CLOUXTER

¿Qué diablos es Gobierno de Nube?

eBook

continuous evolution

CLOUXTER

Contenidos

CLOUXTER

Introducción

Acerca de este eBook

Este libro electrónico pretende ayudar a los responsables de la toma de decisiones de las pequeñas y medianas empresas a entender los beneficios de aplicar un Gobierno de Nube.

Aprenderás:

- Los motivos por los cuales te beneficia aplicar un Gobierno de Nube
- Diferentes escenarios donde se hace mal uso de la Nube
- Acciones que se pueden llevar a cabo para establecer una gestión efectiva de Nube
- Conceptos básicos para entender el Gobierno de Nube
- La operación efectiva en escenarios de múltiples cuentas en AWS
- La implementación del Gobierno de Nube por Clouxter

CLOUXTER

¿Qué esperan lograr las empresas cuando deciden Adoptar la Nube?

Hay varias motivaciones para migrar a la nube y mover las diferentes cargas de trabajo adoptando un modelo de consumo y de tecnología basado en la nube.

1

Construir: enfocándote más en la diferenciación de hacer soluciones para tus clientes que marquen la diferencia con el resto de competidores de tu segmento..

2

Moverse muy rápido: desde la idea de una solución hasta su implementación.

3

Mantenerse seguro: buscando ambientes seguros y con cumplimiento a las regulaciones que le apliquen a la industria que pertenezcas.

En la actualidad, la carga que supone la gestión de las infraestructuras, sobre todo a medida que envejecen, limita fundamentalmente la capacidad de muchas empresas para innovar y seguir siendo competitivas. Las pequeñas y medianas empresas están sometidas a una presión cada vez mayor para hacer más con menos y utilizar los valiosos recursos de TI para crear diferenciación a través de aplicaciones que apoyen sus necesidades empresariales.

CLOUXTER

Características de las cargas de trabajo en la Nube

Los ambientes que se aprovisionan en la nube para las diferentes cargas de trabajo deben tener ciertas características.

