Seguridad a escala: gobernanza en AWS

Análisis de las características de AWS que pueden aliviar los problemas locales

Noviembre de 2013

(Consulte http://aws.amazon.com/compliance para acceder a la versión más actualizada de este documento)

Tabla de contenido

Resumen

En AWS se puede ejecutar prácticamente todo lo que se ejecuta de forma local: sitios web, aplicaciones, bases de datos, aplicaciones móviles, campañas de correo electrónico, análisis de datos distribuidos, almacenamiento y redes privadas. Los servicios que ofrece AWS están diseñados para funcionar conjuntamente, por lo que puede crear soluciones completas. Una ventaja que se suele pasar por alto de la migración de cargas de trabajo a AWS es la capacidad de conseguir un nivel superior de seguridad, a escala, utilizando las numerosas características de gobernanza que se ofrecen. Por los mismos motivos que la entrega de infraestructura en la nube tiene ventajas sobre la entrega local, la gobernanza basada en la nube ofrece un coste menor de entrada, operaciones más sencillas y mayor agilidad al proporcionar más supervisión, control de seguridad y automatización central. En este documento se describe cómo puede conseguir un alto nivel de gobernanza de los recursos de TI con AWS. Este documento, junto con los documentos técnicos Riesgos y conformidad de AWS y Lista de comprobación de la auditoría de seguridad, puede ayudarle a entender las características de seguridad y gobernanza integradas en los servicios de AWS, de forma que pueda incorporar beneficios y prácticas recomendadas de seguridad al crear su entorno integrado con AWS.

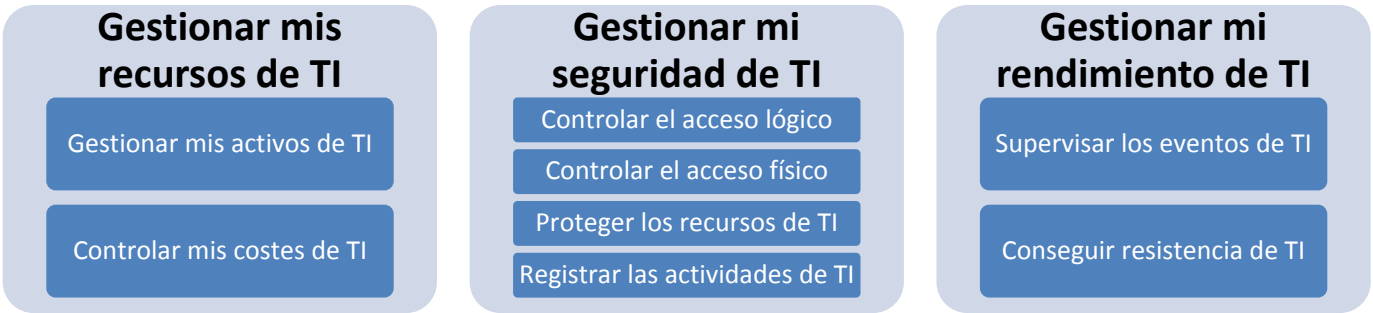
Introducción

Los organismos reguladores y del sector han creado una trama compleja de leyes y normativas nuevas y heredadas que exigen un extenso abanico de medidas seguridad y gobernanza organizativa. Por tanto, las empresas de investigación calculan que muchas empresas dedican hasta el 75 % del dinero empleado en TI a gestionar la infraestructura y solo gastan el 25 % en aspectos de TI que están relacionados directamente con las actividades de sus empresas. Una de las formas clave de mejorar esta métrica consiste en abordar de forma más eficiente los requisitos de gobernanza de TI administrativa. Hay una forma sencilla y eficaz de hacerlo que pasa por aprovechar las características de gobernanza integradas de AWS.

Si bien AWS ofrece diversas características de gobernanza de TI, puede resultar complicado decidir cómo empezar y qué implementar. En este documento se examinan los dominios habituales de gobernanza de TI; para ello se ofrece el caso de uso (o el problema local), las características de AWS relacionadas y las propuestas de valor de gobernanza asociadas al uso de dichas características. Este documento está diseñado para ayudarle a alcanzar los objetivos de cada dominio de gobernanza de TI[1].

