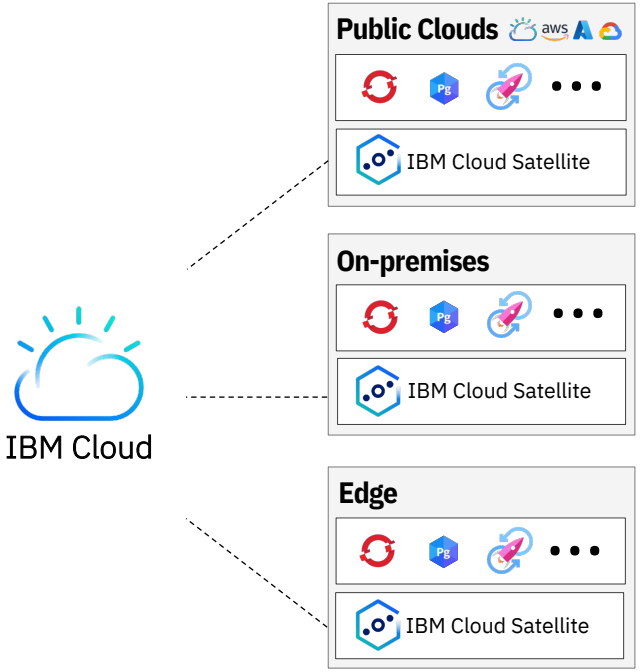
OpenShift on Satellite

MAPFRE

IBM Cloud Satellite

Cargas de trabajo ubicadas donde se necesiten



Ubicación

Infraestructura controlada por el cliente fuera de los centros de datos de IBM Cloud

El cliente administra sus hosts (infraestructura) dentro de una ubicación

Flexibilidad

Ejecutar la aplicación donde tenga sentido

Para cargas de trabajo reguladas, problemas de soberanía y gravedad de datos, migraciones, plataformas perimetrales, baja latencia

Control

Inventario auditable de todas las conexiones de red y el tráfico

Observabilidad centralizada

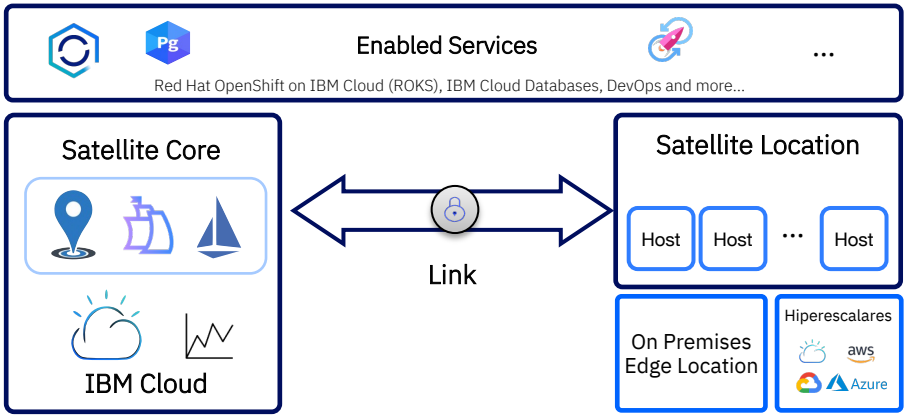
IBM Cloud for Financial Services Validated

Arquitectura de referencia Satellite para FS Cloud

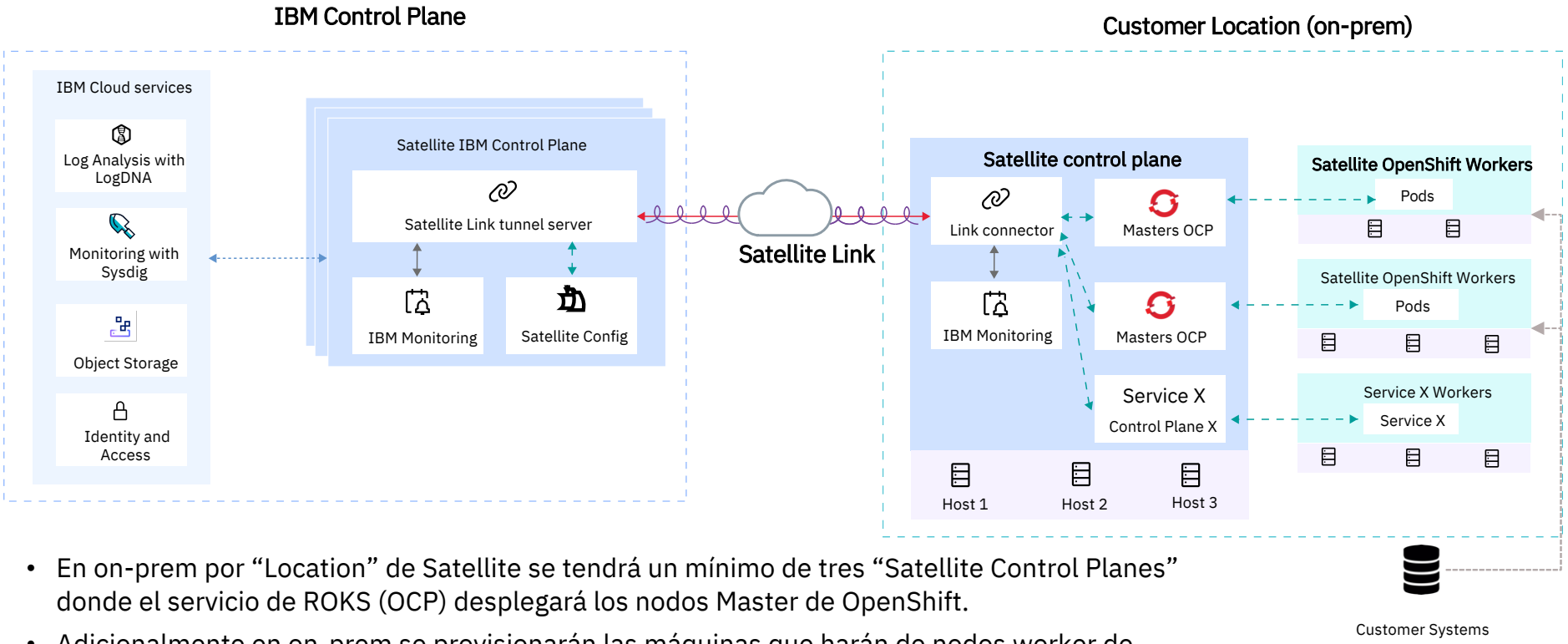
IBM Cloud Satellite. Componentes clave

- Satellite Core – Control Plane (Istio, Razee,..)
- Ubicación – Lugar fuera de IBM Cloud para ejecutar servicios y aplicaciones.
- Link – Tunel SSL gestionado entre la “Localización Satellite” e IBM Cloud.

