPRuleSet, AWSManagedRulesWordPressRuleSet, ...
- **Groupes de règles de réputation IP** - bloquer les demandes en fonction de la source (par exemple, les IP malveillantes)
  -AWSManagedRulesAmazonIpReputationList,AWSManagedRulesAnonymousIpList
- **Groupe de règles gérées pour le contrôle des robots** - bloque et gère les demandes des robots.
  - AWSManagedRulesBotControlRuleSet

AWS WAF -Distributed denial of Service Attack (DDoS)



AWS WAF -Distributed denial of Service Attack (DDoS)

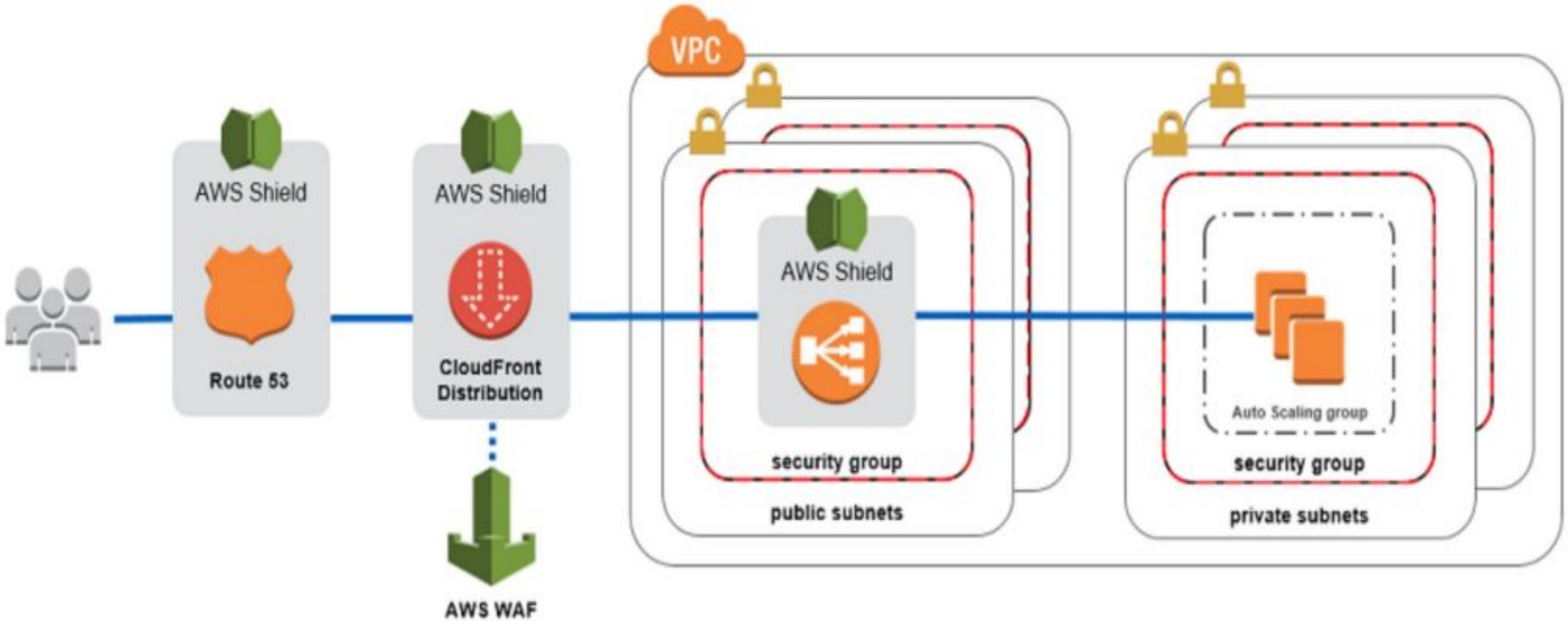
- Déni de service distribué (DDoS) :
  - Lorsque votre service est indisponible parce qu'il reçoit trop de demandes.
  - Inondation SYN (couche 4) : envoi d'un trop grand nombre de demandes de connexion TCP.
  - Réflexion UDP (couche 4) : incite d'autres serveurs à envoyer un grand nombre de requêtes UDP.
  - Attaque par inondation DNS : submerge le DNS de sorte que les utilisateurs légitimes ne peuvent pas trouver le site.
  - Attaque Slow Loris : un grand nombre de connexions HTTP sont ouvertes et maintenues.