Este documento sigue el enfoque de los ámbitos principales de los marcos de gobernanza de TI que se suelen implementar (por ejemplo, CoBIT, ITIL, COSO, CMMI, etc.); no obstante, los dominios de gobernanza de TI alrededor de los que se organiza este documento son genéricos para que cualquier cliente pueda utilizarlo con el fin de evaluar las características de gobernanza de AWS frente a lo que se puede hacer con los recursos y las herramientas locales. Se abordan los dominios siguientes de gobernanza de TI con un enfoque de “caso de uso”:

Quiero mejorar…



[1] Si bien este documento técnico contiene una lista de características de gobernanza, no contiene todas las características disponibles ya que se siguen desarrollando continuamente. Hay más tutoriales, herramientas para desarrolladores y documentación en http://aws.amazon.com/resources/.

Gestionar los recursos de TI

Gestionar los activos de TI

La identificación y la gestión de sus recursos de TI es el primer paso para una gobernanza de TI eficaz. Los activos de TI pueden variar desde los enrutadores, conmutadores, servidores, hosts y firewalls de alta gama hasta las aplicaciones, los servicios, los sistemas operativos y otros activos de software implementados en la red. Es de vital importancia tener un inventario actualizado de los activos de hardware y software para tomar decisiones sobre actualizaciones y compras, hacer un seguimiento del estado de la garantía, resolución de problemas y por motivos de seguridad. Cada vez es más necesario disponer de un listado de inventario detallado de los activos para ofrecer vistas e informes completos bajo demanda. Además, algunas normativas de conformidad exigen específicamente inventarios de activos detallados. Por ejemplo, FISMA, SOX, PCI DSS e HIPAA exigen inventarios exactos de activos como parte de sus requisitos. No obstante, la naturaleza de los diversos recursos locales combinados puede hacer que el mantenimiento de este listado sea laborioso en el mejor de los casos e imposible en el peor. A menudo, las empresas tienen que emplear soluciones de terceros para automatizar el listado de inventario de los activos y, aún así, no siempre es posible ver un inventario detallado de cada tipo de activo en una sola consola.

Con AWS, dispone de varias características que permiten obtener rápida y fácilmente un inventario exacto de sus recursos de TI de AWS. A continuación se indican esas características, junto con instrucciones y enlaces a más información:

Característica de gobernanza de AWS	Cómo se consigue seguridad a escala
Página Actividad de la cuenta	Ofrece un listado resumido de los recursos de TI en el que se detalla el uso de cada servicio por región. Más información.
Inventario de almacenes de Amazon Glacier	Ofrece un inventario de datos de Glacier mostrando todos los recursos de TI de Glacier. Más información.
AWS CloudHSM	Ofrece control virtual y físico sobre las claves de cifrado proporcionando HSM dedicados del cliente para el almacenamiento de claves. Más información.
AWS Data Pipeline Task Runner	Ofrece procesamiento automatizado de tareas mediante la llamada selectiva de tareas de AWS Data Pipeline y la notificación posterior del estado de esas tareas. Más información.
AWS Management Console	Ofrece un inventario en tiempo real de los activos y los datos; muestra todos los recursos de TI que se ejecutan en AWS, por servicio. Más información.
API de AWS Storage Gateway	Ofrece la posibilidad de realizar inventarios de activos y datos mediante programación; utiliza interfaces de programación, herramientas y scripts para gestionar los recursos. Más información.

Controlar los costes de TI

Es posible controlar mejor los costes de TI mediante la obtención de recursos de la forma más rentable y entendiendo los costes de los servicios de TI. Sin embargo, puede resultar complicado e impreciso gestionar y hacer un seguimiento de los costes y el ROI asociados al gasto local en recursos de TI porque los cálculos son muy complejos; la planificación de la capacidad, las predicciones de uso, los costes de compra, la depreciación, el coste de capital y los costes de las instalaciones son solo algunos aspectos que dificultan el cálculo del coste total de propiedad.

AWS dispone de varias características que le permiten entender y controlar fácilmente y con precisión los costes de sus recursos de TI. Con AWS puede conseguir ahorros de costes de hasta el 80 % en comparación con las implementaciones locales equivalentes[2]. A continuación se indican esas características, junto con instrucciones y enlaces a más información:

Característica de gobernanza de AWS	Cómo se consigue seguridad a escala
Página Actividad de la cuenta	Ofrece siempre una vista de los gastos en recursos de TI mostrando los recursos utilizados por servicio. Más información.
Lanzamiento de una instancia de idempotencia de Amazon EC2	Ayuda a impedir el lanzamiento erróneo de recursos e incurrir en costes adicionales al evitar errores de tiempos de espera o de conexión al lanzar instancias adicionales. Más información.
Etiquetado de recursos de Amazon EC2	Ofrece una asociación entre los gastos en recursos y las unidades de negocio mediante la aplicación de etiquetas personalizadas a los recursos informáticos en las que se pueden realizar búsquedas. Más información.
AWS Account Billing	Proporciona características de facturación fáciles de utilizar que le permiten supervisar y pagar su factura; se detallan los recursos utilizados y los costes informáticos reales asociados en los que se ha incurrido. Más información.
AWS Management Console	Ofrece una vista única de los factores de coste mostrando todos los recursos de TI que se ejecutan en AWS por servicio, incluidos los costes reales y tasa de ejecución. Más información.
Precios de los servicios de AWS	Ofrece información fundamental sobre las tarifas de los recursos de TI de AWS, indicando los precios de cada producto de AWS y características específicas de precios. Más información.
AWS Trusted Advisor	Ayuda a optimizar el coste de los recursos de TI al identificar los recursos que no se utilizan y los recursos inactivos. Más información.
Alarmas de facturación	Ofrecen alertas proactivas sobre el gasto en recursos de TI mediante el envío de notificaciones de las actividades de gastos. Más información.

[2] Consulte el documento técnico Total Cost of Ownership para obtener más información acerca de los ahorros de costes globales que se consiguen con AWS

Facturación unificada	Ofrece control de costes centralizado y visibilidad de los costes de distintas cuentas al combinar varias cuentas de AWS en una sola factura. Más información.
Precio de pago por uso	Ofrece recursos informáticos y servicios que puede utilizar para crear aplicaciones en cuestión de minutos con el sistema de pago por uso sin costes de compra ni costes de mantenimiento continuo por adelantado gracias al escalado automático a varios servidores cuando la demanda de su aplicación aumenta. Más información.

Gestionar la seguridad de TI

Controlar el acceso físico a los recursos de TI

La gestión del acceso físico es un componente clave de los programas de gobernanza de TI. Además de las cerraduras, las alarmas de seguridad, los controles de acceso y la videovigilancia que definen los componentes tradicionales de la seguridad física, los controles electrónicos sobre el acceso físico son también indispensables para lograr una seguridad física eficaz. El sector tradicional de la seguridad física está en rápida transición y están surgiendo áreas de especialización que hacen que la seguridad física sea mucho más compleja. Puesto que las consideraciones y los controles de seguridad física locales son cada vez más complejos, existe una necesidad creciente de profesionales cualificados y especializados de seguridad de TI para gestionar el importante esfuerzo que es necesario para conseguir un control físico efectivo con credenciales de acceso para tarjetas y lectores de tarjetas, controladores y servidores para alojar datos sobre la seguridad física.

Con AWS, puede externalizar de manera sencilla y eficaz los controles relacionados con la seguridad física de la infraestructura de AWS a los especialistas en AWS que disponen de los conocimientos y los recursos necesarios para proteger el entorno físico. AWS dispone de varios auditores independientes que validan la seguridad física de los centros de datos durante todo el año, dando fe del diseño y probando detalladamente la eficacia de nuestros controles de seguridad física. Obtenga más información acerca de los programas de auditoría de AWS y los controles de seguridad física asociados siguientes:

Característica de gobernanza de AWS	Cómo se consigue seguridad a escala
Controles de acceso físico SOC 1 de AWS	Ofrece transparencia en los controles existentes que impiden el acceso no autorizado a los centros de datos. Los controles están diseñados, probados y auditados debidamente por una empresa independiente de auditoría. Más información.
Controles de acceso físico SOC 2 de AWS	Ofrece transparencia en los controles existentes que impiden el acceso no autorizado a los centros de datos. Los controles están diseñados, probados y auditados debidamente por una empresa independiente de auditoría. Más información.

Controles de acceso físico PCI DSS de AWS	Ofrece transparencia en los controles existentes que impiden el acceso no autorizado a los centros de datos, pertinentes para el estándar de seguridad de los datos del sector de las tarjetas de pago (PCI DSS). Los controles están diseñados, probados y auditados debidamente por una empresa independiente de auditoría. Más información.
Controles de acceso físico ISO 27001 de AWS	Ofrece transparencia en los controles y procesos existentes que impiden el acceso no autorizado a los centros de datos, pertinentes para el estándar de prácticas recomendadas de seguridad ISO 27002. Los controles están diseñados, probados y auditados debidamente por una empresa independiente de auditoría. Más información.
Controles de acceso físico de FedRAMP de AWS	Ofrece transparencia en los controles y procesos existentes que impiden el acceso no autorizado a los centros de datos, pertinentes para el estándar de prácticas recomendadas NIST 800-53. Los controles están diseñados, probados y auditados debidamente por una empresa independiente de auditoría acreditada por el gobierno. Más información.