  Utilizado por IBM para las acciones de gestión sobre el cluster y por el cliente para la comunicación bidireccional con servicios de IBM Cloud
- Satellite enabled Services – Catálogo de IBM de servicios habilitados para Satellite, como ROKS, bases de datos, COS, etc.



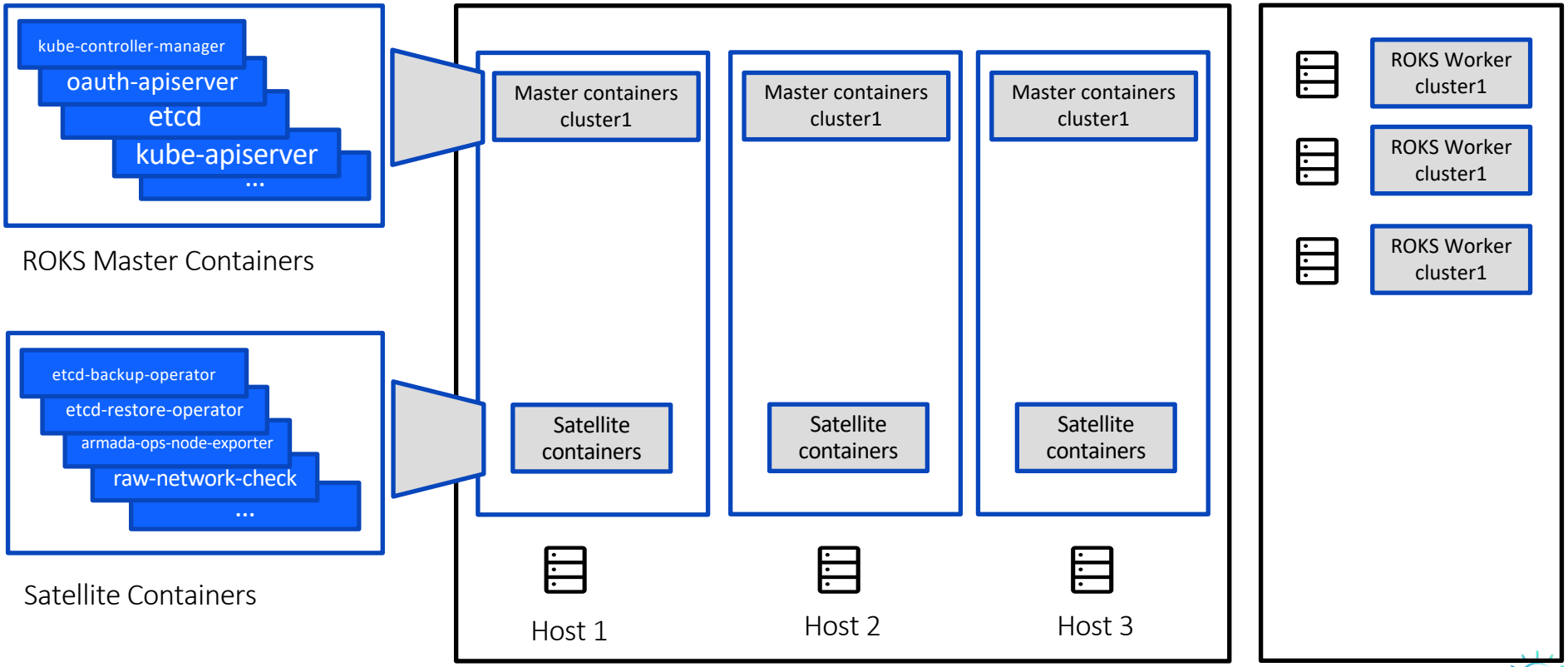
IBM Cloud Satellite. ROKS



- En on-prem por “Location” de Satellite se tendrá un mínimo de tres “Satellite Control Planes” donde el servicio de ROKS (OCP) desplegará los nodos Master de OpenShift.
- Adicionalmente en on-prem se provisionarán las máquinas que harán de nodos worker de OpenShift para cada cluster a desplegar. La configuración de los workers igualmente se realizará como parte del despliegue del servicio de ROKS

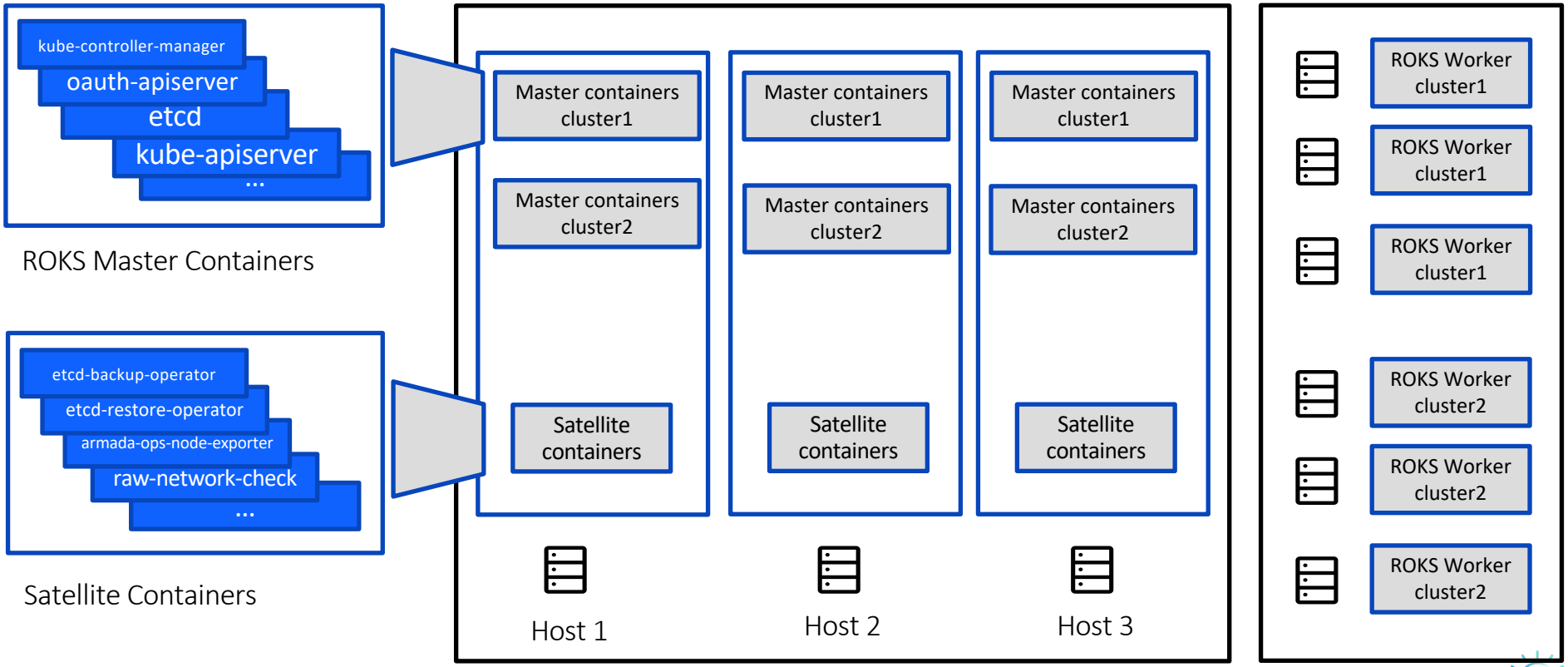
IBM Cloud Satellite. Ubicación del cliente – Control Planes

