Hoja de datos de privacidad de Elastic

AutoOps en Cloud Connect

Los clientes son responsables de realizar su propia evaluación independiente de la información en este documento. Este documento: (a) tiene fines meramente informativos, (b) representa las ofertas de productos, servicios y prácticas actuales de Elastic, que están sujetas a cambios sin previo aviso, y (c) no crea ningún compromiso ni garantía por parte de Elastic y sus afiliadas, proveedores o licenciantes. Las responsabilidades y obligaciones de Elastic frente a sus clientes se rigen por los acuerdos de Elastic, y este documento no forma parte ni modifica ningún acuerdo entre Elastic y sus clientes.

 © 2025 Elasticsearch B.V. Todos los derechos reservados.

Resumen del producto: AutoOps en Cloud Connect

La evolución de las arquitecturas de búsqueda distribuida ha requerido un avance equivalente en la gestión operativa y las capacidades de diagnóstico. Elastic AutoOps en Cloud Connect representa una utilidad conectada al cloud diseñada para proporcionar detección de problemas en tiempo real, análisis automatizado de causas raíz y recomendaciones de rendimiento accionables para los clusters de Elasticsearch, lo que permite a las organizaciones obtener información de nivel experto sin la necesidad de mantener una infraestructura de monitoreo local completa.

La arquitectura de Elastic AutoOps se basa en un modelo conectado al cloud, especialmente relevante para usuarios empresariales autogestionados que ejecutan despliegues en Elastic Cloud Enterprise (ECE), Elastic Cloud on Kubernetes (ECK) o hardware independiente en forma local. Este modelo garantiza que, aunque la telemetría de diagnóstico se analice en Elastic Cloud, el contenido real que reside en los índices del cliente nunca salga del entorno local. Al limitar estrictamente el procesamiento de datos a metadatos operativos y proporcionar controles robustos de transparencia, Elastic garantiza que las organizaciones puedan optimizar sus cargas de trabajo de búsqueda más complejas sin comprometer la privacidad de sus datos. Para usar AutoOps con tu ECE, ECK o cluster autogestionado de Elasticsearch, primero necesitas crear una cuenta de Elastic Cloud o iniciar sesión en tu cuenta existente. Un asistente de instalación te guía a través de los pasos para instalar Elastic Agent y enviar métricas desde tu cluster a AutoOps en Elastic Cloud.

- **Tipo de producto:** Software
- **Modelo(s) de despliegue:**
    - Cloud (SaaS)

Datos procesados en AutoOps

El procesamiento de datos dentro de Elastic AutoOps se divide estrictamente entre los datos administrativos necesarios para operar el servicio y los metadatos operativos necesarios para diagnosticar el estado del cluster. Es fundamental tener en cuenta que AutoOps está diseñado para ser una solución de solo lectura con respecto al contenido del cliente; no accede, obtiene ni almacena los documentos o los datos fuente del cliente gestionados dentro del cluster.

Categorías de datos personales necesarios para acceder y usar Elasticsearch:

Para gestionar el servicio, se procesan ciertas categorías de datos personales. Estos datos son esenciales para mantener un acceso seguro, gestionar las suscripciones y garantizar un log auditable de las interacciones del sistema.

- **Identificadores de administrador y usuario:** esto incluye nombres, direcciones de correo electrónico y números de teléfono proporcionados durante el registro de la cuenta, las interacciones de soporte y las configuraciones de notificación de eventos.
- **Credenciales y licencias:** los nombres de usuario, las contraseñas (cifradas), las cookies de sesión y los registros de actividad se procesan para gestionar el acceso seguro y aplicar el control de acceso basado en roles (RBAC).

Registros de auditoría: el sistema registra las acciones administrativas, como cuando se registra un cluster o cuando se modifica la configuración de notificaciones, para garantizar la responsabilidad y la auditoría de seguridad.

Las categorías adicionales de datos personales que se procesan pueden incluir, entre otras, los datos contenidos en:

- Metadatos operativos y métricas de diagnóstico
    - Ejemplos: información detallada de los shards, estadísticas completas de los nodos, configuraciones de todo el cluster, resumen general del estado, listas de índices y plantillas componibles, tareas activas del cluster.
        - La recopilación de estas métricas permite a AutoOps realizar análisis complejos, como identificar desequilibrios entre fragmentos, detectar un uso elevado de la CPU y localizar consultas de búsqueda e indexación lentas. Aunque algunos de estos campos, como los nombres de los índices o los nombres de host de los nodos, podrían identificar indirectamente la infraestructura interna tal y como la ha configurado el cliente, no contienen los datos empresariales reales ni los registros de los usuarios finales almacenados en los índices.

