



l'histoire de l'ESP RainMaker

comment nous avons construit « votre » nuage IdO

Amey Inamdar, Espressif

Les appareils connectés au nuage constituent les éléments principaux de l'IdO. Cependant, avec les fournisseurs de solutions nuage complètes, les fabricants d'appareils perdent une partie du contrôle des données, et la mise en place d'une solution nuage en partant de zéro représente un effort considérable. Chez Espressif, nous nous sommes rendu compte de ces difficultés et avons décidé de proposer une solution qui permet d'obtenir le meilleur des deux mondes.

Le « I » de IdO est l'abréviation d'internet. L'internet, et donc la connectivité au nuage, fait partie intégrante des appareils connectés afin de bénéficier des avantages de la connectivité. Les appareils qui se connectent au nuage pour y envoyer des données et recevoir des commandes représentent une valeur ajoutée, non seulement pour les utilisateurs finaux, mais aussi pour offrir des fonctions utiles aux fabricants d'appareils. Cependant, pour les consommateurs, l'utilisation d'un nuage IdO comporte des risques sur le plan de la sécurité et de la confidentialité comme aussi des problèmes d'extensibilité, et accroissent les défis d'ingénierie pour les fabricants d'appareils.

C'était un choix naturel pour de nombreux fabricants d'appareils de s'adresser à divers fournisseurs de solutions IdO complètes qui proposent

leur propre plateforme sur le nuage, toute prête à l'emploi disposant des applications correspondantes pour les appareils mobiles. Toutefois, les fabricants d'appareils n'ont pas pu se différencier suffisamment et ont perdu le contrôle nécessaire sur les données générées dans le nuage. D'autre part, certains fabricants d'appareils auraient eu la possibilité de construire leur propre nuage à partir de zéro, mais cela représentait un effort trop important, y compris pour en assurer la maintenance.

Chez Espressif, nous avons compris ce dilemme et décidé de proposer une solution qui reprend le meilleur des deux mondes. D'une part, nous voulions fournir des fonctionnalités complètes pour le nuage, et d'autre part, offrir aux clients la propriété des données, un contrôle maximal et une personnalisation optimale, afin qu'ils n'aient pas à repartir de zéro. C'est ainsi qu'est né ESP RainMaker.

Choisir l'architecture du nuage

Le premier choix consistait à déterminer l'architecture du nuage à utiliser (**figure 1**).

Vous avez peut-être déjà entendu dire que le nuage n'est que l'ordinateur de quelqu'un d'autre. Cette boutade est effectivement vraie. Mais l'important, c'est la manière dont l'ordinateur d'autrui est utilisé pour héberger votre application. Avec l'essor des technologies de virtualisation, des serveurs puissants sont utilisés pour héberger plusieurs applications sur le même matériel, complètement indépendantes les unes des autres. Avec les machines virtuelles (pensez à VMware) vous pouvez exécuter plusieurs instances du système d'exploitation sur le même matériel, tandis qu'avec les technologies de conteneurs (Kubernetes, Docker), vous pouvez avoir des environnements d'exploitation parallèles sur le même matériel. Bien que cela soit formidable, ces deux architectures vous obligent à vous préoccuper des logiciels à exécuter

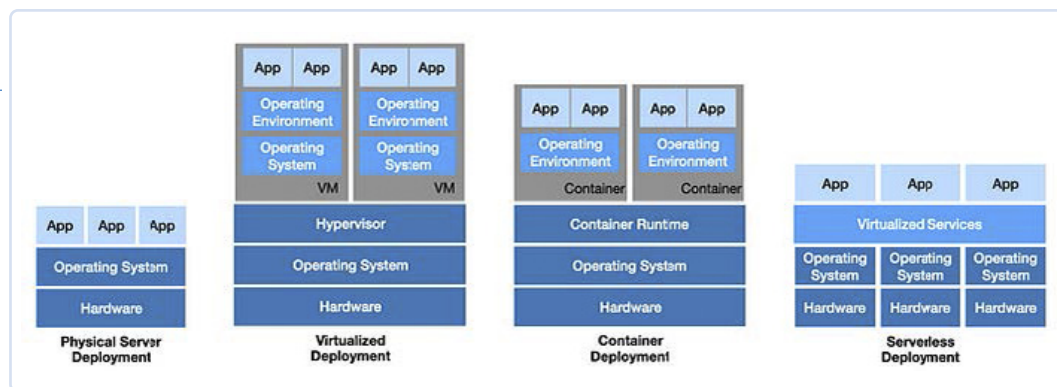


Figure 1. Évolution des architectures en nuage.