Reutilización de nodos master entre clusters



IBM Cloud Satellite. Ubicación del cliente – Control Planes

Reutilización de nodos master entre clusters



Dimensionamiento Control Plane

4 vCPU, 16 GB RAM (CoreOS)	16 vCPU, 64 GB RAM (CoreOS)

Number of control plane hosts	Max clusters in location	Example of max worker nodes in location	Max cluster size
6 hosts	Up to 3 clusters	20 workers across 3 clusters, or 80 workers across 2 clusters	60 workers per cluster
9 hosts	Up to 5 clusters	40 workers across 5 clusters, or 140 workers across 3 clusters	60 workers per cluster
12 hosts	Up to 8 clusters	60 workers across 8 clusters, or 200 workers across 4 clusters	60 workers per cluster

Aunque el requerimiento sean 4vCPU la recomendación es poner 8vCPU

Satellite divide los Control Plane por zona, tener 6 Control Plane implica tener 2 Control Plane por “zona”, lo que da garantías de Alta Disponibilidad adicionales al Quorum de ETCD.
Durante las actualizaciones o en caso de fallo de un Control Plane habrá un nodo por zona disponible en caso de fallo del nodo “activo”.

Para “Locations” con un único cluster no productivo se podrían desplegar únicamente 3 nodos Control Plane, siendo recomendable aumentar los recursos a 8vCPU y 32GB

https://cloud.ibm.com/docs/satellite?topic=satellite-location-sizing

Ejemplo Despliegue OpenShift en Satellite

En cada ubicación geográfica de MAPFRE:

Un “Satellite Location” dedicada a producción (seguridad y red)

Nodos Control Plane dedicados al Cluster de producción, seis nodos para aumentar las capacidades de HA en producción.
Nodos Workers dedicados

Un “Satellite Location” común para entornos previos

Contenedores de todos los masters de cada Cluster distribuidos en seis control planes de Satellite
Nodos Workers dedicados por Cluster

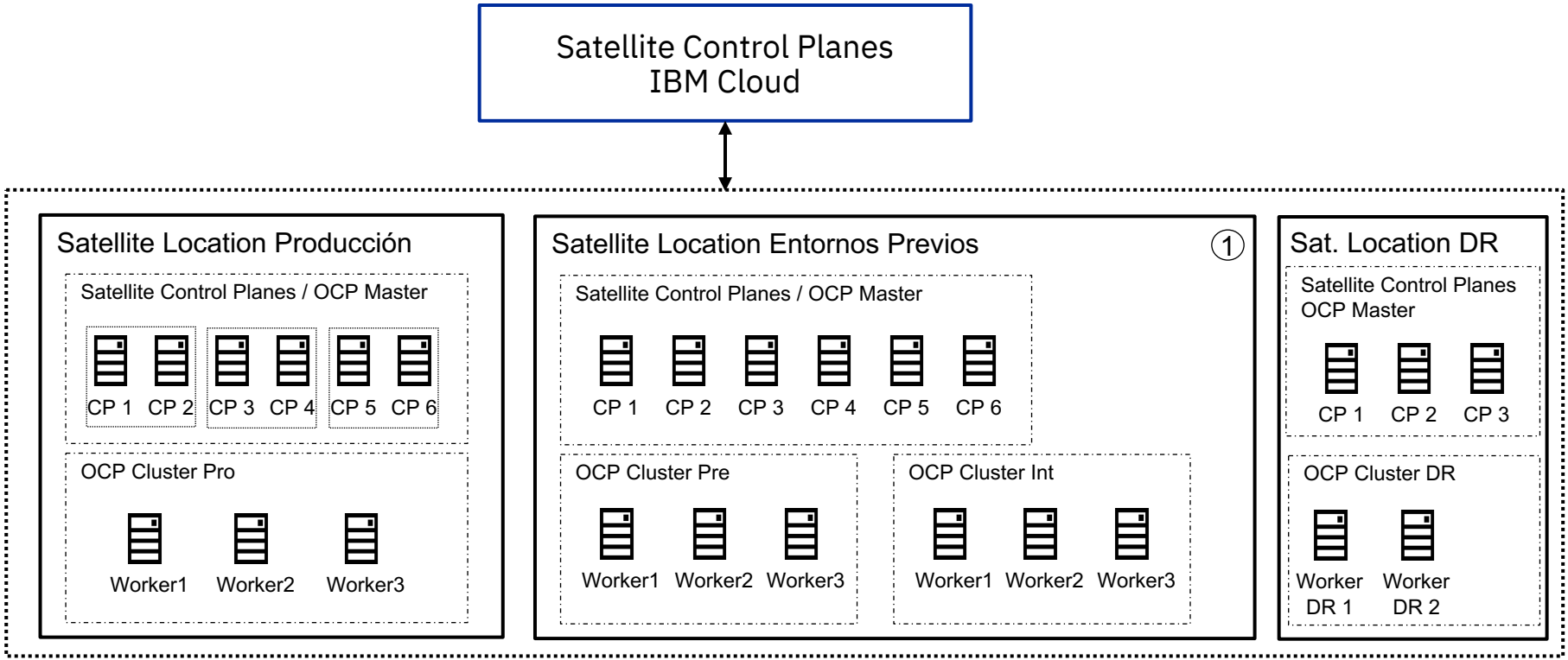
Un “Satellite Location” de Disaster Recovery

Dependiendo de los tiempos de RTO necesarios para las aplicaciones a recuperar:

1. Sin Location de Disaster Recovery pre-aprovisionada
2. Location mínima de Disaster Recovery
   Configuración mínima de 3 Nodos Control Plane
   Configuración mínima de 2 Nodos Worker
   En tiempo de DR se amplia capacidad.
3. Location de Disaster Recovery igual que la Location de Producción

Todas estás location múltiplicadas por 3 para cubrir España, EEUU y Brasil

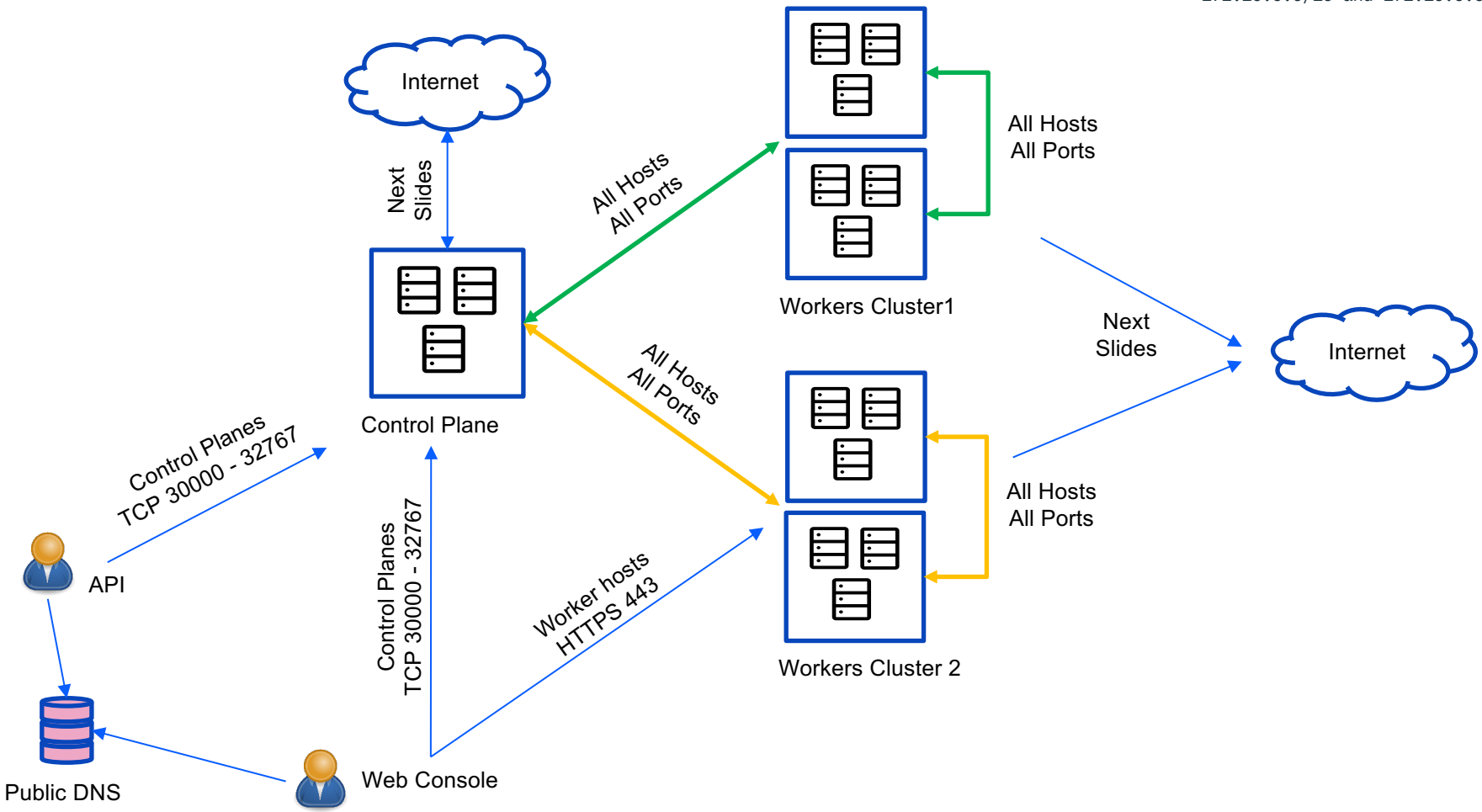
Ejemplo Despliegue OpenShift en Satellite



① Pendiente de decidir si los entornos previos serán “namespace” en un solo cluster o diferentes clusters

Requerimientos de Conectividad

CoreOS Reserved IP Ranges:
172.20.0.0/16 and 172.16.0.0/16



Satellite/ROKS requerimientos conectividad

- Desde los servicios desplegados en Satellite no se podrá acceder a servicios del cliente con IPs en los rangos: 172.20.0.0/16 y 172.16.0.0/16

- Ancho de banda mínimo de 100 Mbps, recomendado 1 Gpbs

- Connectividad con IBM Cloud. La location on-prem puede estar desconectada un máximo de 7 dias de IBM Cloud. Durante la desconexión las funcionalidades de gestión desde cloud no estarán disponibles. Pasado el tiempo máximo configurado el sistema sigue funcionando, sin las funcionalidades de gestión o autenticación con IBM Cloud hasta la reconexión. En esta situación si los nodos se reinician manualmente se pierden y hay que reemplazarlos. A las dos semanas desconectado se borra la location.

- Las comunicaciones son iniciadas por la Location. No se ha de habilitar comunicación entrante hacía los nodos.
  Una vez establecido el tunel SSL (Satellite Link) hay trafíco entrante a través del tunel contra el API de Satellite desplegado en los Control Planes. El tráfico esta filtrado por defecto para que solo el tráfico con origen en el servicio de gestión de Satellite pueda pasar por el túnel.

