Principios básicos de IoT

Abril de 2016

Avisos

Este documento se suministra únicamente con fines informativos. Representa la oferta actual de productos y prácticas de AWS a partir de la fecha de publicación de este documento. Dichas prácticas y productos pueden modificarse sin previo aviso. Los clientes son responsables de realizar sus propias evaluaciones independientes de la información contenida en este documento y de cualquier uso de los productos o servicios de AWS, cada uno de los cuales se ofrece “tal cual”, sin garantía de ningún tipo, ya sea explícita o implícita. Este documento no genera ninguna garantía, declaración, compromiso contractual, condición ni certeza por parte de AWS, sus filiales, proveedores o licenciantes. Las responsabilidades y obligaciones de AWS con respecto a sus clientes se controlan mediante los acuerdos de AWS y este documento no forma parte ni modifica ningún acuerdo entre AWS y sus clientes.

Contenido

Resumen

En este documento se describen los principios básicos que deben tenerse en cuenta al desarrollar una estrategia para Internet de las cosas (IoT, Internet of Things). Su finalidad es ayudar a los clientes a entender los beneficios de Amazon Web Services (AWS) y por qué la plataforma en la nube de AWS puede constituir el componente esencial en que se sustenten los principios básicos de una solución de IoT. Además, se proporciona información general de los servicios de AWS que deben formar parte de una estrategia de IoT global. Este documento está dirigido a los responsables de la toma de decisiones que están estudiando las plataformas de Internet de las cosas.

Información general

Una de las propuestas de valor de una estrategia de Internet de las cosas es la capacidad para proporcionar conocimientos sobre contextos que anteriormente no eran visibles para el negocio. Pero para que un negocio pueda desarrollar una estrategia de IoT, antes debe disponer de una plataforma que satisfaga los principios básicos de este tipo de soluciones.

AWS considera fundamentales una serie de libertades básicas que permiten trasladar a las compañías los beneficios organizativos y económicos de la nube. Estas libertades son la razón por la que más de un millón de clientes utilizan ya la plataforma AWS para respaldar prácticamente cualquier carga de trabajo en la nube. Estas libertades son también la razón por la que la plataforma AWS ha demostrado ser el principal catalizador de cualquier estrategia de Internet de las cosas en todo tipo de soluciones, ya sean comerciales, de consumo o industriales.

Los clientes de AWS que trabajan en este espectro de soluciones han identificado una serie de principios básicos que son vitales para el éxito de cualquier plataforma de IoT. Se trata de agilidad, escala, costo y seguridad, aspectos que han demostrado ser esenciales para el éxito a largo plazo de toda estrategia de IoT.

En este documento técnico se utilizan las definiciones siguientes de estos principios:

- Agilidad: libertad para analizar, ejecutar y desarrollar con rapidez las iniciativas técnicas y de negocio sin restricciones.

- Escala: capacidad para expandir la infraestructura de manera transparente en los ámbitos regional o internacional con el fin de satisfacer la demanda operativa.
- Costo: comprensión y control de los costos operativos de una plataforma de IoT.
- Seguridad: comunicación segura desde los dispositivos hasta la nube manteniendo la conformidad y la rapidez de iteración.

Con la plataforma AWS, las compañías pueden crear soluciones ágiles y escalables para adaptarse al crecimiento exponencial de los dispositivos, con la capacidad de administrar los costos, todo ello basándose en algunas de las infraestructuras informáticas más seguras del mundo. Una compañía que seleccione una plataforma que ofrezca estas libertades y promueva estos principios básicos podrá centrar mejor su enfoque organizativo en los factores diferenciadores de su negocio y en el valor estratégico de implementar soluciones en Internet de las cosas.