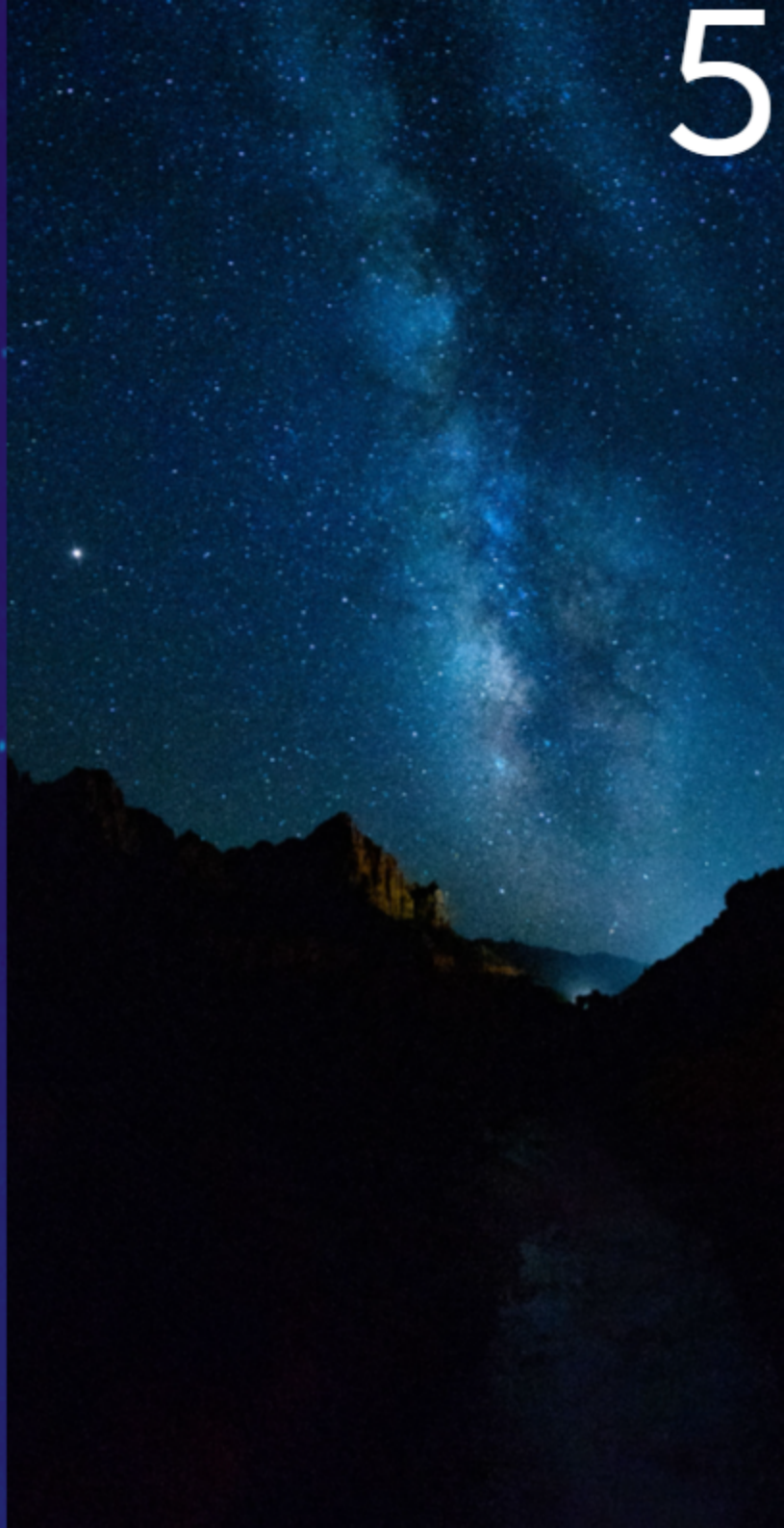
Seguridad y Conformidad

Se habla de ambientes seguros en términos de cumplir las regulaciones específicas para la organizaciones. Muchas se están certificando en procesos básicos de seguridad: seguridad de la información como ISO 27001, algunas otras requieren una certificación más exigente alrededor de seguridad como, PCI, si procesan transacciones de tarjeta de crédito. Hay regulaciones que obligan a un manejo más estricto, tanto de la información, como de los servicios que se exponen.

Escalable y Resiliente

Se refiere a crecer en la medida en que lo requiera la demanda. Quizás en un principio la demanda es pequeña, pocos usuarios, pero a medida que va creciendo y va teniendo éxito la carga de trabajo, la solución que se está desplegando debe poder crecer consecuentemente. Resiliente ante las fallas, ya sean transitorias en los servicios o fallas de aplicación. Se deben establecer mecanismos para la recuperación y continuidad del servicio.

.



CLOUXTER

Adaptable y Flexible
Se refiere a que los ambientes en la nube puedan adaptarse a las necesidades que se tienen. Ya sean necesidades de capacidad, de cumplimiento, funcionales o de servicios que puedan involucrar la carga de trabajo.

Al final, las soluciones que soportan los negocios tienen que ir evolucionando porque las situaciones externas impactan a su desarrollo y a su vez, las aplicaciones reflejan estos procesos de negocio.

Por ejemplo, el contexto de la pandemia obligó a cambiar la forma en que se trabajaba, la atención al usuario y la forma de procesar las solicitudes.

Básicamente, se necesita un entorno que permita mantener la flexibilidad, sin dejar a un lado todos los temas de cumplimiento y conformidad a las regulaciones que apliquen. Ese balance puede complicarse en las organizaciones, por lo que depende de la inercia con la que vengan trabajando en los ambientes on premise desde el punto de vista organizacional, cultural y de tecnología.

Retos en el proceso de Adopción de la Nube
1. Tomar muchas decisiones.

¿Cómo se va a gestionar la identidad de los usuarios? ¿Qué usuarios van a operar las cargas de trabajo? ¿Qué usuarios aprovisionan? En fin, establecer la gestión de identidad de los usuarios, los procesos de trazabilidad de las aplicaciones y los servicios. Cómo hacer ese registro de la trazabilidad, qué está pasando en el entorno para fines de auditoría, optimización y operación en general.

Constantemente se encuentra que en ese proceso de Adopción de la Nube se necesita tomar muchas decisiones.

2. Configurar múltiples cuentas y servicios
La configuración, despliegue y aprovisionamiento de múltiples servicios de cuentas depende de la solución que se está trabajando. Puede ser una carga de trabajo simple que está basada en la infraestructura como servicio, máquinas virtuales. Pueden ser unos servicios básicos de aprovisionamiento, pero en algunos otros casos las soluciones pueden empezar a ser un poco más sofisticadas, utilizar servicios más complejos y requerir una orquestación de múltiples servicios para poder funcionar. En todo ese proceso el pilar de la seguridad sigue siendo importante.

3. Mantener la Seguridad y el Cumplimiento
Garantizar la seguridad, la minimización del riesgo y el cumplimiento es clave. No dejar a un lado la seguridad de los entornos, pues al final en internet, cualquier carga tiene una exposición inevitable.

CLOUXTER

¿Cómo balanceamos las necesidades de los equipos?

En principio los negocios necesitan desarrollar soluciones con rapidez. Esto con el objetivo de desplegar los servicios y funcionalidades para diferenciarse de la competencia. Entonces, ¿cómo se mantiene la innovación y la agilidad sin que el proceso de adopción sea un bloqueante? ¿Qué hacer para que todos los temas de control, gestión y regulación no entorpezcan ese proceso de alta velocidad y agilidad para entregar soluciones?