- Attaques au niveau de l'application :
  - plus complexes, plus spécifiques (niveau HTTP)
  - Stratégies d'éclatement du cache : surcharge de la base de données dorsale en invalidant le cache.

AWS WAF -protection DDoS sur AWS

- **AWS Shield Standard :** protection contre les attaques DDoS pour votre site web et vos applications, pour tous les clients, sans frais supplémentaires.
- **AWS Shield Advanced :** protection DDoS premium 24/7
- **AWS WAF :** filtre les requêtes spécifiques sur la base de règles
- **CloudFront et Route 53 :**
  - Protection de la disponibilité à l'aide d'un réseau périphérique mondial
  - Combiné à AWS Shield, permet d'atténuer les attaques DDoS à la périphérie.- Soyez prêt à évoluer
- tirez parti de la fonction AWS Auto Scaling
- Séparer les ressources statiques (S3 / CloudFront) des ressources dynamiques (EC2 / ALB)

Exemple de référence d'architecture



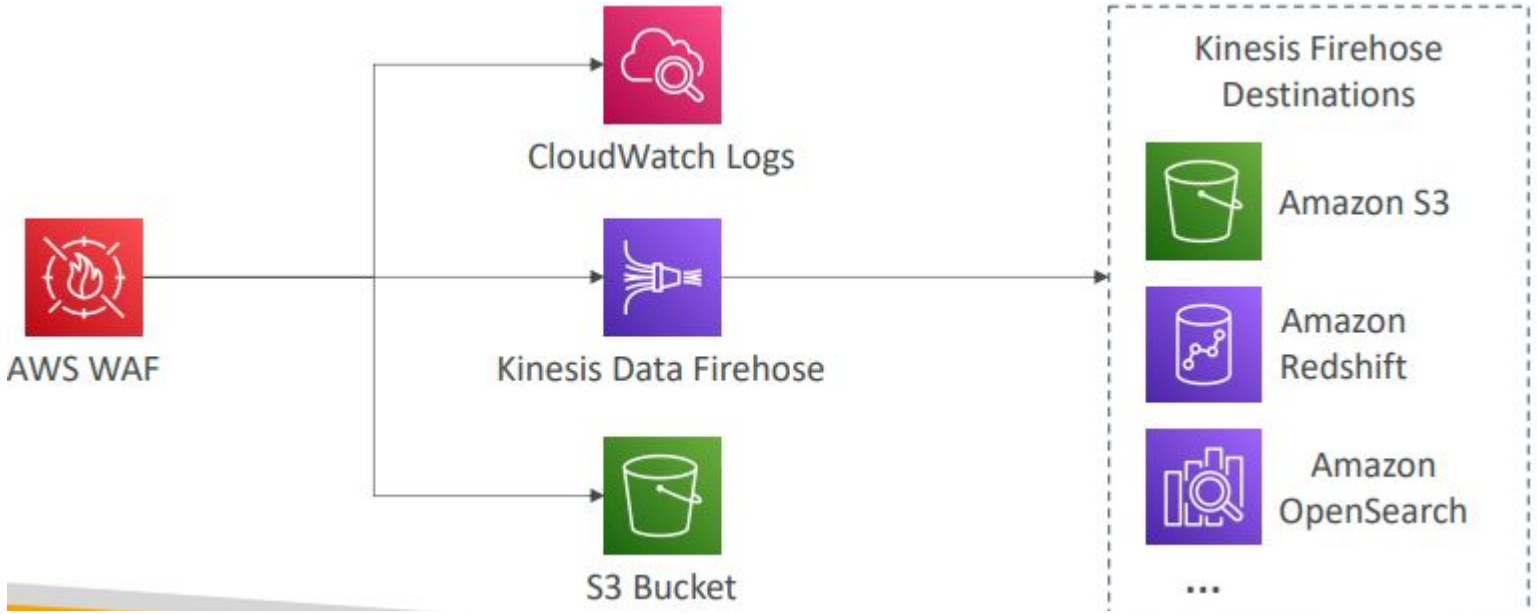
AWS Shield

- **Bouclier AWS Standard :**
  - Service gratuit activé pour chaque client AWS
  - Offre une protection contre les attaques telles que les inondations SYN/UDP, les attaques par réflexion et d'autres attaques de couche 3/couche 4. et d'autres attaques de couche 3/couche 4