Propósito(s) típico(s) de procesar los datos de clientes que se suministran al producto:

El procesamiento de metadatos por parte de Elastic AutoOps tiene como objetivo maximizar la eficiencia operativa de la plataforma Elasticsearch y está pensado para casos de uso como:

- Detección de problemas en tiempo real y análisis de la causa raíz
    - AutoOps correlaciona cientos de métricas para proporcionar una visión unificada del estado del cluster. Por ejemplo, el sistema puede identificar que una transición a un estado de cluster "Rojo" fue precedida por una acumulación de eventos de alta marca de agua en disco durante varios días, lo que permite a los administradores abordar el problema subyacente de almacenamiento antes de que ocurra una interrupción. Este análisis automatizado de causa raíz (RCA) elimina la necesidad de análisis manual de gráficos e índices, que tradicionalmente es un proceso que consume mucho tiempo para los equipos de DevOps.
- Optimización de recursos y costos
    - El análisis de métricas de uso de recursos, como la carga de la CPU, el uso de memoria y las operaciones de E/S de disco, permite a AutoOps identificar los nodos infrautilizados o los índices configurados de manera ineficiente. Al identificar cuellos de botella en la ingesta o malas configuraciones de estructuras de datos, la utilidad proporciona caminos claros de resolución para mejorar la eficiencia de los recursos y reducir los costos de hardware. Por ejemplo, la vista del Optimizador de plantillas analiza mapeos y configuraciones para sugerir optimizaciones que reduzcan la sobrecarga de almacenamiento.
- Integración de soporte y diagnóstico colaborativo
    - Una visión importante del modelo de privacidad de AutoOps es la característica "Mejor soporte". Los clientes pueden otorgar a los ingenieros de soporte de Elastic acceso de solo lectura a sus diagnósticos de AutoOps. Este contexto compartido permite a los ingenieros ver exactamente lo mismo que el cliente, lo que facilita una resolución más rápida y precisa de los tickets de soporte sin necesidad de subir manualmente los paquetes de diagnóstico. Este mecanismo facilita la prestación de soporte bajo el principio de "mínimo privilegio", donde el acceso a los datos de diagnóstico es temporal y está explícitamente autorizado por el cliente.

Datos de uso del producto

En los despliegues de Elastic Cloud que utilizan AutoOps, Elastic recopila de forma automática cierta información relacionada con el uso del producto. Dichos datos de uso del producto se procesan como se describe en la Declaración de privacidad del producto de Elastic.

Acceso a los datos del cliente

- **Acceso por parte de los clientes:**
    - Los clientes conservan el control total y la propiedad de los datos que ingieren, utilizando el control de acceso basado en roles (RBAC) integrado para definir permisos granulares y aplicar el principio de privilegio mínimo. A través de una interfaz unificada basada en el cloud, los usuarios pueden acceder a métricas de alto nivel, eventos de estado en tiempo real y visualizaciones detalladas de rendimiento para sus nodos, índices y shards.
    - Para proporcionar a los clientes que ejecutan clústeres autogestionados una visibilidad completa de los datos que se comparten, AutoOps Elastic Agent incluye un archivo de configuración de depuración. Al reiniciar el agente con esta configuración, los administradores pueden ver localmente una muestra de los datos recopilados del clúster antes de que se envíen a Elastic Cloud. Esto permite una evaluación proactiva de la información que se divulga y respalda las revisiones internas de cumplimiento.
    - Los clientes pueden decidir qué tipo de datos puede extraer el agente Elastic. Leer aquí.
- **Acceso por parte de Elastic**
    - En cuanto a las ofertas de Elastic Cloud, un número limitado de empleados de Elastic tiene acceso privilegiado al entorno de producción únicamente para la gestión, el mantenimiento y el soporte de la plataforma. Este acceso se ajusta estrictamente a los principios de menor privilegio y necesidad de saber, y se revisa y modifica de manera regular según sea necesario. Elastic no tiene acceso a los datos en los despliegues autogestionados, y solo accederá al contenido del cliente en los despliegues en el cloud cuando el cliente lo indique (por ejemplo, al prestar servicios de soporte a petición del cliente).
    - El procesamiento de datos dentro de Elastic AutoOps se divide estrictamente entre los datos administrativos necesarios para operar el servicio y los metadatos operativos necesarios para diagnosticar el estado del cluster. Es fundamental tener en cuenta que AutoOps está diseñado como una solución de solo lectura con respecto al contenido del cliente; no accede, recupera ni almacena los documentos ni los datos de eventos de origen gestionados dentro del cluster, lo que facilita una resolución de problemas más rápida y precisa dentro de un contexto compartido, al tiempo que garantiza que los datos comerciales reales permanezcan dentro del entorno local del cliente.
    - Elastic ha implementado un registro centralizado, que abarca logs de proxies, logs de acceso, logs de Elasticsearch y logs de Auditbeat para registrar todo el acceso a los datos del cliente y a los sistemas en los que residen. Los equipos internos de Elastic desarrollan e implementan activamente detecciones para actividades sospechosas en cuentas internas y acceso no autorizado, lo que incluye el monitoreo de integridad de archivos e indicadores de apropiación de cuenta.

