centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 889B

Guía de Configuración segura para Monitorización y gestión

MARZO 2022

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.03.29 17:48:54 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-115-X

Fecha de Edición: marzo de 2022
Sidertia Solutions S.L. ha participado en la realización y modificación del presente documento y sus anexos.

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN)

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Marzo de 2022

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1. GUÍA DE CONFIGURACIÓN SEGURA PARA MONITORIZACIÓN Y GESTIÓN

1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA

Esta guía muestra la activación y configuración de los servicios de Oracle Cloud Infrastructure (OCI) para la monitorización y gestión de las cargas de trabajo en la nube pública de Oracle, siguiendo las exigencias del Esquema Nacional de Seguridad (ENS).

La principal utilidad de esta guía es identificar los servicios de monitorización, supervisión y gestión que deben configurarse, cumpliendo con las distintas medidas de seguridad que establece el Esquema Nacional de Seguridad. A su vez, se añaden referencias a la documentación oficial del fabricante con el objetivo de facilitar la lectura y comprensión por parte del usuario de esta guía.

La nomenclatura de algunos servicios o tecnologías descritos se documenta en el glosario de abreviaturas, incluido como anexo al documento.

Para finalizar, se incluye un resumen de las medidas detalladas anteriormente para realizar un control de la configuración a modo de “checklist”.

1.2 DEFINICIÓN DEL SERVICIO

Oracle Cloud Infrastructure (OCI) es un conjunto de servicios complementarios en la nube que permite la creación y ejecución de una amplia gama de aplicaciones y servicios en un entorno de alta disponibilidad.

OCI brinda servicios funcionales para la monitorización y gestión del rendimiento tanto de las aplicaciones como de la infraestructura del sistema. Además, permite, a través de los servicios de monitorización, la recopilación de datos y métricas estableciendo una comunicación interactiva entre OCI y cualquier otro destino.

Dentro de los modelos que ofrece OCI, esta guía se centrará en el modelo de Infraestructura como Servicio (IaaS) y en el modelo de Plataforma como Servicio (PaaS).

a) **IaaS:** Es un tipo de modelo de servicio de Cloud Computing en el que los recursos de computación se alojan en la nube. Las organizaciones pueden usar el modelo IaaS para trasladar parte o la totalidad de su uso de la infraestructura de centro de datos in situ o localizada a la nube, donde será propiedad de un proveedor de nube y estará administrada por este. Entre estos elementos de infraestructura se pueden incluir hardware de computación, red y almacenamiento, así como otros componentes y software.

b) **PaaS:** Es un conjunto de servicios que permite crear y gestionar aplicaciones modernas en la era digital, on-premises o en la nube. Proporciona la infraestructura y los componentes que permiten a los desarrolladores, administradores de TI y usuarios crear, integrar, migrar, implementar, proteger y administrar sistemas y aplicaciones. Para ayudar a mejorar la productividad, PaaS ofrece componentes de programación listos para usar que permiten a los desarrolladores integrar nuevas características en sus aplicaciones, incluidas tecnologías innovadoras como inteligencia artificial (IA), chatbots, blockchain y el Internet of Things (IoT).

Esto también incluye suites de herramientas de desarrollo de aplicaciones, lo que incluye servicios nativos en la nube, Kubernetes, Docker, motores de contenedor y mucho más.

Monitorización y gestión es una plataforma evolucionada basada en un conjunto de herramientas de monitorización, que permite la proactividad en la gestión de la infraestructura. No solo se trata de mecanismos que recopilan datos y métricas para elaborar tendencias, patrones y estadísticas, sino que permite la interacción mediante las alertas que automatizan acciones correctivas.

El conjunto de herramientas de monitorización y gestión permite una clasificación general de sus funciones en los distintos ámbitos en los que operan. Así pues, dentro de la monitorización y gestión de alertas se puede encontrar la recopilación de métricas, la definición de canales de notificación y la personalización de las alertas adaptadas a las necesidades de la infraestructura.

Por otro lado, en el ámbito de la gestión de logs se puede encontrar la recopilación de logs de sistema, auditoría y logs personalizados que definen las alertas. A la hora de gestionar los datos y las métricas, existen herramientas de monitorización y gestión que permiten la elaboración de estadísticas y tendencias que detectan anomalías y patrones mediante un panel de control centralizado.

Finalmente, las herramientas de monitorización y gestión permiten la monitorización de transacciones comerciales de un extremo a otro, pruebas sintéticas y monitorización real de las actividades del usuario. Para facilitar la comprensión, las distintas herramientas de monitorización y gestión pueden ser enmarcadas dentro de los siguientes estadios:

a) **Recopilación de métricas y gestión de alertas**: Los servicios encargados de la recopilación de métricas y logs se realizan en un mismo lugar. Las alertas pueden ser generadas en base a la definición de reglas. Los servicios de recopilación de logs y métricas son los siguientes:
   i. OCI Logging (Registro)
   ii. OCI Monitoring (Supervisión)
   iii. OCI Alerts (Alertas)

b) **Integración**: El conjunto de logs y métricas recopilados pueden ser enriquecidos con otros datos procedentes de sistemas externos on-premises o bien pueden ser exportados para las herramientas de alimentación externa:
   i. OCI Service Hub
   ii. OCI Management Agent (Agente de gestión)
   iii. OCI RestAPI

c) **Análisis**: Los datos recopilados pueden ser analizados dentro de las capacidades que permiten las aplicaciones de análisis de OCI para la elaboración de estadísticas, patrones, tendencias y la generación de alertas:
   i. OCI Logging Analytics (Análisis de registro)
   ii. OCI Database Management (Gestión de bases de datos)
   iii. OCI Operation Insight (Estadísticas de operaciones)

iv. OCI Application Performance Monitoring (APM)

A continuación, se enumeran los servicios y componentes que permiten la monitorización, supervisión y gestión del rendimiento tanto de la infraestructura como de las aplicaciones en la nube de OCI:

a) **Application Perfomance Monitoring (APM):** Proporciona un conjunto completo de funciones para la supervisión de las aplicaciones y el diagnóstico de problemas de rendimiento.

b) **Database Management (Gestión de bases de datos):** Brinda funciones completas de diagnóstico y gestión del rendimiento de la base de datos para la supervisión y gestión de las bases de datos de Oracle.

c) **Java Management (Gestión de Java):** Permite la gestión y generación de informes dentro de OCI para la monitorización del uso de Java en la organización.

d) **Logging Analytics (Análisis de registro):** Oracle Cloud Logging Analytics es una solución en la nube en OCI que permite la indexación, búsqueda y análisis de todos los datos log de las aplicaciones y la infraestructura del sistema.

e) **Logging (Registro):** El servicio de registro es un panel único altamente escalable y totalmente gestionado para todos los logs del tenant. Proporciona acceso a los registros desde los recursos de OCI y permite registros de activación, gestión y búsqueda.

f) **Management Agent (Agente de gestión):** Es un componente que permite la comunicación interactiva de baja latencia y recopilación de datos entre OCI y cualquier otro destino para uso de otros servicios de monitorización y supervisión.

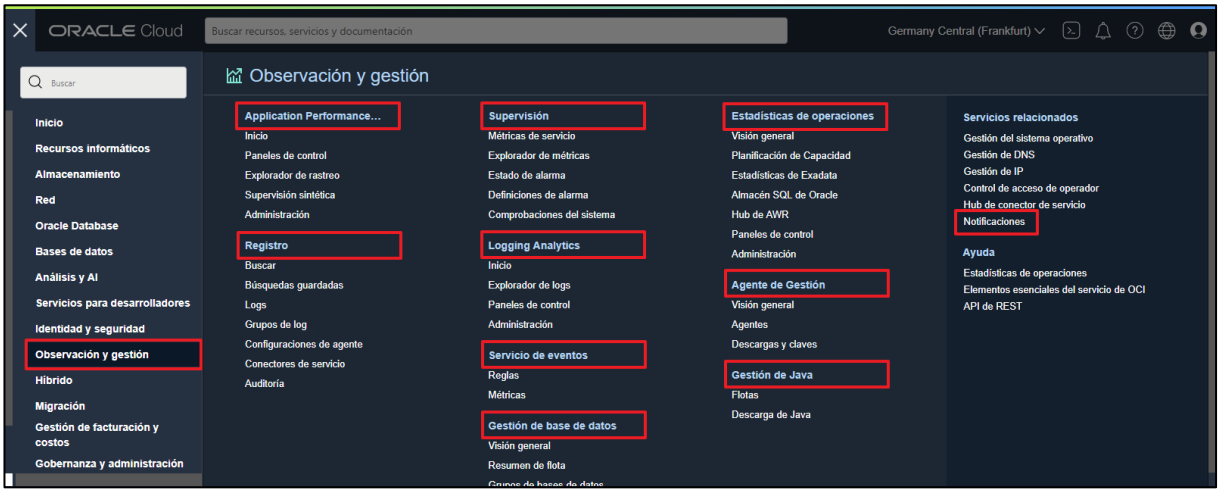
g) **Monitoring (Supervisión):** El servicio de supervisión permite la consulta de métricas y la gestión de alarmas que supervisan el estado, la capacidad y el rendimiento de los recursos en la nube.

h) **Notifications (Notificaciones):** Permite la difusión de mensajes a componentes distribuidos al dispararse las alarmas, conectores de servicio y reglas de evento a través de un patrón de publicación-suscripción, proporcionando mensajes seguros, altamente fiables, de baja latencia y duraderos para aplicaciones alojadas en OCI y externamente.

i) **Operations Insights (Estadísticas de operaciones):** Proporciona estadísticas completas sobre el uso de los recursos y la capacidad de las bases de datos y los hosts, permitiendo el análisis de los recursos de almacenamiento y CPU, previniendo problemas de capacidad e identificando problemas de rendimiento de SQL en toda la flota de bases de datos.

j) **Service Connector Hub:** Proporciona un lugar central para describir, ejecutar y monitorear los movimientos de datos entre servicios, como Logging, Object Storage, Streaming, Logging Analytics y Monitoring. También puede activar Functions para el procesamiento de datos livianos y Notifications para configurar alertas.

k) **Resource Manager (Gestor de recursos):** Automatiza el despliegue y las operaciones de todos los recursos de OCI. Mediante el modelo de infraestructura como código (IaC), el servicio se basa en Terraform, un estándar del sector de código abierto que permite a los ingenieros DevOps desarrollar y desplegar la infraestructura en cualquier lugar.



Menú de navegación OCI Observación y gestión.

Para obtener más información sobre el gestor de recursos, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/ResourceManager/home.htm

Nota: El servicio Database Management (Gestión de base de datos) y Operations Insights (Estadísticas de operaciones) se detallarán en profundidad en la guía de seguridad "CCN-STIC-889D Guía de Configuración segura para OCI Database-Instancias VM".

1.3 SERVICIOS DE MONITORIZACIÓN Y GESTIÓN

1.3.1 APPLICATION PERFORMANCE MONITORING (APM)

Las organizaciones dependen de sus aplicaciones para ofrecer procesos de negocio esenciales. A medida que el énfasis se desplaza hacia el acceso remoto y en línea, la precisión, la velocidad y la coherencia se convierten en fundamentales.

Application Performance Monitoring (APM) es un servicio que proporciona un juego completo de funciones para la supervisión de aplicaciones y el diagnóstico de incidencias de rendimiento. Esto incluye la supervisión de los diversos componentes y la lógica de aplicación en los clientes, servicios de terceros y los niveles informáticos de backend, tanto de forma local como en la nube.

A continuación, se muestran las funciones de Application Performance Monitoring (APM):

a) **Rastreo distribuido:** Recopila y procesa datos de rastreo de instancia de transacción mediante orígenes de datos de Application Performance Monitoring (APM), rastreadores de código abierto o directamente mediante la API. El rastreo distribuido supervisa el rendimiento, el volumen y la ratio de errores de las transacciones y notifica las incidencias.