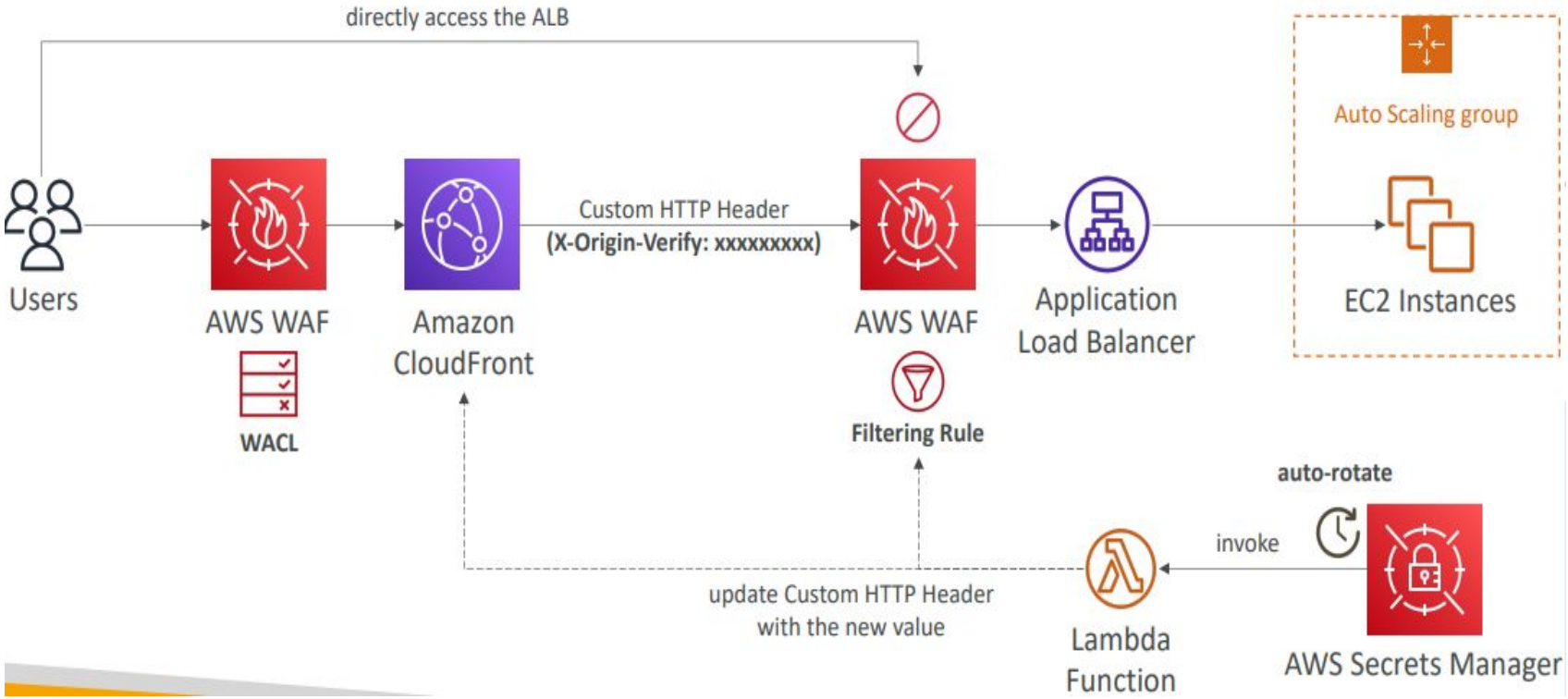
- **AWS Shield Advanced :**
  - Service optionnel d'atténuation des attaques DDoS (3 000 $ par mois et par organisation)
  - Protège contre les attaques plus sophistiquées sur **Amazon EC2, Elastic Load Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator, Route 53**
  - Accès 24/7 à l'équipe de réponse DDoS (DRP) d'AWS
  - Protection contre des frais plus élevés en cas de pics d'utilisation dus à des attaques DDoS

