FARONICS™ Cloud

Architecture et sécurité - Vue d’ensemble

Introduction

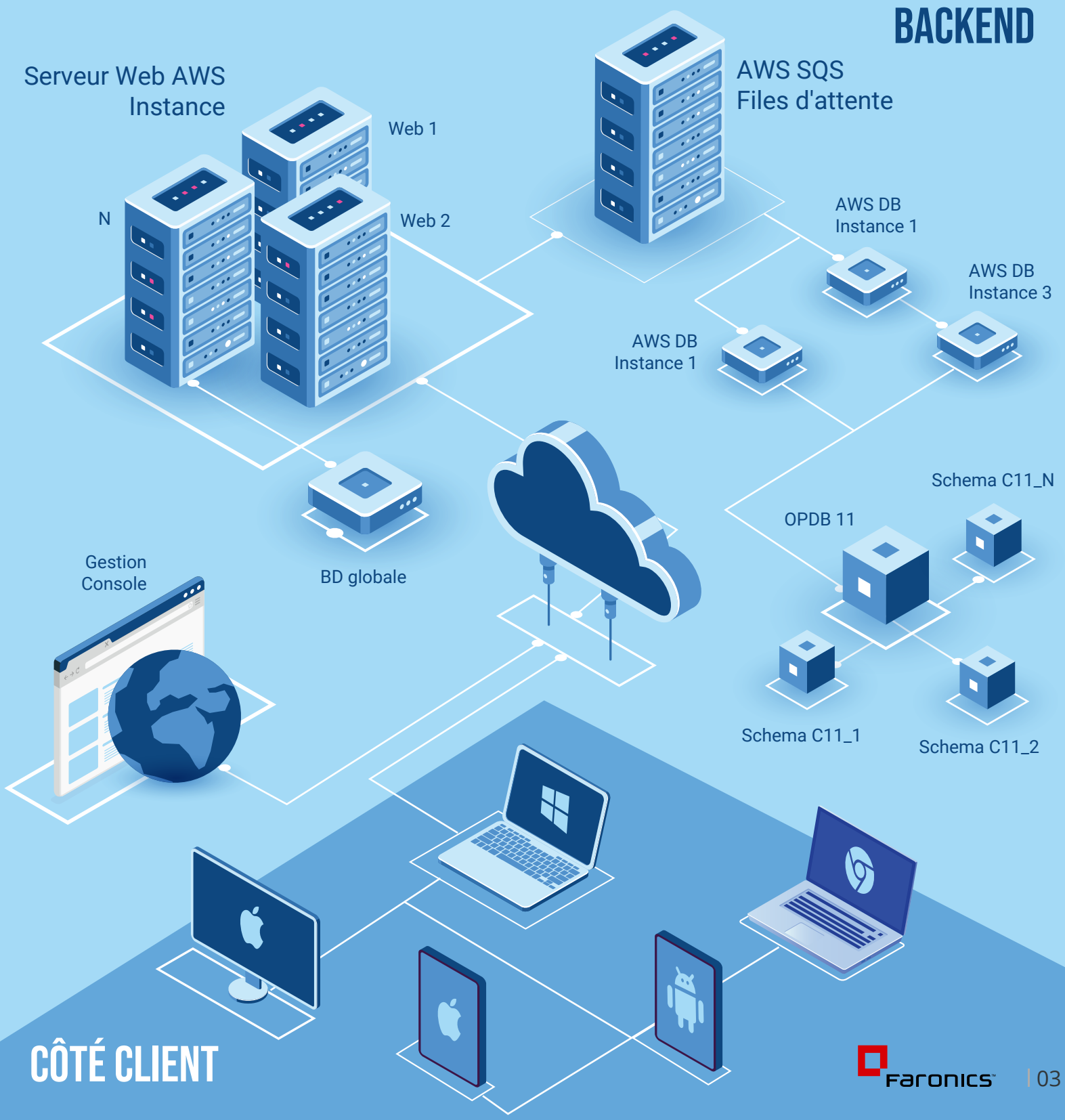
Faronics Cloud se rapporte à Faronics Cloud Deep Freeze et Faronics Cloud Deploy (ci-après appelés “Faronics Cloud”).

Faronics Cloud est une plateforme unifiée qui permet à ses clients de simplifier la gestion de leurs terminaux via Internet. Elle incorpore un large éventail de services, tels que la gestion des PC et des Mac, la gestion des appareils mobiles, un antivirus, une gestion des applications par liste blanche, la protection des données, l'administration d'actifs, la gestion de l'énergie et bien plus.