Principios básicos de IoT

Agilidad

Uno de los principales beneficios que las compañías buscan al crear una solución de IoT es la capacidad para cuantificar las oportunidades de manera eficiente. Estas oportunidades dependen de la fiabilidad de los datos de los sensores, del diagnóstico remoto y del control remoto entre usuarios y dispositivos. Las compañías capaces de recopilar de manera eficiente estas métricas pueden explorar diversas hipótesis de negocio a partir de sus datos de IoT. Por ejemplo, los fabricantes pueden crear soluciones de análisis predictivo que midan, prueben y ajusten el ciclo de mantenimiento idóneo para sus productos a lo largo del tiempo. El ciclo de vida de IoT consta de las diferentes fases precisas para adquirir, fabricar, incorporar, probar, implementar y administrar grandes flotas de dispositivos físicos. Al desarrollar estos dispositivos físicos, el proceso en cascada introduce complicaciones y puntos de fricción que pueden restar agilidad de negocio. Esto, combinado con los costos iniciales del hardware derivados de desarrollar e implementar los recursos físicos a gran escala, suele dar lugar a la necesidad de conservar los dispositivos instalados en uso durante periodos prolongados, con el fin de obtener el retorno de la inversión (ROI, Return On Investment) necesario.

En un momento en que los desafíos y oportunidades que tienen ante sí las compañías no deja de crecer, la división de TI se convierte en factor de diferenciación competitiva, con la misión de sustentar el desempeño de negocio, el desarrollo de productos y las operaciones. Para que la estrategia de IoT de una compañía sea una ventaja competitiva, la organización de TI depende de la existencia de un amplio abanico de herramientas a su disposición que promuevan la interoperabilidad de la solución de IoT en su conjunto y entre un surtido heterogéneo de dispositivos. Las compañías que pueden alcanzar el equilibrio correcto entre los procesos en cascada de los lanzamientos de hardware y las metodologías ágiles de desarrollo de software pueden optimizar de manera continua el valor que se desprende de su estrategia de IoT.

Escalabilidad y presencia global

Junto con el crecimiento exponencial de los dispositivos conectados, cada *cosa* del Internet de las cosas comunica paquetes de datos que requieren una conectividad de confianza y un almacenamiento duradero. Antes de las plataformas en la nube, los departamentos de TI adquirían hardware adicional mantenían una capacidad infrautilizada y sobre aprovisionada para poder abarcar el crecimiento sostenido de la cantidad de datos (telemetría) emitidos por los dispositivos. Con IoT, la organización ha de responder al reto de administrar, monitorizar y proteger el ingente número de conexiones de red de todos estos dispositivos conectados y dispersos.

Además de la posibilidad de escalar y ampliar la solución en el ámbito de una ubicación regional, las soluciones de IoT requieren poder abarcar el ámbito global y distintas ubicaciones físicas. Las soluciones de IoT deben implementarse en varias ubicaciones físicas para satisfacer los objetivos de negocio de una solución empresarial global, tales como conformidad de los datos, soberanía sobre la información y reducción de la latencia de las comunicaciones, para mejorar la capacidad de respuesta de los dispositivos instalados sobre el terreno.

Costos

Con frecuencia, el mayor valor de una solución de IoT reside en los datos de telemetría y contextuales que se generan y envían desde los dispositivos. Para construir una infraestructura local, se requiere un capital inicial para adquirir el hardware. Pero puede tratarse de un gasto fijo y elevado que no esté relacionado directamente con el valor que la telemetría del dispositivo producirá en algún momento futuro. Para equilibrar la necesidad de recibir telemetría en la

actualidad con el valor incierto que se extraerá de los datos de telemetría en el futuro, la estrategia de IoT debe basarse en una plataforma en la nube elástica y escalable. Con la plataforma AWS, la compañía solo paga por los servicios que consume y no se requiere un contrato a largo plazo. Un modelo de precios flexible y basado en el consumo permite asumir el costo de la solución de IoT y obtener acceso directamente a la infraestructura correspondiente al mismo tiempo que se obtiene el valor de negocio extraído de la introducción, el procesamiento, el almacenamiento y el análisis de la telemetría recibida por esa misma solución.

Seguridad

Una solución de IoT se basa íntegramente en la seguridad. La seguridad de las cosas ha de ser un requisito incorporado en todos los aspectos del propio diseño, porque los dispositivos pueden enviar grandes cantidades de información confidencial y los usuarios finales de las aplicaciones de IoT también pueden controlarlos directamente. Las soluciones de IoT no solo se deben diseñar pensando en la seguridad, sino que los controles de seguridad deben permear todas y cada una de las capas de la solución. Pero la seguridad no es una fórmula estática. Las aplicaciones de IoT deben ser capaces de modelar, monitorizar e iterar de forma constante las prácticas recomendadas en la materia. En Internet de las cosas, la superficie de ataque es distinta que en una infraestructura web tradicional. La omnipresencia de la computación ubicua significa que las vulnerabilidades de IoT pueden permitir ataques que cuesten vidas, por ejemplo, si se viera comprometido el sistema de control de los oleoductos o las redes eléctricas.