Analiza la carga, los patrones de uso, el rendimiento y la capacidad en las dimensiones listas para usar y personalizadas.

b) **Supervisión sintética:** Evalúa la disponibilidad de la aplicación mediante pruebas periódicas desde varios puntos estratégicos, garantizando la detección temprana de incidencias de disponibilidad y rendimiento sistémico.

c) **Supervisión de usuario real:** Proporciona información sobre la experiencia del usuario final directamente desde el explorador, identificando la degradación del rendimiento mediante la supervisión del tiempo de carga de página y la acción del usuario.

d) **Supervisión del servidor:** Recopila métricas de uso y rendimiento de los servidores de aplicaciones supervisados, proporcionando funciones de creación de gráficos y alertas mediante la integración con el servicio de supervisión (Monitoring) de OCI.

APM utiliza agentes y rastreos como orígenes de datos que recopilan y cargan datos, como las métricas y los períodos para la supervisión. A continuación, se muestra la lista de tipos de orígenes de datos que se usan con APM:

a) **Agentes de explorador de APM:** Para el registro de la interacción del usuario con sitios web y el envío de métricas y períodos a APM.

b) **Agentes JAVA de APM:** Para el registro de los períodos y las métricas del servidor de aplicaciones y envío a APM.

c) **Rastreadores JAVA de APM:** Para el registro de los períodos de OpenTracing mediante métricas de aplicación y envío de períodos y métricas a APM.

d) **Rastreadores de código abierto:** Para la carga de datos de rastreo en APM.

e) **API:** Para la carga de datos de rastreo mediante llamadas a la API.

f) **Supervisiones sintéticas:** Para el envío de métricas de rendimiento a APM tanto de una URL como del flujo de trabajo de transacción de usuario registrado en un script.

Para obtener más obtener información sobre el servicio APM, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/application-performance-monitoring/index.html

1.3.2 JAVA MANAGEMENT (GESTIÓN DE JAVA)

El servicio de gestión de Java es una infraestructura de generación de informes y gestión dentro de OCI. Permite observar y gestionar el uso de Java en la organización. Además, el servicio está integrado con los servicios de la plataforma de OCI para la monitorización y gestión del uso de Java SE tanto en local como en la nube.

El cliente puede realizar las siguientes acciones:

a) El uso de estadísticas de JMS que optimizan las cargas de trabajo en toda la organización como el escritorio, servidor o la nube.

b) Protección de sus inversiones en Java SE identificando las instalaciones de Java obsoletas y aplicaciones no autorizadas.

JMS ayuda a los administradores de sistemas en la gestión y control de los siguientes elementos:

a) Gestión y control de todas las versiones Java que se han ejecutado y se ejecutan tanto en los entornos de desarrollo como de producción.

b) Gestión sobre cuáles son los proveedores que proporcionan las instalaciones de Java en su entorno.

c) Control de las aplicaciones que utilizan instalaciones Java previstas.

d) Conocer si se están ejecutando aplicaciones no autorizadas.

e) Conocer cuántas instalaciones de Java obsoletas existen en los entornos de producción y desarrollo.

Oracle aprovecha de forma única su experiencia para obtener estadísticas fundamentales sobre el comportamiento, el cumplimiento y el rendimiento de las aplicaciones Java.

Puede obtener más información del servicio consultando el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/jms/index.html

1.3.3 LOGGING (REGISTRO)

El servicio de registro proporciona acceso a todos los logs de los recursos del tenant Los logs proporcionan información de diagnóstico crítica que describe el rendimiento de los recursos y cómo se está accediendo a ellos.

Se puede utilizar Logging (Registro) para activar, gestionar y buscar logs. Los tres tipos de logs existentes son los siguientes:

a) **Logs de auditoría:** Son logs relacionados con eventos emitidos por el servicio OCI Audit (Auditoría). Estos logs están disponibles en la página Auditoría de registro o se pueden encontrar en la página Buscar junto con el resto de los logs.

b) **Logs de servicios:** Son logs emitidos por los servicios nativos de OCI, como API Gateway, Events, Functions, Load Balancing, Object Storage (Almacenamiento de Objetos) y logs de flujo de VCN. Cada uno de estos servicios soportados tiene categorías de registro predefinidas que pueden ser activadas o desactivadas en sus respectivos recursos.

c) **Logs personalizados:** Logs que contienen información de diagnóstico de aplicaciones personalizadas, otros proveedores de nube o un entorno local. Los logs personalizados se recopilan mediante la API o mediante la configuración del agente de supervisión unificado.

Un log es un recurso de primera clase de OCI que almacena y captura eventos de log recopilados en un contexto determinado. Cada log tiene un OCID que se almacena en un grupo de logs. Un grupo de logs es una recopilación de logs almacenados en un compartimento. Los logs y los grupos de logs se pueden buscar, accionar y transportar.

Puede obtener más información relacionada con el servicio de registro en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Logging/home.htm

1.3.4 LOGGING ANALYTICS (ANÁLISIS DE REGISTRO)

OCI Logging Analytics es la solución en la nube de OCI que visualiza todos los datos de log de las aplicaciones e infraestructura de Oracle Cloud. Mediante esta herramienta, es posible añadir y analizar todos los logs a través de estadísticas correlacionadas para la supervisión.

El servicio de análisis de registro proporciona varias formas de obtener estadísticas operativas de los logs del tenant:

a) Usando la interfaz de usuario del explorador de logs.

b) Agregando información de log a los paneles de control.

c) Utilizando las API en la recopilación de datos para su análisis.

d) Integrando con otros servicios de OCI.

Las visualizaciones interactivas ofrecen varias posibilidades para desglosar los datos. Usando la función Clúster para reducir millones de entradas de log a un pequeño juego de firmas de log interesantes, lo que facilita la revisión. Por otro lado, la función Enlazar permite el análisis de logs en una transacción o la identificación de patrones anómalos mediante la vista agrupada.

Puede obtener más información relacionada con el servicio de análisis de registro en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/logging-analytics/index.html

1.3.5 MANAGEMENT AGENT (AGENTE DE GESTIÓN)

Los agentes de gestión sirven para recopilar los datos relacionados con los servicios u otros orígenes que se desee supervisar. El componente de agente de gestión gestiona el ciclo de vida del agente de gestión y los plugins de los servicios.

Puede obtener más información relacionada con el servicio de agente de gestión en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/management-agents/index.html

1.3.6 MONITORING (SUPERVISIÓN)

El servicio de Monitoring o Supervisión supervisa los recursos de OCI y gestiona las alarmas a fin de notificar en caso de que las métricas alcancen los valores especificados.

Las métricas se envían al servicio de Supervisión en forma de puntos de datos no procesados o pares de marca de tiempo-valor, junto con las dimensiones y los metadatos. Las métricas provienen de una variedad de fuentes como:

a) Métricas de recursos publicadas automáticamente por los recursos de OCI.

b) Métricas personalizadas.

c) Datos enviados a nuevas métricas o métricas existentes mediante Service Connector Hub.

Para acceder a los datos de las métricas y alarmas se utiliza la Consola, la CLI o la API. Cuando se consulta una métrica, el servicio de Supervisión devuelve datos agregados según los parámetros especificados. Se puede especificar un rango de tiempo, una estadística y un intervalo. La Consola muestra un gráfico de supervisión por métrica para los recursos seleccionados y los datos agregados en cada gráfico reflejan la estadística y el intervalo seleccionados.

Nota: Los recursos de métricas carecen de OCID.

La función Alarmas del servicio de Supervisión publica mensajes de alarma en destinos configurados y gestionados por el servicio de Notificaciones. Cada destino constituye un tema con un conjunto de suscriptores.

Puede obtener más información sobre la publicación de métricas personalizadas en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Monitoring/Tasks/publishingcustommetrics.htm

Para obtener más información relacionada con Service Connector Hub, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/service-connector-hub/home.htm

Para obtener más información relacionada con el servicio de Supervisión, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Monitoring/home.htm

1.3.7 NOTIFICATIONS (NOTIFICACIONES)

El servicio OCI Notificaciones envía mensajes a componentes distribuidos a través de un patrón de publicación-suscripción que proporciona seguridad y fiabilidad, a través de los canales de comunicación.

Cuando se publica un mensaje en un tema, el servicio de Notificaciones envía este mensaje a todas las suscripciones del tema, pudiendo seleccionar un formato fácil de recordar para aumentar la legibilidad humana del contenido de un mensaje.

Notificaciones envía mensajes cuando se disparan reglas de eventos, se acoplan alarmas, se ejecutan conectores de servicio o alguien publica directamente un mensaje.

Los tipos de mensajes que puede enviar el servicio de notificaciones se enumeran a continuación:

a) **Reglas de evento:** El servicio de notificaciones envía mensajes de evento cuando se disparan las reglas. Por ejemplo, se puede configurar un mensaje para las nuevas bases de datos.

b) **Alarmas:** El servicio de notificaciones envía mensajes de alarma cuando se incumplen las alarmas. Por ejemplo, se puede configurar un mensaje de alarma para un uso elevado de CPU.

c) **Conectores de servicio:** El servicio de notificaciones envía mensajes de conector de servicio cuando se ejecutan los conectes de servicio. Por ejemplo, se puede configurar un conector de servicio para enviar logs de uso.

d) **Publicación directa:** El servicio de notificaciones puede enviar mensajes cuando un administrador o un servicio o una aplicación publica mensajes directamente.

Puede obtener más información sobre el servicio de Notificaciones consultando el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Notification/home.htm

1.3.8 EVENTS (SERVICIO DE EVENTOS)

OCI Events (Eventos) es un servicio que habilita la automatización de cambios de estado de los recursos del tenant. Los servicios de OCI emiten eventos, que son mensajes estructurados que indican cambios en los recursos. Los eventos utilizan el formato estándar del sector CloudEvents de Cloud Native Computing Foundation (CNCF).

Este estándar permite la interoperabilidad entre diferentes proveedores de nube o proveedores de sistemas locales y de nube. Un evento puede ser una operación de creación, lectura, actualización o supresión (CRUD), un cambio de estado del ciclo de vida de los recursos o un evento del sistema que afecte a un recurso. Por ejemplo, se puede emitir un evento cuando se complete o falle una copia de seguridad o cuando se agregue, actualice o suprima un archivo de un bucket en Object Storage.

Los servicios emiten distintos tipos de eventos para los recursos, que se distinguen como tipos de eventos. Los tipos de eventos son los cambios que producen eventos mediante un recurso determinado. Para ver una lista de servicios que producen eventos y los tipos de eventos que controlan dichos servicios, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Events/Reference/eventsproducers.htm

Se puede trabajar con eventos creando reglas. Las reglas incluyen un filtro definido para especificar los eventos producidos por los recursos en el tenant.

Las reglas deben especificar también una acción que se disparará cuando el filtro encuentre un evento coincidente. Las acciones son respuestas definidas para las coincidencias de eventos. Cuando el filtro de la regla encuentra una coincidencia, el servicio de eventos entrega el evento coincidente a uno o más de los destinos identificados en la regla. Sin embargo, solamente se puede entregar eventos a determinados servicios de OCI como Notifications (Notificaciones), Streaming y Functions (Funciones), con una regla.

1.3.9 SERVICE CONNECTOR HUB

Service Connector Hub es un servicio gratuito que proporciona un lugar centralizado donde los administradores pueden administrar y monitorizar los movimientos de datos en todos los servicios OCI y de OCI a servicios de terceros. Además, el servicio se integra con Monitoring para emitir métricas, como bytes transferidos, errores en el origen o destino y actualización de datos que pueden ser usados para crear alarmas que activen las soluciones manuales o automatizadas.

Por otro lado, el servicio se integra también con OCI IAM, lo que permite a los administradores configurar fácilmente políticas granulares que rigen el acceso y la interacción con los conectores de servicio.

Finalmente, para obtener una visión general sobre Service Connector Hub, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/service-connector-hub/overview.htm

2. CONFIGURACIÓN SEGURA PARA MONITORIZACIÓN Y GESTIÓN

Las medidas de seguridad se dividen en tres grupos, Marco organizativo, Marco Operacional y Medidas de Protección del Esquema Nacional de Seguridad. En los siguientes puntos, se detallan los grupos Marco operacional y Medidas de protección con las medidas que aplican en la Categoría Alta del ENS.

