

RESUMEN EJECUTIVO

Los servicios Life™ de Vertiv™ ofrecen información continua sobre la operación de equipos críticos de energía y enfriamiento para mejorar el rendimiento, optimizar los procesos de servicio para agilizar la resolución de problemas, así como ofrecerle mayores conocimientos sobre los equipos y el servicio a cualquier organización de manera costo efectiva. Los servicios Life de Vertiv conectan sistemas críticos con ingenieros de Vertiv que monitorean y analizan de forma continua los datos de operación en tiempo real para identificar tendencias, predecir comportamientos y responder de inmediato a condiciones fuera de lo normal, ya sea resolviendo problemas de forma remota o despachando a un ingeniero de campo.

Los detalles técnicos de este servicio son el tema de este documento.

Beneficios y resumen general del servicio

DESCRIPCIÓN DE BENEFICIOS

	Mantiene un rendimiento óptimo	El análisis especializado y continuo basado en datos de los sistemas críticos de potencia y enfriamiento permite la maximización continua de la confiabilidad y eficiencia de los equipos.
	Reduce el tiempo de inactividad	El diagnóstico remoto y la conexión directa con el servicio de campo proporciona la reacción y la respuesta más rápidas posibles, que mejoran las tasas de resolución de incidentes en primera instancia, así como el tiempo de reparación.
	Minimiza los gastos generales	Los servicios Life de Vertiv son un enfoque rentable para asegurar la disponibilidad y rendimiento de los sistemas críticos, los cuales ofrecen amplios conocimientos y una rápida respuesta, sin tener personal exclusivo en el sitio para monitorear y gestionar el mantenimiento del equipo.
	Información integral	Todas las condiciones operativas del equipo se supervisan en conjunto con cualquier actividad de resolución remota y se completa un informe integral disponible en un horario fijo definido por el cliente.

Plataforma en la nube de los servicios Life™ de Vertiv™

Nube

El servidor en la nube es parte fundamental de la oferta de servicios ya que facilita la conexión remota desde cualquier parte del mundo y minimiza la necesidad de equipos para dar el servicio.

Utilizar la nube es clave para dar:

Acción impulsada por datos

Los ingenieros del sistema remoto llevan a cabo actividades de monitoreo, análisis y respuesta para optimizar el estado de los sistemas críticos. Estos ingenieros reciben capacitación especializada para identificar de forma rápida y precisa anomalías y condiciones de alarma y en caso de ser necesario, pueden escalar cualquier comportamiento complejo a los departamentos técnicos de Vertiv.

Respuesta en tiempo real

Los datos en tiempo real permiten dar respuesta en tiempo real a anomalías potenciales y los Servicios Life™ de Vertiv™ detectan los problemas operativos tan pronto como suceden. Desencadena una acción de servicio inmediata para evitar problemas o eliminar horas o días del tiempo para la reparación, lo cual evita o reduce los periodos de inactividad.

Experiencia conectada

Los ingenieros de servicio de Vertiv pueden resolver muchas anomalías de forma remota y están conectados con la organización de servicio local de Vertiv para resoluciones en sitio. En caso de que sea necesario, pueden despachar de forma oportuna a un ingeniero de servicio local, preparado con un diagnóstico, con el fin de llegar listo incluso con piezas de repuesto necesarias.

Arquitectura

La plataforma en la nube está hecha de varios componentes como una aplicación móvil (Vertiv Advisor*), un portal de administración de inventarios del cliente (utilizado por el sistema remoto) y obviamente, el propio equipo crítico.