et à maintenir, de la manière d'évoluer en fonction de l'augmentation/diminution du nombre d'appareils (c'est le travail d'ingénieurs spécialisés DevOps). Alors que nous voulions que nos clients disposent de leur propre nuage IdO, nous ne pouvions pas les accabler de ces efforts. C'est là qu'un paradigme relativement nouveau d'architecture nuage « sans serveur » nous est venu à l'aide, offrant la promesse de construire un nuage IdO facile à maintenir.

L'architecture sans serveur ne se débarrasse pas des serveurs. Les abstractions sont simplement réalisées à un niveau supérieur. Par exemple, vous obtenez un courtier MQTT (*Message Queuing Telemetry Transport*) sans avoir à vous soucier du logiciel MQTT qu'il utilise, du nombre de connexions d'appareils qu'il peut prendre en charge ou de la plateforme sur laquelle il tourne. Amazon Web Services (AWS) fournit de tels services gérés, qui nous ont permis de mettre en œuvre notre nuage IdO. Parmi les nombreux services gérés, AWS IoT Core fournit un courtier MQTT géré, DynamoDB (Service de base de données NoSQL dans le cloud) fournit une base de données noSQL gérée, S3 (*Amazon Simple Storage Service*, abrégé S3) fournit le stockage et, surtout, Lambda fournit une « fonction en tant que service », où vous pouvez mettre en œuvre la logique sans vous soucier de l'endroit où l'exécuter.

Avec cette mise en œuvre basée sur les services gérés AWS, ESP RainMaker correspond à la combinaison des configurations de divers services et de leurs interactions, et de la mise en œuvre de fonctionnalités par le biais de fonctions Lambda. Il est important de noter qu'il peut être déployé avec n'importe quel compte AWS. Ceci permet facilement de créer une implémentation nuage IdO que les clients peuvent déployer dans leur propre compte AWS et contrôler ainsi entièrement les données et la personnalisation.

Gérer l'extensibilité

Le nuage IdO doit généralement se préoccuper d'un grand nombre d'appareils et d'utilisateurs (par le biais d'applications mobiles ou d'autres clients tels que des assistants vocaux) qui se connectent au nuage et lui envoient des messages. Ce nombre varie en fonction du secteur d'activité et, pour les fabricants d'appareils grand public, peut atteindre des millions d'appareils et d'utilisateurs. Il est donc important de s'assurer que la mise en œuvre de l'informatique en nuage puisse s'adapter à un grand nombre d'utilisateurs.

AWS gérant les différents services, il est logique de supposer que vous

n'avez pas à vous soucier de l'extensibilité du backend (serveur) du nuage. Si cela est en grande partie vrai, il n'en reste pas moins que chaque service peut avoir certaines limites. Par exemple, le nombre maximum de fonctions lambda (= fonction anonyme, sans nom) s'exécutant simultanément dans le compte AWS, est limité. Cela nécessite une réflexion approfondie sur l'architecture pour s'assurer que le système est conçu de manière à gérer un grand nombre de messages en utilisant une file d'attente appropriée. Cela signifie également que le micrologiciel de l'appareil et les applications mobiles doivent gérer correctement les erreurs.

Aujourd'hui, ESP RainMaker est testé par plus de 3,5 millions d'appareils et d'utilisateurs qui se connectent et communiquent via le nuage (figure 2).