AWS WAF -web ACL-logging

- Vous pouvez envoyer vos logs à un groupe de logs :
  - un groupe de journaux Amazon CloudWatch Logs - 5 Mo par seconde
  - Amazon Simple Storage Service (Amazon S3) bucket - intervalle de 5 minutes
  - Amazon Kinesis Data Firehose - limité par les quotas Firehose



Architecture de solution -Améliorer la sécurité de CloudFront Origin avec AWS WAF et AWS Secrets Manager



WAF vs Firewall Manager vs Shield

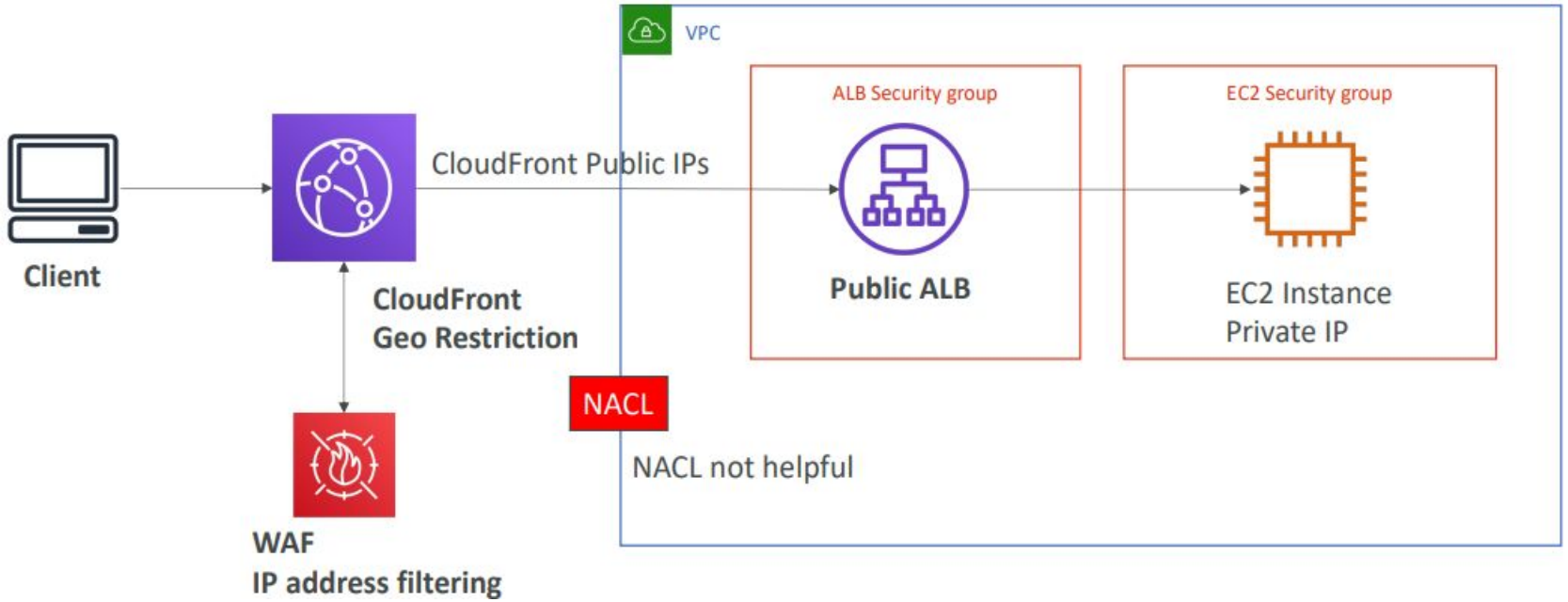
AWS WAF

AWS Firewall Manager

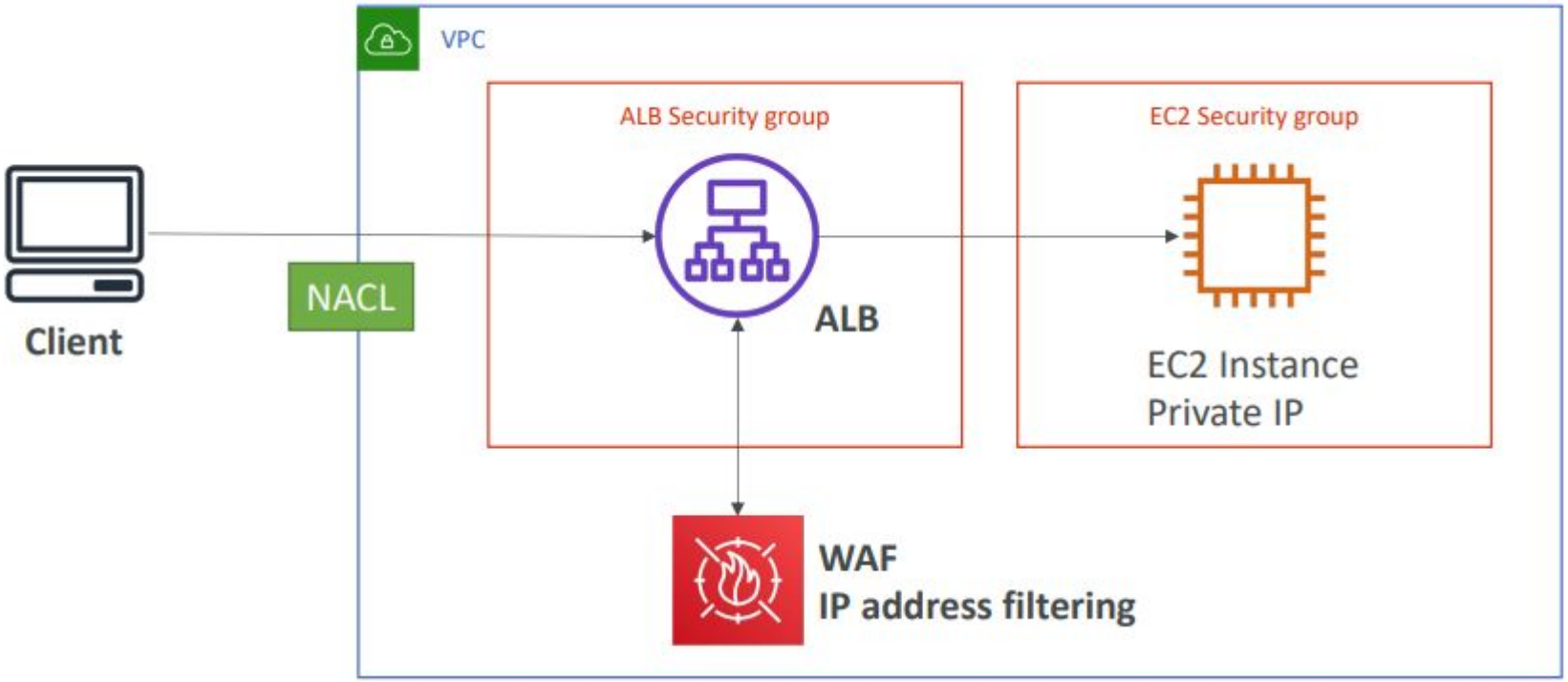
AWS Shield

- WAF, Shield et Firewall Manager sont utilisés ensemble pour une protection complète- Définissez vos règles d'ACL Web dans le WAF
- Pour une protection granulaire de vos ressources, le WAF seul est le bon choix.
- Si vous souhaitez utiliser AWS WAF pour plusieurs comptes, accélérez la configuration du WAF, automatiser la protection de nouvelles ressources, utilisez Firewall Manager avec AWS WAF.
- Shield Advanced ajoute des fonctionnalités supplémentaires à AWS WAF, telles que l'assistance dédiée de l'équipe de réponse Shield (Shield Response Team)et la création de rapports avancés.
- Si vous êtes sujet à des attaques DDoS fréquentes,