2.1 MARCO OPERACIONAL

Este grupo está formado por las medidas a tomar para proteger la operación del sistema como un conjunto integral de componentes para un fin. Para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos, se aplicarán las medidas de seguridad indicadas en este anexo, las cuales serán proporcionales a las dimensiones de seguridad relevantes en el sistema a proteger y la categoría del sistema de información a proteger.

Se considera, en este sentido, que la organización ha dispuesto todos aquellos mecanismos de control físico necesarios, con objeto de evitar el acceso a la nube existentes por parte de personal no autorizado.

2.1.1 CONTROL DE ACCESO

El conjunto de medidas que establece el Control de acceso cubre todas las acciones que, bien preparatorias o ejecutivas, están orientadas a determinar qué o quién puede o no acceder a un recurso del sistema mediante una determinada acción. Con el cumplimiento de todas las medidas, se garantizará que nadie accederá a recursos sin la debida autorización. Adicionalmente, se establecerá la necesidad de que el uso del sistema quede registrado para detectar y reaccionar ante una incidencia de seguridad o fallo del sistema pudiendo configurarlo en Oracle mediante el Servicio OCI Identity and Access Management (OCI IAM).

A continuación, se enumeran las siguientes medidas de seguridad basadas en el control de acceso. Para obtener más información relacionada con la configuración del servicio (OCI IAM), consulte la guía de seguridad “CCN-STIC-889A Guía de Configuración segura para IAM y servicios de seguridad”.

2.1.1.1 IDENTIFICACIÓN

Esta medida especifica los mecanismos que garantizan la autenticidad y trazabilidad de las diferentes entidades. Esto genera una identificación singular para cada organización, usuario, proceso o servicio. De esta manera, se conocerá quién recibe qué derechos sobre los recursos y quién ha hecho el qué sobre los mismos.

Para el uso de los servicios de monitorización y gestión de OCI, es necesario la creación de cuentas de usuario, grupos y políticas definidas para el control de acceso a los recursos del sistema, a través del servicio OCI IAM.

2.1.1.2 REQUISITOS DE ACCESO

Oracle implementa el control de acceso a los recursos en la nube a través del servicio OCI IAM, cumpliendo con el principio de mínimo privilegio al no asignar, por defecto, ninguna cuenta de usuario a ningún grupo.

Los requisitos de acceso se aplican atendiendo a la necesidad de proteger los recursos del sistema mediante mecanismos que impidan y dificulten su uso, salvo a aquellas entidades que disfruten de los derechos de acceso suficientes.

Los derechos de acceso permiten el uso de los recursos del sistema y deben ser controlados y gestionados por el responsable del recurso, atendiendo, siempre, a la política y normativa de seguridad de la organización, que debe, a su vez, atender con el principio del mínimo privilegio.

Oracle dispone, para la gestión de control de acceso, distintos tipos de recursos soportados en cada servicio disponibles en el menú de OCI Observación y gestión. Cada tipo de recurso soporta, a su vez, variables generales que agregan condiciones a una política específica asignada a los usuarios en particular o grupos.

A continuación, se detallarán los requisitos de acceso de los servicios de monitorización y gestión de OCI:

a) **Application Performance Monitoring (APM):** Para usar el servicio APM se debe configurar una serie de requisitos para permitir la comunicación entre los distintos componentes y servicios cumpliendo, a su vez, con los requisitos de acceso establecidos por el ENS:

   i. Cree un compartimento para organizar y aislar los recursos facilitando la gestión y el acceso seguro.

   ii. Cree usuarios y grupos de usuarios mediante el servicio de Identity and Access Management (IAM) de OCI siguiendo las directrices establecidas por el ENS.

   iii. Establezca políticas sobre el recurso apm-domains, para determinar quién puede realizar qué funciones sobre los recursos.

   iv. Asigne permisos del servicio de supervisión de OCI para acceder a las métricas de APM en el explorador de métricas y generar alarmas.

   v. Conceda permisos de notificaciones de OCI para la creación de alarmas.

   vi. Otorgue permisos del panel de control de gestión para crear paneles de control personalizados en APM.

b) **Logging (Registro):** Los logs contienen información de diagnóstico crítica que indica el rendimiento y el acceso a los recursos. Para ello, se debe usar grupos de logs para organizar los logs. A través de los grupos de logs, se puede limitar el acceso a los mismos mediante la configuración de políticas de IAM.

Para configurar los requisitos de acceso establecidos por el ENS se debe configurar los siguientes apartados:

i. Cree un compartimento, cuentas de usuario y grupos de usuarios.

ii. Configure permisos de tipo manage en el grupo de logs (log-group) y acceso al recurso para la activación de logs de servicio en un recurso.

c) **Logging Analytics (Análisis de registro):** Al ser un servicio regional, se debe configurar en el tenant de OCI la región que se desea utilizar. Una vez seleccionada la región, para la activación del servicio y el cumplimiento de los requisitos de acceso establecidos por el ENS, se debe configurar lo siguiente:

i. Activación del acceso de Logging Analytics a su familia de funciones. Para ello, debe crearse una política de IAM de nivel de servicio.

ii. Uso de compartimentos para la creación de recursos como entidades o grupos de logs.

iii. Creación de grupos de usuarios y configuración del acceso que definan las políticas de control de acceso establecido por el ENS.

iv. Posibilidad de configurar políticas de acceso a través de las familias de funciones: loganalytics-features-family y loganalytics-resources-family.

d) **Monitoring (Supervisión):** Utiliza métricas para supervisar recursos y alarmas para notificar que dichas métricas han alcanzado los disparadores especificados por las alarmas. Para tener un control de acceso riguroso y que cumple con los requisitos establecidos por el ENS, se debe configurar los siguientes apartados:

i. Configuración de compartimentos, grupos de usuarios, grupos dinámicos y políticas que controlen el acceso a los servicios y recursos (metrics y alarms) de Supervisión, a través del servicio OCI IAM.

e) **Notifications (Notificaciones):** Usa los canales de comunicación para la publicación de mensajes mediante temas y suscripciones. Para una configuración segura y un control de acceso basado en las directrices del ENS, se debe configurar lo siguiente:

i. Configuración de compartimentos, grupos de usuarios y políticas que controlen el acceso al servicio a través de políticas IAM sobre los recursos ons-family, ons-topics y ons-subscriptions.

ii. Gestionar temas, suscripciones y publicación de mensajes mediante políticas IAM.

f) **Servicio Events (eventos):** Para la gestión automatizada basada en los cambios de estado de los recursos del tenant, se debe configurar los siguientes elementos del servicio Events (eventos):

i. Cree una política de IAM para Events (eventos).

ii. Cree un tema y una suscripción para usarlo como una acción y gestione las políticas de acceso para trabajar con reglas en un compartimento.

g) **Management Agent (Agente de gestión):** Los siguientes elementos de configuración son relevantes para configurar y trabajar con el componente de agente de gestión en OCI:

   i. Cree un compartimento, cuentas de usuarios y grupos de usuarios.

   ii. Cree políticas para el grupo de usuarios y gestión de los recursos OCI del agente de gestión: management-agents y management-agent-install-keys.

   iii. Cree un grupo dinámico para todos los agentes de gestión.

   iv. Cree y asigne políticas al grupo dinámico para la comunicación del agente de gestión con el servicio de agente de gestión.

h) **Java Management Service (Servicio de gestión de Java):** Se debe configurar los siguientes elementos para usar el servicio JMS:

   i. Cree un compartimento para los recursos de JMS, cuentas de usuario y grupos de usuarios.

   ii. Configure un nuevo espacio de nombres de etiqueta y cree una nueva clave de etiqueta.

   iii. Administre políticas de acceso y gestión de flotas de JMS, agentes de gestión y espacios de nombres de etiquetas, métricas y claves de instalación de agentes.

   iv. Cree un grupo dinámico para todos los agentes y asigne políticas para permitir la comunicación de los agentes con el servicio JMS.

i) **Service Connector Hub:** Se debe configurar políticas sobre el recurso serviceconnectors para mostrar, crear, actualizar o suprimir conectores de servicio en el tenant.

2.1.1.3 SEGREGACIÓN DE FUNCIONES Y TAREAS

La segregación de funciones y tareas que establece el ENS se basa en definir y aplicar un control de acceso de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas, evitando la posibilidad de abusar de los derechos de un usuario autorizado para cometer alguna acción ilícita.

Oracle dispone de un control de acceso basado en roles (RBAC) que puede gestionarse mediante el servicio de OCI IAM, proporcionando a los administradores el control necesario sobre el acceso de los usuarios a los recursos de monitorización y gestión y las acciones que puedan realizar sobre estos recursos.

2.1.1.4 PROCESO DE GESTIÓN DE DERECHOS DE ACCESO

El proceso de gestión de derechos de acceso a los servicios de monitorización y gestión de OCI deben ser limitados, atendiendo siempre a los principios marcados por el ENS como el mínimo privilegio, necesidad de conocer y capacidad de autorizar.

El principio de mínimo privilegio indica la necesidad de reducir al mínimo los privilegios de cada usuario para el cumplimiento de sus obligaciones. Además, debe existir la necesidad de conocer para la asignación de los privilegios, de manera que la información pueda quedar compartimentada y accesible solamente si existe dicha necesidad.

Por último, solamente el personal con capacidad de autorizar podrá conceder, alterar o anular la autorización de acceso a los recursos de monitorización y gestión desde el servicio de OCI IAM.

2.1.2 EXPLOTACIÓN

Se incluyen en este apartado, todas aquellas medidas designadas como parte de la explotación de los servicios. El ENS define, a través de ellas, una serie de procesos tanto para el control como para la gestión que deberán llevarse a cabo por parte de las entidades.

Las medidas atienden a diferentes tareas que deberán ser llevadas a la práctica por el departamento de informática.

2.1.2.1 MANTENIMIENTO

La medida establece una seguridad mínima que debe aplicarse de igual forma en todas las categorías del ENS.

En lo relativo a los servicios de monitorización y gestión de OCI, se debe hacer hincapié en los agentes de gestión, ya que son piezas fundamentales de software para el funcionamiento de dichos servicios, porque permite la comunicación interactiva de baja latencia entre OCI y cualquier otro destino. Además, son los encargados de la recopilación de datos y métricas de entidades, aplicaciones y hosts para el análisis basado en rendimiento.

Para el caso del servicio de gestión de Java, se puede crear flotas para gestionar un conjunto de instancias que comparten un enfoque de gestión común.

En el siguiente enlace, Oracle proporciona orientación y recomendaciones útiles para configurar una flota:

https://docs.oracle.com/es-ww/iaas/jms/doc/fleet-management.html

Para mantener el equipamiento lógico se aplicará lo siguiente:

a) Se atenderá a las especificaciones de los fabricantes en lo relativo a la instalación y mantenimiento de los agentes de gestión.

b) Se efectuará un seguimiento continuo de los anuncios de defectos.

Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la aplicación o no de la actualización.

Finalmente, se puede actualizar los agentes Java de APM a la versión más reciente disponible. El cambio de versión del agente Java de APM está soportado mediante el aprovisionamiento de una versión más reciente del archivo instalador del agente Java de APM. Para obtener más información relacionada con el cambio de versión de agente Java de APM, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/application-performance-monitoring/doc/apm-java-agent-upgrade.html

2.1.2.2 REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS

El ENS establece en esta medida que deben registrarse todas las actividades del usuario realizadas en el sistema, de manera que pueda guardarse la información correspondiente a los siguientes puntos:

a) El registro indicará quién realiza la actividad, cuándo ha sido realizada y sobre qué información se ha realizado dicha actividad.

b) Aquellas actividades realizadas por los usuarios, especialmente los operadores y administradores del sistema en el momento en que pueden acceder a la configuración y realizan acciones de mantenimiento en el sistema.

c) Deberán registrarse tanto las actividades realizadas con éxito como los intentos fracasados.

d) La determinación de las actividades y el nivel de detalle se determinarán en base al análisis de riesgos realizado sobre el sistema.