Gestion des coûts opérationnels

Dans une architecture nuage traditionnelle, vous payez généralement pour le calcul, le stockage et la mémoire de vos machines virtuelles. Dans l'architecture sans serveur, l'unité de facturation change. Vous devez payer pour les ressources réellement utilisées, telles que le nombre d'appareils connectés et le temps de connexion total, le nombre de messages MQTT, le nombre de lectures/écritures dans la base de données, la quantité de données stockées dans S3, ainsi que les ressources consommées par les fonctions lambda exécutées. Bien qu'il s'agisse d'un modèle de tarification à l'usage, l'utilisateur du service payant ce qu'il consomme, il se peut que les coûts soient bien plus élevés si votre architecture et votre implémentation ne sont pas optimisées.

Le coût d'exploitation pour les clients était l'un des critères clés lors de la conception de l'ESP RainMaker. L'objectif était facile à définir. Nous voulions développer un backend nuage qui fonctionnerait même pour une ampoule intelligente ; certainement le dispositif IdO le moins cher. Il a fallu beaucoup d'effort pour choisir avec soins les services AWS afin de s'assurer qu'ESP RainMaker puisse atteindre cet objectif. De plus, l'implémentation a été considérablement ajustée pour atteindre un nombre optimal de lectures/écritures dans la base de données, le choix du langage d'implémentation pour utiliser un minimum de ressources pour l'exécution, et ainsi de suite.

ESP RainMaker a actuellement plusieurs clients qui vendent des ampoules à bas prix répondant aux exigences en matière de coûts opérationnels.

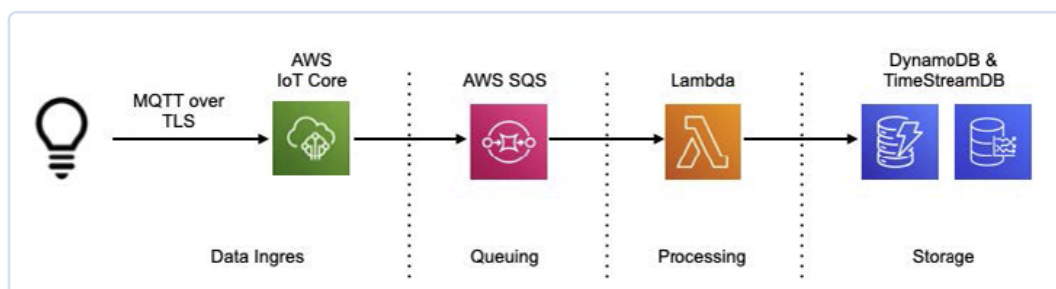


Figure 2. Exemple de traitement des messages de l'appareil dans ESP Rainmaker.

Figure 3. Composants de l'ESP RainMaker.

Sécurité des données et protection de la vie privée

L'utilisation des services gérés par AWS a également permis de garantir la sécurité des données. Ils offrent des méthodes standard d'authentification, d'autorisation, de stockage de données cryptées, de pare-feu applicatifs, etc. Par exemple, le courtier AWS IoT Core MQTT fournit une authentification des appareils basée sur un certificat X.509. Ce qui permet à la fois à un appareil d'authentifier le nuage et au nuage d'authentifier l'appareil. Les polices IAM permettent un contrôle précis des autorisations. Le pare-feu des applications web WAF offre une protection contre les attaques DoS et DDoS sur les points d'extrémité du service RESTful.

ESP RainMaker utilise toutes ces méthodes de sécurité de la manière prescrite, en garantissant une authentification et une autorisation appropriées par des méthodes standards, et il n'y a pas d'escalade de privilèges inutiles. Nous avons également travaillé avec une société tierce de test et de certification pour nous assurer qu'ESP RainMaker met en œuvre toutes les fonctionnalités requises pour répondre aux exigences en matière de confidentialité des données, afin de permettre aux clients de se conformer facilement à la GDPR lorsqu'ils déploient ESP RainMaker pour leur propre compte.

Le nuage IdO ne suffit pas à lui seul

Bien que le backend en nuage constitue une partie importante de la solution IdO complète, il n'est pas suffisant. Du point de vue de l'appareil IdO connecté, en plus du nuage auquel il se connecte, il est tout aussi important de disposer d'un micrologiciel pour l'appareil, d'applications pour smartphone mobile permettant de configurer et d'effectuer des contrôles, et d'intégrer des assistants vocaux, qui dans la maison intelligente sont devenus le moyen le plus naturel pour les utilisateurs de communiquer avec les appareils connectés (figure 3).