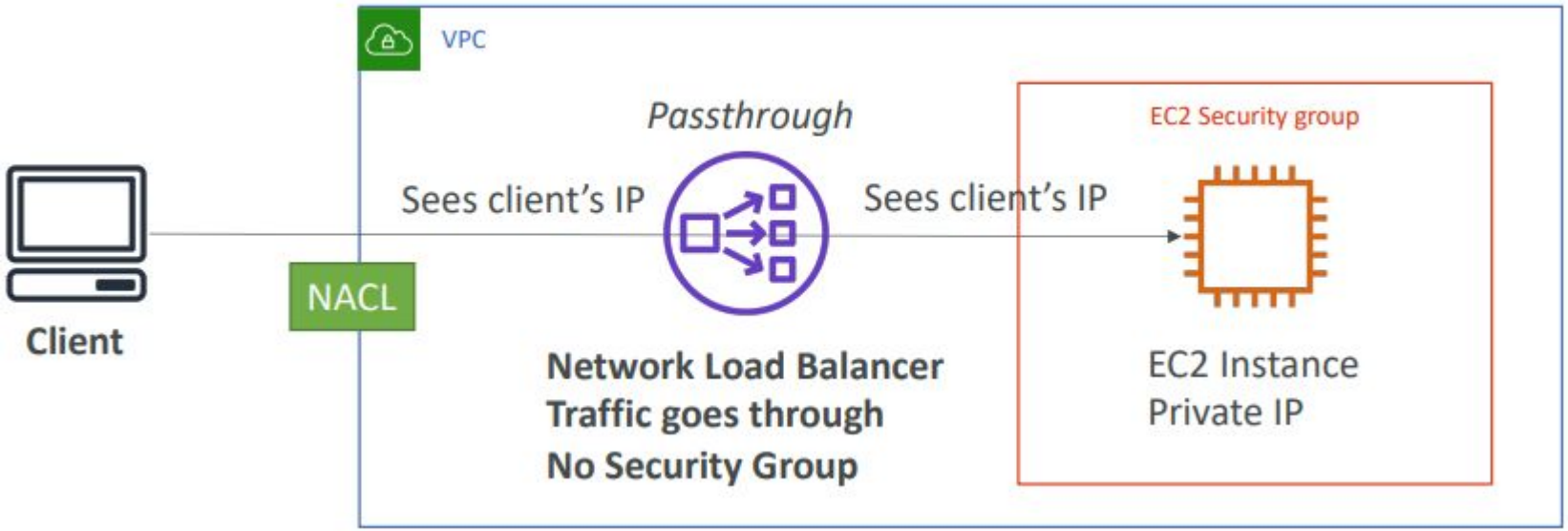
Bloquer une adresse IP -ALB, Cloudfront et WAF



Bloquer une adresse IP -ALB+ WAF



Bloquer une adresse IP avec NLB



Plan

- AWS KMS
- Secret Manager
- SSM Parameter Store
- CloudHSM
- AWS ACM
- Security Hub
- AWS Firewall Manager
- AWS WAF
- Amazon Detective
- AWS Inspector

Amazon detective

Amazon detective

Analysez et visualisez les données de sécurité pour étudier les éventuels problèmes de sécurité avec amazon detective.

Enquêter sur les incidents

Déterminez l'ampleur de l'activité malveillante, son impact et la cause sous-jacente en analysant l'historique des activités pertinentes à la recherche de modèles.