Por otro lado, es clave la perspectiva de control, el gobierno. Saber qué es lo que está pasando, saber en dónde se están consumiendo los recursos. Reducir el desperdicio, gestionar la identidad, garantizar que los usuarios sean los que deben ser y que puedan hacer solo lo que deben hacer, sin privilegios innecesarios. Es imprescindible tener trazabilidad, rastro de lo que está pasando, que se pueda aprovisionar de manera estandarizada y efectiva los diferentes recursos que se requieran para las cargas de trabajo.

1

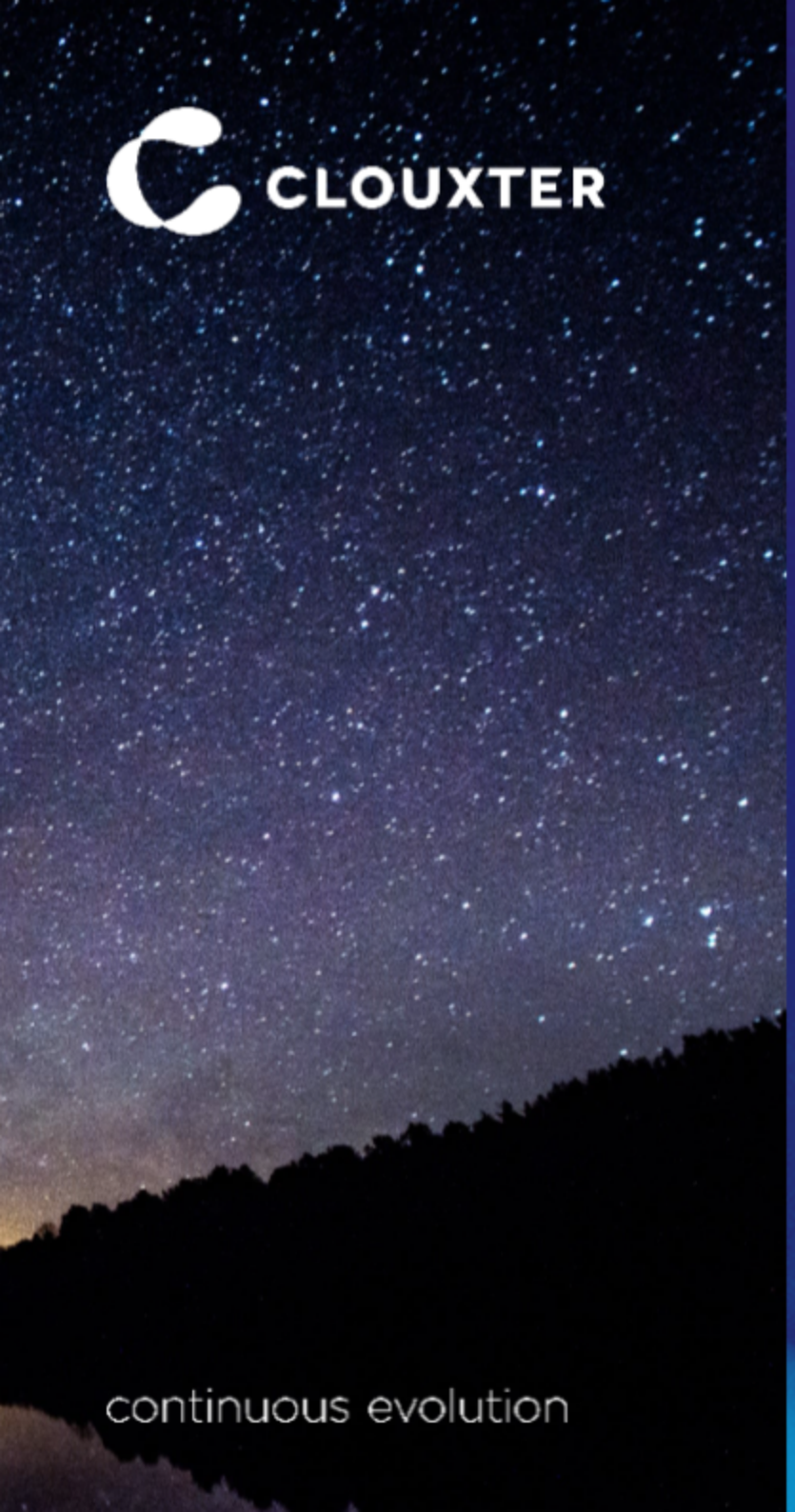
El gobierno de nube para poder ser gestionable efectivamente debe ser centralizado con una escala bastante amplia, pensando en las múltiples cargas de trabajo que pueda tener la organización.

2

Se requiere una manera efectiva para configurar y gobernar la nube a escala desde los procesos de habilitación de servicios, aprovisionamiento de recursos y la operación de las cargas de trabajo.

3

Es importante combinar la agilidad de los negocios con el control que exige el gobierno y los temas de cumplimiento.