Una de las dinámicas que dificulta la seguridad de IoT se refiere al propio ciclo de vida de un dispositivo físico y a las restricciones del hardware de los sensores, microcontroladores, accionadores y las bibliotecas que llevan incluidas. Estos factores restrictivos pueden limitar las prestaciones de seguridad que aplique cada dispositivo. Ante esta dinámica adicional, las soluciones de IoT han de adaptar continuamente su arquitectura, firmware y software con el fin de adelantarse a los cambios en el panorama de la seguridad. Si bien los factores restrictivos de los dispositivos pueden presentar riesgos, obstáculos y posibles inconvenientes adicionales que contrapongan la seguridad al costo, crear una solución de IoT segura debe ser el objetivo primordial para cualquier organización.

Servicios de AWS para soluciones de IoT

La plataforma AWS proporciona la base sobre la que sustentar una estrategia de IoT ágil, escalable, segura y rentable. Para lograr el valor de negocio que IoT puede aportar a una organización, los clientes deben evaluar la amplitud y profundidad de los servicios de AWS que suelen utilizarse en las implementaciones de IoT distribuidas y a gran escala. AWS ofrece una gama de servicios para acelerar el plazo de lanzamiento: desde SDK de dispositivos para software incrustado, a procesamiento de datos en tiempo real y servicios de computación basados en eventos.

En las secciones siguientes describiremos los servicios de AWS más frecuentes que se usan en las aplicaciones de IoT y los pondremos en relación con los principios básicos de una solución de IoT.

AWS IoT

Internet de las cosas no puede existir sin las *cosas*. Lo primero que debe hacer cada solución de IoT es establecer las conexiones, para comenzar a interaccionar con los dispositivos. AWS IoT es un servicio administrado de AWS que aborda los desafíos de conectar, administrar y utilizar grandes flotas de dispositivos para una aplicación. La combinación de escalabilidad de la conectividad con los mecanismos de seguridad para la transmisión de datos en el seno de AWS IoT aporta la base de las comunicaciones que forma parte de la solución de IoT. Una vez que se han enviado los datos a AWS IoT, la solución tiene a su disposición todo un ecosistema de servicios de AWS que abarcan bases de datos, servicios móviles, big data, análisis, aprendizaje automático, etc.

Gateway para dispositivos

Una gateway para dispositivos es la responsable de mantener las sesiones y suscripciones de todos los dispositivos conectados de una solución de IoT. La gateway para dispositivos de AWS IoT permite las comunicaciones seguras y bidireccionales entre los dispositivos conectados y la plataforma AWS a través de MQTT, WebSockets y HTTP. Los protocolos de comunicaciones como MQTT y HTTP permiten a la compañía utilizar los protocolos estándar de la industria en lugar de uno propietario que podría limitar la interoperabilidad en el futuro.

Al tratarse de un protocolo de publicación y suscripción, MQTT propicia de forma inherente los patrones de comunicación escalables y con tolerancia a errores,

además de permitir un amplio abanico de opciones de comunicación entre los dispositivos y la puerta de enlace para dispositivos. Estos patrones de mensajes pueden abarcar desde la comunicación entre dos dispositivos hasta los modelos de difusión, en que un dispositivo envía un mensaje a otros muchos sobre un tema común. Además, el protocolo MQTT expone distintos niveles de calidad de servicio (QoS, Quality of Service) para controlar la retransmisión y entrega de mensajes a medida que se publican para los suscriptores. La combinación de las prestaciones de publicación y suscripción con QoS no solo hace posible que las soluciones de IoT controlen cómo interaccionan los dispositivos de una solución, sino que también genera mayor previsibilidad respecto a cómo se entregan y confirman los mensajes o se reintenta su envío en caso de error de la red o de un dispositivo.

