DAWAN Paris 11 Rue Antoine Bourdelle, 75015 PARIS
DAWAN Lille 1 Rue Esquermoise, 59800 LILLE
DAWAN Nantes 32 Boulevard Vincent Gâche, 44000 NANTES
DAWAN Lyon 253 Cours la Fayette, 69006 LYON
DAWAN Bordeaux 4 Avenue Eugene et Marc Dulout, 33600 Pessac
DAWAN Toulouse 1 Place Occitane, 31000 TOULOUSE
DAWAN Marseille 23 rue de la République, 13002 Marseille
DAWAN Strasbourg 37 rue du Fossé des Treize, 67000 Strasbourg
DAWAN Montpellier 26 allée de Mycènes: 34000 Montpellier

AWS: INITIATION

Frédéric KIBANZA

Catalogue de formations sur https://www.dawan.fr
Contactez notre service commercial au 09.72.37.73.73

DAWAN – Reproduction interdite sans autorisation

PRÉSENTATION DE LA FORMATION

- Qui suis-je? « mon parcours » « mes compétences »
- Exprimer votre besoin:
  - Le contexte IT
  - Votre environnement de travail
  - Vos objectifs pour cette formation
- Y a-t-il des personnes avec un handicap ?

DAWAN – Reproduction interdite sans autorisation

LOGISTIQUE

- Horaires : 9h30 – 17h30, le premier jour.
- Pauses et déjeuner (probablement 13h00 – 14h00)
- Signer votre feuille de présence
- Créer votre compte pour les exercices sur qwiklabs.com
- Récupérer votre support de cours Papier ou électronique.
- Support ppt remis à discrétion.

DAWAN – Reproduction interdite sans autorisation

TEST

- Avez-vous déjà utilisé un environnement AWS, Azure, Google, IBM ou autre ?
- Utilisez-vous de la virtualisation?
- Connaissez-vous l'extension de fichier VHDX?
- Comment peut-on définir le Cloud Computing (CC) ?
- Quels sont les différents modèles du CC?

DAWAN – Reproduction interdite sans autorisation

OBJECTIFS

- Appréhender les principaux services de CC
- Comprendre les concepts du CC et de la virtualisation
- Les défis techniques, la sécurité, etc.
- Découvrir les services fournis par Amazon
- Découvrir les Services Clés (IAAS, PAAS, SAAS)
- Avec ces acquis, vous serez en mesure de comprendre :
  - Les scénarios d'utilisation
  - L'impact sur les infrastructures informatiques
  - Savoir créer et gérer des VMs
  - Les aspects règlementaires, coût, humain et technique

DAWAN – Reproduction interdite sans autorisation

INTRODUCTION 1/2

INTRODUCTION 2/2

- Vous serez en mesure de discuter des aspects des architectures AWS et de la manière dont elles s'articulent pour créer des systèmes complexes.

- Vous allez acquérir une expérience pratique de la création d'architectures avec les divers scénarios en utilisant les services AWS.

- Vous serez en mesure de concevoir des solutions IT optimales en suivant les meilleures pratiques et modèles de conception du cloud AWS.

DAWAN – Reproduction interdite sans autorisation

RÔLES DES TACHES DANS AWS CLOUD

https://aws.amazon.com/fr/training/course-descriptions/job-roles/

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

CERTIFICATION

Source:https://aws.training

PRÉPARATION À LA CERTIFICATION

- www.examtopics.com

Welcome to ExamTopics | Login | Sign up

EXAMTOPICS - Expert Verified, Online, **Free**.

MAIL US
team@examtopics.com

LOCATION
Chicago IL, USA

HOME | POPULAR EXAMS | VIEW ALL EXAMS | NEWS | ABOUT | CONTACT | FORUM

Amazon AWS Certified Solutions Architect - Associate SAA-C02 Exam Actual Questions

The questions for AWS Certified Solutions Architect - Associate SAA-C02 were last updated at Jan. 17, 2021.

Viewing page **1** out of 57 pages.

Viewing questions 1-5 out of 284 questions

Custom View Settings

Topic 1 - Single Topic

Question #1 *Topic 1*

A solutions architect is designing a solution where users will be directed to a backup static error page if the primary website is unavailable. The primary website's DNS records are hosted in Amazon Route 53 where their domain is pointing to an Application Load Balancer (ALB).
Which configuration should the solutions architect use to meet the company's needs while minimizing changes and infrastructure overhead?

A. Point a Route 53 alias record to an Amazon CloudFront distribution with the ALB as one of its origins. Then, create custom error pages for the distribution.

B. Set up a Route 53 active-passive failover configuration. Direct traffic to a static error page hosted within an Amazon S3 bucket when Route 53 health checks determine that the ALB endpoint is unhealthy.

C. Update the Route 53 record to use a latency-based routing policy. Add the backup static error page hosted within an Amazon S3 bucket to the record so the traffic is sent to the most responsive endpoints.

D. Set up a Route 53 active-active configuration with the ALB and an Amazon EC2 instance hosting a static error page as endpoints. Route 53 will only send requests

Les avantages du CC :

- Remplace les coûts en capitaux par des coûts variables
- Importantes économies d'échelle
- Évite les risques de sur et sous-dimensionnement
- Vitesse et souplesse accrues
- Évite des dépenses inutiles pour le fonctionnement et la maintenance de centres de données
- À l'international en quelques minutes

DAWAN – Reproduction interdite sans autorisation

❑Cas typiques d'utilisation

- ➢Hébergement de sites web
- ➢Stockage et partage de données
- ➢Reprise après sinistre
- ➢Développement et test
- ➢Analyse des données

LES PRINCIPAUX ACTEURS

Certification:

❑ **Google Cloud**

- Architect Cloud
- Ingénieur Data
- Administrateur G Suite

❑ **AWS**

- Architecte de solutions
- Ingénieur DevOps
- Développeur

❑ **Azure**

- MCSA: Cloud Platform
- MTA: IT Infrastructure
- MCSA: Linux on AZURE
- MCSE : Cloud platform and infrastructure, etc.

- Tendances du Cloud Computing

Source: RightScale 2017 State of the Cloud Report

TENDANCES DU CLOUD COMPUTING 1/6

TENDANCES DU CLOUD COMPUTING 2/6

IaaS/PaaS market (Source: Jefferies)

Cloud vendor	Annualized revenue	% of market	Year-over-year growth
Amazon Web Services	$18.34 billion	51%	42%
Microsoft Azure	$6.17 billion	17%	89%
IBM Cloud	$4.03 billion	11%	22%
Google Cloud Platform	$2.05 billion	6%	125%
Alibaba Cloud	$1.79 billion	5%	92%
Salesforce	$1.78 billion	5%	31%
Oracle Cloud	$1.59 billion	4%	20%
Subtotal	$35.75 billion	86%	54%
Total Gartner estimate	$41.79 billion	100%	33%

— Google Cloud vs AWS (marché IaaS/PaaS) Img src : MarketWatch

TENDANCES DU CLOUD COMPUTING 3/6

	2018	2019	2020	2021	2022
Cloud Business Process Services (BPaaS)	41.7	43.7	46.9	50.2	53.8
Cloud Application Infrastructure Services (PaaS)	26.4	32.2	39.7	48.3	58.0
Cloud Application Services (SaaS)	85.7	99.5	116.0	133.0	151.1
Cloud Management and Security Services	10.5	12.0	13.8	15.7	17.6
Cloud System Infrastructure Services (IaaS)	32.4	40.3	50.0	61.3	74.1
Marché total	196.7	227.8	266.4	308.5	354.6

— Croissance du marché du cloud et leaders du segment (Source de l'image : Synergy.com)

https://info.flexera.com/SLO-CM-REPORT-State-of-the-Cloud-2020

https://www.srgresearch.com/articles/half-yearly-review-shows-150-billion-spent-cloud-services-and-infrastructure