En la página Auditoría, dentro del recurso de Registro del menú de OCI Observación y gestión, se puede explorar los logs de auditoría. Los logs de auditoría también se pueden encontrar desde la página Buscar seleccionando en cada compartimento el grupo de logs /_Audit.

Para ver y buscar logs de auditoría se debe tener los permisos necesarios y relacionados con el recurso audit-events del servicio Audit de OCI. Para obtener más información relacionada con los permisos que se pueden aplicar sobre el recurso del servicio de Audit, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Identity/Reference/auditpolicyreference.htm

Por otro lado, es necesario disponer también de los permisos para realizar búsquedas de logs. Para obtener más información sobre los permisos necesarios para buscar logs, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Logging/Concepts/searchinglogs.htm

A continuación, se describen los pasos a realizar para filtrar los logs de auditoría:

a) Haga clic en el menú de navegación de OCI → Observación y gestión → Registro → Auditoría.

b) Aparecerá la lista de logs de auditoría en el compartimento actual. Seleccione un compartimento en el que se disponga de permisos para trabajar.

c) En usuario, agregue filtros de usuario y en recurso, añada filtros de recurso.

d) En tipos de solicitud de acción, se puede seleccionar una operación de acción o varias entre las siguientes:

   i. GET

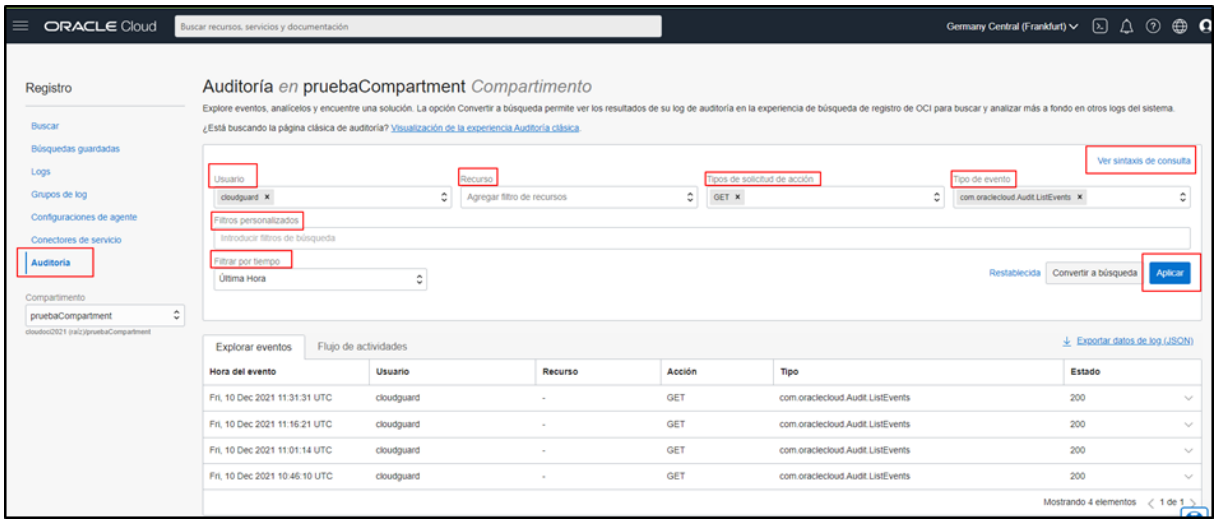
   ii. POST

   iii. PUT

   iv. PATCH

   v. DELETE

e) En tipo de evento, agregue filtros de evento.



Panel de Auditoría, dentro de Registro.

Ejemplo de un log de auditoría.

f) Se pueden configurar filtros personalizados.

g) En filtrar por tiempo, seleccione uno de los periodos de tiempo predefinidos y haga clic en Aplicar.

La opción Convertir a búsqueda permite ver los resultados de log de auditoría en la página Buscar para realizar análisis en profundidad en otros logs del sistema.

Cuadro de búsqueda de logs de auditoría.

En el separador Explorador de eventos, cada entrada de log se organiza en términos de Hora de evento, Usuario, Recurso, Tipo, Acción y Estado. Cada entrada muestra los datos de log en una vista de campo JSON, donde existe, también, la opción para exportar los datos de log.

Finalmente, el ENS indica activar los registros de actividad en los sistemas para la recolección de actividades mencionadas con anterioridad. Para ello, se hará uso de logs de auditoría registrados por el Servicio Audit de OCI. En consecuencia, se deberá revisar informalmente los registros de actividad para identificar patrones anormales y, también, se dispondrá de un sistema automático de recolección de registros y correlación de eventos en una consola de seguridad centralizada.

2.1.2.3 PROTECCIÓN DE LOS REGISTROS DE ACTIVIDAD

El ENS establece la implementación de mecanismos orientados a la protección de los registros de actividad. Estas medidas deben determinar el periodo de retención de los registros, asegundado la fecha y la hora, permitiendo el mantenimiento de los registros sin alteración ni eliminación por parte del personal no autorizado. Además, deben realizarse copias de seguridad ajustándose a los mismos requisitos.

OCI dispone del Servicio Audit (Auditoría) que registra automáticamente llamadas a todos los puntos finales soportados de la interfaz pública de programación de aplicaciones (API) como eventos de log.

Actualmente, todos los servicios soportan el registro mediante Audit. Los eventos de log registrados por el servicio Audit incluyen llamadas a la API realizadas por la consola de OCI, la interfaz de línea de comandos (CLI), Software Development Kits (SDK), sus propios clientes personalizados u otros servicios de OCI.

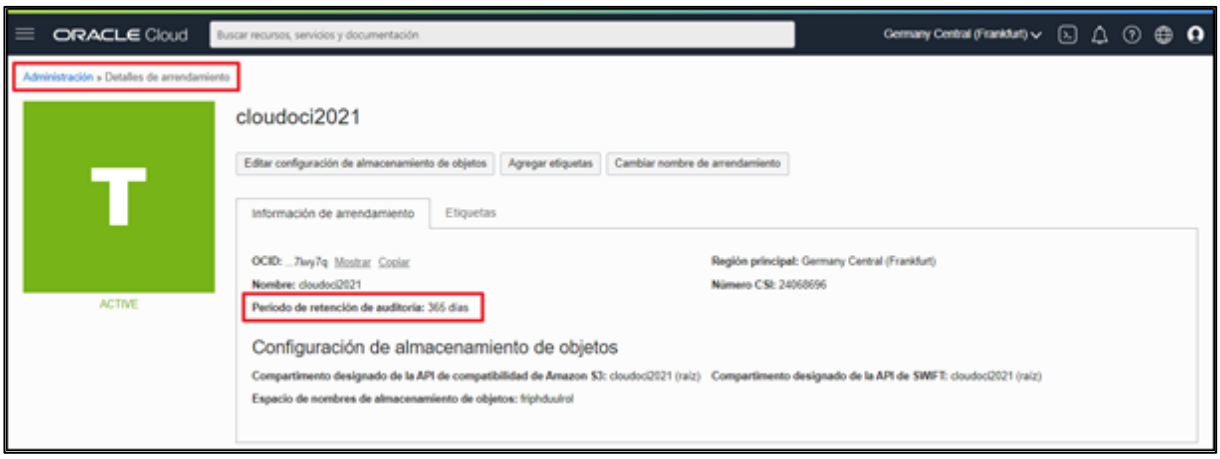
Puede ampliar la información acerca del servicio Audit de Oracle, en el siguiente enlace:

https://docs.oracle.com/es-ww/iaas/Content/Audit/Concepts/auditoverview.htm

Otro espacio donde localizar registros son los logs de registros, que se localizan en el menú OCI → Observación y gestión → Registro → Logs.

Hay que diferenciar entre distintos tipos de logs. Los logs más relevantes en seguridad son los Audit Logs. Esto afecta a los eventos de acceso y tienen una retención de 365 días. Estos logs no se pueden borrar, ni reducir los días de retención. Pero sí es posible mantener un número mayor de días realizando una exportación donde el tiempo puede ser los que desee el cliente. Esta petición se realiza a través del servicio My Oracle Support (MOS). Servicio ofrecido los 365 días al año, 24x7, con opción de configuración del idioma y sin coste adicional para el cliente al cual se puede acceder a través del siguiente enlace.

https://support.oracle.com/



Configuración por defecto de los logs de auditoría con una retención de 365 días en el tenant.

Puede ampliar la información de la exportación masiva de eventos de logs desde el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Audit/Concepts/bulkexport.htm

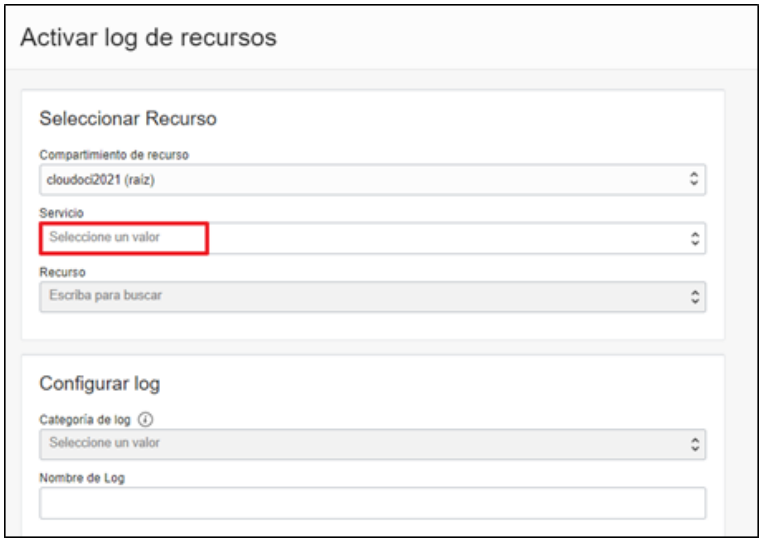
También puede trasladar los logs de auditoría a un bucket. Los buckets, tienen un ciclo de vida de gestión de almacenamiento con lo cual, un cliente puede almacenar esos eventos durante el tiempo que quiera, o purgar esos datos.

Menú de almacenamiento para la creación de un bucket para una mayor retención de logs.

Otro tipo de logs son los que producen los servicios gestionados de OCI. Estos tienen una retención máxima de 180 días y se pueden ajustar desde un mes hasta los seis meses. Luego se podrán archivar en un bucket y aumentar esta retención.

Detalle de la creación de un Log de eventos estableciendo un periodo de retención específico.

Al activar un log de servicio, éste puede localizarse en el servicio de Logging (registro), donde se centralizan todos los logs.



Detalle de la creación de un log de eventos de un servicio concreto.

Puede ampliar la información del servicio de Logs en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Logging/Concepts/service_logs.htm

2.1.3 MONITORIZACIÓN DEL SISTEMA

Según el ENS, los sistemas deben estar sujetos a medidas de monitorización de su actividad. El sistema de monitorización debe disponer de herramientas de detección o de prevención de intrusión, así como poder recopilar los datos necesarios atendiendo a la categoría del sistema para conocer el grado de implantación de las medidas de seguridad que apliquen, de las detalladas en el Anexo II y, en su caso, para proveer el informe anual requerido por el artículo 35 del RD 3/2010, de 8 de enero, por el que se regula el ENS.

2.1.3.1 SISTEMA DE MÉTRICAS

El ENS establece para la categoría alta la recopilación de los datos necesarios atendiendo a la categoría del sistema, para conocer el grado de implantación de las medidas de seguridad que apliquen y proveer el informe anual requerido. También es necesario la recopilación de los datos para valorar el sistema de incidentes, permitiendo conocer el número de incidentes, así como el tiempo en cerrar el 50% y el 90% de los mismos.

A su vez, se recopilarán datos para conocer la eficiencia del sistema de seguridad TIC, en cuanto a los recursos consumidos por horas y presupuesto.

Para ello, OCI dispone de varias herramientas para la recopilación de datos para el cumplimiento de la norma, permitiendo supervisar de forma activa y pasiva los recursos de la nube mediante las funciones de métricas, alarmas, registros y eventos.