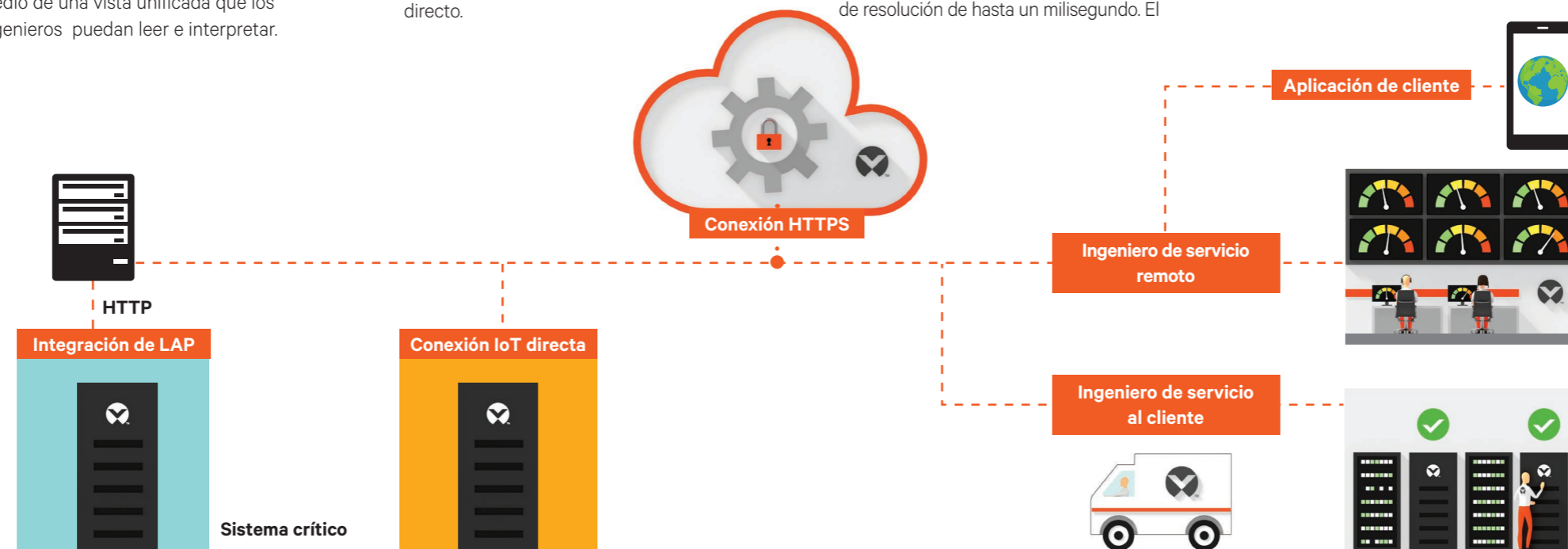
Esta plataforma se ha integrado a sistemas existentes por medio de LAP (Life Access Point) tal y como lo demuestra la siguiente imagen:

- Sistema crítico**
 El sistema que está diseñado y operado para proteger una carga crítica.
- Ingenieros de servicios remotos**
 Los ingenieros de servicios remotos llevan a cabo actividades de monitoreo, análisis y respuesta para optimizar el estado de los sistemas críticos. Estos cuentan con los siguientes datos:
 - Eventos (estados, advertencias, alarmas)
 - Medidas en formato COV (con límites aplicados)
 - Parámetros para los dispositivos
 Estos datos operativos se muestran por medio de una vista unificada que los ingenieros puedan leer e interpretar.

- Ingenieros de servicio al cliente**
 Los ingenieros de servicio al cliente llevan a cabo cualquier actividad de análisis y respuesta necesaria en el sitio del cliente, asegurándose de restaurar los sistemas críticos de forma rápida, segura y precisa a un estado de disponibilidad óptimo.
- Aplicación del cliente***
 La nueva plataforma le permite al cliente tener un panorama de la ejecución de los servicios de Vertiv gracias al concepto de tiempo real que ofrece la nube. Disponible solamente para equipo de IoT directo.

Life Legacy existente utiliza el modelo de "llamada" para transmitir los datos. Para situaciones críticas, genera una llamada de emergencia a la plataforma tan pronto como se captura la información. Sin embargo, para la información que no es crítica, los datos no se transfieren de inmediato a la plataforma, más bien y por lo general, se envían un día completo después. Esta lógica continuaría siendo válida para los dispositivos que no sean IoT.

- IoT directo**
 La nueva plataforma está aumentando la seguridad de datos por medio de HTTPS y le da al usuario acceso directo a la información.



Seguridad de datos

Recolección de datos

Los datos críticos de los sistemas se comunican de forma segura por medio de HTTPS al centro de servicio remoto. Esta conexión HTTPS incluye el uso de certificados SSL. Esto garantiza que todos los datos que se transfieren al centro de servicios remoto estén completamente encriptados y que no los pueda leer ningún tercero no deseado. Los datos críticos se transfieren conforme se recopilan para garantizar un análisis oportuno. También se encuentra presente un caché limitado local para mitigar interrupciones a la red.

Tipo de datos recopilados

Los mensajes del sistema crítico, los parámetros operativos y los datos de identificación se recopilan y transmiten a centros de servicio remoto de Vertiv.

Los mensajes de estatus y alarma contienen información vital relacionada con el estado del sistema crítico y se utiliza para iniciar una respuesta rápida ante incidentes.