- Es posible configurar el tráfico HTTP saliente a través de un proxy HTTP

- Es necesario disponer de un “tunel / puente TCP” o habilitar conectividad directa desde los Control Planes a Internet para tráfico TCP a un host:puerto conocido

- Es posible la configuración de una Linea dedicada entre MAPFRE e IBM Cloud

- Latencias:

1. 200ms RTT desde la location on-prem a IBM Cloud en la region seleccionada para la gestión
2. 100ms RTT entre nodos “Control Plane/Master” y “Worker”
3. 10 ms RTT entre nodos “Control Plane/Master”
4. 10 ms RRT entre nodos “Worker”

https://cloud.ibm.com/docs/satellite?topic=satellite-reqs-host-network
https://cloud.ibm.com/docs/satellite?topic=satellite-host-latency-test
https://cloud.ibm.com/docs/satellite?topic=satellite-disconnected-use

Satellite/ROKS requerimientos conectividad

- Los hosts deben tener conectividad de entrada en la interfaz de red principal a través de la puerta de enlace predeterminada o el firewall del sistema:

Descripción	IP origen	IP destino	Protocolos y puertos
Permitir que los hosts que están asignados a los servicios en la ubicación se comuniquen entre sí y con el Control Plane de Satélite	Todos los hosts	Todos los hosts	Todos los puertos y protocolos
Acceder a la API para realizar cambios en un clúster de OpenShift y acceder a la consola web de OpenShift o a través del enrutador de OpenShift	Clientes o usuarios autorizados	Hosts de Control plane	TCP 30000 - 32767
Acceder a la consola web para un clúster de OpenShift a través del enrutador de OpenShift	Clientes o usuarios autorizados	Hosts de OpenShift cluster	TCP 443

Satellite/ROKS requerimientos conectividad de salida (Frankfurt)

Control Planes	IBM Control Plane Communication	c124.eu-de.satellite.cloud.ibm.com c124-1.eu-de.satellite.cloud.ibm.com c124-2.eu-de.satellite.cloud.ibm.com c124-3.eu-de.satellite.cloud.ibm.com c124-e.eu-de.satellite.cloud.ibm.com	30000 - 32767	TCP
All Hosts	IBM Control Plane Communication	origin.eu-de.containers.cloud.ibm.com	443	HTTPS
Control Planes	Cloud Object Storage (ETCD Backup)	s3.eu.cloud-object-storage.appdomain.cloud *.s3.eu.cloud-object-storage.appdomain.cloud	443	HTTPS
Control Planes	Link tunnel server endpoint	c-01-ws.eu-de.link.satellite.cloud.ibm.com c-02-ws.eu-de.link.satellite.cloud.ibm.com c-03-ws.eu-de.link.satellite.cloud.ibm.com c-04-ws.eu-de.link.satellite.cloud.ibm.com api.link.satellite.cloud.ibm.com	443	HTTPS
Control Planes	Akamai	api.eu-de.link.satellite.cloud.ibm.com config.eu-de.satellite.cloud.ibm.com eu-de.containers.cloud.ibm.com config.satellite.cloud.ibm.com	443	HTTPS
All Hosts	IBM Container Registry	icr.io registry.bluemix.net de.icr.io registry.eu-de.bluemix.net	443	HTTPS
All Hosts	Cloud Monitoring	ingest.private.eu-de.monitoring.cloud.ibm.com	443, 6443	HTTPS
All Hosts	Cloud Log Analysis	api.eu-de.logging.cloud.ibm.com	80, 443	HTTP/S

- Especial atención a la conectividad por TCP a los dominios “c123”, esta comunicación no es HTTP y se ha de habilitar la conectividad directa desde los nodos control plane o a través de un “bridge” TCP, no es possible solo usar Proxy HTTP para esta conexión

https://cloud.ibm.com/docs/satellite?topic=satellite-reqs-host-network-outbound
https://cloud.ibm.com/docs/satellite?topic=satellite-reqs-host-network-outbound-fra

Satellite/ROKS requerimientos conectividad de salida (Frankfurt)

All Hosts	Connect to IBM	cloud.ibm.com containers.cloud.ibm.com api.link.satellite.cloud.ibm.com	443	HTTPS
All Hosts	Cloud Identity and Access Management	iam.bluemix.net iam.cloud.ibm.com	443	HTTPS
Control Planes	LaunchDarkly service	app.launchdarkly.com clientstream.launchdarkly.com	443	HTTPS
All Hosts	NTP	0.rhel.pool.ntp.org 1.rhel.pool.ntp.org 2.rhel.pool.ntp.org 3.rhel.pool.ntp.org Or configure NTP with on-prem NTP Server	123	UDP
All Hosts	RedHat Services / Repository	registry.redhat.io quay.io cdn.quay.io cdn01.quay.io cdn02.quay.io sso.redhat.com mirror.openshift.com storage.googleapis.com/openshift-release quayio-production-s3.s3.amazonaws.com api.openshift.com console.redhat.com registry.access.redhat.com sso.redhat.com	80, 443	HTTP/S

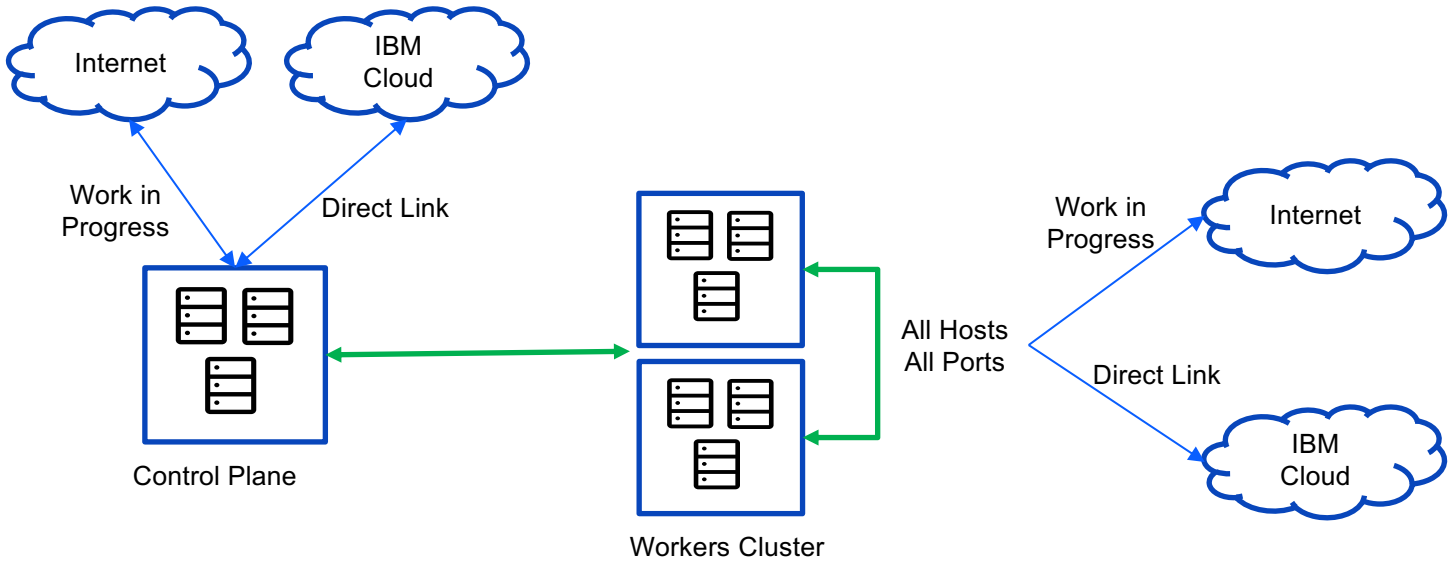
https://cloud.ibm.com/docs/satellite?topic=satellite-reqs-host-network-outbound
https://cloud.ibm.com/docs/satellite?topic=satellite-reqs-host-network-outbound-fra

Satellite/ROKS requerimientos conectividad – Direct Link MPLS (Frankfurt)

Desde Enero 2023 es posible configurar Satellite y ROKS en Satellite para que la comunicación con IBM Cloud se realice a través del servicio de “Linea Dedicada” de IBM Cloud (Direct Link).