Finalmente, es fundamental la gestión de los permisos para el control de los recursos en OCI, evitando el acceso indeseado a las herramientas de monitorización y gestión que detallan la actividad del sistema y su salud mediante la recopilación continua de datos y métricas.

2.1.3.1.1 RECOPILACIÓN DE MÉTRICAS Y GESTIÓN DE ALERTAS

a) **Monitoring (Supervisión):** OCI dispone del Servicio Monitoring para la recopilación de datos para el cumplimiento de la norma, el cual le permite supervisar de forma activa y pasiva los recursos en la nube mediante las funciones de métricas y alarmas.

El servicio Monitoring utiliza métricas para supervisar recursos y alarmas a fin de notificar en caso de que estas métricas alcancen los disparadores especificados por las alarmas.

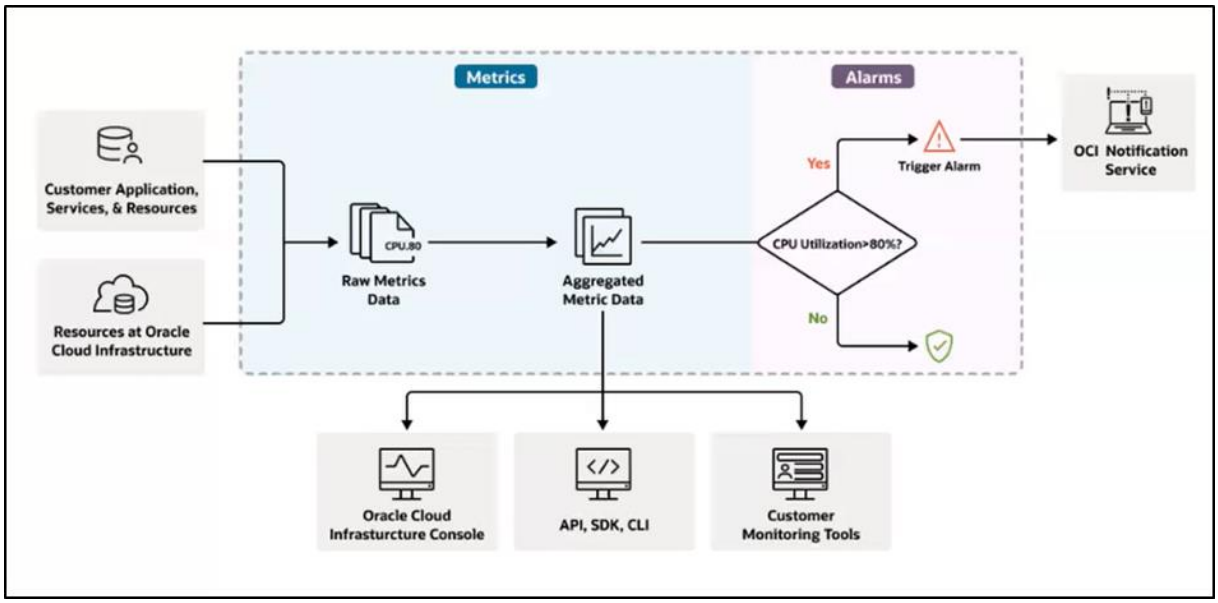


Imagen del esquema del funcionamiento de Monitoring.

Cuando se consulte una métrica, el servicio Monitoring devuelve datos agregados según los parámetros especificados. Se puede especificar un rango (por ejemplo, las últimas 24 horas), una estadística y un intervalo. La Consola muestra un gráfico de supervisión por métrica para los recursos seleccionados.

Los datos agregados en cada gráfico reflejan la estadística y el intervalo seleccionados. Las solicitudes de API pueden filtrar por dimensión y especifican una resolución. Las respuestas de API incluyen el nombre de la métrica junto con su compartimento de origen y el espacio de nombre de métrica. Además, se puede suministrar los datos agregados a una biblioteca de visualización o de gráficos.

Para obtener más información relacionada con la visualización de gráficos de métricas por defecto, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Monitoring/Tasks/viewingcharts.htm

Es posible acceder a los datos de métricas y alarmas mediante la Consola, la CLI y la API desde el propio recurso.

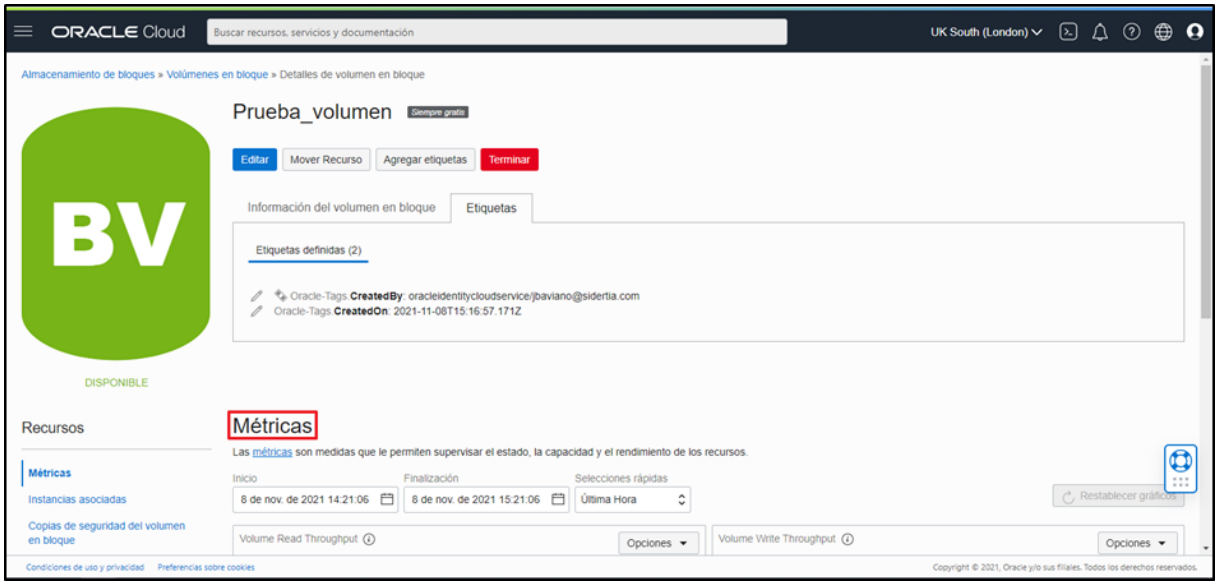


Imagen de ejemplo de la localización de métricas dentro de un recurso de almacenamiento.

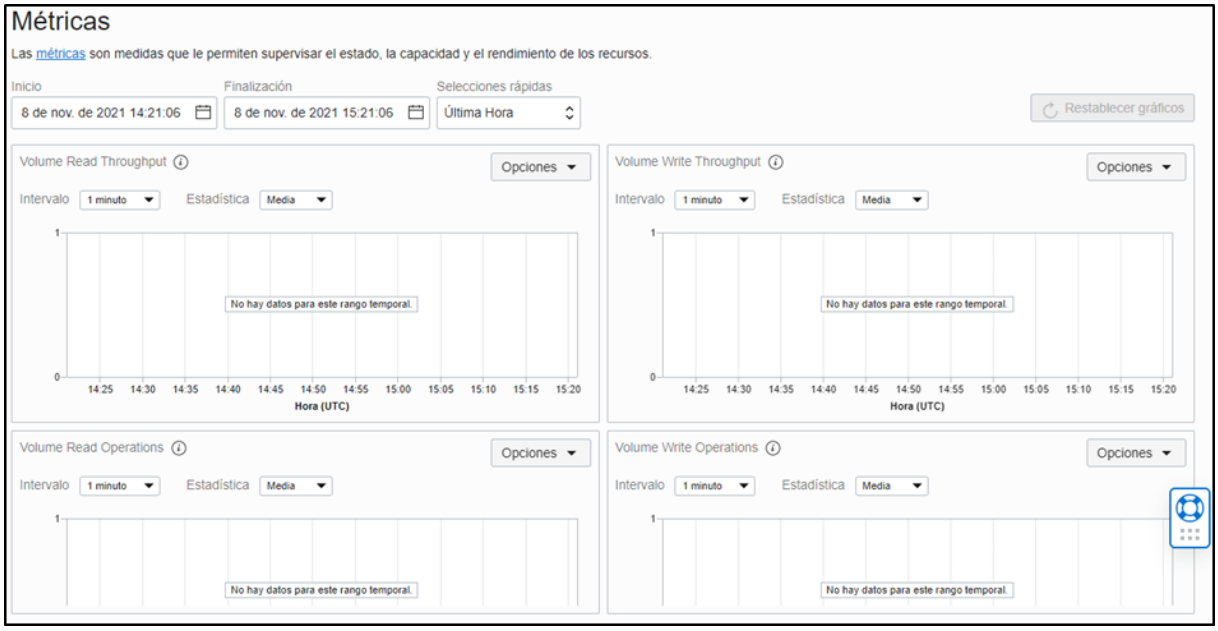


Imagen de la visión de las métricas mostradas por defecto de un recurso.

No obstante, desde la propia consola de gestión de Supervisión pueden recogerse las métricas de servicio, así como el explorador de métricas, estados y definiciones de alarma y comprobaciones del sistema.

Para ello, se debe navegar por el menú de OCI → Observación y gestión → Supervisión → Métricas de servicio.

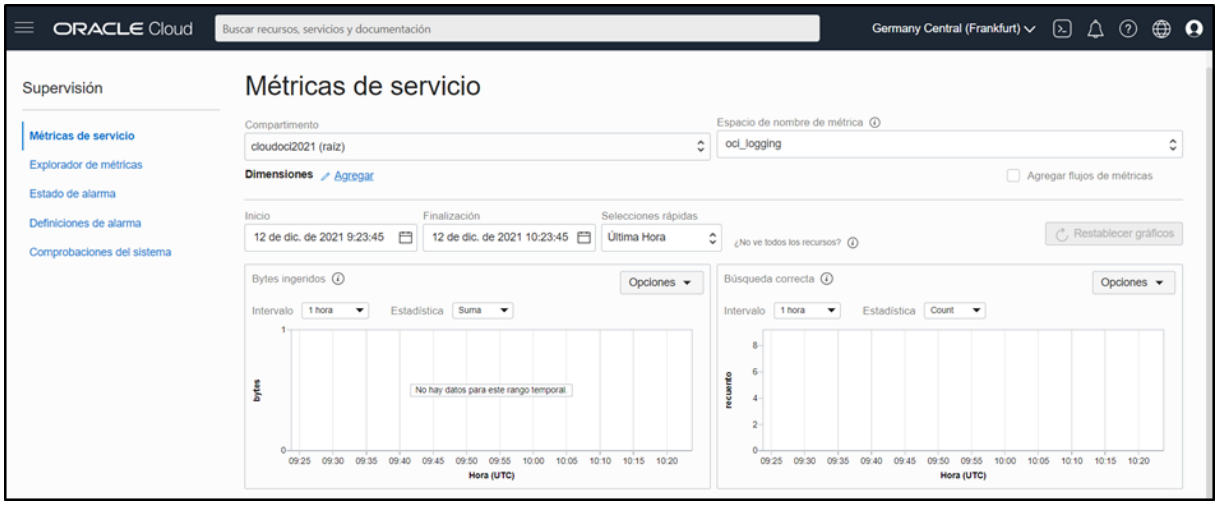


Imagen del Panel de control de Supervisión.