Controlar el acceso lógico a los recursos de TI

Uno de los objetivos principales de la gobernanza de TI es la gestión eficaz del acceso lógico a los sistemas informáticos y los datos. No obstante, muchas organizaciones se esfuerzan por escalar sus soluciones locales para satisfacer la creciente cantidad de consideraciones y complejidades que rodean al acceso lógico, en constante cambio, incluida la capacidad de establecer una regla de privilegios mínimos, gestionar permisos para los recursos, abordar los cambios en las funciones y las necesidades de información, y el crecimiento de datos confidenciales. Los principales problemas persistentes de gestión del acceso lógico en un entorno local están relacionados con la concesión de acceso a los usuarios según lo siguiente:

- Función (es decir, usuarios internos, contratistas, personas externas, socios, etc.).
- Clasificación de los datos (por ejemplo, confidenciales, solo para uso interno, privados, públicos, etc.).
- Tipo de datos (por ejemplo, credenciales, datos personales, información de contacto, datos relacionados con el trabajo, certificados digitales, contraseñas cognitivas, etc.).

AWS ofrece varias características de control para gestionar eficazmente el acceso lógico según una matriz de casos de uso basados en los privilegios mínimos. A continuación se indican esas características, junto con instrucciones y enlaces a más información:

Característica de gobernanza de AWS	Cómo se consigue seguridad a escala
Listas de control de acceso (ACL) de Amazon S3	Ofrece permisos y condiciones centrales añadiendo condiciones específicas para controlar la forma en que un usuario puede utilizar AWS, como la hora del día, la dirección IP de origen, si utiliza o no SSL, o si se ha autenticado con un dispositivo de Multi-Factor Authentication. Puede ver más información aquí y aquí.

Políticas de depósito de Amazon S3	Ofrece la posibilidad de crear reglas condicionales para gestionar el acceso a depósitos y objetos al permitirle restringir el acceso según la cuenta y según atributos de la solicitud, como la referencia HTTP y la dirección IP. Más información.
Autenticación de cadenas de consulta de Amazon S3	Permite conceder acceso HTTP o del navegador a recursos que requerirían normalmente autenticación; para ello se utiliza la firma de la cadena de consulta para proteger la solicitud. Más información.
AWS CloudTrail	Registra las acciones de API o de la consola (por ejemplo, registra si alguien cambia una política de depósito, detiene una instancia, etc.), lo que permite capacidades de supervisión avanzadas. Más información.
AWS IAM Multi-Factor Authentication (MFA)	Aplica MFA en todos los recursos al solicitar un token para iniciar sesión y acceder a los recursos. Más información.
Política de contraseñas de AWS IAM	Ofrece la posibilidad de gestionar la calidad y los controles sobre las contraseñas de los usuarios al permitirle definir una política para las contraseñas utilizadas por los usuarios de IAM que especifique que las contraseñas deben tener una longitud determinada, deben incluir una selección de caracteres, etc. Más información.
Permisos de AWS IAM	Ofrece la posibilidad de gestionar fácilmente los permisos al permitirle especificar quién tiene acceso a los recursos de AWS y qué acciones pueden realizar en dichos recursos. Más información.
Políticas de AWS IAM	Permite conseguir una gestión detallada de los accesos con privilegios mínimos al permitirle crear varios usuarios dentro de su cuenta de AWS, asignarles credenciales de seguridad y gestionar sus permisos. Más información.
Funciones de AWS IAM	Ofrece la posibilidad de delegar temporalmente el acceso a usuarios o a servicios que normalmente no tienen acceso a sus recursos de AWS; para ello se define un conjunto de permisos de acceso a los recursos que un usuario o un servicio necesita. Más información.
AWS Trusted Advisor	Ofrece una evaluación automatizada de gestión de la seguridad al identificar y escalar posibles problemas de seguridad y de permisos. Más información.

Proteger los recursos de TI

La protección de los recursos de TI es la piedra angular de los programas de gobernanza de TI. Sin embargo, en los entornos locales, se debe tomar una lista interminable de medidas de seguridad cuando se pone en marcha un servidor nuevo. Por ejemplo, hay que actualizar las políticas de firewall y de control de acceso, hay que verificar que la imagen del servidor recién creada sea conforme con la política de seguridad, y hay que verificar que todos los paquetes de software están actualizados. A menos que estas tareas de seguridad se automaticen y entreguen de manera que puedan seguir el ritmo de las necesidades tan dinámicas de la empresa, las organizaciones que utilizan exclusivamente enfoques tradicionales de gobernanza harán que los usuarios eludan los controles de seguridad o causarán costosos retrasos para la empresa.