Ce document fournit une vue d'ensemble de haut niveau de l'architecture cloud de Faronics. Il décrit comment la sécurité et la confidentialité des données des clients sont sécurisées par toutes les parties concernées dans le cadre du modèle de responsabilité partagée. Ce document décrit également les politiques, les processus et les pratiques de sécurité que l'équipe Faronics applique pour assumer ses propres responsabilités en matière de sécurité du nuage Faronics.

Architecture - Vue d'ensemble

Faronics Cloud est constitué de deux parties principales :
Composants côté client et composants côté dorsal (backend).



Composants côté client

Chaque ordinateur géré (client) contient un agent cloud et divers services, comme spécifié dans les paramètres de la politique du client. Pour certains services spécifiques, le client peut, en option, installer un ordinateur à rôle de serveur de cache dans son réseau local afin d'économiser la bande passante. Les administrateurs système accèdent à la console de gestion via leur navigateur Internet.

Composants Backend

Les éléments du backend de Faronics Cloud sont hébergés sur Amazon Web Services (AWS). L'environnement de production est hébergé dans deux régions AWS : Ouest des États-Unis (Oregon) et UE (Irelande). L'environnement de répliques de sauvegarde est hébergé dans deux régions AWS : Est des États-Unis (Virginie nord) et UE (Francfort) pour la reprise après sinistre. Une ferme de serveurs Web reçoit et répond à toutes les requêtes des clients gérés et des consoles Cloud, transmettant les requêtes au serveur de base de données via AWS Simple Queue Service (SQS) pour le traitement. Une base de données globale hébergée sur les instances AWS Multi-AZ RDS stocke les données système requises à l'échelle mondiale. Une base de données séparée contient les schémas de base de données isolés créés pour chaque client.

Faronics Cloud et la protection de la confidentialité

La sécurité des informations et la confidentialité des clients sont primordiales pour Faronics. En suivant les meilleures pratiques de sécurité du secteur, Faronics s'engage à sécuriser les données et la confidentialité des clients contre le vol, la fuite, la compromission de l'intégrité et le piratage, qu'ils soient accidentels ou délibérés.

Modèle de responsabilité partagée

En tant que solution cloud, la responsabilité de la sécurité des données est partagée par AWS (le fournisseur de services cloud de Faronics Cloud), Faronics (fournisseur de services cloud à ses clients), et les clients de Faronics Cloud

L'infrastructure et les services d'AWS respectent plusieurs normes spécifiques au secteur, notamment :

Cloud Security Alliance (CSA)

HIPAA

Motion Picture Association of America (MPAA)

AWS fournit des informations détaillées concernant son environnement de contrôle informatique par le biais de livres blancs, de rapports, de certifications, d'accréditations et d'autres attestations de tiers. Pour plus d'informations, consultez le livre blanc sur le risque et la conformité disponible sur leur site Web : http://aws.amazon.com/security.

Faronics est responsable de la sécurité du système d'exploitation dorsal, du réseau, des configurations de pare-feu, de la gestion de la plateforme et des applications, ainsi que des données des clients. Nos politiques et pratiques en matière de sécurité sont décrites dans les sections “Protection des données et de la vie privée des clients” et “Politiques et pratiques en matière de sécurité”, ci-dessous.

Les clients de Faronics Cloud sont responsables de la sécurité de leurs données en gérant l'accès et les autorisations pour leurs comptes Faronics Cloud, en assurant la sécurité des informations d'identification et en utilisant des mots de passe robustes.

Protection des données et de la vie privée des clients

Données clients recueillies

Faronics ne recueille des informations personnelles que pour les raisons suivantes :

- Pour développer, gérer et fournir nos produits et services à nos clients.
- Pour contacter nos clients pour les informer des mises à jour, des mises à niveau et des améliorations des produits et des services.
- Pour contacter nos clients soit directement, soit par l'intermédiaire de l'un de nos revendeurs, pour leur offrir la possibilité de renouveler les services.
- Pour contacter directement nos clients au sujet de produits et de services susceptibles de les intéresser.
- Pour garantir des normes de service élevées aux clients.
- Pour vérifier l'identité d'un client.
- Pour répondre aux exigences réglementaires.