Sombras, registro de dispositivos y motor de reglas

AWS IoT integra otras características que son esenciales para crear una aplicación de IoT robusta. El servicio AWS IoT incluye un motor de reglas, capaz de filtrar, transformar y reenviar los mensajes de los dispositivos a medida que se reciben en la gateway para dispositivos. El motor de reglas utiliza una sintaxis basada en SQL que selecciona los datos de las cargas de mensajes y activa las acciones en función de las características de los datos de IoT. AWS IoT también incluye la función de sombras de dispositivos, que mantiene representaciones virtuales de estos. La sombra del dispositivo sirve de canal de mensajes para enviar comandos de manera confiable a un dispositivo y almacenar el último estado conocido de este en la plataforma AWS.

Para administrar el ciclo de vida de una flota de dispositivos, AWS IoT posee un registro de dispositivos. Este constituye la ubicación central donde se almacena y consulta un conjunto predefinido de atributos relacionados con cada cosa. El registro de dispositivos admite la creación de una vista de administración integral de la solución de IoT que permite controlar las asociaciones entre las cosas, las sombras, los permisos y las identidades.

Seguridad e identidad

Para los dispositivos conectados, la plataforma de IoT debe aplicar los conceptos de identidad, privilegios mínimos, cifrado y autorización a lo largo de todo el ciclo de vida de desarrollo del hardware y del software. AWS IoT cifra el tráfico de entrada y salida del servicio mediante el protocolo Transport Layer Security (TLS) y es compatible con la mayoría de los paquetes de cifrado. Para la identificación, AWS IoT exige al dispositivo conectado que se autentique mediante un certificado X.509. Cada certificado se debe aprovisionar, activar y,

por último, instalar en un dispositivo para poder utilizarlo como identidad válida en AWS IoT. Con el fin de respaldar esta separación entre la identidad y el acceso de los dispositivos, AWS IoT cuenta con políticas de IoT para las identidades de los dispositivos. Además, AWS IoT utiliza las políticas de AWS Identity and Access Management (AWS IAM) para los usuarios, los grupos y los roles de AWS. El uso de las políticas de IoT permite a la organización controlar la autorización o denegación de las comunicaciones sobre los temas de IoT para cada identidad de dispositivo concreta. Tanto las políticas y los certificados de AWS IoT como AWS IAM se han diseñado de tal forma que admitan la configuración de listas blancas explícitas para los canales de comunicación de todos los dispositivos del ecosistema de AWS IoT de una compañía.

Servicios basados en eventos

Para hacer realidad los principios de escalabilidad y flexibilidad de una solución de IoT, la organización debe incorporar las técnicas de una arquitectura basada en eventos. Una arquitectura basada en eventos promueve comunicaciones escalables y desacopladas durante la creación, el almacenamiento, el consumo y la reacción a los eventos de interés que se producen en una solución de IoT. Lo primero que se debe hacer con los mensajes que se generan en una solución de IoT es clasificarlos y asignarlos a una serie de eventos. A continuación, dicha solución debe asociar estos últimos con la lógica de negocio que ejecuta los comandos y, posiblemente, genera nuevos eventos en el sistema de IoT. La plataforma AWS proporciona varios servicios de aplicaciones para construir una arquitectura de IoT distribuida y basada en eventos.

Las arquitecturas que se basan en eventos de forma intrínseca dependen de la capacidad de almacenar los eventos de manera duradera y transferírselos a un ecosistema de suscriptores interesados. Para admitir la organización de eventos desacoplados, la plataforma AWS cuenta con diversos servicios de aplicaciones diseñados para almacenar los eventos de forma confiable y para admitir la computación basada en eventos altamente escalable. Una solución de IoT basada en eventos debe utilizar Amazon Simple Queue Service (Amazon SQS), Amazon Simple Notification Service (Amazon SNS) y AWS Lambda como componentes fundamentales de la aplicación para crear flujos de trabajo de eventos simples y complejos. Amazon SQS es un servicio de colas de mensaje rápido, duradero, escalable y completamente administrado. Amazon SNS es un servicio web que publica los mensajes de una aplicación y los entrega inmediatamente a los suscriptores u otras aplicaciones. AWS Lambda se ha diseñado para ejecutar código en respuesta a los eventos, con administración automática de los recursos

informáticos subyacentes. AWS Lambda puede recibir notificaciones directamente de otros servicios de AWS y responder a ellas. En una arquitectura de IoT basada en eventos, la lógica de negocio se ejecuta en AWS Lambda con el fin de determinar cuándo se han producido los eventos de interés en el contexto de un ecosistema de IoT.