Se pueden consultar los servicios que pueden emitir métricas a Supervisión en el siguiente enlace a Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Monitoring/Concepts/monitoringoverview.htm#SupportedServices

Para obtener más información sobre la creación de consultas de métricas desde la consola o desde la API, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Monitoring/Tasks/buildingqueries.htm

Por otro lado, el servicio de Supervisión permite crear y asignar una prioridad a un conjunto de alarmas por cada métrica. La prioridad puede establecerse dentro de los siguientes parámetros:

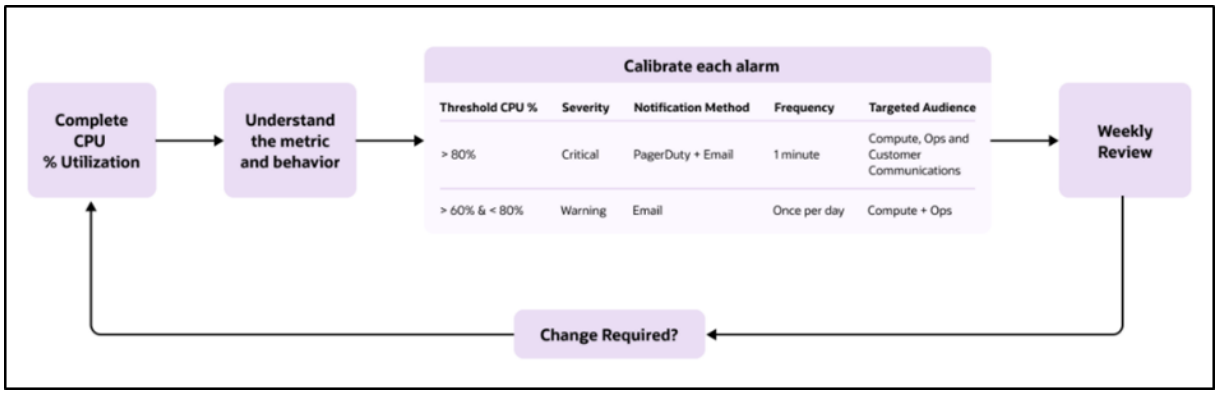
i. **En riesgo:** las métricas indican que el recurso está en riesgo de ser inoperable. Por ejemplo, para la métrica CpuUtilization está registrando un valor superior al 80% de CPU de una instancia concreta, disparando la alarma que notifica al equipo de operaciones para que puedan llevar a cabo la reparación.

ii. **No óptimo:** los valores de métricas indican que el recurso se encuentra en niveles no óptimos. Por ejemplo, cuando el umbral típico no óptimo para la métrica CpuUtilization oscila entre un 60 y un 80%. Si una instancia informática se encuentra dentro de este rango, la alarma configurada decide notificar al equipo de operaciones indicando la prioridad para la toma de decisiones.

iii. **El recurso está activo o caído:** los valores de métricas indican que el recurso no es accesible o no está operativo. Por ejemplo, cuando la métrica CpuUtilization está ausente durante más de cinco minutos. Una instancia que infrinja este umbral no es accesible o no funciona, por lo que la alarma se dispara para notificar a los responsables de la instancia informática.

Los valores de métricas dados acorde a los niveles de prioridad de las alarmas configuradas deben definirse mediante canales de notificación específicos para las alertas, seleccionando el intervalo correcto de la alarma para la métrica, y teniendo en cuenta la posibilidad de personalizar las alarmas.

La recomendación de seguridad, basada en las buenas prácticas de ajuste rutinario de las alarmas indica la necesidad de revisar las alarmas de forma periódica. La revisión periódica garantiza que la configuración sea óptima, porque calibra el umbral de detalles, la gravedad y notificación de cada alarma.



Flujo de ajuste rutinario en la configuración de las alarmas.

La configuración óptima de las alarmas aborda factores que deben ser considerados como la importancia del recurso, el comportamiento apropiado del recurso y el ruido de notificaciones aceptable.

Finalmente, para actualizar una alarma en modo básico o avanzado, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Monitoring/Tasks/managingalarms.htm

b) **Servicio Events (eventos):** El servicio de eventos permite habilitar la automatización basada en los cambios de estado de los recursos del tenant. En general, los servicios de OCI emiten eventos, que son mensajes estructurados que indican cambios en los recursos.

Por otro lado, las reglas incluyen un filtro definido que especifica los eventos producidos por los recursos en el tenant. El filtro es flexible, ya que se puede definir los filtros que coincidan solo con determinados eventos o bien basados en la forma en que se etiquetan los recursos o en la presencia de valores específicos del propio evento.

Las reglas deben especificar también una acción que se disparará cuando el filtro encuentre un evento coincidente. Las acciones son respuestas definidas para las coincidencias de eventos. Sin embargo, solamente se pueden crear acciones para los servicios de Notifications (Notificaciones), Streaming y Functions (Funciones), siendo este último el que más posibilidades ofrece para originar acciones, debido a que una función es un código diseñado a medida y opera según la necesidad en la que haya sido codificado.

Para crear una regla es necesario disponer de los permisos necesarios para su gestión, además de especificar un tema en el servicio de Notificaciones para la entrega de eventos coincidentes.

Desde la consola, se va a crear una regla de ejemplo con un patrón que coincida con los eventos de creación de buckets emitidos por Object Storage:

i. Abra el menú de navegación de OCI → Observación y Gestión → Servicio de eventos → Reglas.

ii. Seleccione el compartimento con permiso para trabajar y, a continuación, haga clic en Crear regla.

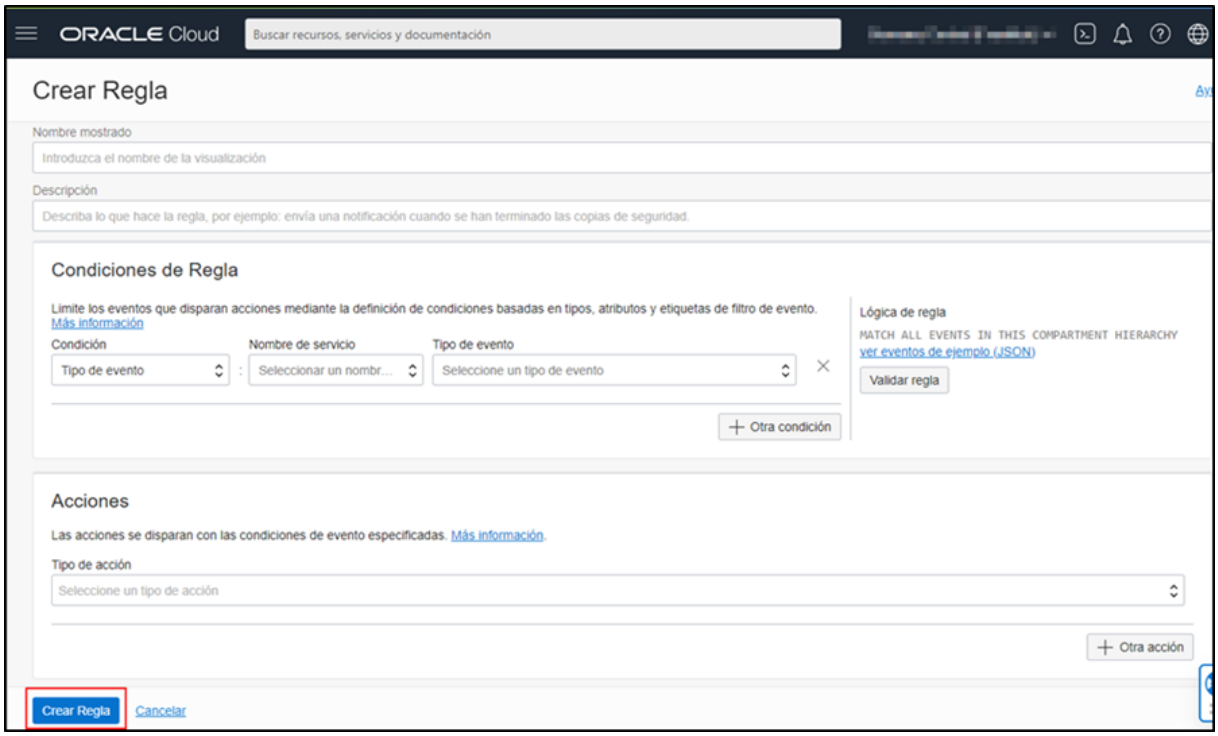
iii. Introduzca el nombre y una descripción que evite en todo momento información confidencial.

iv. En Coincidencia de evento, seleccione Tipo de evento.

v. En Nombre de servicio, seleccione Object Storage.

vi. En Tipo de evento, seleccione Object Storage - Crear bucket.

vii. En Acciones, se debe especificar las acciones que se dispararán cuando el filtro encuentre una coincidencia.



Cuadro de diálogo para crear una regla.

viii. Haga clic en Crear regla.

ix. A continuación, debe crear un bucket y conectarse a la cuenta de correo electrónico especificada en el procedimiento anterior para recibir la notificación sobre el bucket que se está creando.

Nota: Se recibirá notificaciones cada vez que se cree un bucket en el compartimento, hasta que se desactive la regla.

Para obtener más información relacionada con Eventos coincidentes con filtros, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Events/Concepts/filterevents.htm

Para obtener más información relacionada con la Gestión de reglas para el servicio de eventos, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Events/Task/managingrules.htm

c) **Notifications (Notificaciones):** El servicio de Notificaciones difunde mensajes a componentes distribuidos a través de un patrón de publicación - suscripción, lo que proporciona mensajes seguros y altamente fiables para aplicaciones externas y aplicaciones alojadas en OCI.

Para utilizar el servicio de Notificaciones es necesario crear un tema y una suscripción para la publicación de los mensajes. Cuando se publica un mensaje en un tema, el servicio de Notificaciones envía este mensaje a todas las suscripciones del tema.

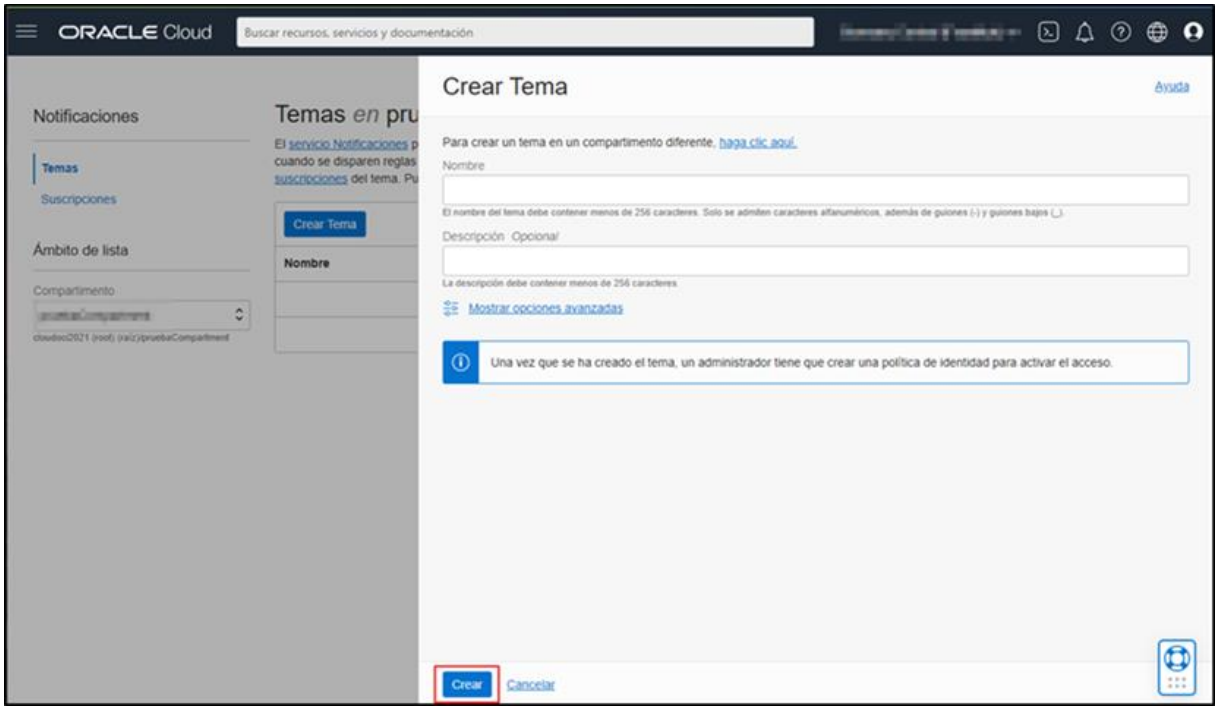
A continuación, se detallan los pasos a seguir para la creación de un tema desde la consola:

i. Navegue por el menú de OCI → Servicios para desarrolladores → Integración de Aplicación → Notificaciones.

ii. Haga clic en Crear tema para su configuración:

iii. **Nombre:** Especifique un nombre único en el tenant. La validación es sensible a mayúsculas/minúsculas. No se debe introducir información confidencial.

iv. **Descripción:** Introduzca una descripción para el tema sin añadir información confidencial. La opción de descripción es opcional.