DAWAN – Reproduction interdite sans autorisation

TENDANCES DU CLOUD COMPUTING 4/6

les parts de marché du Cloud Public SaaS

https://www.srgresearch.com/articles/saas-spending-hits-100-billion-annual-run-rate-microsoft-extends-its-leadership

TENDANCES DU CLOUD COMPUTING 5/6

- Marché du Cloud Public IaaS et PaaS
  - 2017 – 2018 (en Million de Dollars US)

Société	2018Chiffre d'affaires	2018Part de marché (%)	2017Chiffre d'affaires	2017Part de marché (%)	2018-2017Croissance (%)
Amazon	15,495	47.8	12,221	49.4	26.8
Microsoft	5,038	15.5	3,130	12.7	60.9
Alibaba	2,499	7.7	1,298	5.3	92.6
Google	1,314	4.0	820	3.3	60.2
IBM	577	1.8	463	1.9	24.7
Autres	7,519	23.2	6,768	27.4	11.1
Total	**32,441**	**100.0**	**24,699**	**100.0**	**31.3**

DAWAN – Reproduction interdite sans autorisation

TENDANCES DU CLOUD COMPUTING 6/6

- Amazon Web Services (AWS)

https://press.aboutamazon.com/news-releases/news-release-details/amazoncom-announces-first-quarter-sales-17-597-billion

- Microsoft Azure

https://www.microsoft.com/en-us/Investor/earnings/FY-2019-Q3/press-release-webcast

- Alibaba

https://www.alibabagroup.com/en/news/press_pdf/p190515.pdf

- Google Cloud Platform (GCP)

https://abc.xyz/investor/static/pdf/2019Q2_alphabet_earnings_release.pdf?cache=3d0a3db

- IBM

https://www.redhat.com/en/about/press-releases/ibm-closes-landmark-acquisition-red-hat-34-billion-defines-open-hybrid-cloud-future

DAWAN – Reproduction interdite sans autorisation

CLOUD OPEN SOURCES

- Nextcloud
- Eucalyptus
- OpenNebula
- OpenStack
- Niftyname
- Nimbus

LES DIFFÉRENTES BRIQUES 1/2

- ❑ IaaS
- ❑PaaS
- ❑SaaS

LES DIFFÉRENTES BRIQUES 2/2

QUELLE UTILISATION POUR LE IAAS?

- Exemple d'utilisation
  - Test et développement
  - Hébergement de site web
  - Sauvegarde externalisée,
  - PRA …

AVANTAGE DE IAAS

- Éliminer les dépenses d’investissement
- Réduire les coûts de fonctionnement
- Adaptation des ressources en fonction de l'activité

IaaS BENEFITS

No more equip to buy	Opex vs. Capex	Lower TCO
99.999% SLA Uptime	High Availability	Rapid Deployment
VMware Enterprise Plus	Flexible Infrastructure	Scalable Resources
Multi-Level Security	Reliability	Compliance
Trusted Partner	24 x 7 x 365 Support	Greener IT

DAWAN – Reproduction interdite sans autorisation

EXEMPLE DE PLATEFORME SAAS

- CRM
- Messagerie collaborative / visioconférence
- ERP

AVANTAGES DU SAAS

- Paiement en fonction de l’utilisation
- Gestion de l’infrastructure matérielle effectuée par le provider
- Disponibilité, sécurité, mises à jour, correctif à la charge du provider
- Mise en place d’un nouveau service très aisé
- Plus de licence à acheter
- Accès depuis n’importe quel endroit de la planète

DAWAN – Reproduction interdite sans autorisation

LE PAAS

- Plateforme d’exécution dans le cloud
- Exécution des applications de l’entreprise

EXEMPLE DE PLATEFORME PAAS

- Infrastructure de développement
- Analyse de données, Big data
- Externalisation d’une application développée en interne

AVANTAGES DU PAAS

- Maintenance de la plateforme matérielle par le provider
- L’entreprise peut exécuter et configurer ses propres applications
- Ressources matérielles adaptées en fonction du besoin

LES CONTEXTES D'EXTERNALISATION DU SI

CLOUD, PRIVE, PUBLIC

- France, 2015 – 2017 (en % de décideurs interrogés) - Echantillon : 100 décideurs ouverts au cloud computing

ARCHITECTURE CLOUD/HYBRIDE ET ON-PREMISE 1/2

	On-Premise	Cloud/Hybride
Dimensionnement	❑ Sur ou Sous dimensionnement	❑ A la demande (élasticité)
Coût	❑ Fixe (CAPEX)	❑ A l'utilisation (OPEX)
Maintenance	❑ Requiert une équipe d'expert (réseau, stockage, etc.)	❑ N/A

DAWAN – Reproduction interdite sans autorisation

ARCHITECTURE CLOUD/HYBRIDE ET ON-PREMISE 2/2

DAWAN – Reproduction interdite sans autorisation

- Module 1

DAWAN – Reproduction interdite sans autorisation

QU’EST-CE QUI S’EN VIENT?

❑Aperçu

- Qu'est-ce que le cloud? Qu'est-ce qu'AWS?
- Design de conception du cloud
- Un cadre bien conçu
- Infrastructure mondiale AWS
- Conception d’architecture à grande échelle.

DAWAN – Reproduction interdite sans autorisation

Le système d'exploitation Internet

DAWAN – Reproduction interdite sans autorisation

AMAZON.COM 1/3

- Nous sommes en 2000, le nouveau service de site Web d'achat Amazon.com a du mal à devenir hautement disponible et à évoluer efficacement.

DAWAN – Reproduction interdite sans autorisation

AMAZON.COM 2/3

- Les outils de e-commerce en ligne d'Amazon.com étaient « déstructurés":

- Les applications et les architectures ont été construites sans planification appropriée

- Les services devaient être séparés les uns des autres.

- **Solution**: Les outils sont devenus un ensemble d'APIs bien documentées. C'est qui est devenue la norme pour le développement de services chez Amazon.

DAWAN – Reproduction interdite sans autorisation

AMAZON.COM 3/3

- Problèmes persistants
  - Amazon.com avait toujours du mal à créer des applications rapidement.
  - La construction des composants de base de données, les machines et des stockages prennent 3 mois pour leur mise en place.
  - Chaque équipe Amazon construit ses propres ressources, sans planification d'échelle ou de réutilisation.
  - **Solution:** Création d'un service interne pour créer des architectures hautement disponibles, évolutives et fiables en plus de leur infrastructure. En 2006, ils ont commencé à vendre ces services sous le nom d'AWS.

DAWAN – Reproduction interdite sans autorisation

QU'EST-CE QUE LE CLOUD? QU'EST-CE QU'AWS?

Ressources programmables

Capacités dynamiques

Payez au fur et à mesure

- Quels autres avantages offre le cloud?

DAWAN – Reproduction interdite sans autorisation

SIX AVANTAGES DU CLOUD COMPUTING

Échangez une dépense en capital contre une dépense variable

Bénéficiez d'économies d'échelle massives

Arrêtez de deviner la capacité

Augmentez la vitesse et l'agilité

Concentrez-vous sur ce qui compte

Devenez mondial en quelques minutes

DAWAN – Reproduction interdite sans autorisation

AWS Well-Architected Framework

DAWAN – Reproduction interdite sans autorisation

THE AWS WELL-ARCHITECTED FRAMEWORK

Security | Reliability | Cost Optimization | Performance Efficiency | Operational Excellence

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

SÉCURITÉ

Fondement d'identité

Permettre la traçabilité

la sécurité à tous les niveaux

Stratégies d'évaluation et d'atténuation des risques.