Antipatrones del Gobierno de Nube

1. El primer error es pretender usar la nube como si fuera un Datacenter on premise. La nube es algo mucho más sofisticado en términos de capacidades, servicios, funcionalidad, granularidad y flexibilidad.

Normalmente en un entorno on premise se tiene una serie de recursos, como múltiples servidores, que atienden una carga de trabajo particular. Algunas de esas cargas son desplegadas en una máquina virtual. Entonces, aunque todos esos recursos estén desplegados en una red local de un Datacenter representan diferentes cargas de trabajo que están todas en una red.

¿Qué pasa si se quiere llevar esas cargas de trabajo a la nube?

Es común que se empiece creando una cuenta en la nube de AWS para luego, en la VPC, que es una red virtual, desplegar las diferentes cargas trabajo: bases de datos, máquinas virtuales, almacenamiento, etc. Ese escenario es un antipatrón.

Una de las grandes características de la nube es que se puede segregar, tener un grano mucho más pequeño de agrupamiento y aislamiento de las diferentes cargas de trabajo.

Tratar de imitar un ambiente on premise en la nube no es una buena práctica. La idea es aprovechar esas ventajas para organizar mejor.

CLOUXTER

Otro antipatrón es empezar en la cuenta de AWS y crear una VPC para la primera carga de trabajo. Esta es operada por el equipo de Analytics, el equipo de bases de datos y un business architect que está a cargo del proyecto. Para otra carga de trabajo tienen un contratista que es el desarrollador y unos operadores que atienden la gestión de esa carga de trabajo. Por su parte, los sitios web de la compañía, están bajo el equipo de marketing.

Aunque se crea un entorno con mayor aislamiento, la segregación del acceso a los diferentes recursos es muy difícil de hacer, es dispendiosa. ¿Cómo segrego y garantizo que los usuarios solo accedan a X recursos de una VPC? Es posible, pero todo el detalle que implica poder garantizar y mantener esa gestión se vuelve enredado.

¿Qué pasa si esos usuarios no tienen la segregación correcta sino que afectan a otros recursos que estén alojados en esa máquina virtual? Así empieza un problema con relación a que pronto las acciones que haga este equipo sobre el recurso, pueda no solo impactar a la carga de trabajo de las que son responsables, sino también a las otras cargas de trabajo que lo utilizan.

Segregar el acceso por recurso puede no ser la mejor manera cuando todo está en una sola cuenta.

Es ahí cuando se complica la administración, la operación y la segregación del costo sigue siendo un issues si no se tiene una gestión de metadata correcta sobre los recursos.

Otro antipatrón es no utilizar una sola cuenta para colocar todas las cargas de trabajo o varias cargas de trabajo, precisamente por las complejidades que surgen en los temas operativos de administración de gestión de costos.