Chez Espressif, nous avons créé tous ces composants. Le SDK (Software Development Kit, en français KDL = Kit de Développement Logiciel) d'ESP RainMaker pour l'appareil est entièrement open source et facile à intégrer grâce aux nombreux exemples qu'il propose. Les applications de référence iOS et Android sont également entièrement open source. ESP RainMaker comprend les instructions d'Alexa et de Google Assistant. En outre, le nuage n'est guère utile s'il ne peut pas être utilisé pour améliorer le produit grâce à des informations techniques et commerciales. Pour cela, nous avons construit un module de surveillance à distance des appareils, ESP-Insights, qui récolte un journal des événements survenus, des analyses de crashes, un suivi des métriques, et surtout, facilite la création de requêtes étoffées sur les données. Ce module est disponible via le tableau de bord web d'ESP RainMaker, qui permet également la mise à jour à distance (OTA - *Over-The-Air update*), le regroupement d'appareils, le contrôle d'accès basé sur les rôles et les informations commerciales.

Préparer l'avenir

Le protocole Matter apporte la normalisation tant attendue pour les appareils domestiques intelligents. Matter est un protocole de réseau local. La connectivité au nuage peut donc être considérée comme orthogonale avec Matter. Néanmoins, le cloud joue un rôle dans la gestion des appareils et l'accès à distance à ces derniers. ESP RainMaker offre un support Matter Fabric qui peut être utilisé pour créer votre propre



écosystème Matter. Une combinaison de backend ESP RainMaker et d'applications téléphoniques mettent en œuvre la structure Matter avec l'infrastructure PKI complète requise pour la structure Matter. Les bases de données des appareils, des utilisateurs et des ACL sont synchronisées en toute sécurité entre plusieurs applications. De plus, lorsque vous avez un contrôleur de maison intelligente qui se connecte à RainMaker, vous pouvez fournir un contrôle à distance à partir de vos applications mobiles, non seulement à vos propres appareils, mais aussi à d'autres appareils Matter.

Avec ESP RainMaker, nous avons également annoncé la prise en charge de l'intégration de la topologie réseau Mesh-Lite. Avec Mesh-Lite vous pouvez avoir un réseau Wifi maillé dédié à vos appareils IdO de plus grande portée et couvrant également des zones qui seraient à considérer comme mortes dans la maison. Les appareils IdO basés sur la puce ESP32 agissent comme des points d'accès pour permettre la connexion à d'autres appareils, formant ainsi une topologie maillée (proche d'une arborescence). Avec ESP RainMaker, les utilisateurs peuvent facilement créer le réseau maillé et approvisionner les nœuds à l'intérieur de celui-ci.

Pour commencer

Nous avons construit le nuage ESP RainMaker en tenant compte de considérations que tout fabricant d'appareils devrait également respecter lors de la mise en œuvre de sa propre plateforme IdO en nuage. Plus important encore, Espressif fournit une plateforme entièrement personnalisable. Pour les développeurs, Espressif fournit également une instance ESP RainMaker gérée par Espressif ainsi que des applications téléphoniques disponibles dans les magasins d'applications respectifs. Vous pouvez utiliser le tableau de bord web pour la gestion des appareils et effectuer des mises à jour OTA. Ainsi, vous pouvez non seulement évaluer les fonctionnalités, mais aussi créer vos projets pour votre usage personnel.

Lorsque vous commencez, vous pouvez utiliser n'importe quelle carte de développement Espressif et suivre les étapes mentionnées dans le guide « Get Started » [1].

VF : Jean-Philippe Nicolet — 230621-04

À propos de l'auteur

Amey Indamar est le directeur du marketing technique chez Espressif. Il a 20 ans d'expérience dans le domaine des systèmes embarqués et des appareils connectés, ayant occupé des postes dans l'ingénierie, la gestion de produits et le marketing technique. Il a travaillé avec de nombreux clients pour construire des appareils connectés basés sur la connectivité Wifi et Bluetooth.

LIEN

[1] Démarrer avec ESP RainMaker :
<https://rainmaker.espressif.com/docs/get-started>