DAWAN – Reproduction interdite sans autorisation

FIABILITÉ

- Acquérir dynamiquement des ressources informatiques pour répondre à la demande
- Récupérez rapidement des pannes d'infrastructure ou de service
- Atténuez les perturbations telles que:
  - Mauvaises configurations
  - Problèmes de réseau transitoires

DAWAN – Reproduction interdite sans autorisation

OPTIMISATION DES COÛTS

- Mesurer l'efficacité
- Éliminez les dépenses inutiles
- Envisagez d'utiliser des services gérés

DAWAN – Reproduction interdite sans autorisation

L'EXCELLENCE OPÉRATIONNELLE

- La possibilité d'exécuter et de surveiller des systèmes
- Pour améliorer continuellement le processus et les procédures de soutien.

Deployed

Updated

Operated

EFFICACITÉ DES PERFORMANCES

- Choisissez des ressources efficaces et maintenez leur efficacité à mesure que la demande évolue
- Démocratiser les technologies avancées
- Sympathie mécanique

DAWAN – Reproduction interdite sans autorisation

Infrastructure mondiale AWS

DAWAN – Reproduction interdite sans autorisation

CENTRES DE DONNÉES AWS

- Un seul centre de données héberge généralement des dizaines de milliers de serveurs
- Tous les centres de données sont en ligne, pas à "froids"
- Équipement de réseau personnalisé AWS:
  - Source Multi-ODM
  - Pile de protocoles réseau personnalisés.

DAWAN – Reproduction interdite sans autorisation

ZONES DE DISPONIBILITÉ AWS

Chaque zone de disponibilité est:

- Composé **d'un ou plusieurs** centres de données
- Conçu pour **l'isolation des défauts**
- Interconnecté avec d'autres zones de disponibilité à l'aide de liaisons **privées** à haut débit.

- Vous pouvez choisir vos zones de disponibilité

- AWS recommande de répliquer dans la zone de disponibilité pour la résilience

RÉGIONS AWS

Chaque région AWS est composée d'au moins **deux zones de disponibilité**.

- AWS a **21 régions** dans le monde
- Vous activez et contrôlez la **réplication des données** dans les régions
- La communication entre les régions utilise l'infrastructure de **réseau de base AWS**

RÉGIONS ACTUELLES DE L'INFRASTRUCTURE MONDIALE AWS

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

EMPLACEMENTS INFRASTRUCTURE MONDIAUX DE PÉRIPHÉRIQUES AWS

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS Identity and Access Management (IAM)

DAWAN – Reproduction interdite sans autorisation

Le besoin architectural

Votre organisation est assez grande maintenant que les membres se spécialisent dans des rôles. Vous avez besoin de la protection et du contrôle d'accès offerts par l'autorisation obligatoire.

Aperçu du module :

- Utilisateur, groupes et rôles IAM
- Gestion des identités fédérées
- Amazon Cognito
- Organisations AWS

DAWAN – Reproduction interdite sans autorisation

Utilisateurs de compte et IAM

DAWAN – Reproduction interdite sans autorisation

L'UTILISATEUR RACINE DU COMPTE AWS

Ce compte a un accès complet à tous les services et ressources AWS.

- détails de facturation
- Données personnelles
- Toute votre architecture et ses composants

L'utilisateur root du compte AWS a une puissance *extrême* et ne peut pas être limité

DAWAN – Reproduction interdite sans autorisation

UNE FAÇON PLUS SÛRE D'ADMINISTRER

Créer un utilisateur administrateur IAM

Verrouillez les informations d'identification de l'utilisateur root

Utiliser l'utilisateur administrateur IAM

DAWAN – Reproduction interdite sans autorisation

TOUT LE MONDE VEUT DIRIGER LE MONDE

Problème: vous devez être en mesure de restreindre l'accès de manière granulaire

AWS IDENTITY AND ACCES MANAGEMENT

- S'intègre à d'autres services AWS
- Gestion des identités fédérées
- Accès sécurisé pour les applications
- Autorisations granulaires

PRINCIPES D’IAM

UTILISATEUR IAM

UTILISATEUR FÉDÉRÉ

RÔLE IAM

FOURNISSEUR D'IDENTITÉ (idP)

DAWAN – Reproduction interdite sans autorisation

UTILISATEURS IAM

Les utilisateurs IAM ne sont pas des comptes AWS distincts, ce sont des utilisateurs de votre compte.

Chaque utilisateur a ses propres informations d'identification.

Les utilisateurs IAM sont autorisés à effectuer des actions AWS spécifiques en fonction de leurs autorisations.

LA CREATION D'UN UTILISATEUR IAM

Il n'y a pas d'autorisations par défaut

L'accès à l'AWS Management Console ou à la CLI doit être explicitement accordé

ACCORDER LA PERMISSION

- Une déclaration formelle d'une ou plusieurs autorisations
- Évalué au moment de la demande
- Stratégies IAM contrôle UNIQUEMENT l'accès aux services AWS
- IAM n'a pas de visibilité au-dessus de l'hyperviseur

Comment IAM détermine les autorisations:

ACCORDER LA PERMISSION

Policy

- Basé sur les ressources - Attaché à une ressource AWS
- Basé sur l'identité - Attaché à un principal IAM

DAWAN – Reproduction interdite sans autorisation

POLITIQUE BASÉE SUR L'IDENTITÉ

Politique basée sur l'identité

Attaché à:

- Utilisateur
- Groupe
- Rôle

Contrôle:

- Actions réalisées
- Quelles ressources
- Quelles conditions sont requises

Types de politiques:

- Géré par AWS
- Géré par le client
- En ligne

DAWAN – Reproduction interdite sans autorisation

POLITIQUES BASÉES SUR LES RESSOURCES

Politiques basées sur les ressources

Attaché à:

- Ressources AWS telles qu'Amazon S3, Amazon Glacier et AWS KMS

Contrôle:

- Actions autorisées par un mandataire spécifique
- Quelles conditions sont requises
- Sont toujours des politiques en ligne
- Aucune stratégie basée sur les ressources gérées par AWS

DAWAN – Reproduction interdite sans autorisation

IDENTITÉS AVEC AUTORISATIONS ATTACHÉES

APPLICATION DES AUTORISATIONS

EXEMPLE DE STRATÉGIE IAM 1/2

```
{
 "Version": "2012-10-17",
 "Statement":[{
 "Effect":"Allow",
 "Action":["dynamodb:*","s3:*"],
 "Resource":["arn:aws:dynamodb:region:account-number-without-hyphens:table/table-name",
 "arn:aws:s3:::bucket-name",
 "arn:aws:s3:::bucket-name/*"]
 },
 {
 "Effect":"Deny",
 "Action":["dynamodb:*","s3:*"],
 "NotResource":["arn:aws:dynamodb:region:account-number-without-hyphens:table/table-name",
 "arn:aws:s3:::bucket-name",
 "arn:aws:s3:::bucket-name/*"]
 }
 ]
}
```

EXEMPLE DE STRATÉGIE IAM 2/2

```
{
 "Version": "2012-10-17",
 "Statement":[{
 "Effect":"Allow",
 "Action":["dynamodb:*","s3:*"],
 "Resource":["arn:aws:dynamodb:region:account-number-without-hyphens:table/table-name",
 "arn:aws:s3:::bucket-name",
 "arn:aws:s3:::bucket-name/*"]
 },
 {
 "Effect":"Deny",
 "Action":["dynamodb:*","s3:*"],
 "NotResource":["arn:aws:dynamodb:region:account-number-without-hyphens:table/table-name",
 "arn:aws:s3:::bucket-name",
 "arn:aws:s3:::bucket-name/*"]
 }
 ]
}
```

Permets aux utilisateurs d'accéder à une table DynamoDB spécifique et ...