CLOUXTER

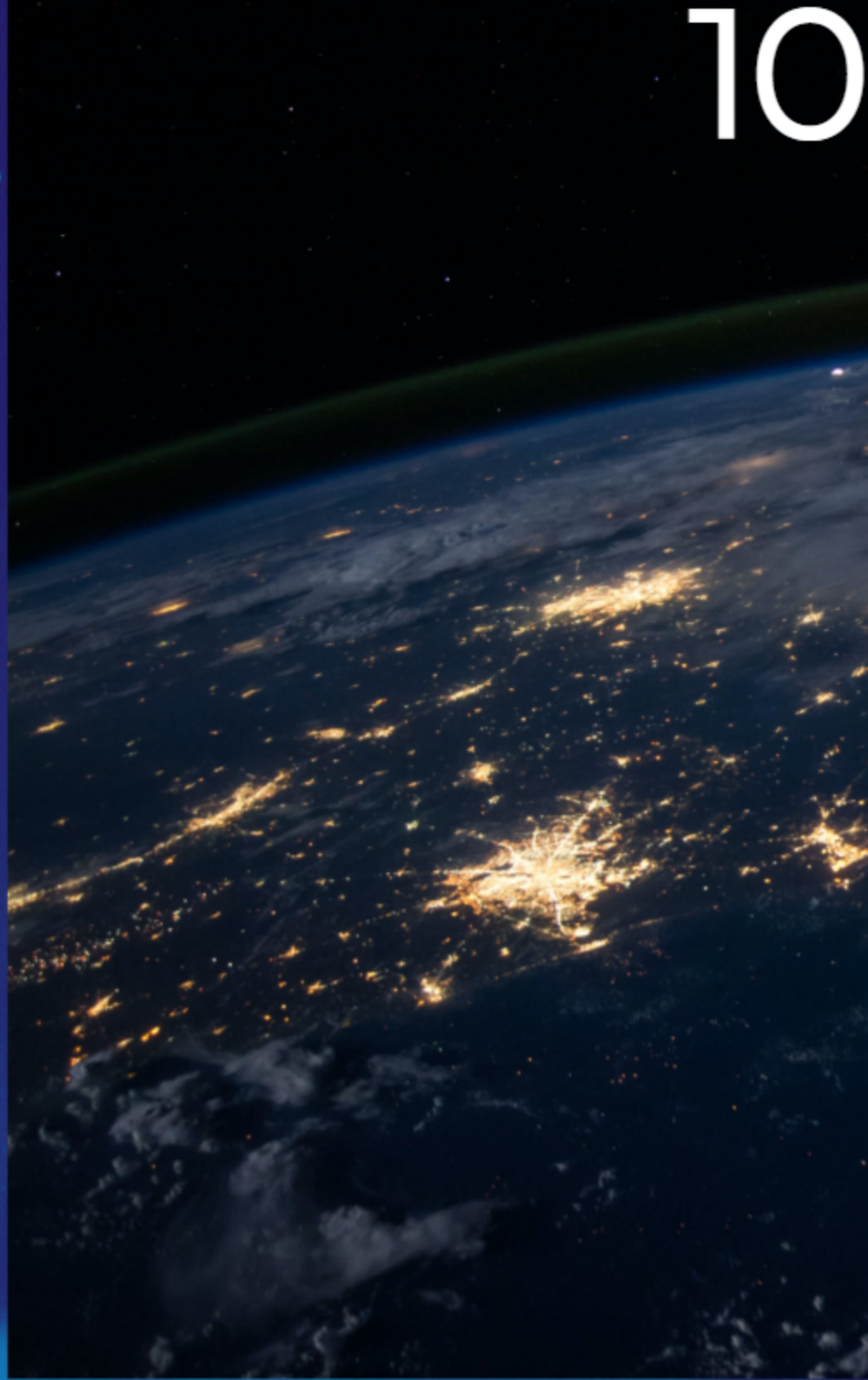
Gestión efectiva de Nube

Se necesitan establecer algunos aspectos para poder hacer una gestión efectiva. Uno de ellos es crear fronteras de seguridad y de recursos. No solo la VPC, que es una frontera técnica de acceso de red sino desde la perspectiva de seguridad, de administración de usuarios desde AWS.

Los límites de las APIS y los servicios, es necesario controlar y establecer qué servicios se pueden usar y cómo se implementan.

Por ejemplo, limitar el tipo de servicios de cómputo y poner reglas sobre el consumo. No solo para términos de seguridad sino también para términos de recursos y potencialmente mantenerlo controlado.

La segregación de facturación (consumo de recursos) es importante para poder asignar los centros de costos correctos, identificar el costo por área. El proyecto cuesta A en desarrollo, B en QA y C en producción. Así se tiene totalmente controlado el costo y no se va todo como "el costo de TI".



CLOUXTER

Modelos de cuentas AWS

Una Cuenta

Se puede empezar con una cuenta para las primeras cargas de trabajo.

Varias Cuentas

Se pueden tener varias cuentas para segregar por cargas, por ambientes por diferentes criterios que se decidan.

Miles Cuentas

Se puede llegar a tener miles de cuentas en la Nube de AWS.

Una cuenta no cuesta nada pero permite crear fronteras entre las diferentes cargas de trabajo. Una aproximación es tener cuentas por función, por carga de trabajo o por ambientes.

Cuentas por Función / Carga
Pasamos de tener cinco cargas de trabajo en una sola cuenta, en el escenario de antipatrón, a tener cuatro cuentas que tienen diferentes cargas de trabajo en ellas. Hay diferentes criterios para hacer esa segregación. Lo importante es establecer las fronteras.

Escenario Multicuenta
Aquí surgen preguntas y decisiones. Primero, ¿cómo gestionar la identidad entre varias cuentas? Cómo centralizo esa gestión de identidad, autenticación, autorización, acceso a los recursos.

Segundo, ¿cómo mantengo la trazabilidad de los recursos y las cargas de trabajo? ¿Tengo que entrar a cada entorno para saber qué está pasando? Tercero, ¿cómo establecer los controles de seguridad y cumplimiento transversales o de manera centralizada? Recordemos que debemos tener la forma de medir qué pasa y verificar que se cumpla esa condición. Cuarto, ¿cómo gestiono una segregación adecuada de costos? ¿Cuáles son esos criterios y cómo lo puedo separar y gestionar correctamente?

Para todo esto hay un concepto que se llama el Landing Zone o Zona de Aterrizaje

CLOUXTER

¿Qué es un Landing Zone?

Es donde aterrizan las cargas de trabajo. Es un entorno multicuenta que puede ser escalable y se configura basado en las mejores prácticas. Es el punto de partida sobre el cual llevamos nuevas cargas de trabajo, cargas de trabajo existentes y establecemos también entornos para prueba y experimentación. En conclusión, una landing zone, es el punto de partida para migrar las cargas de trabajo en una organización.