Dans le système Faronics Cloud, les données clients suivantes peuvent être collectées en fonction des services utilisés par le client :

- Identité du client et informations sur le compte, y compris le nom de l'organisation, le nom d'utilisateur, le mot de passe, le titre, le numéro de téléphone, l'adresse électronique, etc.
- Informations sur l'appareil du client, y compris le nom de l'appareil, l'adresse IP, l'adresse MAC, la date et l'heure de la connexion au serveur Faronics Cloud, etc.
- Informations sur l'utilisation de l'appareil par le client, y compris la date et l'heure de connexion de l'utilisateur, les logiciels installés sur l'appareil, l'utilisation logicielle de l'appareil, etc.
- Configurations et sélections du service Faronics Cloud.

Segmentation des données clients

Faronics Cloud segmente les données des clients (dont les détails de l'appareil mais pas les informations personnelles) dans des schémas de base de données dédiés dans lesquels toutes les tables appartiennent à un client spécifique. Chaque schéma de base de données spécifique à un client est hébergé sur une instance de base de données partagée dans AWS. L'architecture est suffisamment flexible pour que les clients puissent demander une instance de base de données dédiée à leurs données. Notez que des coûts supplémentaires peuvent être facturés au client pour isoler les données.

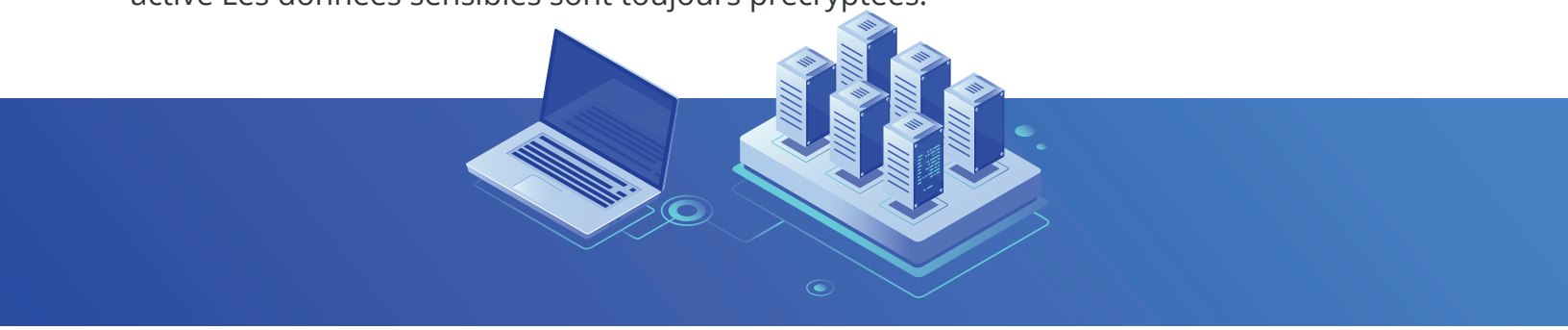
Protection des données des clients en transit

Les serveurs de Faronics Cloud utilisent le cryptage HTTPS (TLS 1.2). Faronics crypte les données statiques sensibles des clients, telles que les mots de passe, les politiques et les chaînes de connexion aux bases de données, en fonction du type de données :

- Les hachages de mots de passe utilisent un cryptage à sens unique.
- Les chaînes de connexion à la base de données sont cryptées à l'aide d'un algorithme Rijndael de 256 bits.
- Les politiques sont chiffrées à l'aide d'un algorithme de chiffrement de flux RC4 pris en charge par Microsoft Base Cryptographic Provider, en fonction du service spécifique.

Protection des données des clients stockées

Les données de sauvegarde de Faronics Cloud sont stockées dans AWS avec le cryptage activé Les données sensibles sont toujours précryptées.



Politiques et pratiques de sécurité

Politiques et pratiques de sécurité en matière de développement et d'assurance qualité

Les processus de développement et d'assurance qualité de Faronics sont conçus en tenant compte des risques et des vulnérabilités en matière de sécurité. Les meilleures pratiques pertinentes comprennent, sans s'y limiter, les éléments suivants :

- Les versions du code source sont analysées à la recherche de malware et tous les codes de sécurité sont examinés avant d'être déployés.
- L'équipe de développement effectue régulièrement des tests de pénétration au niveau des applications, comme le prescrivent les meilleures pratiques et recommandations du secteur.
- L'équipe chargée des opérations teste les plans de continuité des activités et de reprise après sinistre pour les services critiques, selon un calendrier défini et d'après différents scénarios de perte.
- Des tests de sécurité sont effectués sur toutes les versions avant leur déploiement.
- Amélioration continue de la sécurité dans le cadre du cycle de vie du développement des systèmes/logiciels (SDLC) en utilisant les postures de sécurité “Empêcher les intrusions” et “Gérer l'intrusion”.