Los servicios de AWS tales como Amazon SQS, Amazon SNS y AWS Lambda pueden separar el consumo de los eventos de la lógica de negocio y procesamiento que se les aplica. Esta separación de las responsabilidades genera flexibilidad y agilidad en una solución integral. Además, permite modificar rápidamente la lógica de activación de eventos o aquella que se utiliza para agregar los datos contextuales de las distintas partes de un sistema. Por último, permite introducir cambios en una solución de IoT sin bloquear el flujo continuo de datos enviados entre los dispositivos finales y la plataforma AWS.

Automatización y operaciones de desarrollo

En las soluciones de IoT, el lanzamiento inicial de una aplicación es el principio de un planteamiento a largo plazo que consiste en refinar una y otra vez las ventajas de negocio de una estrategia de IoT. Tras ese primer lanzamiento, la mayor parte del tiempo y el esfuerzo se dedicarán a agregar nuevas características a la solución de IoT actual. Para cumplir el principio de conservar la agilidad durante todo el ciclo de vida de la solución, los clientes deben evaluar los servicios que permiten un desarrollo y una implementación rápidos a medida que cambian las necesidades del negocio. Al contrario que las arquitecturas web tradicionales, en que las tecnologías de operaciones de desarrollo se aplican tan solo a los servidores backend, una aplicación de IoT requiere también la posibilidad de desplegar los cambios incrementalmente en una serie de dispositivos heterogéneos conectados globalmente. Con la plataforma AWS, la compañía puede implementar prácticas de operaciones de desarrollo en los servidores y en los dispositivos con el fin de automatizar las actividades.

Las aplicaciones implementadas en la plataforma en la nube de AWS pueden sacar partido de las diversas tecnologías de desarrollo de operaciones en AWS. Para obtener información general sobre las operaciones de desarrollo de AWS, recomendamos consultar el documento *Introduction to DevOps on AWS*[1]. Si bien la mayoría de las soluciones presentan diferencias en lo que se refiere a requisitos de implementación y operaciones, las soluciones de IoT pueden utilizar AWS CloudFormation para definir mediante código la infraestructura de los servidores. La infraestructura tratada como código presenta beneficios porque no solo se

puede reproducir y comprobar, sino que también es más fácil de implementar en otras regiones de AWS. Las compañías que utilizan AWS CloudFormation conjuntamente con otras herramientas de desarrollo de operaciones mejoran en gran medida la agilidad y el ritmo de los cambios de aplicaciones.

Para diseñar una solución de IoT que cumpla los principios de seguridad y agilidad, las organizaciones también deben actualizar los dispositivos conectados después de haberlos implementado en el entorno. Las actualizaciones del firmware aportan a la compañía un mecanismo para agregar nuevas características a los dispositivos y constituyen un medio esencial para distribuir los parches de seguridad durante la vida útil de dichos dispositivos. Para implementar las actualizaciones de firmware en los dispositivos conectados, la solución de IoT debe almacenar previamente este firmware en un servicio con acceso global como Amazon Simple Storage Service (Amazon S3) que ofrece almacenamiento en la nube seguro, duradero y altamente escalable.
A continuación, la solución de IoT puede implementar Amazon CloudFront, un servicio de red de entrega de contenido (CDN, Content Delivery Network) global, para llevar el firmware almacenado en Amazon S3 a los puntos de presencia de menor latencia para los dispositivos conectados. Por último, el cliente puede utilizar las sombras de AWS IoT para enviar comandos a los dispositivos y pedirles que descarguen la nueva versión del firmware de una dirección URL prefirmada de Amazon CloudFront que restrinja el acceso a los objetos de firmware disponibles a través de la CDN. Una vez completada la actualización, el dispositivo debe confirmar que esta se ha llevado a cabo correctamente enviando un mensaje a la solución de IoT. Organizar este puñado de servicios para efectuar las actualizaciones de firmware permite a los clientes controlar su enfoque de operaciones de desarrollo de dispositivos y escalarlo de tal forma que esté coordinado con su estrategia general de IoT.

En IoT, los procedimientos de automatización y operaciones de desarrollo no se limitan a los servicios de aplicaciones que se implementan en la plataforma AWS, sino que incluyen también los dispositivos que se han implementado como parte de la arquitectura de IoT en su conjunto. Diseñar un sistema que permita efectuar de forma periódica y generalizada las actualizaciones correspondientes a los cambios del firmware y del nuevo software permite a las organizaciones iterar cíclicamente los procesos de extracción de valor de su solución de IoT e innovar de manera continua a medida que se presentan nuevas oportunidades de mercado.