... un compartiment Amazon S3 spécifique et

Une **instruction de refus** explicite garantit que les principaux ne peuvent pas utiliser d'autres ressources DynamoDB ou S3 autres que la table et le compartiment spécifiés.

Une instruction de **refus explicite** est **prioritaire** sur une instruction d'autorisation.

Organisation de mes utilisateurs

DAWAN – Reproduction interdite sans autorisation

GROUPE D'UTILISATEURS IAM 1/4

GROUPE D'UTILISATEURS IAM 2/4

GROUPE D'UTILISATEURS IAM 3/4

GROUPE D'UTILISATEURS IAM 4/4

EN CAS D'UN TEST D'UNE JOURNÉE, QUE FAIRE?

Que faire si je ne souhaite pas continuer à ajouter ou à changer un utilisateur entre différents groupes?

Et si je ne souhaite pas donner des informations d'identification permanentes à quelqu'un ou à quelque chose?

DAWAN – Reproduction interdite sans autorisation

PRINCIPES D’IAM

UTILISATEUR IAM

UTILISATEUR FÉDÉRÉ

RÔLE IAM

FOURNISSEUR D'IDENTITÉ (idP)

DAWAN – Reproduction interdite sans autorisation

EN CAS D'UN TEST D'UNE JOURNÉE, QUE FAIRE?

Que faire si je ne souhaite pas continuer à ajouter ou à changer un utilisateur entre différents groupes?

Et si je ne souhaite pas donner des informations d'identification permanentes à quelqu'un ou à quelque chose?

DAWAN – Reproduction interdite sans autorisation

Fédérer les utilisateurs

RÔLES IAM 1/2

Un rôle vous permet de définir un ensemble d'autorisations pour accéder aux ressources dont un utilisateur ou un service a besoin.

- Les autorisations ne sont pas associées à un utilisateur ou à un groupe IAM.
- Les autorisations sont attachées à un rôle et le rôle est assumé par l'utilisateur ou le service.

DAWAN – Reproduction interdite sans autorisation

RÔLES IAM 2/2

Cas d'utilisation:

- Fournir aux ressources AWS un accès aux services AWS
- Fournir un accès aux utilisateurs authentifiés en externe
- Fournir l'accès à des tiers
- Changez de rôle pour accéder aux ressources dans:
    - Votre compte AWS
    - Tout autre compte AWS (accès entre comptes)

DAWAN – Reproduction interdite sans autorisation

ASSUMER UN RÔLE

AWS Management Console

AWS Command Line Interface (AWS CLI)

AssumeRole API call

AWS Security Token Service (AWS STS)

PRÉSENTATION DE STS IDENTITY BROKER

PROCESSUS IDENTITY BROKER STS

SAML

Enterprise (identity provider)
Service provider
aws
LDAP identity store
1 User browses to IdP
2 IdP authenticates user
Portal/ IdP
3 IdP returns SAML assertion
4 Post the SAML assertion to sign-in
5 Redirected to console
AWS sign-in

AMAZON COGNITO

Service entièrement géré qui fournit l'authentification, l'autorisation et la gestion des utilisateurs pour les applications Web et mobiles

- Groupes d'utilisateurs
- Pools d'identité

EXEMPLE AMAZON COGNITO

ZONE AWS

Une solution qui aide les clients à configurer plus rapidement un environnement AWS sécurisé et multi-compte basé sur les meilleures pratiques AWS, comprenant:

Structure multi-comptes

Distributeur automatique de compte

Accès utilisateur

Notifications

Comptes multiples

DAWAN – Reproduction interdite sans autorisation

De combien de comptes AWS votre organisation a-t-elle besoin?

Dev

Test

Production

DAWAN – Reproduction interdite sans autorisation

RECOMMANDATIONS AWS

One account – multiple VPCs

Multiple accounts – One VPC per account

PLUSIEURS COMPTES AWS

Peut être utilisé pour l'isolement:

- Unités commerciales distinctes, environnements de développement / test / production

Peut être utilisé pour la sécurité:

- Comptes séparés pour les charges de travail réglementées, différentes zones géographiques, régissant d'autres comptes

L'accès entre comptes n'est pas activé par défaut

DAWAN – Reproduction interdite sans autorisation

STRATÉGIES D'UTILISATION DE PLUSIEURS COMPTES AWS

Gestion centralisée de la sécurité	Compte AWS unique
Séparation des environnements de production, de développement et de test	Trois comptes AWS
Plusieurs départements autonomes	Plusieurs comptes AWS
Gestion centralisée de la sécurité avec plusieurs projets indépendants autonomes	Plusieurs comptes AWS

DAWAN – Reproduction interdite sans autorisation

UTILISATION DE PLUSIEURS COMPTES POUR LA GOUVERNANCE

COMMENT GÉRER TOUS CES COMPTES?

Gestion de compte centralisée

- Gestion de compte en groupe
- Accès basé sur des règles aux services AWS
- Création et gestion automatisées de comptes
- Facturation consolidée
- Basé sur l'API

DAWAN – Reproduction interdite sans autorisation

RECOMMANDATIONS AWS

ORGANISATIONS AWS: ILLUSTRÉES

SCHÉMA ARCHITECTURAL À GRANDE ÉCHELLE

L'ARCHITECTURE LA PLUS SIMPLE

Le besoin architectural

Vous venez de démarrer et avez besoin d'un moyen simple de distribuer, stocker et analyser les données de manière fiable dans le cloud.

Aperçu du module

- Problèmes qu'Amazon "Simple Storage Service" (Amazon S3) peut résoudre
- Meilleure efficacité du stockage
- Problèmes qu'Amazon Glacier peut résoudre
- Choisir une région

DAWAN – Reproduction interdite sans autorisation

Amazon S3

Le besoin architectural

Vous venez de démarrer et avez besoin d'un moyen simple de distribuer, stocker et analyser les données de manière fiable dans le cloud.

Aperçu du module

- Problèmes qu'Amazon "Simple Storage Service" (Amazon S3) peut résoudre
- Meilleure efficacité du stockage
- Problèmes qu'Amazon Glacier peut résoudre
- Choisir une région

DAWAN – Reproduction interdite sans autorisation

AMAZON S3 1/2

Stockage au niveau objet

Conçu pour une durabilité de 99,999999999%

Déclencheurs d'événements

AMAZON S3 2/2

Quels problèmes cela vous aide-t-il à résoudre?

DAWAN – Reproduction interdite sans autorisation

UTILISATION D'AMAZON S3 CAS 1

Stockage et distribution de contenu Web et de médias statiques

https://[bucket name].s3.amazonaws.com

https://[bucket name].s3.amazonaws.com/Video.mp4

AMAZON S3 CONTRÔLE D'ACCÈS - GENERAL

CONTRÔLE D'ACCÈS AMAZON S3 - STRATÉGIES DE COMPARTIMENT

Bucket Policies

```
{
  "Version": "2012-10-17",
  "Id": "S3PolicyId1",

  "Statement": [

    {
      "Sid": "IPAllow",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::examplebucket/*",
      "Condition": {
         "NotIpAddress": {"aws:SourceIp":
"54.240.143.0/24"}

      }
    }
  ]
}
```

AWS Policy Generator

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

POINTS D'ACCÈS AMAZON S3

Les points d'accès Amazon S3 sont des noms d'hôte uniques avec des stratégies d'accès dédiées qui décrivent comment accéder aux données à l'aide de ce point de terminaison.