Faronics a mis en place des processus de développement de logiciels et de gestion des versions afin de contrôler la mise en œuvre des changements majeurs, notamment les suivants :

- Les modifications prévues sont identifiées et documentées, y compris la création de spécifications de fonctionnalités et de conceptions de composants.
- Les objectifs, les priorités et les scénarios de l'entreprise sont identifiés lors de la planification du produit.
- L'état de préparation opérationnelle est examiné selon des critères prédéfinis, en évaluant le risque et l'impact globaux.
- Tests, autorisations et gestion des modifications sur la base de critères d'entrée et de sortie pour les environnements DEV (développement), INT (tests d'intégration), STAGE (préproduction) et PROD (production), le cas échéant.
- Faronics assure l'assainissement des entrées dans les bases de données et des entrées des utilisateurs en utilisant les meilleures pratiques suivantes :
  - Les entrées sont limitées par une validation de base et un échappement approprié.
  - Utilisation de SqlCommand et SqlParameters de .NET.
  - Les requêtes SQL ne sont jamais directement manipulées ou concaténées.

Politiques et pratiques en matière de sécurité des opérations

En suivant les meilleures pratiques de sécurité de l'industrie, les activités de Faronics Cloud sont conçues pour fournir une protection robuste et la confidentialité des données des clients. Les politiques pertinentes comprennent, sans s'y limiter, les éléments suivants :

- Le service AWS IAM (Identity and Access Management, gestion d'identité et d'accès) est utilisé pour la gestion de l'authentification des utilisateurs, des groupes et des rôles dans l'environnement backend.
- AWS VPC (Cloud virtuel privé), ACL (liste de contrôle d'accès) réseau et groupe de sécurité est utilisé pour contrôler l'infrastructure dorsale (instances EC2 et instance RDS).
- Les activités sur la plateforme AWS sont auditées en utilisant AWS CloudTrail.
- Les modifications apportées au site de production du cloud Faronics sont effectuées conformément aux directives du document sur la gestion des changements.
- Les éléments et les processus sont prestataires des privilèges d'utilisateur minimaux nécessaires à l'accomplissement de leurs tâches.
- Le personnel autorisé interne de Faronics ayant accès aux données des clients dans le service cloud de Faronics est tenu d'utiliser la connexion MFA (Multi-Factors Authentication).
- L'infrastructure du système est configurée pour assurer la redondance et le basculement e douceur.

- Les données sont régulièrement sauvegardées et les sauvegardes sont périodiquement validées pour être restaurées à des fins de reprise après sinistre. Les normes de sauvegarde, les politiques, les procédures et les contrôles sont vérifiés et documentés.
- Les services cloud peuvent être restaurés dans une zone de disponibilité différente au sein de la même région AWS, ou dans différentes régions AWS, en cas de panne d'électricité d'un centre de données, de panne de réseau ou d'une autre situation de catastrophe. Les processus de régénération sont définis et documentés.
- Les activités font l'objet d'audits de sécurité internes réguliers, basés sur des traces, des journaux et d'autres informations, réalisés par les administrateurs système et d'autres groupes impliqués dans les opérations de routine.

Références et lectures complémentaires

AWS Security Best Practices (par Amazon Web Service)

Treacherous 12 Top Threats to Cloud Computing Plus: Industry Insights (par Cloud Security Alliance (CSA))

OWASP Top 10 2017 - The Ten Most Critical Web Application Security Risks

Pour en savoir plus sur les avantages qu'apportent les solutions Faronics à vos environnements informatiques, visitez le site Web www.faronics.com

ÉTATS-UNIS
5506 Sunol Blvd, Suite 202
Pleasanton, CA, 94566 USA

Appel gratuit : 1-800-943-6422
Fax Appel gratuit : 1-800-943-6488
sales@faronics.com

CANADA ET INTERNATIONAL
609 Granville Street, Suite 1400
P.O. Box 10362, Pacific Centre
Vancouver, BC, V7Y 1G5

Téléphone : +1-604-637-3333
Télécopie : +1-604-637-8188
sales@faronics.com

EUROPE
8 The Courtyard, Eastern Road,
Bracknell, Berkshire
RG12 2XB, United Kingdom

Téléphone : +44 (0) 1344 206 414
eurosales@faronics.com

SINGAPOUR
6 Marina Boulevard
#36-22 The Sail At Marina Bay
Singapore, 018985

Téléphone : +65 6509 4993
Télécopie : +65 6722 8634
sales@faronics.com.sg