Administración y seguridad

En IoT, la seguridad consiste en mucho más que anonimizar los datos: se trata de la capacidad para obtener información detallada, así como para auditar y controlar el sistema íntegramente. La seguridad de IoT incluye la posibilidad de monitorizar los eventos en toda la solución y de reaccionar ante ellos para lograr los niveles deseados de conformidad y gobernanza. En AWS, la seguridad es nuestra máxima prioridad. El modelo de responsabilidad compartida de AWS aporta a las organizaciones la flexibilidad, la agilidad y el control que precisan para implementar sus requisitos de seguridad.[2] AWS administra la seguridad **de** la nube y los clientes son los responsables de la seguridad **en** la nube. Los clientes conservan el control de los mecanismos de seguridad que deciden implementar para proteger sus datos, aplicaciones, dispositivos, sistemas y redes. Además, las empresas pueden aprovechar la amplia gama de herramientas administrativas y de seguridad que AWS y los socios de AWS proporcionan para crear una solución de IoT que sea fuerte, aislada lógicamente y segura, para una flota de dispositivos.

El primer servicio de monitorización y visibilidad que debe activarse es AWS CloudTrail. AWS CloudTrail es un servicio web que registra las llamadas al API de AWS para una cuenta y entrega los archivos de registro a Amazon S3. Una vez activado AWS CloudTrail, la solución debe incorporar procesos de seguridad y gobernanza basados en la información en tiempo real de las llamadas al API efectuadas en toda la cuenta de AWS. AWS CloudTrail proporciona un nivel de visibilidad y flexibilidad adicional al crear la apertura operativa de un sistema y efectuar iteraciones en él.

Además de registrar las llamadas al API, los clientes deben activar Amazon CloudWatch para todos los servicios de AWS que se utilicen en el sistema. Amazon CloudWatch permite a las aplicaciones monitorizar las métricas de AWS y crear otras personalizadas generadas por la propia aplicación. A su vez, estas métricas pueden activar alertas basadas en los eventos de que se trate. A las métricas de Amazon CloudWatch se suma Amazon CloudWatch Logs. En ellos se almacenan logs adicionales de los servicios de AWS o de las aplicaciones de los clientes y permiten activar eventos basándose en esas métricas adicionales. Los servicios de AWS, tales como AWS IoT, se integran directamente con Amazon CloudWatch Logs. Estos últimos se pueden leer dinámicamente como flujo de datos y procesarse mediante la lógica de negocio y el contexto del sistema, para detectar en tiempo real cualquier anomalía o amenaza de seguridad.

Combinar servicios como Amazon CloudWatch y Amazon CloudTrail con las prestaciones de las identidades y políticas de AWS IoT permite a la compañía obtener de forma inmediata datos valiosos sobre las prácticas de seguridad desde el principio de la estrategia de IoT y satisfacer las necesidades de una implementación de seguridad proactiva en la propia solución de IoT.

Combinación de servicios y soluciones

Para entender mejor el uso que realizan los clientes, predecir tendencias o ejecutar una flota de IoT con más eficacia, las organizaciones deben recopilar y procesar una cantidad de datos de dispositivos conectados potencialmente enorme y, además, deben ser capaces de conectar con grandes flotas de *cosas* y administrarlas.

AWS ofrece una amplia gama de servicios para recopilar y analizar grandes conjuntos de datos, que solemos denominar big data. Estos servicios pueden estar estrechamente integrados en una solución de IoT para hacer posible la recopilación, el procesado y el análisis de los datos de la solución, y también para corroborar o refutar hipótesis basadas en datos de IoT. La capacidad de formular preguntas y responderlas en la misma plataforma que la utilizada para administrar flotas de *cosas* evita que una organización realice trabajo no diferenciado y agiliza la innovación empresarial.