Es un ambiente que va a permitir crecer progresivamente. No necesariamente se debe tener la versión definitiva de landing zone el primer día. Se puede empezar con ciertas características, controles y definiciones en la medida que se determinan cuáles cargas de trabajo se llevan a la Nube. Es posible añadir y configurar nuevos controles, condiciones políticas y recursos que van a ser parte de esa landing zone.

Sin duda este es un componente clave en el concepto del Gobierno de Nube.

CLOUXTER

Habilitación del Gobierno de Nube

Habilitar el Gobierno de Nube es un proceso iterativo que empieza con la configuración del landing zone. Esta puede ser una versión inicial sencilla. A partir de ahí se establecen una serie de controles y de reglas que se necesitan cumplir en las cargas de trabajo y en los usuarios alrededor de todo el entorno. Además, se empieza a automatizar el aprovisionamiento de nuevos entornos para poder llevar más cargas de trabajo. Para ello se automatizan procesos de definición, por ejemplo de la VPC, de algunos recursos estándares que se puedan definir estableciendo un modelo centralizado de identidad.

Esa identidad que se auténtica ante la landing zone funciona para acceder a las diferentes cuentas y a los diferentes recursos que allí están alojados.

Esta habilitación de gobierno de Nube logra mantener la agilidad, el poder desarrollar nuevas soluciones y poder utilizar los servicios nativos de la nube, que otorgan mayor agilidad y cadencia en la entrega de soluciones. Todo esto manteniendo el control centralizado en temas de políticas de identidad, trazabilidad y costos que se necesitan para para crecer en la Nube.

CLOUXTER

Caso de Uso - Marco Inicial de Multicuenta AWS

¿Cómo se ve gráficamente en lo que es una estructura de cuentas?

Se puede empezar pequeño sin hacer la versión definitiva el día uno. Es posible poder crecer y evolucionar en la medida que se van definiendo y estableciendo los controles y las condiciones sobre las cuales deben correr nuevas cargas de trabajo o cargas de trabajo que tienen más restricciones de cumplimiento.

No se tiene que hacer una migración de un día para otro.
No se tienen que migrar todas las cargas de un día para otro.
No se tienen que tener todas las definiciones el día cero antes de empezar.

Inicialmente se pueden tener ambientes un poco más simplificados en donde se establece una estructura de multicuentas y se definen unidades organizacionales. Estas son grupos de cuentas que comparten unas políticas comunes.

Primero, se definen unidades organizacionales de cuentas core de la landing zone que tienen controles específicos que permiten, por ejemplo, acceso limitado a los logs de solo lectura. Están los servicios compartidos, como la gestión de identidad, la configuración y monitoreo de seguridad que son transversales a toda la landing zone. Por otro lado, están las unidades organizacionales donde se alojan las cargas de trabajo de manera aislada. Allí se tiene el Sandbox que sería el espacio donde se colocan cuentas para que los desarrolladores experimenten y exploren los servicios que están disponibles en AWS de manera segura. Si hay algún problema se mantendrá sólo en ese entorno, además de limitar el consumo.

CLOUXTER

Ahora, las otras cargas ya productivas para desarrollo, para pruebas, dependiendo de la organización, normalmente empiezan con algunos ambientes. Se puede empezar con un proyecto completo en múltiples ambientes o con un ambiente de pruebas para llevar las cargas de trabajo y empezar a entender cómo funciona, definir más fácilmente los controles que se quieren aplicar y desplegar en la landing zone. Este proceso es viable.

Ambos casos pueden perfectamente evolucionar a una estructura un poco más compleja en donde se pueda tener múltiples ambientes, múltiples unidades organizacionales, N cuentas agregadas, en las cuales tienen propósitos específicos, ya sean organizados por proyectos o ambientes con criterios de políticas que aplican transversalmente a todas esas cuentas.

Un escenario es que algunos equipos tengan una unidad organizacional en la que van a probar las políticas que van a aplicar en otra unidad. Despliegan las políticas, prueban en las cuentas que están en esa unidad y una vez garantizan que las políticas que definieron funcionan sin ningún problema, entonces trasladan la política a la unidad organizacional que necesitan.

Aplicar la gestión de cuentas suspendidas o excepciones de políticas

Existen casos en los que alguna cuenta necesita excepciones por X condición de software, X condición de algún Partner de negocio. Por ejemplo, los security groups, los grupos de seguridad, que son firewalls para las instancias y algunos recursos, se necesita que no solo tengan habilitado el puerto 443, sino el puerto 80. En algunos casos es una política que se aplica, pero tenemos una aplicación que no corre o los clientes no se pueden conectar al puerto 443, sino que se conectan al puerto 80 exclusivamente, entonces es una carga de trabajo que tiene una excepción de la política transversal, no funciona la política estándar que tenemos. Ese es el caso de las excepciones.