AWS proporciona diversas características de seguridad que le permiten proteger fácil y eficazmente sus recursos de TI. A continuación se indican esas características, junto con instrucciones y enlaces a más información:

Característica de gobernanza de AWS	Cómo se consigue seguridad a escala
AMI de Amazon Linux	Permite implementar de forma coherente una imagen de “oro” (reforzada) desarrollando una imagen privada que se utilizará en todas las implementaciones de instancias. Más información.
Instancias dedicadas de Amazon EC2	Proporciona una red privada virtual aislada, garantiza que las instancias informáticas de Amazon EC2 están aisladas en el nivel de hardware y lanza estas instancias en una VPC. Más información.
Asistente de lanzamiento de instancias de Amazon EC2	Hace posible un proceso coherente de lanzamiento al imponer restricciones sobre las imágenes de máquinas disponibles cuando se lanzan instancias. Más información.
Grupos de seguridad de Amazon EC2	Ofrece un control específico sobre el tráfico de entrada y de salida al actuar como un firewall que controla el tráfico de una o varias instancias. Más información.
Archivos de Amazon Glacier	Ofrece un servicio económico de almacenamiento a largo plazo para la protección y el almacenamiento duradero de archivos de datos y copias de seguridad mediante el uso de cifrado AES de 256 bits de forma predeterminada. Más información.
Cifrado en el cliente de Amazon S3	Permite cifrar los datos antes de enviarlos a Amazon S3 mediante la creación de una biblioteca propia que cifra los datos de los objetos en el cliente antes de cargarlos en Amazon S3. AWS SDK para Java también puede cifrar automáticamente los datos antes de cargarlos en Amazon S3. Más información.
Cifrado en el servidor de Amazon S3	Ofrece el cifrado de objetos en reposo y de claves gestionadas por AWS mediante el uso de cifrado AES de 256 bits para los datos de Amazon S3. Más información.

Amazon VPC	Proporciona una red virtual muy similar a una red tradicional local, pero con las ventajas que supone utilizar la infraestructura escalable de AWS. Permite crear secciones aisladas de forma lógica de AWS en las que puede lanzar recursos de AWS en una red virtual que defina. Más información.
Aislamiento lógico de Amazon VPC	Ofrece aislamiento virtual de recursos al permitir que las imágenes de máquinas estén aisladas de otros recursos de la red. Más información.
ACL de red de Amazon VPC	Ofrece un aislamiento de "tipo firewall" para las subredes asociadas al controlar el tráfico de entrada y salida en el nivel de subred. Más información.
Direcciones IP privadas de Amazon VPC	Ayuda a proteger las direcciones IP privadas frente a la exposición a Internet al enrutar el tráfico a través de una instancia de traducción de direcciones de red (NAT) en una subred pública. Más información.
Grupos de seguridad de Amazon VPC	Ofrece un aislamiento de "tipo firewall" para las instancias asociadas de Amazon EC2 al controlar el tráfico de entrada y salida en el nivel de instancia. Más información.
Plantillas de AWS CloudFormation	Permite implementar de forma coherente una imagen de máquina concreta junto con otros recursos y configuraciones al aprovisionar la infraestructura con scripts. Más información.
AWS Direct Connect	Elimina la necesidad de una conexión pública de Internet a AWS al establecer una conexión de red dedicada desde sus instalaciones al centro de datos de AWS. Más información.
Conexiones de VPN locales de hardware y software	Ofrece un control específico sobre la seguridad de la red al permitir conexiones seguras a AWS desde redes existentes. Más información.
Puertas de enlace privadas virtuales	Ofrece un control específico sobre la seguridad de la red al proporcionar una forma de crear una conexión de VPN de hardware con su VPC. Más información.