La perspectiva de cohesión de arquitectura de elevado nivel de una solución de IoT que integra IoT, big data y otros servicios se denomina arquitectura pragmática. La arquitectura pragmática está compuesta por capas de soluciones:

- Cosas: el dispositivo y la flota de dispositivos
- Capa de control: el punto de control para obtener acceso a la capa de velocidad y el nexo de administración de la flota.
- Capa de velocidad: el bus de datos de entrada de telemetría del dispositivo de ancho de banda elevado y el bus de comandos de dispositivo de salida.
- Capa de servicio: el punto de acceso para sistemas y personas desde el que interactúan con los dispositivos en una flota para el análisis, el archivado y la correlación de datos, y también usar visualizaciones en tiempo real de la flota.

Arquitectura pragmática

La arquitectura pragmática es una perspectiva cohesionada única de cómo los preceptos básicos de IoT se manifiestan como una solución de IoT cuando se usan los servicios de AWS.

Un escenario de una solución de IoT basada en arquitectura pragmática es el procesamiento de datos emitidos por los dispositivos, que recibe el nombre de telemetría. En el diagrama anterior, después de que un dispositivo autentica mediante un certificado de dispositivo obtenido del servicio AWS IoT en la capa de control, el dispositivo envía periódicamente los datos de telemetría a la puerta de enlace para dispositivos de AWS IoT en la capa de velocidad. El motor de reglas de IoT procesa después esos datos de telemetría como un evento que Amazon Kinesis o AWS Lambda proporcionarán a los usuarios web para que lo utilicen en las interacciones con la capa de servicios.

Otro escenario de una solución de IoT basada arquitectura pragmática es enviar un comando a un dispositivo. En el diagrama anterior, la aplicación del usuario escribiría el valor deseado del comando en la sombra de IoT del dispositivo de destino. Después, la sombra de AWS IoT y la puerta de enlace de dispositivos colaborarían para superar el obstáculo de una red intermitente y transmitir el comando al dispositivo específico.

Esto son solo dos escenarios para dispositivos que puede encontrar en la amplia gama de soluciones para la arquitectura pragmática. Ninguno de estos escenarios responde a la necesidad de procesar la potencialmente gran cantidad de datos que recopilan los dispositivos conectados, y de ahí la importancia de tener un backend de big data integrado. El backend de big data de este diagrama es

coherente con todo el ecosistema de soluciones de big data en tiempo real y en modo de lotes para cuya creación los clientes ya aprovechan la plataforma AWS. Dicho de otro modo, desde la perspectiva de big data, la telemetría de IoT equivale a los "datos ingeridos" en las soluciones de big data. Si desea leer más información sobre las soluciones de big data en AWS, utilice el enlace a continuación.

Las empresas han usado la plataforma AWS para crear numerosas soluciones de big data de todo tipo. La arquitectura pragmática muestra que, si se construye la solución de IoT en la misma plataforma, se puede utilizar todo el ecosistema de soluciones de big data.

Resumen

Definir su estrategia para Internet de las cosas puede ser un revulsivo que abra la puerta a innovaciones de negocio excepcionales. A medida que las organizaciones comienzan a esforzarse en sus propias innovaciones de IoT, es fundamental seleccionar una plataforma que promueva los principios básicos: agilidad empresarial y técnica, escalabilidad, costos y seguridad. La plataforma de AWS va más allá de los preceptos básicos de una solución de IoT, puesto que no solo proporciona los servicios de IoT, sino que los ofrece junto con otros servicios de plataforma más amplios, profundos y valorados con una presencia global. Gracias a estos servicios adicionales, disfrutará de la libertad necesaria para incrementar el control de su empresa sobre su propio destino y para que las soluciones de IoT de su empresa iteren más rápidamente y proporcionen los resultados que persigue su estrategia de IoT.

Como pasos siguientes en la evaluación de plataformas de IoT, le recomendamos que *lea* la sección a continuación, en la que encontrará más información sobre AWS IoT, soluciones de big data en AWS y casos prácticos de clientes en AWS.

Colaboradores

Este documento ha sido elaborado por:

- Olawale Oladehin, arquitecto de soluciones, Amazon Web Services
- Brett Francis, arquitecto principal de soluciones de seguridad, Amazon Web Services

Documentación adicional

Si desea leer más sobre este tema, consulte estas fuentes:

- Servicio de AWS IoT
- Getting Started with AWS IoT
- Casos prácticos de AWS
- Opciones de análisis de big data en AWS

Notas

[1] https://do.awsstatic.com/whitepapers/AWS_DevOps.pdf

[2] https://aws.amazon.com/compliance/shared-responsibility-model/