Ces points prennent en charge:

- Utilisateur unique
- Applications
- Groupes d'utilisateurs ou d'applications

DAWAN – Reproduction interdite sans autorisation

UTILISATION D'AMAZON S3 CAS 2

Héberger des sites Web statiques entiers

Fichiers HTML, images, vidéos et scripts cotés client

DAWAN – Reproduction interdite sans autorisation

UTILISATION D'AMAZON S3 CAS 1

Stockage et distribution de contenu Web et de médias statiques.

https://[bucket name].s3.amazonaws.com

https://[bucket name].s3.amazonaws.com/Video.mp4

UTILISATION D'AMAZON S3 CAS 2

Héberger des sites Web statiques entiers

Fichiers HTML, images, vidéos et scripts cotés client

DAWAN – Reproduction interdite sans autorisation

GESTION DES VERSIONS D'AMAZON S3

* Envisagez d'utiliser le verrouillage d'objet S3 pour la conservation ou la protection des données

CONTRÔLE D'ACCÈS AMAZON S3 - CORS

```
<CORSConfiguration>
 <CORSRule>
  <AllowedOrigin>http://www.example.com</AllowedOrigin>
  <AllowedMethod>PUT</AllowedMethod>
  <AllowedMethod>POST</AllowedMethod>
  <AllowedMethod>DELETE</AllowedMethod>
  <AllowedHeader>*</AllowedHeader>
 <MaxAgeSeconds>3000</MaxAgeSeconds>
 <ExposeHeader>x-amz-server-side-encryption</ExposeHeader>
 <ExposeHeader>x-amz-request-id</ExposeHeader>
 <ExposeHeader>x-amz-id-2</ExposeHeader>
 </CORSRule>
</CORSConfiguration>
```

UTILISATION AMAZON S3 CAS 3

Magasin de données pour le calcul et l'analyse à grande échelle

Analyse des transactions financières

Analyse du flux de clics

Transcodage multimédia

UTILISATION D'AMAZON S3 CAS 4

Outil de sauvegarde

DÉPLACEMENT DE DONNÉES DANS AMAZON S3

MULTIPLE TÉLÉCHARGEMENT AVEC AMAZON S3 1/2

MULTIPLE TÉLÉCHARGEMENT AVEC AMAZON S3 2/2

ACCÉLÉRATION DE TRANSFERT AMAZON S3

DÉPLACEMENT DE DONNÉES DANS AMAZON S3

AWS Snowball

Transport de données à l'échelle du pétaoctet

AWS Snowball

Transport de données à l'échelle de l'exaoctet

DAWAN – Reproduction interdite sans autorisation

QUAND DEVRIEZ-VOUS UTILISER AMAZON S3?

Meilleurs cas d'utilisation
Lorsque vous devez écrire une fois, lisez plusieurs fois.
Accès aux données épineux.
Grand nombre d'utilisateurs et diverses quantités de contenu.
Ensembles de données croissants.

Cas d'utilisation déconseillés
Blocage des exigences de stockage
Changement fréquent des données
Stockage d'archives à long term

COÛTS AMAZON S3

Payez uniquement ce que vous utilisez y compris:

Go par mois

Transfert vers d'autres régions ou sur Internet.

METTRE, COPIER, PUBLIER, LISTER et LIRE de requêtes

Vous n'avez PAS à payer pour:

Transfert vers Amazon S3

Transférer vers Amazon EC2 dans la même région ou vers CloudFront

Amazon S3 Glacier

DAWAN – Reproduction interdite sans autorisation

AMAZON S3 GLACIER

Stockage de données à long terme

Archivage ou sauvegarde

Stockage à très faible coût

ARCHIVAGES ET COFFRES-FORTS AMAZON S3 GLACIER

DAWAN – Reproduction interdite sans autorisation

COÛTS LIÉS À AMAZON S3 GLACIER

Récupération des données d'Amazon Glacier

Récupération accélérée

Récupération standard

Récupération en masse

DAWAN – Reproduction interdite sans autorisation

CLASSES DE STOCKAGE AMAZON S3 / AMAZON S3 GLACIER

S3 Standard:
Frequently accessed data

S3 Standard IA:
Long-lived, infrequently accessed data

S3 One Zone IA:
Long-lived, infrequent, but rapid access

Amazon Glacier / Deep Archive:
Archiving rarely accessed data

Amazon S3 Intelligent Tiering
Automatically moves your objects between two access tiers of storage

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

POLITIQUES DE CYCLE DE VIE 1/4

Les stratégies de cycle de vie Amazon S3 vous permettent de supprimer ou de déplacer des objets en fonction de leur âge.

POLITIQUES DE CYCLE DE VIE 2/4

Les stratégies de cycle de vie Amazon S3 vous permettent de supprimer ou de déplacer des objets en fonction de leur âge.

POLITIQUES DE CYCLE DE VIE 3/4

Les stratégies de cycle de vie Amazon S3 vous permettent de supprimer ou de déplacer des objets en fonction de leur âge.

POLITIQUES DE CYCLE DE VIE 4/4

Les stratégies de cycle de vie Amazon S3 vous permettent de supprimer ou de déplacer des objets en fonction de leur âge.

Choisir des régions pour vos architectures

DAWAN – Reproduction interdite sans autorisation

CHOISIR UNE RÉGION 1/4

Stockage des données et conformité réglementaire

Existe-t-il des lois régionales sur la confidentialité des données?

Les données client peuvent-elles être stockées en dehors du pays?

Pouvez-vous respecter votre obligation de gouvernance?

DAWAN – Reproduction interdite sans autorisation

CHOISIR UNE RÉGION 2/4

Proximité des utilisateurs aux données

De petites différences de latence peuvent avoir un impact sur l'expérience client

Choisissez la région la plus proche de vos utilisateurs

Disponibilité des services et fonctionnalités

Certains services ne sont pas encore disponibles dans toutes les régions

Peut utiliser certains services interrégionale, mais avec une latence accrue

Service étendu à de nouvelles régions régulièrement

DAWAN – Reproduction interdite sans autorisation

CHOISIR UNE RÉGION 4/4

Rentabilité

- Les coûts varient selon la région
- Certains services comme Amazon S3 ont des coûts de transfert de données
- Considérez la rentabilité de la réplication de l'environnement intégrale dans une autre région

DAWAN – Reproduction interdite sans autorisation

Ajout d'une couche de calcul.

DAWAN – Reproduction interdite sans autorisation

AJOUT DE LA COUCHE DE CALCUL

Le besoin architectural

Vous devez exécuter des applications qui seront utilisées par un nombre d'utilisateurs cohérent, mais restreint.

Vue d'ensemble du module

- Amazon Elastic Compute Cloud (Amazon EC2)
- Types et familles d'instances
- Volumes Amazon Elastic Block Store (Amazon EBS)
- Options de conformité

DAWAN – Reproduction interdite sans autorisation

Ajout des machines avec Amazon EC2

DAWAN – Reproduction interdite sans autorisation

À QUELS BESOINS AMAZON EC2 PEUT-IL RÉPONDRE?

hébergement Web

Bases de données

Authentification

Tout ce qu'un serveur peut faire

MACHINES VIRTUELLES ET SERVEURS PHYSIQUES

Amazon EC2 peut résoudre certains problèmes qui sont plus difficiles avec un serveur sur site.

Lors de l'utilisation de ressources temporaire

Décisions basées sur les données

Itérations rapides

Libre de faire des erreurs

Lancement d'instances AMAZON EC2 avec Amazon Machine Images (AMIs)

AMAZON EC2 ET AMIs 1/2

AMAZON EC2 ET AMIs 2/2

COMMENT OBTENIR UNE « AMI »?

HOW DO AMIs HELP?