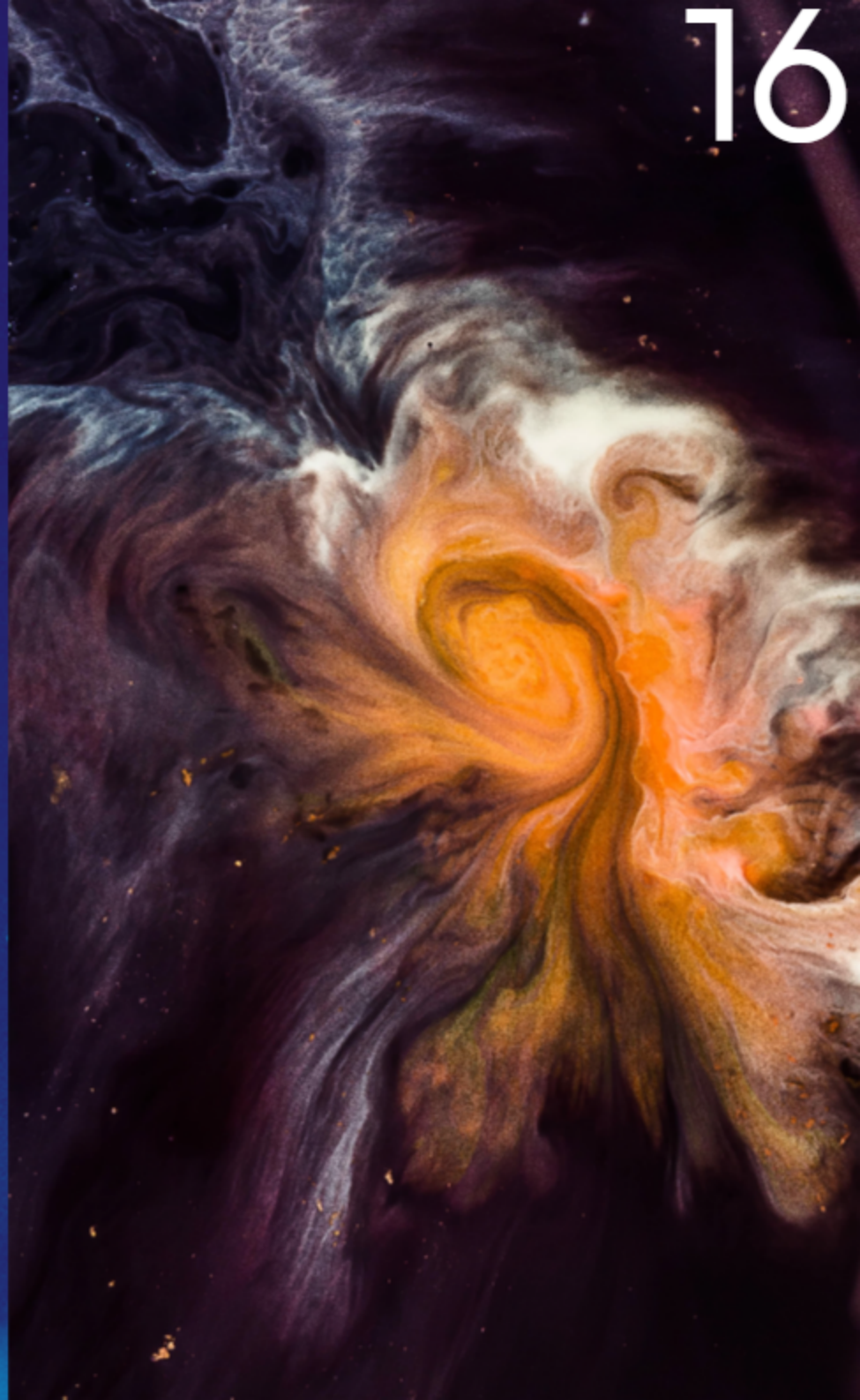
Se pueden tener todos los entornos que se quieran dentro de la estructura del landing zone, pero ¿cómo opera una estructura de este estilo? Aquí básicamente debemos enfocarnos en cuatro aspectos principales.

CLOUXTER

4 Aspectos importantes de un Modelo Efectivo de Operación de Nube

1. Poder instrumentar y monitorear los recursos sobre los cuales corren las cargas de trabajo en término de métricas específicas.
2. Auditar que los controles se están aplicando correctamente, que las configuraciones son adecuadas dentro de las definiciones de nuestra organización.
3. Tener la visibilidad correcta, poder ver de manera centralizada las métricas y el estado general de salud de todas las cargas de trabajo.
4. Poder accionar alrededor de las cargas de trabajo de manera automática a partir de condiciones que identificamos en roomtime, en tiempo de ejecución.