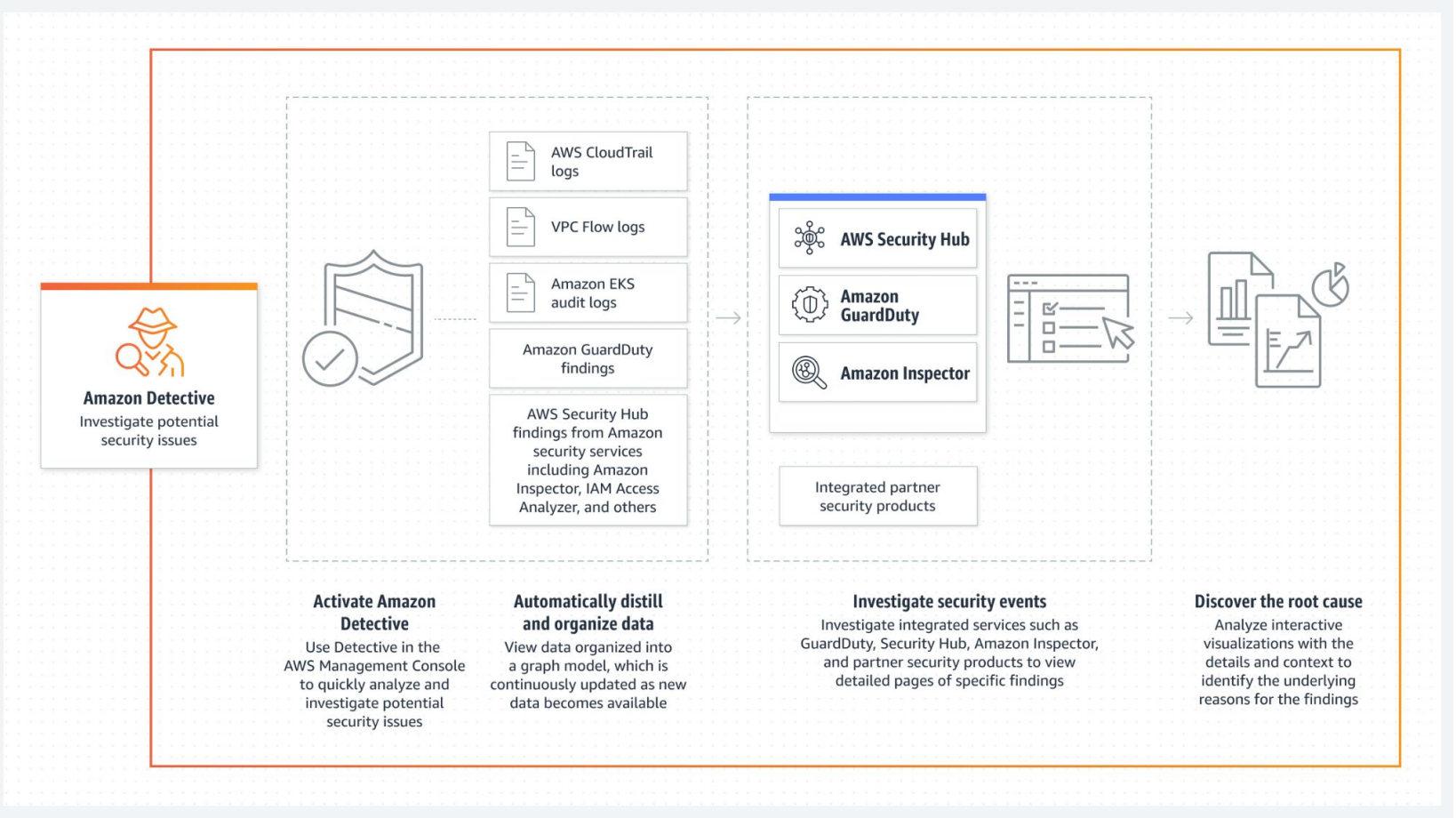
Triage des résultats de sécurité

Vérifiez ou infirmez les résultats suspects en examinant les rôles AWS Identity and Access Management (IAM), les utilisateurs, les adresses IP et les comptes AWS.

Traquer les menaces

Concentrez-vous sur des ressources spécifiques, telles que les instances Amazon Elastic Compute Cloud (EC2), et examinez les visualisations détaillées des activités associées.

Amazon Detective -fonctionnement



Plan

- AWS KMS
- Secret Manager
- SSM Parameter Store
- CloudHSM
- AWS ACM
- Security Hub
- AWS Firewall Manager
- AWS WAF
- Amazon Detective
- AWS Inspector

Amazon Inspector

- Évaluations de sécurité automatisées
- Pour les instances EC2
  - Utilisation de l'agent AWS System Manager (SSM)
  - Analyse de l'accessibilité involontaire au réseau
  - Analyse du système d'exploitation en cours d'exécution par rapport aux vulnérabilités connues
- Pour les images de conteneurs poussées vers Amazon ECR
  - Évaluation des images de conteneurs au fur et à mesure qu'elles sont poussées
- Pour les fonctions Lambda
  - Identifie les vulnérabilités logicielles dans le code de la fonction et les dépendances du paquetage dépendances des paquets
  - Évaluation des fonctions au fur et à mesure de leur déploiement
- Rapports et intégration avec AWS Security Hub
- Envoi des résultats à Amazon Event Bridge