Gestionar el registro de los recursos de TI

Un elemento importante al servicio de la protección de TI es el registro de los recursos de TI. El registro es fundamental para la gobernanza de TI en una amplia variedad de casos de uso, incluidos pero sin limitarse a: detección y seguimiento de comportamientos sospechosos, ayuda en análisis forenses, cumplimiento de los requisitos de conformidad, apoyo al mantenimiento y las operaciones de TI y redes, gestión y reducción de los costes de seguridad de TI, supervisión de los niveles de servicio y ayuda para los procesos empresariales internos. Las empresas dependen cada vez más de una gestión eficaz de los registros para apoyar funciones básicas de gobernanza, incluida la gestión de costes, la supervisión de los niveles de servicio y las aplicaciones de línea de negocio, y otras actividades centradas en la conformidad y la seguridad de TI. La encuesta SANS Log Management Survey sobre la gestión de registros muestra que las organizaciones buscan constantemente más usos de sus registros, pero tienen problemas para conseguir que los casos de uso que utilizan recursos internos recopilen y analicen esos registros. Al haber más tipos de registros que recopilar y analizar procedentes de diferentes recursos de TI, las organizaciones se enfrentan a la sobrecarga manual que supone normalizar los datos de registro que se encuentran en formatos muy diferentes, así como las funcionalidades de búsqueda, correlación y generación de informes. La gestión de los registros es una capacidad clave para la supervisión de la seguridad, el cumplimiento y la toma de decisiones efectiva para las decenas o cientos de miles de actividades cotidianas.

AWS dispone de varias características de registro que le permiten registrar y hacer un seguimiento de manera eficaz del uso de sus recursos de TI. A continuación se indican esas características, junto con instrucciones y enlaces a más información:

Característica de gobernanza de AWS	Cómo se consigue seguridad a escala
Registros de acceso de Amazon CloudFront	Proporciona archivos de registro con información acerca del acceso de los usuarios finales a sus objetos. Los registros se pueden distribuir directamente a un depósito específico de Amazon S3. Más información.
Registros de base de datos de Amazon RDS	Ofrece una forma de supervisar varios archivos de registro generados por sus instancias de base de datos de Amazon RDS. Se utilizan para diagnosticar, resolver problemas y corregir problemas de configuración o de rendimiento de bases de datos. Más información.
Vencimiento de objetos de Amazon S3	Proporciona un vencimiento automatizado de los registro al programar la eliminación de objetos tras un período de tiempo definido. Más información.
Registros de acceso al servidor de Amazon S3	Ofrece registros de las solicitudes de acceso con detalles acerca de la solicitud como el tipo de solicitud, el recurso con el que se realizó la solicitud, y la hora y la fecha en que se procesó la solicitud. Más información.
AWS CloudTrail	Ofrece registros de las acciones de seguridad realizadas a través de AWS Management Console o de las API. Más información.

Gestionar el rendimiento de TI

Supervisar y responder a eventos

La gestión y la supervisión del rendimiento de TI se ha convertido en una parte estratégicamente importante de todo programa de gobernanza de TI. La supervisión de TI es un elemento fundamental de la gobernanza que permite prevenir, detectar y corregir problemas de TI que pueden afectar al rendimiento y a la seguridad. En lo que respecta a la gestión del rendimiento de TI, el obstáculo fundamental de la gobernanza en entornos locales es que se enfrenta a varios sistemas de supervisión para gestionar cada capa de los recursos de TI, y la combinación de herramientas de gestión y procesos de TI propietarios produce una complejidad sistémica que en el mejor de los casos puede reducir el tiempo de respuesta y en el peor de los casos puede afectar a la eficacia de la supervisión y gestión del rendimiento de TI. Además, la complejidad y la sofisticación crecientes de las amenazas de seguridad hacen que las capacidades de supervisión y respuesta a eventos tengan que evolucionar continuamente y con rapidez para poder afrontar las amenazas emergentes. Por tanto, la gestión del rendimiento local se enfrenta continuamente a desafíos mayores en lo que respecta a la compra de infraestructura, escalabilidad, capacidad para simular condiciones de prueba en varias geografías, etc.

AWS dispone de varias características de supervisión que le permiten supervisar y gestionar sus recursos de TI de forma sencilla y eficaz. A continuación se indican esas características, junto con instrucciones y enlaces a más información:

Característica de gobernanza de AWS	Cómo se consigue seguridad a escala
Amazon CloudWatch	Ofrece datos estadísticos que puede utilizar para ver, analizar y definir alarmas sobre el comportamiento operativo de las instancias. Entre estas métricas se incluyen la utilización de la CPU, el tráfico de red, la entrada y salida, y la latencia. Más información.
Alarmas de Amazon CloudWatch	Ofrece alarmas coherentes para eventos importantes proporcionando métricas, alarmas y notificaciones personalizadas de eventos. Más información.
Estado de la instancia de Amazon EC2	Proporciona comprobaciones del estado de la instancia que resumen los resultados de las pruebas automatizadas y ofrecen información acerca de ciertas actividades que están programadas para las instancias. Utiliza comprobaciones automatizadas para detectar si hay algún problema específico que afecte a sus instancias. Más información.
Equipo de gestión de incidentes de Amazon	Proporciona detección, supervisión y gestión continuas de incidentes con operadores disponibles 24 horas al día los 7 días de la semana los 365 días del año para detectar, diagnosticar y resolver determinados eventos de seguridad. Más información.
Reconocimiento selectivo de TCP de Amazon S3	Permite mejorar el tiempo de recuperación tras un gran número de pérdidas de paquetes. Más información.
Amazon Simple Notification Service	Ofrece alarmas coherentes para eventos importantes al gestionar la entrega de mensajes a extremos o clientes suscriptores. Más información.