Es necesario el despliegue de un “Reverse Proxy” (NGINX, HAProxy) gestionado por el cliente en IBM Cloud.

La documentación sobre las conexiones con terceros que no se realizarían sobre Direct Link está en proceso.



Satellite/ROKS Seguridad

- La autenticación de los usuarios se realiza a través del IAM de IBM Cloud. Es posible federar el IAM de IBM Cloud con Proveedores de Identidad del cliente mediante SAML 2.0.
- Los nodos de la location on-prem se configuran con dos discos duros, el segundo disco duro es donde se almacena la información correspondiente al servicio y en el caso de ROKS los contenedores. Este disco está cifrado “en descanso” mediante claves gestionadas por IBM.
- La Base de datos ETCD de Kubernetes está cifrada “en descanso” mediante claves gestionadas por IBM
- Se realiza back-up de la base de datos ETCD cada 8 horas a un bucket de almacenamiento de objetos de IBM Cloud propiedad del cliente. Este bucket puede estar cifrado con claves gestionadas por el cliente.
- La conexión entre IBM Cloud y la Location on-prem se realiza mediante un tunel SSL (TLS 1.3) configurado automáticamente al desplegar la Location. El servicio de ROKS en IBM Cloud Satellite soporta la utilización de lineas dedicadas (Direct Link) entre on-prem e IBM Cloud.
- El tráfico entrante de gestión está filtrado para que solo el tráfico con origen en los Control Planes de Satellite de IBM Cloud pueda pasar por el tunel.
- SREs de IBM solo tienen acceso a servicios de gestión desplegados en los nodos Control Plane. No tienen access al cluster OpenShift desplegado on-prem

https://cloud.ibm.com/docs/satellite?topic=satellite-data-security

Satellite/ROKS HA y DR (Opción 2)

- El despliegue mínimo de la solución se realiza en Alta disponibilidad por defecto.
  - 3/6 Nodos Control Plane
  - 2 Nodos Worker
- La alta disponibilidad de la infraestructura, al tratarse de un servicio on-prem, es responsabilidad del cliente.
- Cada 8 horas se realiza un backup de la base de datos ETCD y se almacena en un bucket propiedad del cliente en Almacenamiento de Objetos de IBM Cloud.
- El backup del almacenamiento utilizado para las aplicaciones desplegadas en la Plataforma es responsabilidad del cliente.
- En caso de perdida de 2 de los 3 Control Plane se inicia el proceso de Disaster Recovery mediante incidente de prioridad uno a través de IBM Cloud.
  - El cliente ha de provisionar la nueva infraestructura necesaria para recuperar los Control Plane
  - IBM reconfigura los Control Plane restaurando el último backup disponible.

https://cloud.ibm.com/docs/satellite?topic=satellite-ha

Disaster Recovery Opción 1– Velero / OADP

Solución basada en “Openshift Application Data Protección” (OADP), distribución de Velero para OpenShift con soporte.

Requiere de almacenamiento S3 accessible desde Pro y DR

Procedimiento gestionado por MAPFRE

Entorno DR activo 24*7 con dimensionamiento mínimo

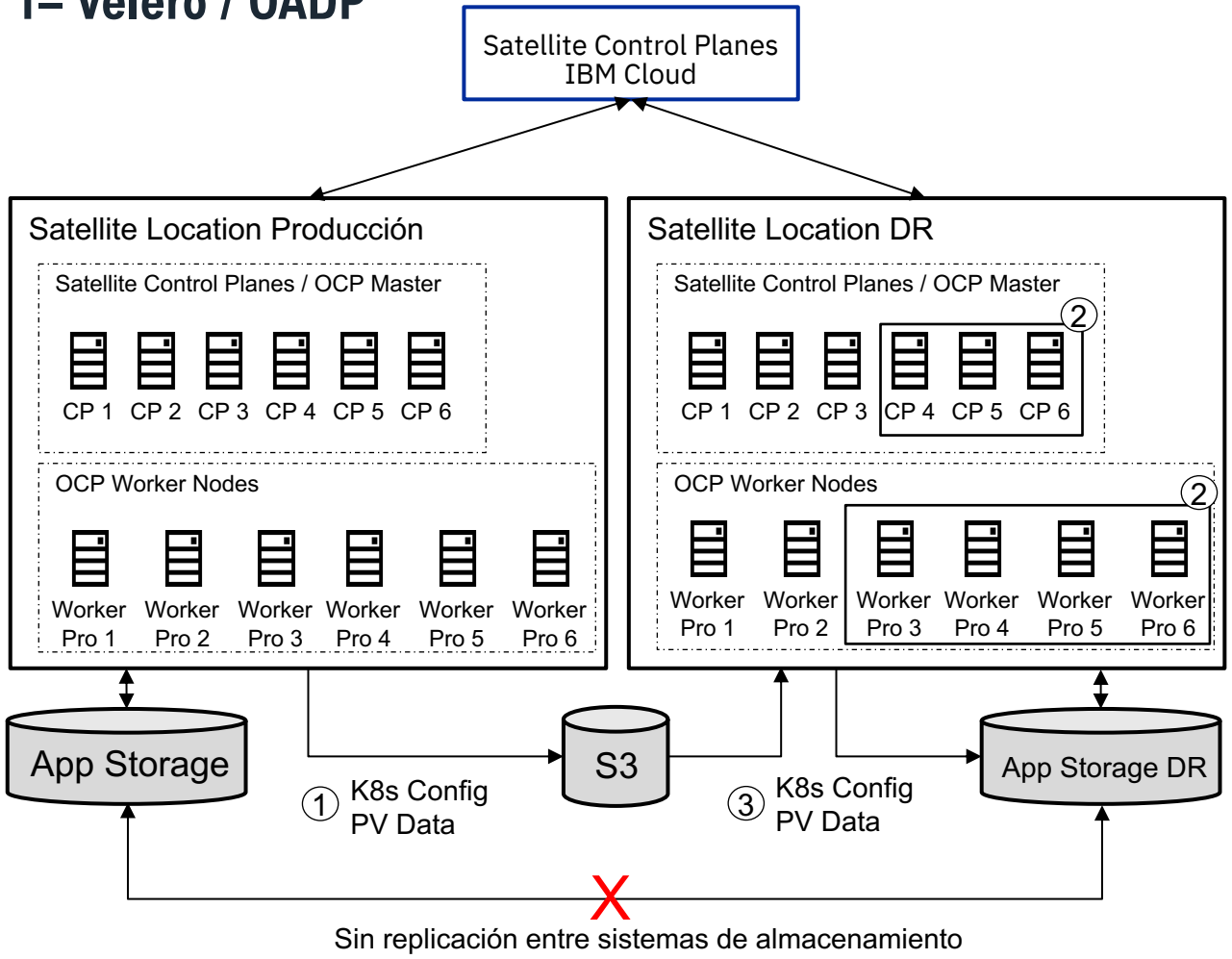
1. OADP backup periódico de:
   - Objetos k8s
   - Datos de aplicación