Repeatability

Reusability

Recoverability

Marketplace Solutions

Backups

GÉNÉRATEUR D'IMAGES EC2

EC2 Image Builder simplifie la création, la maintenance, la validation, le partage et le déploiement d'images de serveur Linux ou Windows

Image source → Générateur d'image EC2 → Personnaliser le logiciel installé sur l'image → Image source avec des modèles fournis par AWS ou personnalisés → Images de test → Distribution de l'image

Lancement d'instances AMAZON EC2 avec Amazon Machine Images (AMIs)

LANCEMENT D'INSTANCES EC2 AVEC DES DONNÉES UTILISATEUR

RÉCUPÉRATION D'INFORMATIONS SUR VOTRE INSTANCE EC2 AVEC INSTANCE METATADA 1/2

Metadata	Value
instance-id	i-1234567890abcdef0
mac	00-1B-63-84-45-E6
public-hostname	ec2-203-0-113-25.compute-1.amazonaws.com
public-ipv4	67.202.51.223
local-hostname	ip-10-251-50-12.ec2.internal
local-ipv4	10.251.50.12

RECUPERATION D'INFORMATIONS SUR VOTRE INSTANCE EC2 AVEC INSTANCE METATADA 2/2

Metadata	Value
instance-id	i-1234567890abcdef0
mac	00-1B-63-84-45-E6
public-hostname	ec2-203-0-113-25.compute-1.amazonaws.com
public-ipv4	67.202.51.223
local-hostname	ip-10-251-50-12.ec2.internal
local-ipv4	10.251.50.12

Amazon EC2 et le stockage des données

Quels sont les problèmes résolus par Amazon Elastic Block Store (Amazon EBS)?

L'application nécessite un stockage au niveau du bloc

Le magasin d'instances est éphémère

Besoin des données persistant pendant les arrêts

Besoin de sauvegarder des volumes de données.

Gardez à l'esprit : Plusieurs volumes d'Amazon EBS peuvent se trouver sur la même instance, mais chaque volume ne peut être associé qu'à une seule instance à la fois.

TYPES DE VOLUMES AMAZON EBS 1/2

Solid-State Backed

Volume Type	SSD à usage général (gp2)	SSD IOPS provisionné (io1)
Description	Volume SSD à usage général qui équilibre le prix et les performances pour une grande variété de charges de travail	Volume SSD le plus performant pour les charges de travail critiques à faible latence ou à haut débit
Cas d'utilisation	• Recommended for most workfload	• Critical business applications that require sustained IOPS performance • Large database workfload

DAWAN – Reproduction interdite sans autorisation

TYPES DE VOLUMES AMAZON EBS 2/2

Hard-Disk Backed

Volume Type	Disque dur à débit optimisé (st1)	Disque dur froid (sc1)
Description	Volume de disque dur à faible coût conçu pour une utilisation fréquente et exigeante en débit	Volume de disque dur le plus économique, conçu pour le moins des charges de travail et très peu d'utilisation
Cas d'utilisation	• Streaming workfloads • Big Data • Data warehouses • Log processing • Cannot be a boot volume	• Throughput-oriented storage for large volumes of data that is infrequently accessed • Scenarios where the lowest storage cost is important • Cannot be a boot volume

DAWAN – Reproduction interdite sans autorisation

INSTANCES OPTIMISÉES POUR AMAZON EBS

EBS Optimized Instance

- Optimized configuration stack
- Additional dedicated capacity for Amazon EBS I/O
- Minimizes contention between Amazon EBS and other traffic
- Options between 425 Mbps and 14,000 Mbps

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

SYSTÈMES DE FICHIERS PARTAGÉS

Que faire si plusieurs instances doivent utiliser le même stockage?

Amazon EBS only attaches to one instance

Amazon S3 is an option but is not ideal

Amazon EFS and Amazon FSx are perfect for this task

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AMAZON ELASTIC FILE SYSTEM (EFS)

Amazon EFS
(Linux Workloads)

NFSv4 protocol

Shared Across

- Availability Zones
- Regions
- VPCs
- Account

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AMAZON FSx

Amazon FSx (Windows Workloads)

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Shared Access

- AWS Accounts
- VPC's
- AWS Regions
- AWS Availability Zones

Amazon FSx (Lustre Workloads)

SYSTÈMES DE FICHIERS PARTAGÉS

Que faire si plusieurs instances doivent utiliser le même stockage?

Amazon EBS only attaches to one instance

Amazon S3 is an option but is not ideal

Amazon EFS and Amazon FSx are perfect for this task

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Types d'instances Amazon EC2

DAWAN – Reproduction interdite sans autorisation

EC2 INSTANCES – QUE TROUVE-T-ON DANS UN NOM?

m5.large

m is the family name

5 Is the generation number

large is the size of the instance

Examples

t2.large

c5.xlarge

p3.2xlarge

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

EC2 INSTANCES - SIZES

Model	vCPU
m5.large	2
m5.xlarge	4
m5.2xlarge	8
m5.4xlarge	16
m5.12xlarge	48
m5.24xlarge	96

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

EC2 INSTANCES – TYPES 1/2

Le choix du bon type est très important pour:

Efficient utilization of your instances

Reducing unneeded cost

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

EC2 INSTANCES – TYPES 2/2

General Purpose	A1, T3, T3a, T2, M6g, M5, M5a, M5n, M4
Compute Optimized	C5, C5n, C4
Memory Optimized	R5, R5a, R5n, R4, X1e, X1, High Mem., z1d
Accelerated Computing	P3, P2, Inf1, G4, G3, F1
Storage Optimized	I3, I3en, D2, H1

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

EC2 - EXEMPLE À USAGE GÉNÉRAL

Good for burstable workloads like website and web applications

Model	vCPU	Baseline Performance/vCPU	CPU Credits / Hour	Mem (GiB)	Storage
t3.nano	2	5%	6	0.5	EBS-Only
t3.micro	2	10%	12	1	EBS-Only
t3.small	2	20%	24	2	EBS-Only
t3.medium	2	20%	24	4	EBS-Only
t3.large	2	30%	36	8	EBS-Only
t3.xlarge	4	40%	96	16	EBS-Only
t3.2xlarge	8	40%	192	32	EBS-Only

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

EC2 - EXEMPLE OPTIMISÉ POUR LE CALCUL

Optimized for compute-intensive workloads

Model	vCPU	Mem (GiB)	Storage	EBS Bandwidth (Mbps)
c5.large	2	4	EBS-Only	Up to 2,250
c5.xlarge	4	8	EBS-Only	Up to 2,250
c5.2xlarge	8	16	EBS-Only	Up to 2,250
c5.4xlarge	16	32	EBS-Only	2,250
c5.9xlarge	36	72	EBS-Only	4,500
c5.18xlarge	72	144	EBS-Only	9,000

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

EC2 - EXEMPLE D'OPTIMISATION DE LA MÉMOIRE

Memory heavy applications or when you need more RAM than CPU

Model	vCPU	Mem (GiB)	Storage (GiB)	Dedicated EBS Bandwidth (Mbps)	Networking Performance (Gbps)
r5.large	2	16	EBS-Only	up to 3,500	Up to 10
r5.xlarge	4	32	EBS-Only	up to 3,500	Up to 10
r5.2xlarge	8	64	EBS-Only	up to 3,500	Up to 10
r5.4xlarge	16	128	EBS-Only	3,500	Up to 10
r5.12xlarge	48	384	EBS-Only	7,000	10
r5.24xlarge	96	768	EBS-Only	14,000	25

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

EC2 - EXEMPLE D'OPTIMISATION DU CPU

Performant GPU-based instances

Commonly used for machine/deep learning

Model	GPUs	vCPU	Mem (GiB)	GPU Mem (GiB)	GPU P2P
p3.2xlarge	1	8	61	16	-
p3.8xlarge	4	32	244	64	NVLink
p3.16xlarge	8	64	488	128	NVLink
p3.dn24x	12	96	768	256	NVLink

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

EC2 - EXEMPLE D'OPTIMISATION DU STOCKAGE

Up to 16 TB of HDD-based local storage with high disk throughput

Model	vCPU	Mem (GiB)	Networking Performance	Instance Storage (GB)
h1.2xlarge	8	32	Up to 10 Gigabit	1 x 2,000 HDD
h1.4xlarge	16	64	Up to 10 Gigabit	2 x 2,000 HDD
h1.8xlarge	32	128	10 Gigabit	4 x 2,000 HDD
h1.16xlarge	64	256	25 Gigabit	8 x 2,000 HDD

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

PROCESSEURS INTEL XEON ET INSTANCES EC2 1/2

All current EC2 instance types include:

- Intel AES-NI: Reduces performance hit due to encryption
- Intel AVX (AVX2, AVX-512): Improve floating-point performance. Only available on HVM deployments.