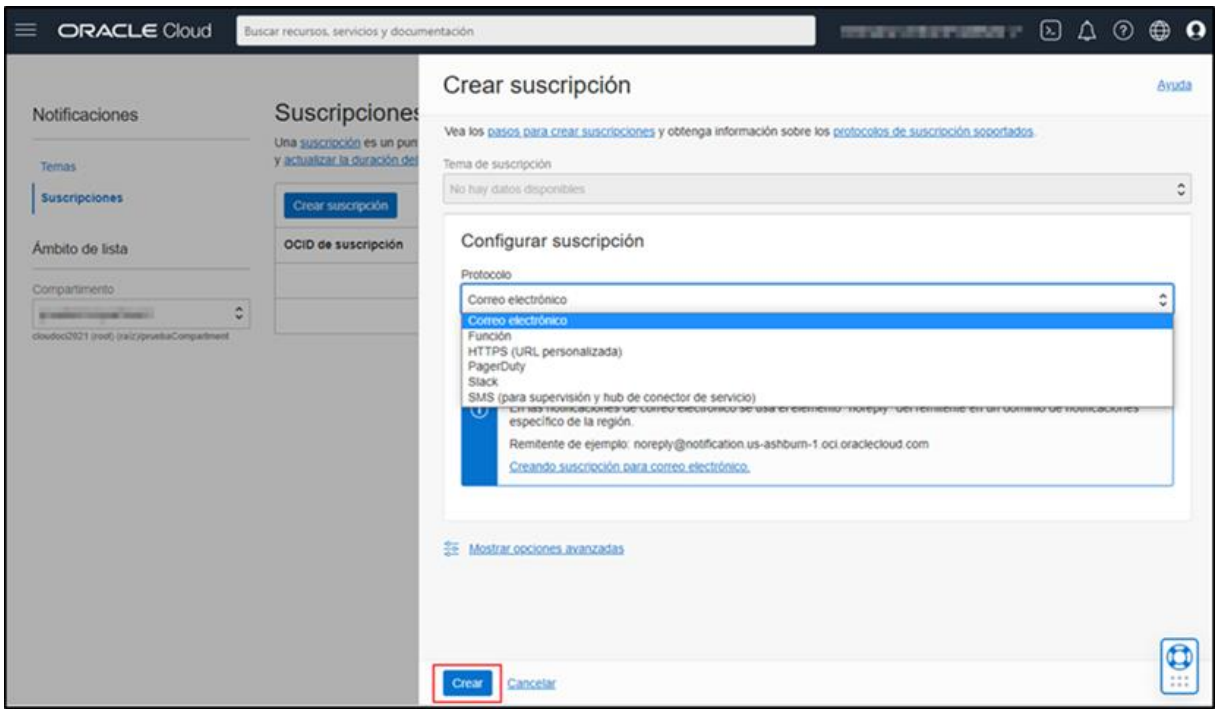
Cuadro de diálogo para crear un tema.

Por otro lado, es necesario crear una suscripción en el servicio de Notificaciones para la difusión de mensajes a los componentes distribuidos.

v. Abra el menú de navegación de OCI → Servicios para desarrolladores → Integración de Aplicación → Notificaciones.

vi. Haga clic en el nombre del tema al que se desea agregar la suscripción.

vii. En la página de detalles del tema, haga clic en Crear una suscripción.



Cuadro de diálogo para crear una suscripción.

viii. En cuadro de diálogo Crear suscripción, se debe escoger el protocolo que se necesite entre suscripción de correo electrónico, suscripción de función, suscripción HTTPS (URL personalizada), suscripción de PagerDuty, suscripción de Slack y suscripción de SMS.

ix. Haga clic en Crear.

Las suscripciones que utilicen protocolos que necesitan confirmación, como el correo electrónico, permanecerán en estado “Pendiente” hasta que se reciba la confirmación.

Nota: Las nuevas suscripciones deben crearse en el mismo compartimento que el tema. Sin embargo, es posible moverlas a diferentes compartimentos una vez estén creadas.

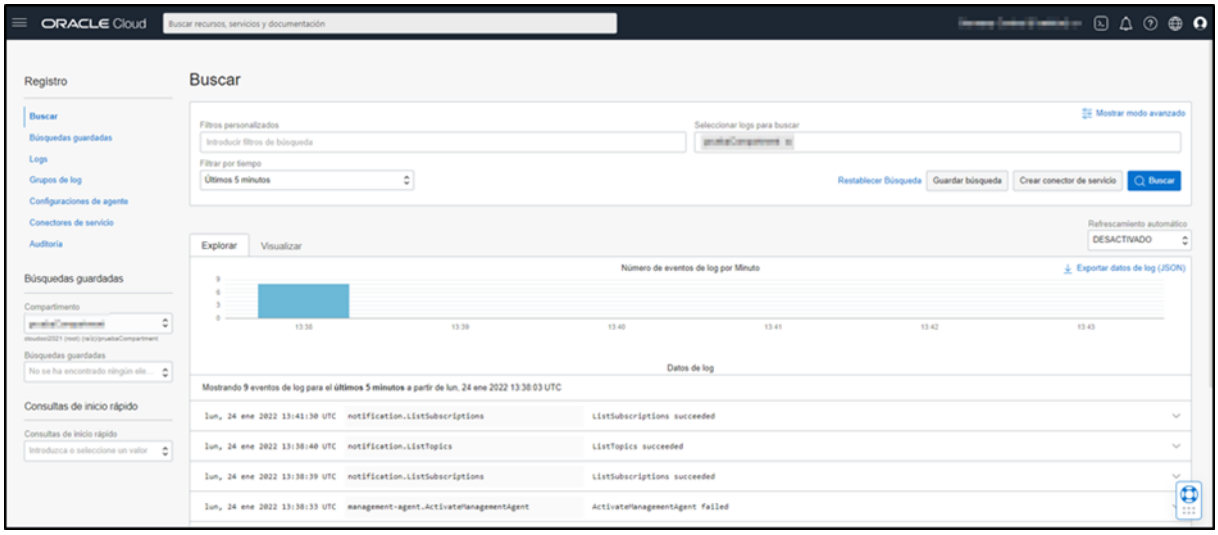
Para obtener más información relacionada con la configuración de los distintos protocolos de suscripción, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Notification/Tasks/managingtopicsandsubscriptions.htm

d) **Logging (Registro):** El servicio de registro de OCI es un panel único, altamente escalable y totalmente gestionado para todos los logs del tenant. El servicio de registro proporciona acceso a los logs desde los recursos de OCI. Estos logs incluyen información de diagnóstico crítica que describe el rendimiento de los recursos y cómo se está accediendo a ellos.

Cuando se activa un log, el log debe ser agregado a un grupo de logs creado previamente. Los grupos de logs son contenedores lógicos de logs que sirven para organizar y optimizar la gestión de logs mediante la aplicación de IAM o la agrupación de logs para el análisis.

Los logs se indexan en el sistema y se pueden buscar mediante la consola, la API y la CLI. Se puede ver y buscar logs abriendo el menú de navegación de OCI → Observación y gestión → Registro → Buscar.



Panel de búsqueda de registros.

Al buscar logs, éstos pueden ser correlacionados por varios logs simultáneamente. Por ejemplo, se puede ver los resultados de varios logs o grupos de logs o incluso un compartimento completo con una consulta.

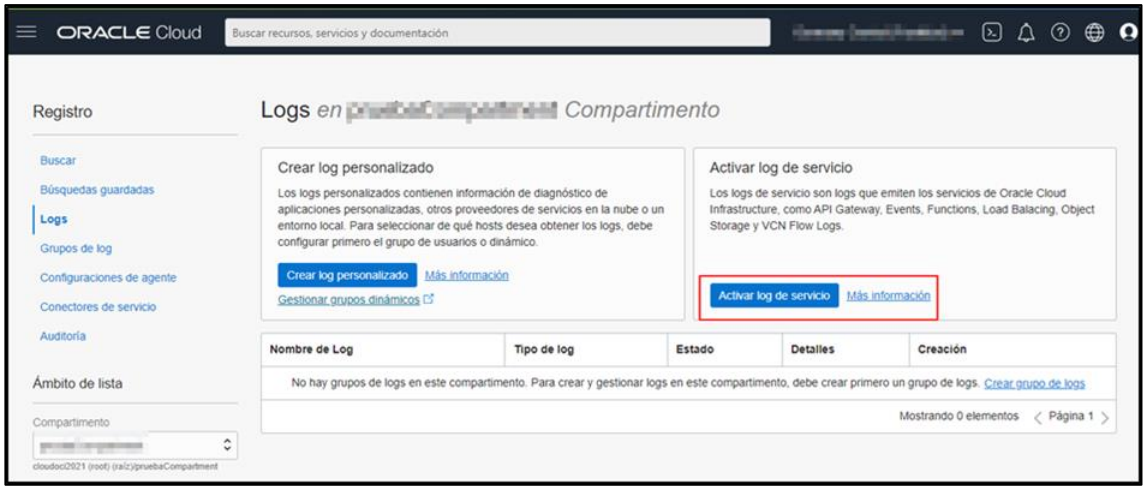
Después de activar un log, las entradas de log comienzan a aparecer en la página de detalles del log. Los logs pueden activarse directamente en el propio recurso o bien en la página central de logs del menú de navegación de OCI Observación y gestión.

Al activar un log en un recurso específico, se debe especificar la categoría. Los diferentes recursos pueden tener diferentes categorías. Por ejemplo, las reglas del servicio Events (Eventos) tienen el recurso Logs disponible para la gestión de registros. La regla puede emitir un log según la categoría incluida en el campo Categoría correspondiente.

A continuación, se describe la activación del registro en la página Logs:

i. Navegue por el menú de navegación de OCI → Observación y gestión → Registro → Logs.

ii. En la página de Logs, haga clic en Activar log de servicio. Aparecerá el panel Activar log de recursos.



Panel de logs.

iii. Seleccione un compartimento en el que tenga permiso para trabajar.

iv. Elija un servicio en la lista Servicio.

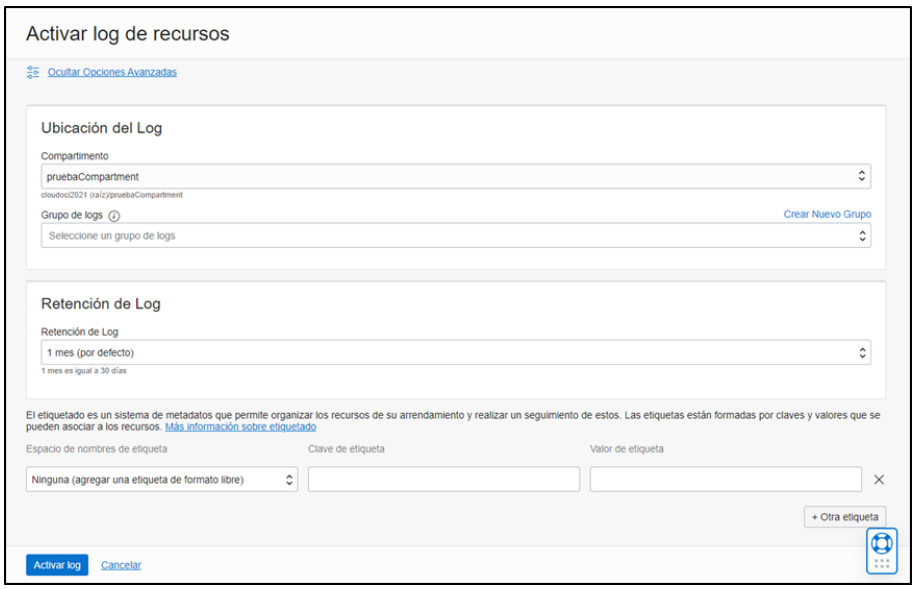
v. Escoja un recurso, añadiendo el servicio, compartimento y el recurso.

vi. Configure la categoría del log y el nombre de log.

vii. En opciones avanzadas, especifique la ubicación del log: seleccionar compartimento y grupo de logs.

viii. En Retención de log, seleccione un valor temporal de la lista.

ix. Aplique cualquier información relacionada con el etiquetado en los campos Espacio de nombres de etiqueta, Clave de etiqueta y Valor, y Haga clic en Activar log.