Amazon Inspector

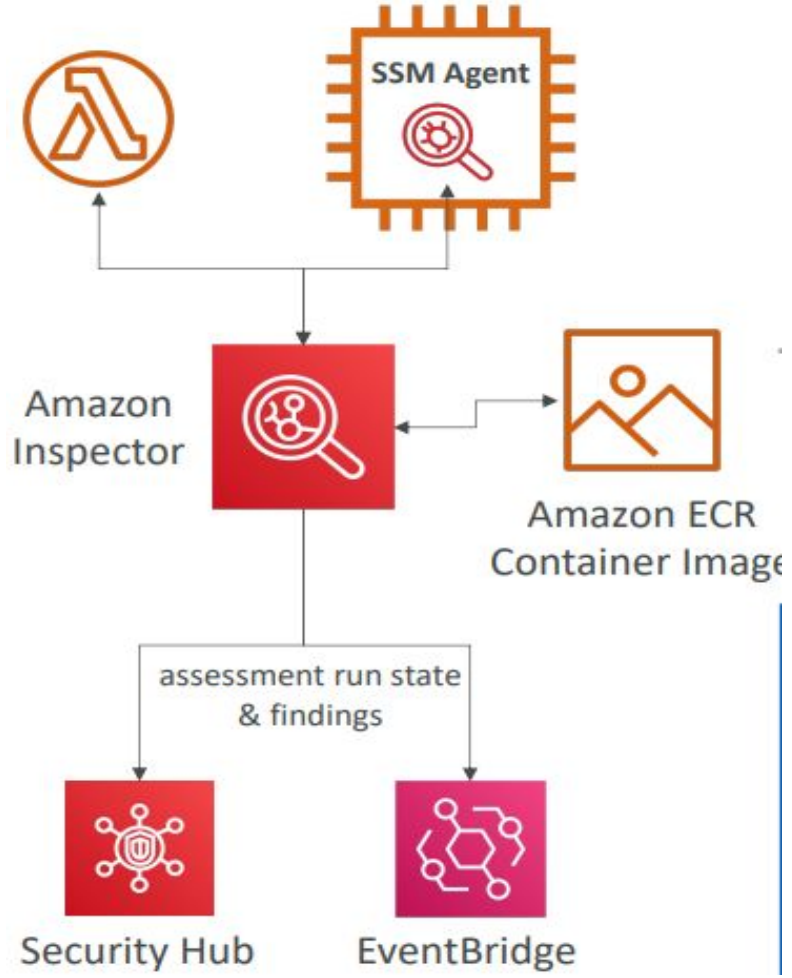
- Évaluations de sécurité automatisées

- Pour les instances EC2
  - Utilisation de l'agent AWS System Manager (SSM)
  - Analyse de l'accessibilité involontaire au réseau
  - Analyse du système d'exploitation en cours d'exécution par rapport aux vulnérabilités connues

- Pour les images de conteneurs poussées vers Amazon ECR
  - Évaluation des images de conteneurs au fur et à mesure qu'elles sont poussées

- Pour les fonctions Lambda
  - Identifie les vulnérabilités logicielles dans le code de la fonction et les dépendances du paquetage dépendances des paquets
  - Évaluation des fonctions au fur et à mesure de leur déploiement

- Rapports et intégration avec AWS Security Hub
-
- Envoi des résultats à Amazon Event Bridge



Amazon Inspector

- Rappel : uniquement pour les instances EC2, les images de conteneurs et les fonctions Lambda.
- Analyse continue de l'infrastructure, uniquement en cas de besoin- Vulnérabilités des paquets (EC2, ECR & Lambda)
- base de données CVE- Accessibilité du réseau (EC2)
- Un score de risque est associé à toutes les vulnérabilités afin de les classer par ordre de priorité.

MERCI POUR VOTRE AIMABLE ATTENTION!

EAZYTraining

Alphonsine Lahda

Lahda Biassou Alphonsine

Ingénieure cloud et Formatrice