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

GÉNÉRATIONS ET COÛT DES INSTANCES

Les instances de nouvelle génération ont généralement de meilleurs rapports performance / prix

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Options de tarification Amazon EC2

DAWAN – Reproduction interdite sans autorisation

EC2 PRINCING OPTIONS

On-Demand Instances

Reserved Instances

Savings Plans

Spot Instances

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

ON-DEMAND INSTANCE 1/2

- Pay for compute capacity per second (Amazon Linux and Ubuntu) or by the hour (all other OS)
- No long-term commitments
- No upfront payments
- Increase or decrease your compute capacity depending on the demands of your application

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

ON-DEMAND INSTANCE 2/2

- Pay for compute capacity per second (Amazon Linux and Ubuntu) or by the hour (all other OS)
- No long-term commitments
- No upfront payments
- Increase or decrease your compute capacity depending on the demands of your application

Résout le besoin de capacité de calcul immédiate

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

RESERVED INSTANCES 1/2

Can provide a significant discount for your architectures.

- Pre-pay for capacity
- Standard RI, Convertible RIs, Scheduled RIs
- Three upfront payment methods
- Can be shared between multiple accounts (within a billing family)

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

RESERVED INSTANCES 2/2

Can provide a significant discount for your architectures.

- Pre-pay for capacity
- Standard RI, Convertible RIs, Scheduled RIs
- Three upfront payment methods
- Can be shared between multiple accounts (within a billing family)

Offre la possibilité de réserver la capacité à l'avance, ce qui réduit les coûts

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

SAVINGS PLANS 1/2

- Compute Savings Plans provide the most flexibility and help to reduce your costs by up to 66%
- EC2 Instance Savings Plans apply to a specific instance family within a Region and provide the largest discount (up to 72%, just like Standard RIs)

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

SAVINGS PLANS 2/2

- Compute Savings Plans provide the most flexibility and help to reduce your costs by up to 66%
- EC2 Instance Savings Plans apply to a specific instance family within a Region and provide the largest discount (up to 72%, just like Standard RIs)

Pas besoin de coordonner vos achats RI

DAWAN – Reproduction interdite sans autorisation

SPOT INSTANCE 1/2

- Purchase unused Amazon EC2 capacity
- No more bidding! – prices based on long term trends of supply & demand
- Interruption notice provided 2 minutes prior to instance termination
- Flexibility is the key to success

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

SPOT INSTANCE 2/2

- Purchase unused Amazon EC2 capacity
- No more bidding! – prices based on long term trends of supply & demand
- Interruption notice provided 2 minutes prior to instance termination
- Flexibility is the key to success

Spot peut offrir jusqu'à 90% de réduction sur les prix à la demande. Les instances Spot sont appropriées pour les charges de travail sans état et tolérantes aux pannes.

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AMAZON EC2 DEDICATED OPTIONS

Dedicated Instances

Dedicated Hosts

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AMAZON EC2 DEDICATED INSTANCES 1/2

Dedicated Instances

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AMAZON EC2 DEDICATED INSTANCES 2/2

Dedicated Instances

Dedicated instances are physically isolated from other AWS accounts

Helps meet requirements for regulatory compliance or software license use

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AMAZON EC2 DEDICATED HOSTS 1/2

Dedicated Hosts

A *dedicated host* is a full physical server with EC2 instance capacity fully dedicated to your use.

Host ID: h-039725dyhe980010

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AMAZON EC2 DEDICATED HOSTS 2/2

Dedicated Hosts

A *dedicated host* is a full physical server with EC2 instance capacity fully dedicated to your use.

Host ID: h-039725dyhe980010

Helps meet *strict* requirements for regulatory compliance or software license use

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AMAZON EC2 TENANCY

	Only your AWS account on the hardware?	Description
Default	No	Your instance runs on shared hardware.
Dedicated Instance	Yes	Runs on a non-specific piece of hardware.
Dedicated Host	Yes	Runs on a specific piece of hardware of your choosing, over which you receive greater control.

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS COMPUTE OPTIMIZER

AWS Compute Optimizer recommends optimal AWS compute resources for your workloads to reduce costs and improve performance by using machine learning to analyze historical utilization metrics.

Lower costs by up to 25%

Optimize performance with actionable recommendations

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

GARDER UNE TRACE DE VOTRE INSTANCE

Assign metadata **tags** to your AWS resources to help you:

Manage

Search

Filter

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

BONNES PRATIQUES SUR LE TAG

- Format standardisé et sensible à la casse pour les balises
- Mettre en œuvre des outils automatisés pour aider à gérer les ressources des balises
- Préférez utiliser trop de balises plutôt que trop peu
- N'oubliez pas qu'il est facile de modifier les balise
- Exemples: Version de l'application, ENV, Nom DNS, identifiant de la pile d'applications

Vous aide à comprendre ce que font vos ressources et leur impact sur les coûts

DAWAN – Reproduction interdite sans autorisation

Amazon EC2 Considerations

DAWAN – Reproduction interdite sans autorisation

ARCHITECTURAL CONSIDERATIONS 1

Does your compute layer require the lowest latency and highest packet-per-second network performance possible?

Cluster Placement Groups

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

ARCHITECTURAL CONSIDERATIONS 2

Do you have applications that have a small number of critical instances that should be kept separate from each other?

Spread Placement Groups

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

ARCHITECTURAL CONSIDERATIONS 3

Do you have large distributed and replicated workloads such as HDFS, HBase and Cassandra running on EC2?

Partition Placement Groups

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

RTO/RPO and Backup Recovery Setup

DAWAN – Reproduction interdite sans autorisation

Automation

The architectural need

You need to start automating to keep growing. Your organization has many different architectures and needs a way to consistently deploy, manage, and update them.

Module Overview

- Why Automate?
- Automating Infrastructure
- Automating Deployment

DAWAN – Reproduction interdite sans autorisation

Why Should You Automate?

Without Automation

Long manual process to build an architecture

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Risks from Manual Processes

In Genral

If you have to manually change something in your production environment,
you are putting yourself at risk.

Manual processes are risks without reward.

Automating Your Infrastructure

DAWAN – Reproduction interdite sans autorisation

Automation of Your Infrastructure

AWS CloudFormation

Provides a common language to describe your AWS infrastructure

Creates and builds those described resources in an automated manner

How Does It Work?

AWS CloudFormation templates

- JSON/YAML formatted file describing the resources to be created
- Treat it as source code: Put it in your repository
- Import existing resources

JSON

```
{
  "Resources" : {
    "HelloBucket" : {
      "Type" : "AWS::S3::Bucket"
    }
  }
}
```

YAML

```
Resources:
 HelloBucket:
  Type: AWS::S3::Bucket
```

Infrastructure as Code (IaC)

AWS Cloud formation supports drift detection

Benefits of IaC

AWS CloudFormation Conditions

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

How Do I Update My Stacks?

Use a DeletionPolicy to preserve or backup a resource when its stack is deleted or updated.