AWS Elastic Beanstalk	Permite supervisar detalles de implementación de las aplicaciones como aprovisionamiento de capacidad, equilibrio de carga, escalado automático y supervisión del estado de las aplicaciones. Más información.
Elastic Load Balancing	Permite distribuir automáticamente el tráfico entrante de las aplicaciones entre varias instancias de Amazon EC2 al detectar las instancias sobreutilizadas y reenrutar el tráfico hacia las instancias infrautilizadas. Más información.

Conseguir resistencia

La planificación de la protección de datos y de la recuperación ante desastres debe ser un componente prioritario de gobernanza de TI para todas las organizaciones. Se puede afirmar que el valor de la recuperación ante desastres no está en tela de juicio; a todas las organizaciones les preocupa su capacidad de recuperación tras un evento o un desastre. Pero la implementación de gobernanza sobre la resistencia de los recursos de TI puede resultar costosa y compleja, además de tediosa y laboriosa. Las empresas se enfrentan a un número creciente de eventos que pueden dar lugar a tiempo de inactividad no planificado e inhibidores operativos. Estos eventos pueden deberse a problemas técnicos (por ejemplo, virus, daños en los datos, error humano, etc.) o a fenómenos naturales (como incendios, inundaciones, cortes de electricidad, apagones debidos a fenómenos meteorológicos, etc.). Por tanto, las organizaciones se enfrentan a mayores costes y complejidad a la hora de planificar, probar y operar sitios locales de conmutación por error debido al continuo crecimiento de los datos.

Ante estos desafíos, la virtualización de servidores que ofrece la informática en la nube hace que los programas de resistencia de calidad sean viables y rentables. AWS dispone de varias características que le permiten conseguir resistencia de los recursos de TI de forma sencilla y eficaz. A continuación se indican esas características, junto con instrucciones y enlaces a más información:

Característica de gobernanza de AWS	Cómo se consigue seguridad a escala
Instantáneas de Amazon EBS	Proporciona volúmenes de almacenamiento predecibles de alta disponibilidad y alta fiabilidad, con control incremental de copia de seguridad de un momento dado de los datos de los servidores. Más información.
Implementaciones en zonas de disponibilidad múltiples (Multi-AZ) de Amazon RDS	Permite salvaguardar los datos en el evento gracias a controles automáticos de disponibilidad y una arquitectura sólida y homogénea. Más información.
AWS Import/Export	Permite mover localmente cantidades masivas de datos creando rápidamente trabajos de importación y exportación mediante la red interna de alta velocidad de Amazon. Más información.
AWS Storage Gateway	Ofrece una integración perfecta y segura entre su entorno local de TI y la infraestructura de almacenamiento de AWS mediante la programación de instantáneas que la puerta de enlace almacena en Amazon S3 en forma de instantáneas de Amazon EBS. Más información.

AWS Trusted Advisor	Proporciona gestión del rendimiento y control de disponibilidad automatizados identificando las opciones para aumentar la disponibilidad y la redundancia de la aplicación de AWS. Más información.
Soluciones completas de terceros	Ofrece almacenamiento de datos seguro y control automatizado de disponibilidad al conectarle fácilmente con un mercado de aplicaciones y herramientas. Más información.
Servicios gestionados de bases de datos no SQL y SQL de AWS	Ofrece almacenamiento de datos seguro y duradero al replicar automáticamente los elementos de datos en varias zonas de disponibilidad de una región con el fin de conseguir alta disponibilidad y durabilidad de los datos. Más información: • Amazon Dynamo DB • Amazon RDS
Implementación en varias regiones	Proporciona diversidad geográfica en ubicaciones de informática, redes eléctricas, líneas de fallas, etc. al ofrecer diversas ubicaciones. Más información.
Comprobaciones de estado y conmutación por error de DNS de Route 53	Supervisa la disponibilidad de los datos de copia de seguridad almacenados, lo que permite configurar la conmutación por error de DNS en configuraciones activo-activo, activo-pasivo y mixtas para mejorar la disponibilidad de su aplicación. Más información.