Los parámetros operativos seleccionados son un recurso para el diagnóstico detallado y el análisis de tendencias, a fin de garantizar una respuesta adecuada que optimiza la salud del sistema crítico. Los dispositivos ofrecen eventos y medidas en un solo panel. Para modelos determinados, se capturan datos de diagnóstico a nivel de control y se reflejan en un evento correspondiente en Life con la posibilidad de alcanzar un tiempo de resolución de hasta un milisegundo. El

número de serie de la unidad se transmite como identificador del sistema crítico. No se transmite información de contacto del cliente.

Control de aplicaciones y acceso a datos

El acceso a los recursos de información y computación utilizados para habilitar los Servicios Life™ de Vertiv™ es controlado y monitoreado. Se utilizan cuentas con nombres para proteger el acceso al servidor de la aplicación y datos relacionados con el sistema crítico. Los privilegios de acceso se dan con base en la necesidad de conocimiento y la segregación de deberes. Las cuentas son gestionadas por un administrador de servicios de un centro autorizado que los verifica y actualiza según sea necesario.

Seguridad física y ambiental

Se restringe el acceso físico no autorizado, daños e interferencia de la información, así como recursos de cálculo.

Se utiliza un mecanismo de control de acceso que incluye el proceso de autorización, revisión y revocación, para darle seguimiento a, así como evitar, el acceso no autorizado a áreas seguras.

Todos los servidores y componentes de la red están protegidos de forma adecuada. Los sistemas críticos como las fuentes de poder ininterrumpidas, los generadores de respaldo y los aires acondicionados se monitorean y controlan para mantener niveles óptimos de protección.

Ciberseguridad

La ciberseguridad garantiza que las computadoras, los datos y las redes de la organización se defiendan de ataques digitales no autorizados, acceso o daño por la implementación de varios procesos, prácticas y tecnologías. Esta seguridad tiene el objetivo de evitar un ataque contra los datos, las redes y la reputación de la compañía.

Pensado en la seguridad

Protección de datos: los datos que se transmiten desde el dispositivo a la nube de servicios Life, están encriptados y utilizan un protocolo de IoT estándar de la industria (AMQP).

Almacenamiento de datos: los datos del dispositivo se almacenan en la nube de servicios Life y todos los niveles de la plataforma están protegidos por medio de servidores de seguridad, acceso de usuarios, API, etc.

Captura de datos: la tarjeta de comunicación actual cuenta con algoritmos y lógica para capturar y registrar datos de dispositivos. El servicio de la nube de servicios Life se suscribe a los servicios de datos centrales y transmite esta información de forma segura.

Auditorías de seguridad: la tarjeta Unity y la nube se auditan por medio de las políticas de seguridad de Vertiv.

Sistemas

Los servicios Life de Vertiv se pueden habilitar para sistemas críticos que también se monitorean con un sistema de gestión de edificios (BMS, por sus siglas en inglés), un sistema para la gestión de la infraestructura de centros de datos (DCIM, por sus siglas en inglés), un sistema de gestión de redes (NMS, por sus siglas en inglés), u otro sistema. Life complementa la misión de estos sistemas de monitoreo, otorgándoles el análisis y la gestión especializados del servicio de Vertiv. Este paquete permite una flexibilidad completa para gestionar uno o varios centros, al mismo tiempo que garantiza la disponibilidad y la eficiencia operativa de los sistemas críticos.

Descripción de la red

Los datos críticos del sistema se transmiten de forma segura por medio de HTTPS al centro de servicios remotos en tiempo real para un mayor análisis.

La tecnología posee las siguientes características amigables con TI:

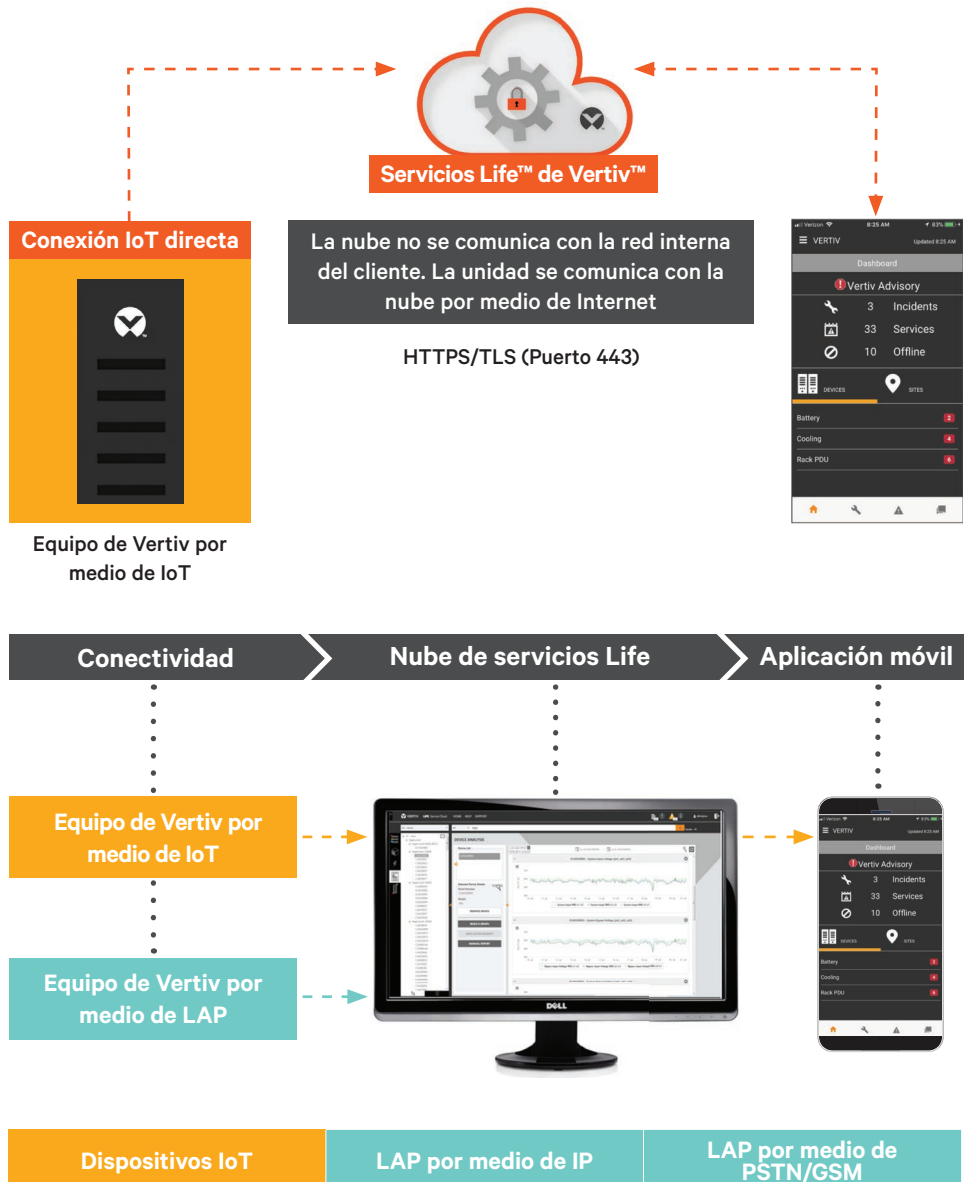
- El sistema crítico inicia la transmisión
- Compatibilidad con el proxy de la red
- Compatibilidad con el servidor de seguridad de la red
- Compatibilidad con la dirección IP asignada por DHCP
- No es necesaria una dirección IP pública
- No es necesaria una dirección IP estática
- No es necesaria una red virtual privada (VPN, por sus siglas en inglés)

Requisitos del cliente

- Dirección IP asignada
- Máscara de red
- Puerta de enlace
- Dirección de servidor DNS
- Dirección de servidor NTP

Habilita el tránsito desde el puerto 443 hasta la siguiente url:

- **Lifeservicecloud.vertivco.com en el puerto 443**
- **Mq-service.vertiv.cloud en el puerto 443.**



	Dispositivos IoT	LAP por medio de IP	LAP por medio de PSTN/GSM
HTTPS	SÍ	por medio de comms. update*	NO
Aplicación móvil	SÍ	por medio de comms. update*	NO
Información crítica	Tiempo real	Tiempo real	Tiempo real
Información no crítica	Tiempo real	por medio de comms. update*	Retraso

*disponible en modelos determinados.

CONECTIVIDAD SEGURA

- Utiliza protocolo IoT estándar de la industria (AMQP)
- Inicia comunicaciones con la nube "Llamar a casa" ("Call Home").
- Puerto para IoT en la tarjeta del dispositivo (SSL/TLS)
- Auditoría para detección continua de amenazas mediante sistema de monitoreo en la nube

Para tener acceso al proceso de garantías de productos, optimizar su experiencia postventa y obtener mayor información registre sus productos Vertiv en Vertiv.com/RegistrotdeProducto