- Los principios de Elastic dictan que solo divulgará o proporcionará acceso a los datos de los clientes cuando la ley lo imponga estrictamente, e incluye protocolos establecidos para impugnar tales solicitudes y notificar a las partes relevantes cuando sea legalmente permisible.

Cumplimiento de las regulaciones de privacidad

Elastic captura, procesa, almacena y protege los Datos personales del cliente de acuerdo con el Anexo de procesamiento de datos del cliente aplicable y los compromisos descritos en esta Hoja de datos de privacidad. Nuestro Centro de confianza es un recurso completo donde encontrarás información sobre nuestras prácticas de privacidad y nuestras iniciativas de cumplimiento normativo.

- **Propiedad de los datos:** los datos del cliente siguen siendo propiedad del cliente. Elastic solo procesa estos datos para los fines especificados en el contrato del cliente y nunca vende los datos de los clientes a terceros.
- **Cumplimiento de GDPR:** las características de Elastic Cloud están diseñadas para respaldar el cumplimiento del Reglamento General de Protección de Datos y otras leyes globales de protección de datos y privacidad. Esto incluye dar prioridad a la seguridad de los datos personales mediante medidas técnicas y organizativas eficaces, y ofrecer un Anexo de procesamiento de datos que cumpla con el GDPR. Nuestro equipo especializado en privacidad de Elastic supervisa el cumplimiento del GDPR.
- **Marco de privacidad de datos (DPF):** Elasticsearch, Inc. está certificado de conformidad con el marco de privacidad de datos UE-EE. UU., la extensión del Reino Unido al marco de privacidad de datos UE-EE. UU. y el marco de privacidad de datos Suiza-EE. UU., según lo establecido por el Departamento de Comercio de los Estados Unidos.
  Transferencia transfronteriza de datos: Elastic legitima las transferencias de datos personales entre las jurisdicciones en las que opera mediante el uso de las Cláusulas contractuales estándar vigentes, así como a través de su participación en el Marco de privacidad de datos para las transferencias hacia Estados Unidos y desde allí en adelante. Además, implementamos medidas complementarias sólidas para proteger los datos durante las transferencias, como el cifrado en tránsito y en reposo, protocolos para impugnar solicitudes de autoridades públicas y la opción para los clientes de seleccionar servidores regionales para el alojamiento.

Portabilidad de datos

Los clientes mantienen el control total sobre los datos que ingestan en sus propios clusters. Para los metadatos procesados por AutoOps, los usuarios pueden acceder a métricas de alto nivel a través de las vistas Visión general y Nodos. Aunque Elastic se encarga de gestionar la telemetría específica almacenada en el cloud, las métricas originales siguen estando disponibles en el cluster autoadministrado del cliente para su extracción a través de las API estándar de Elasticsearch.

Retención y eliminación

Elastic AutoOps aplica políticas estrictas de retención de datos para ajustarse al principio de minimización de datos y a la naturaleza transitoria de la telemetría operativa. Las métricas operativas de AutoOps se conservan durante un período de 10 días en la infraestructura de cloud interna de Elastic. El período de retención de 10 días para las métricas de AutoOps garantiza que las tendencias de rendimiento recientes estén disponibles para el diagnóstico, mientras que los datos más antiguos, que suelen perder su relevancia operativa en entornos dinámicos, se eliminan automáticamente.

Seguridad

Elastic implementa un modelo de seguridad de defensa en profundidad diseñado para proteger los datos de los clientes durante todo su ciclo de vida. El acceso a los sistemas que procesan los datos de AutoOps está regulado por estrictas medidas organizacionales y técnicas. La seguridad de tus datos de Elastic Cloud también depende de que mantengas tu cluster de Elasticsearch configurado de forma segura y de que mantengas la confidencialidad de tus credenciales de inicio de sesión de Elastic Cloud (consulta nuestras Preguntas frecuentes sobre seguridad para obtener más información).