Índice de características de gobernanza de servicios

La información anterior se presenta por dominio de gobernanza. Como referencia, en la tabla siguiente se muestra un resumen de las características de gobernanza agrupadas por los principales servicios de AWS:

Servicio de AWS	**Característica de gobernanza**
Amazon EC2	Lanzamiento de una instancia de idempotencia de Amazon EC2 Etiquetado de recursos de Amazon EC2 AMI de Amazon Linux Instancias dedicadas de Amazon EC2 Asistente de lanzamiento de instancias de Amazon EC2 Grupos de seguridad de Amazon EC2
Elastic Load Balancing	Distribución del tráfico de Elastic Load Balancing

Amazon VPC	Amazon VPC Aislamiento lógico de Amazon VPC ACL de red de Amazon VPC Direcciones IP privadas de Amazon VPC Grupos de seguridad de Amazon VPC Conexiones de VPN locales de hardware y software
Amazon Route 53	Conjuntos de registros de recursos de latencia de Amazon Route 53 Comprobaciones de estado y conmutación por error de DNS de Route 53
AWS Direct Connect	AWS Direct Connect
Amazon S3	Listas de control de acceso (ACL) de Amazon S3 Políticas de depósito de Amazon S3 Autenticación de cadenas de consulta de Amazon S3 Cifrado en el cliente de Amazon S3 Cifrado en el servidor de Amazon S3 Vencimiento de objetos de Amazon S3 Registros de acceso al servidor de Amazon S3 Reconocimiento selectivo de TCP de Amazon S3 Escalado de ventanas de TCP de Amazon S3
Amazon Glacier	Inventario de almacenes de Amazon Glacier Archivos de Amazon Glacier
Amazon EBS	Instantáneas de Amazon EBS
AWS Import/Export	Datos masivos de AWS Import/Export
AWS Storage Gateway	Integración de AWS Storage Gateway API de AWS Storage Gateway
Amazon CloudFront	Amazon CloudFront Registros de acceso de Amazon CloudFront

Amazon RDS	Registros de base de datos de Amazon RDS Implementaciones en zonas de disponibilidad múltiples (Multi-AZ) de Amazon RDS Servicios gestionados de bases de datos no SQL y SQL de AWS
Amazon Dynamo DB	Servicios gestionados de bases de datos no SQL y SQL de AWS
AWS Management Console	Página Actividad de la cuenta AWS Account Billing Precios de los servicios de AWS AWS Trusted Advisor Alarmas de facturación Facturación unificada Precio de pago por uso AWS CloudTrail Equipo de gestión de incidentes de Amazon Amazon Simple Notification Service Implementación en varias regiones
AWS Identity and Access Management (IAM)	AWS IAM Multi-Factor Authentication (MFA) Política de contraseñas de AWS IAM Permisos de AWS IAM Políticas de AWS IAM Funciones de AWS IAM
Amazon CloudWatch	Panel de control de AWS CloudWatch Alarmas de Amazon CloudWatch
AWS Elastic Beanstalk	Supervisión de AWS Elastic Beanstalk
AWS CloudFormation	Plantillas de AWS CloudFormation
AWS Data Pipeline	AWS Data Pipeline Task Runner

AWS CloudHSM	Almacenamiento de claves de CloudHSM
AWS Marketplace	Soluciones completas de terceros
Centros de datos	Controles de acceso físico SOC 1 de AWS Controles de acceso físico SOC 2 de AWS Controles de acceso físico PCI DSS de AWS Controles de acceso físico ISO 27001 de AWS Controles de acceso físico de FedRAMP de AWS

Conclusión

El objetivo principal de la gobernanza de TI es la gestión de los recursos, la seguridad y el rendimiento para conseguir la armonización estratégica con los objetivos empresariales. Dada la tasa de crecimiento y la creciente complejidad de la tecnología, cada vez es más complicado escalar los entornos locales para que ofrezcan las características y los controles detallados necesarios para conseguir una gobernanza de TI de calidad de forma rentable. Por los mismos motivos que la entrega de infraestructura en la nube tiene ventajas con respecto a la entrega local, la gobernanza basada en la nube ofrece un coste inferior de entrada, operaciones más sencillas y mayor agilidad al proporcionar más supervisión y automatización, lo que permite que las organizaciones se centren en su área de negocio.

Referencias y más documentación

¿Qué puedo hacer con AWS? http://aws.amazon.com/solutions/aws-solutions/.

¿Cómo puedo empezar a utilizar AWS? http://docs.aws.amazon.com/gettingstarted/latest/awsgsg-intro/gsg-aws-intro.html.