En tiempo de DR:

2. Aumento de computo del cluster de DR

3. OADP Restore de:
   - Objetos k8s
   - Datos de aplicación

Para recuperar la Location de producción es necesario solicitar la recuperación a IBM Cloud



Disaster Recovery Opción 2 – Satellite Backup & Restore

No hay RTO garantizado en el Retore
No hay entorno de pruebas de DR

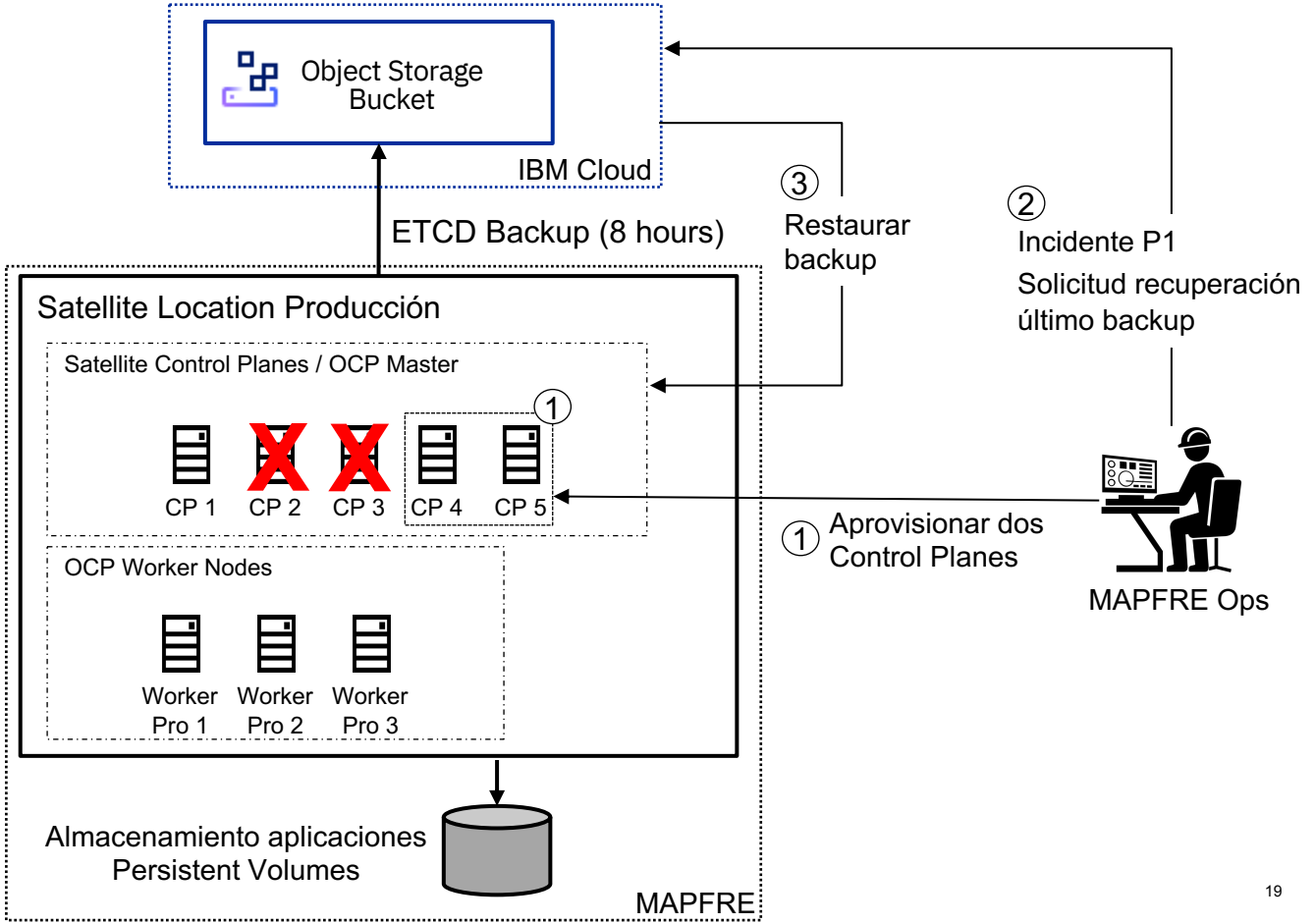
1. MAPFRE aprovisiona dos Host nuevos, los enlaza a la “Location” y los asigna como Control Plane

2. MAPFRE abre ticket Prioridad 1 contra IBM Cloud para recuperar ultimo backup

3. IBM Cloud restaura el backup

Dependiendo del sw desplegado, como por ejemplo bases de datos, harán falta procedimientos específicos del proveedor