Por ejemplo, el auto scaling (auto escalado) es una acción. Cuando los recursos están peligrosamente consumiéndose en alguna carga de trabajo deberían auto escalarse. Para esto, se lanza automáticamente una nueva instancia y así se equilibra la carga con el objetivo de soportar la demanda existente. Otro ejemplo, es actuar de manera automática cuando se identifica que un recurso no está cumpliendo con la regla de configuración que le hemos definido.



CLOUXTER

Modelos de Operación de Nube

¿Qué se necesita para poder operar efectivamente la nube pensando en escenarios multicuenta, en escenarios de gobernabilidad de la tecnología?

Lo primero a tener en cuenta es:

1. Definir cuáles son los dos objetivos del servicio: qué esperamos como resultado para los usuarios finales, clientes, unidades de negocio y qué estrategias se van a definir.
2. Entender y aprovechar al máximo la desechabilidad de los recursos. Esto es algo muy propio de la nube porque tradicionalmente cuando las organizaciones compraban servidores físicos, es un activo que mantienen, y que al final los equipos de TI crean un lazo emocional incluso con el Hardware. Es un caso más común de lo que se imagina.

En la nube a veces es más rápido y efectivo lanzar una nueva instancia que diagnosticar la razón. Entonces, se deben diseñar las soluciones de tal manera que podamos desechar los recursos y reemplazarlos para dar continuidad al servicio.

CLOUXTER

Con el auto scaling, a veces, la forma de recuperar un servicio es lanzando un nuevo recurso y no tratando de resolverlo.
Ese concepto a veces no es fácil de adoptar depende de la inercia en la gestión tecnológica que tengan los equipos.

3. Estandarizar para optimizar, en la medida en que se establezcan mecanismos estándar para definir arquitecturas o condiciones para el uso de ciertos servicios se puede garantizar la optimización de los procesos.

¿Cómo sé que ciertas definiciones son estándar? Se pueden implementar de manera automática con Scripts, comandos, a través de system manager con múltiples servicios que pueda garantizar que las condiciones se repiten.
4. Aplicar las buenas prácticas de Well-Architected (Marco de la Buena Arquitectura de AWS)
5. Las operaciones como código es uno de los principios más importantes en la nube. Justamente esas operaciones como código pueden garantizar la repetibilidad y la consistencia de los resultados, disminuyendo el factor de error humano en la operación.
6. Buscar mecanismos para garantizar la continuidad del servicio. En este punto aplican los Business Continuity Plan (BCP) o Disaster Recovery Plan (DRP), elementos importantes en la Nube para implementarlos dependiendo de cuáles son nuestros criterios más importantes, disponibilidad, rendimiento o costo.
7. Optimizar constantemente el consumo.

Estos son elementos muy importantes que se deben tener en cuenta en la operación de las cargas de trabajo en la nube.

CLOUXTER

Gobierno de Nube en Clouxter

Clouxter ha desarrollado una solución que se llama el Clouxter's Cloud Governance que permite implementar Modelos de Gobierno de Nube aplicado a múltiples clientes.

Tipos de Implementaciones de este modelo de Gobierno de nube:

a. Clientes con un modelo de gobierno dedicado: implementación que es particular para un cliente.
b. Clientes que comparten el mismo modelo de gobierno: tienen políticas estándar, operación estándar y características estándar homogeneizadas. Clouxter se enfoca en aspectos como la gestión de la identidad, políticas y controles, ya sea de detección o de prevención para tomar acciones antes de que suceda un evento desafortunado. Se limita la posibilidad pero no todas las cosas se pueden controlar con prevención, hay algunas que necesitan detección y remediación.
c. Servicios de aprovisionamiento de recursos: estandarizar el aprovisionamiento de nuevas cuentas y aprovisionamiento de las redes.
d. Establecer los modelos de gestión de consumo. Por ejemplo, se definen los planes de ahorro para identificar más fácilmente las cargas de trabajo que son susceptibles a, caso hipotético, reservar capacidad de cómputo y poder ahorrar en ese proceso.

La ventaja de estos modelos es que permiten simplificar aspectos de la implementación y de la operación de las soluciones de nuestros clientes. Los clientes que adoptan estos modelos también tienen una percepción mucho más positiva sobre cómo están llegando a la nube.

En todas estas soluciones de Cloud Governance aplicamos el Well-Architected Framework de forma transversal. Esto quiere decir que todos los pilares: seguridad, confiabilidad, rendimiento, optimización de costos, excelencia operativa y sostenibilidad, hacen parte del diseño e implementación de estas soluciones de cloud governance, lo cual hace que funcione de manera efectiva para nuestros clientes.

¿Estás interesado/a en desarrollar un Modelo de Gobierno que te permita mayor control y cumplimiento de tus recursos desplegados en la Nube?

¡Contáctanos!
biz@clouxter.com

Síguenos para obtener más contenido relevante

@Clouxter @Clouxter @Clouxter @ClouxterCol ClouxterChannel