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

A layered architecture

Front end	CRM web interface, admin interface, analytics dashboard
Backend	Customers, campaigns, products, marketing collateral, analytics
Shared	CRM DBs, common monitoring/alarms, subnets, security groups
Base network	VPCs, internet gateways, VPNs, NATs
Identity	IAM users, groups, roles

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS Quick Starts

Standardized templates

AWS CloudFormation templates
built by AWS Solutions Architects

- Gold-standard deployments in the AWS Cloud
- Based on AWS best practices for security and high availability
- Create entire architectures with one click in less than an hour
- Great for experimentation and building off

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Automating Deployments

Ho Do You Modify Your Fleet ?

Systems Manager

AWS Systems Manager

A set of capabilities that enable **automated configuration** and **ongoing management of systems at scale**

- Across all of your Windows and Linux workload
- Runs in Amazon EC2 or on-premises

What Can It Do?

Run Command

Maintenance Windows

Patch Management

State Manager

Session Manager

Inventory

AWS OpsWorks for Infrastructure and Deployment Automation

Configuration management services

- AWS OpsWorks Stacks
- AWS OpsWorks for Chef Automate
- AWS OpsWorks for Puppet Enterprise

OpsWorks Stacks Has Lifecycle Events

AWS OpsWorks Stacks

Allows you to run scripts on these triggers:

Setup occurs on a new instance after it successfully boots.

Configure occurs on all of the stack's instances when an instance enters or leaves the online state.

Deploy occurs when you deploy an app.

Undeploy occurs when you delete an app.

Shutdown occurs when you stop an instance.

Using AWS OpsWorks Stacks with AWS CloudFormation

Use AWS CloudFormation to build infrastructure (VPC, IAM roles), and deploy the application layer with AWS OpsWorks Stacks.

A Little More Hands Off

DAWAN – Reproduction interdite sans autorisation

General Challenges

- Managing infrastructure around deploying an app can be difficult
- It can take a lot of time to manage and configure servers
- Lack of consistency across multiple projects or applications

DAWAN – Reproduction interdite sans autorisation

AWS Elastic Beanstalk

AWS Elastic Beanstalk

Provisions and operates the infrastructure and manages the application stack for you

Completely transparent—you can see everything that is created

Impossible to outgrow; automatically scales your application up and down

What Do You Control?

Elastic Beanstalk - Environment

Elastic Beanstalk provisions necessary infrastructure resources

Elastic Beanstalk provides you with a unique domain name for your application environment (e.g., yourapp.elasticbeanstalk.com).

- You can resolve your own domain name to this domain name with Route 53

Choosing the Right Solution

ANNEXE

Merci!

RGPD

- Protection des données
  - **Le Cloud Computing , c'est dangereux?**
  - **Modèle Clause de confidentialité:**

https://www.cnil.fr/sites/default/files/typo/document/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf

  - **Comprendre le RGPD**

https://www.cnil.fr/fr/comprendre-le-rgpd

  - **Règlement général**

https://www.cnil.fr/fr/reglement-europeen-protection-donnees

  - **Cloud Act**

https://www.lemagit.fr/conseil/Quelles-differences-entre-CLOUD-Act-et-PARTIOT-Act-et-quels-impacts-sur-les-entreprises-francaises

DAWAN – Reproduction interdite sans autorisation
DAWAN – Reproduction interdite sans autorisation

Glossaire

- **IaaS :** infrastructure as a service
- **PaaS :** platform as a service
- **SaaS** : software as a service
- **DaaS :** Desktop as a service
- **BaaS:** Backend as a service ou Backup as a service
- **Naas :** Network as a service
- **Staas:** Storage as a service
- CassCommunication as a service
- **WaaS:** Workplace as a service
- **MBaaS :** Mobile backend as a service
- **CC:** Cloud Computing
- **VHD:** Virtual Hard Disk
- **AWS:** Amazon Web Services
- **IBM:** International Business Machines
- **OpenStack :** un ensemble de logiciels open source permettant de déployer des infrastructures de cloud computing
- **Docker :** logiciel libre permettant de lancer des applications dans des conteneurs logiciels.
- **Ansible** et **Puppet :** plate-forme logicielle libre pour la configuration et la gestion des ordinateurs.
- **Terraform :** un environnement logiciel "d'infrastructure as code" publié en open-source
- **Big data :** les métadonnées ou les données massives, désigne des ensembles de données devenus si volumineux
- **Clouds Publics :** constituent l'option de déploiement de cloud la plus courante. Les ressources cloud (telles que les serveurs et le stockage) sont détenues et exploitées par un fournisseur de service cloud tiers
- **Cloud privé :** consiste en l'ensemble des ressources de calcul qu'une entreprise ou une organisation utilisent en exclusivité.
- **Cloud hybride :** combine une infrastructure locale, ou cloud privé, avec un cloud public, de façon à ce que l'organisation puisse profiter des deux
- **GCP:** Google Cloud Platform
- **PRA :** plan de reprise d'activité
- **PCA :** plan de continuité d'activité
- **QOS :** quality of service
- **RTO:** Recovery Time Objective
- **RPO:** Recovery Point Objective
- **P2V :** Physical To Virtual
- **VDI :** Virtual Desktop
- **RDS :** Remote Desttop Service
- **SND:** Software Defined Network
- **NFV**: Network Function Virtualization
- **VM :** Virtual Machine

DAWAN – Reproduction interdite sans autorisation
DAWAN – Reproduction interdite sans autorisation

Documentations

- https://siliconangle.com/2017/02/20/wikibon-report-preview-big-can-amazon-web-services-get/
- https://www.marketwatch.com/story/amazon-rules-the-public-cloud-but-google-microsoft-alibaba-are-growing-faster-2017-12-20
- https://cloud.google.com/compute/docs/machine-types
- https://aws.amazon.com/fr/ec2/instance-types/
- http://cloudharmony.com/speedtest-for-aws:ec2
- http://www.gcping.com/
- https://www.cloudping.info/
- https://cloudharmony.com/speedtest
- https://docs.aws.amazon.com/fr_fr/IAM/latest/UserGuide/introduction.html
- https://calculator.s3.amazonaws.com/index.html
- https://www.wellarchitectedlabs.com/
- https://aws.amazon.com/fr/tools/ - outils
- https://docs.aws.amazon.com/whitepapers/latest/aws-overview/aws-overview.pdf#introduction
- http://comparecloud.in/
- https://aws.amazon.com/fr/architecture/icons/
- https://aws.amazon.com/fr/s3/faqs/
- https://aws.amazon.com/fr/s3/pricing/
- https://calculator.aws/
- https://www.ec2instances.info/
- https://www.ec2instances.info/?selected=h1.8xlarge
- http://selec2or.info/

- https://docs.aws.amazon.com/fr_fr/IAM/latest/UserGuide/introduction.html
- https://docs.aws.amazon.com/fr_fr/IAM/latest/UserGuide/id_credentials_mfa.html#id_credentials_mfa-what-is-mfa
- https://authy.com/

- https://docs.saltproject.io/en/3000/topics/cloud/aws.html
- https://puppet.com/integrations/aws/
- https://docs.ansible.com/ansible/latest/scenario_guides/guide_aws.html
- https://aws.amazon.com/fr/cloudformation/faqs/
- https://connect.ed-diamond.com/GNU-Linux-Magazine/GLMF-216/Infrastructure-As-Code-sous-AWS-avec-Terraform
- https://docs.aws.amazon.com/powershell/latest/userguide/pstools-getting-set-up-windows.html#ps-installing-awswindowspowershell
- https://docs.aws.amazon.com/powershell/latest/reference/Index.html
- https://aws.amazon.com/fr/#lang/fr_fr

- https://docs.aws.amazon.com/sdk-for-php/v3/developer-guide/getting-started_installation.html

DAWAN – Reproduction interdite sans autorisation
DAWAN – Reproduction interdite sans autorisation