* El Storage utilizado para las aplicaciones es responsabilidad de MAPFRE



Matriz RACI para ROKS en IBM Cloud Satellite para MAPFRE

Recurso	Gestión de incidencias y operaciones	Gestión de cambios	Gestión de identidad y acceso	Seguridad y conformidad normativa	Recuperación tras desastre
Datos	MAPFRE	MAPFRE	MAPFRE	MAPFRE	
Aplicaciones	MAPFRE	MAPFRE	MAPFRE	MAPFRE	
Observabilidad	Compartida	IBM	Compartida	IBM	IBM
Redes de aplicaciones	Compartida	IBM	IBM	IBM	IBM
Red de clúster	Compartida	IBM	IBM	IBM	IBM
Versión de clúster	IBM	Compartida	IBM	IBM	IBM
Nodos de trabajador	Compartida	Compartida	IBM	IBM	IBM
Maestro	IBM	IBM	IBM	IBM	IBM
Servicio	IBM	IBM	IBM	IBM	IBM
Almacenamiento virtual	* MAPFRE	* MAPFRE	* MAPFRE	* MAPFRE	* MAPFRE
Red virtual	* MAPFRE	* MAPFRE	* MAPFRE	* MAPFRE	* MAPFRE
Hipervisor	* MAPFRE	* MAPFRE	* MAPFRE	* MAPFRE	* MAPFRE
Servidores físicos y memoria	* MAPFRE	* MAPFRE	* MAPFRE	* MAPFRE	* MAPFRE
Almacenamiento físico	* MAPFRE	* MAPFRE	* MAPFRE	* MAPFRE	* MAPFRE
Red física y dispositivos	* MAPFRE	* MAPFRE	* MAPFRE	* MAPFRE	* MAPFRE
Instalaciones y centros de datos	* MAPFRE	* MAPFRE	* MAPFRE	* MAPFRE	
* MAPFRE --> Decisión de MAPFRE para la parte de Infraestructura. kyndryl está realizando la operación de CPD España y Telefonica en CPDs Miami/Sao Paulo					

IBM Cloud Satellite SLAs (I)

SLA de Disponibilidad

El cálculo de los SLA de disponibilidad no incluye el tiempo de inactividad o fallos que tengan que ver con las exclusiones especificadas.

IBM proporciona cuatro niveles de compromiso SLA, que varían dependiendo de la cantidad de redundancia que proporcione el plan de servicios o la configuración del Cliente. Los cuatro niveles son los siguientes:

Tipo de nivel SLA	Redundancia típica
1. Predeterminado (estándar)	1 (único centro de datos)
2. Configuración reforzada	2 (único centro de datos)
3. Alta disponibilidad regional	3+ (dentro de una región)
4. Alta disponibilidad en varias regiones	4+ (en todas las regiones)

Créditos y reclamaciones de SLA

El Cliente es elegible para un crédito según lo siguiente:

Nivel de Servicio de Disponibilidad Mensual				
Nivel 1	**Nivel 2**	**Nivel 3**	**Nivel 4**	**Crédito**
< 99,90 %	< 99,95 %	< 99,99 %	< 99,995 %	10%
< 99,00 %	< 99,50 %	< 99,90 %	< 99,95 %	25%
< 95,00 %	< 95,00 %	< 95,00 %	< 95,00 %	100 %

Fuente : https://www.ibm.com/support/customer/csol/terms?id=i126-9268&lc=es#detail-document

IBM Cloud Satellite SLAs (yII)

Niveles de SLA soportados por servicio

Cada solución soporta al menos un nivel SLA de disponibilidad y muchas soluciones soportan varios niveles. En el caso de las soluciones multinivel, el nivel aplicable dependerá de la configuración que tenga desplegada el cliente. A fin de ser elegible para un nivel de SLA, el Cliente habrá de desplegar la configuración mínima descrita en la tabla siguiente o la configuración estándar asociada a dicho nivel. Independientemente del nivel, los créditos SLA estarán disponibles en estos casos: i) los especificados en la sección 3 para servicios gestionados por el usuario; ii) los especificados en una modificación específica de servicio en la sección 7; o bien, para todos los demás servicios, iii) cuando el Cliente vea mermada su capacidad de usar el servicio.

Servicio	Nivel 1 (99,9 %)	Nivel 2 (99,95 %)	Nivel 3 (99,99 %)	Nivel 4 (99,995 %)	Comentarios
Satellite	✓		✓		Nivel 3: zonas satelitales situadas en 3 ubicaciones de infraestructura independientes Nivel 1: despliegues restantes Consulte la sección 7.3 para obtener información adicional
Red Hat OpenShift on IBM Cloud	✓		✓		Nivel 3: carga de trabajo común distribuida entre más de tres trabajadores en zonas de disponibilidad independientes Nivel 1: configuraciones restantes Consulte la sección 7.3 para obtener detalles sobre cuándo se ejecuta en Satellite.

Fuente : https://www.ibm.com/support/customer/csol/terms?id=i126-9268&lc=es#detail-document

Soporte a incidencias

Soporte básico	Advanced Support	Soporte premium
Descripción	Manejo de casos priorizados y experiencia de soporte en línea con sus necesidades de negocio para su cuenta de Pago por uso, Suscripción o Pago por uso con uso comprometido	Compromiso del cliente en línea con los resultados de su negocio para acelerar la rentabilidad de la cuenta de Pago por uso, Suscripción o Pago por uso con uso comprometido
Disponibilidad	Acceso 24 horas al día, 7 días a la semana al equipo de soporte técnico de IBM Cloud mediante casos, teléfono	Acceso 24 horas al día, 7 días a la semana al equipo de soporte técnico de IBM Cloud mediante
Gravedad del caso	Clasificación de la gravedad del caso disponible	Clasificación de la gravedad del caso disponible
Objetivos de tiempo de la respuesta inicial	Gravedad 1: Menos de una hora Gravedad 2: Menos de dos horas Gravedad 3: Menos de cuatro horas Gravedad 4: Menos de ocho horas	Gravedad 1: Menos de 15 minutos Gravedad 2: Menos de una hora Gravedad 3: Menos de dos horas Gravedad 4: Menos de cuatro horas
Soporte adicional	No aplicable	Gestor de cuentas técnico asignado Comentarios empresariales trimestrales Acceso a expertos
Precios	Pago por uso y Suscripción: a partir de 200 USD al mes o el 10% del consumo si supera el precio inicial mensual Pago por uso con uso comprometido: 10% del consumo	Pago por uso y Suscripción: a partir de 10.000 USD al mes o el 10% del consumo si supera el precio inicial mensual Pago por uso con uso comprometido: 10% del consumo

Definición de nivel de gravedad	Objetivos de tiempo de la respuesta inicial	
Gravedad	**Impacto empresarial**	**Detalles**
4	Mínimo	Una consulta o solicitud no técnica.
3	Cierta	El producto, servicio o las funciones se puede utilizar y el problema no representa un impacto significativo en las operaciones.
2	Significativo	Un producto, servicio, característica empresarial o función del producto o servicio tiene el uso gravemente restringido, o corre el peligro de no cumplir los plazos de la empresa.
1	Crítico	**Sistema o servicio desactivado** Las funciones críticas de negocio son inoperables o una interfaz crítica ha fallado. Esto se aplica normalmente a un entorno de producción e indica la incapacidad de acceder a productos o servicios, lo que da como resultado un impacto crítico en las operaciones. Esta condición requiere una solución inmediata.

Fuente : https://cloud.ibm.com/docs/get-support?topic=get-support-support-plans&locale=es