- **Arquitectura de operaciones automáticas:** la arquitectura de Elastic AutoOps es especialmente relevante para usuarios empresariales autogestionados que ejecutan despliegues en Elastic Cloud Enterprise (ECE), Elastic Cloud on Kubernetes (ECK) o hardware independiente local. Este modelo garantiza que, aunque la telemetría diagnóstica se analiza en el cloud, los datos empresariales subyacentes, el contenido real que reside en los índices del cliente, nunca abandonen el entorno local.
- **Protocolos de comunicación:** Elastic AutoOps emplea dos protocolos de comunicación principales para garantizar una ingesta segura de telemetría. Ambos canales operan sobre el puerto 443 estándar, lo que garantiza la compatibilidad con configuraciones comunes de firewall mientras se mantienen altos estándares de cifrado.
    - Canal de registro (HTTP/HTTPS): este canal se usa para registrar el cluster local con Elastic Cloud. Usa una clave de API de Elastic Cloud que está estrictamente limitada para su uso con el marco de trabajo Cloud Connect.
    - Canal de telemetría (OTLP sobre HTTP): El Protocolo OpenTelemetry (OTLP) se utiliza para recopilar datos operativos. Este canal se autentica mediante un token de AutoOps, que es funcionalmente equivalente a una clave de API y garantiza que solo los agentes autorizados puedan transmitir datos a la organización específica del cliente.
- **Cifrado:** los datos del cliente se cifran en reposo mediante AES-256 y en tránsito mediante TLS 1.2 o superior. Elastic implementa estrictos procedimientos de gestión de claves de cifrado para garantizar que el acceso a datos cifrados esté limitado a procesos y usuarios autorizados. Para los despliegues de cloud hospedado, los datos de los clientes también están protegidos mediante una robusta gestión de claves integrada en la infraestructura del proveedor de servicios en el cloud (CSP).
- **Controles de acceso:** Elastic mantiene controles técnicos, lógicos y administrativos para limitar el acceso a los datos exclusivamente a los usuarios autorizados. Estos controles incluyen medidas como la autenticación multifactorial, normas estrictas sobre la seguridad de las contraseñas y el uso de redes privadas virtuales (VPN) para el acceso administrativo. Además, los controles de acceso basados en roles (RBAC) están integrados en los despliegues de Elastic y la plataforma de administración de Elastic Cloud, lo que permite un control granular sobre los permisos de los usuarios.
- **Logging y monitoreo:** Elastic implementó un sistema de logging centralizado, que incluye logs de proxies, logs de acceso, logs de Elasticsearch y logs de Auditbeat para registrar todo el acceso a los datos del cliente y a los sistemas en los que residen. El equipo de Detección y Respuesta a Amenazas de Elastic usa flujos de trabajo automatizados para detectar e investigar actividad sospechosa en cuentas internas y acceso no autorizado, lo que incluye el monitoreo de la integridad de archivos e indicadores de apropiación de cuenta.
- **Actualizaciones y parches del sistema:** las instancias de Elasticsearch se actualizan y despliegan regularmente según los kernels del sistema operativo más recientes. Se aplican los parches correspondientes de forma oportuna cada vez que se identifica una vulnerabilidad o exposición común (CVE) en cualquier componente de software.

- **Detección y respuesta a incidentes:** Elastic implementó y actualiza continuamente las reglas de detección para actividades sospechosas y accesos no autorizados. Estas detecciones forman parte de flujos de trabajo automatizados que alertan al equipo de Detección y Respuesta a Amenazas, y desencadenan investigaciones de analistas. Elastic usa Elastic Security a nivel interno, que incluye capacidades de detección y respuesta de endpoint e integra fuentes de inteligencia de amenazas para admitir la detección de intrusiones. Permite respuestas automatizadas mediante integraciones con plataformas SOAR de terceros, lo que reduce la probabilidad de una brecha y acelera los tiempos de respuesta.
- **Marco de desarrollo de software seguro (SSDF):** Elastic mantiene un marco de desarrollo de software seguro basado en NIST 800-218. Este marco guía el proceso para diseñar, desarrollar, implementar, supervisar y mantener de forma segura todo el software de Elastic, garantizando un enfoque de "seguridad desde el diseño" y "seguridad por defecto".
- **Reseña de proveedores externos:** Elastic colabora con los principales proveedores de IaaS (AWS, GCP, Azure) y realiza revisiones rigurosas de sus estándares de seguridad y cumplimiento, incluidas las auditorías SOC 2 y las certificaciones ISO 27001 y 27701, como parte de su programa de gestión de riesgos de terceros.
- **Pruebas de penetración:** terceros independientes realizan pruebas anuales de penetración de aplicaciones y redes contra Elastic Cloud, como mínimo. Elastic también cuenta con un programa público de recompensas por errores para pruebas continuas de investigadores.
- **Formación de empleados:** todos los empleados de Elastic deben completar una formación integral en seguridad de la información y protección/privacidad de datos al ser contratados y al menos una vez al año a partir de entonces.