Opciones avanzadas para Activar log de recursos.

Para obtener más información relacionada con los logs de servicio admitidos, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Logging/Concepts/service_logs.htm

Para el uso de la Interfaz de Línea de Comandos (CLI) en la gestión del servicio de Registro, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Logging/Task/using_the_cli_loggroups.htm

Los Logs de auditoría se describen en el apartado 2.1.2.2 REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS.

2.1.3.1.2 ANÁLISIS DE MÉTRICAS

a) **Application Performance Monitoring (APM):** Para obtener una vista completa del rendimiento y la disponibilidad de las aplicaciones y de la experiencia del usuario final en tiempo real. El servicio de APM necesita un dominio APM y la configuración de los orígenes de datos para la recopilación de los datos necesarios.

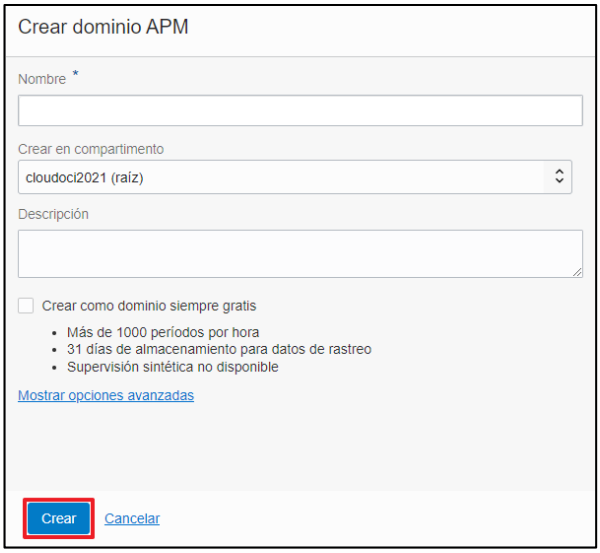
Un dominio APM es un recurso de OCI que contiene los sistemas que está supervisando APM. Para crear un dominio APM en un compartimento se necesita el rol de administrador de la cuenta de Oracle Cloud u otorgar el permiso “manage apm-domains” en el compartimento de destino a un usuario, basado en un estricto control de gestión de acceso mediante políticas definidas en el servicio OCI IAM.

A continuación, se describen los pasos para crear un dominio de APM en la consola de OCI:

i. Abra el menú de navegación de OCI → Observación y gestión → Application Performance Monitoring → Administración.

ii. En la página de Administración, en el panel de la izquierda, seleccione el compartimento en el que desea crear el dominio de APM.

iii. En la página Dominios de APM, haga clic en Crear dominio APM e introduzca los detalles necesarios en el cuadro de diálogo.



Cuadro de diálogo para la creación de un dominio APM.

iv. Haga clic en Crear.

Una vez creado el dominio de APM, se enviará la solicitud de creación de dominio de APM y comenzará un flujo de trabajo asíncrono para cumplir dicha solicitud. El dominio de APM se mostrará en la página Dominios de APM e inicialmente tendrá el estado de Creación. Una vez se crea el dominio de APM, el estado cambia a Activo.

Para crear, actualizar o eliminar un dominio APM a través de la herramienta de comandos CLI, consulte el siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en-us/iaas/tools/oci-cli/3.3.3/oci_cli_docs/cmdref/apm-control-plane.html

En segundo lugar, se debe instalar y configurar varios orígenes de datos (agentes y rastreadores) para el servicio APM. Los orígenes de datos de APM recopilan datos y los cargan en un dominio de APM. Los datos recopilados por los orígenes de datos se denominan observaciones, y para cargar observaciones en APM se necesita la información generada cuando se crea un dominio de APM, como el punto final de carga de datos, las claves de datos públicos y las claves privadas.

Para obtener más información sobre los orígenes de datos disponibles en APM, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/application-performance-monitoring/doc/application-performance-monitoring-data-sources.html

Para obtener más información sobre cómo instalar y configurar varios orígenes de datos de APM, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/application-performance-monitoring/doc/configure-application-performance-monitoring-data-sources.html

b) **Logging Analytics (Análisis de registro):** Es una solución en la nube de OCI que permite indexar, enriquecer, agregar, buscar, analizar, correlacionar, visualizar y supervisar todos los datos de log de sus aplicaciones e infraestructura del sistema en la nube o en las ubicaciones locales.

A continuación, se detallará el flujo de trabajo típico para la configuración y uso del servicio de Análisis de registro:

i. Identificar las entidades cuyos logs se deben recopilar.

ii. Determinar el método de recopilación de logs por ubicación de logs. Para obtener más información, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/logging-analytics/doc/ingest-logs.html

iii. Determinar el método de recopilación de logs por objetivo de la recopilación, bien instalando el agente de gestión en el host para la recopilación continua de logs, o bien cargar los logs en bloque para procesarlos y analizarlos usando la carga bajo demanda.

iv. Configurar el tenant para el uso de OCI Logging Analytics mediante las tareas de configuración previas que puede consultar en el apartado 2.1.1.2 REQUISITOS DE ACCESO.

v. Crear recursos de OCI Logging Analytics como grupos de logs, entidades, orígenes y analizadores según el uso final y el método de recopilación.

   Para obtener más información sobre la creación de una entidad y la asignación de un host a una entidad, consulte el siguiente enlace de Oracle:

   https://docs.oracle.com/es-ww/iaas/logging-analytics/doc/create-logging-analytics-resources.html

   Para obtener más información sobre la creación de un analizador, consulte el enlace:

   https://docs.oracle.com/es-ww/iaas/logging-analytics/doc/create-parser.html

vi. Realizar la recopilación de logs. Si se ha escogido el método de Management Agent para la recopilación de los datos de log, se deben consultar los mensajes de advertencia generados durante la recopilación de logs, para diagnosticar y solucionar problemas relacionados con los orígenes o las entidades.

   Para obtener más información relacionada con la visualización de advertencias de recopilación del agente, consulte el siguiente enlace de Oracle:

   https://docs.oracle.com/es-ww/iaas/logging-analytics/doc/administer-other-actions.html

vii. Seleccionar los gráficos y controles disponibles en el panel de visualización según los parámetros que se configure.

   Para obtener más información sobre la selección del tipo de visualización, consulte el siguiente enlace de Oracle:

   https://docs.oracle.com/es-ww/iaas/logging-analytics/doc/select-visualization-type.html

   Para obtener más información sobre la visualización de datos mediante gráficos y controles, consulte el siguiente enlace de Oracle:

   https://docs.oracle.com/es-ww/iaas/logging-analytics/doc/visualize-data-using-charts-and-controls.html

viii. Buscar logs y aumentar el detalle en las entradas de log específicas para resolver problemas rápidamente, usando la consola de Logging Analytics.

   Para realizar una búsqueda avanzada, consulte el siguiente enlace de Oracle:

   https://docs.oracle.com/es-ww/iaas/logging-analytics/doc/perform-advanced-search.html

   Para realizar una búsqueda avanzada mediante comandos, consulte el siguiente enlace:

   https://docs.oracle.com/es-ww/iaas/logging-analytics/doc/command-reference.html

   Para guardar las búsquedas realizadas mediante la consola de OCI Logging Analyticis, consulte el siguiente enlace de Oracle:

   https://docs.oracle.com/es-ww/iaas/logging-analytics/doc/and-share-log-searches.html

Para crear paneles de control personalizados consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/logging-analytics/doc/create-dashboards.html

2.2 MEDIDAS DE PROTECCIÓN

Este grupo de medidas cubre el espectro de aplicación de mecanismos más amplios en cuanto a dimensión. No obstante, debe tenerse en consideración que incluye una gran variedad de las mismas y que son aplicables desde las más puramente procedimentales, a las puramente físicas o a las de aplicación técnica.

Solo éstas últimas se tendrán en consideración para su implementación en la presente guía y de ellas solo un número limitado es de aplicación sobre las funcionalidades de la nube.

Se considera, en este sentido, que la organización ha dispuesto todos aquellos mecanismos de control físico necesarios, con objeto de evitar el acceso a la nube existentes por parte de personal no autorizado.

2.2.1 PROTECCIÓN DE LA INFORMACIÓN

Este conjunto de medidas trata todo lo relacionado con la protección de la información, desde lo dispuesto por las diferentes leyes nacionales y de la Unión Europea acerca de los datos personales, así como las distintas dimensiones que alcanzan cada uno de los aspectos relacionados con la información, su clasificación, accesos, responsables, tratamiento, almacenamiento, limpieza o destrucción, cuando ésta ya no sea necesaria.

Siendo uno de los activos más valiosos para cualquier organización, la información debe protegerse para garantizar la confidencialidad, disponibilidad e integridad de los datos. Para ello, la información debe ser clasificada e identificada para la aplicación de las medidas necesarias y adecuadas para su preservación. Sin embargo, la mayoría de estas medidas presentan un carácter más organizativo y procedimental, aunque también existen medidas de carácter técnico para permitir la comprobación de dimensiones como la autenticidad de la procedencia y la integridad de la información.

2.2.1.1 DATOS DE CARÁCTER PERSONAL

La aplicación técnica de esta medida se encuentra en el agente de explorador de APM, que registra la interacción del usuario con sitios web y envía métricas de explorador y de supervisión de usuario real a Application Performance Monitoring (APM). El agente identifica la degradación del rendimiento observando de cerca varios aspectos de una aplicación, como las cargas de páginas, el índice de rendimiento de la página/aplicación (Apdex), los errores de script y las llamadas AJAX.

El agente de explorador de APM permite cargar datos y supervisar la experiencia de un usuario con la aplicación sin utilizar un agente de servidor Java de APM. Por este motivo, se debe ocultar la información de identificación personal en la configuración del agente de explorador de APM, mediante un juego de reglas explícitas que evitan mostrar información de identificación personal (PII) en los datos.

No obstante, las reglas de Application Performance Monitoring (APM) por defecto ocultan la información de identificación personal en las URL mediante el reconocimiento de valores monetarios, números de cuenta bancaria y fechas. Sin embargo, las reglas por defecto solo capturan información de identificación personal obvia y no son exhaustivas.

Por lo tanto, se debe evaluar las reglas por defecto y configurar más reglas adicionales que garanticen la confidencialidad y privacidad de los datos personales en la generación de informes del entorno.

Finalmente, para obtener más información relacionada con la ocultación de información de identificación personal, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/application-performance-monitoring/doc/hide-personally-identifiable-information-pii.html

2.2.1.2 CIFRADO

El cifrado de información se determina su dimensión en esta categoría alta del ENS. La información debe cifrarse con un alto nivel de confidencialidad durante su almacenamiento, así como durante su transmisión.

Para el uso de criptografía de las comunicaciones, se estará en lo dispuesto a la norma [mp.com.2] Protección de la confidencialidad.

Por un lado, el cifrado en tránsito proporciona una manera de proteger los datos entre instancias, sistemas de archivos montados mediante el cifrado TLS v.1.2 y logs. Junto con otros métodos de seguridad como Vault (KMS) y el cifrado estático de File Storage.

Por otro lado, los logs de OCI se cifran según los siguientes elementos:

a) Los logs se cifran en ejecución, mientras están en proceso de ser recopilados en OCI Logging.

b) Una vez que los logs se encuentran en el sistema, éstos son cifrados a nivel de disco para entornos comerciales.

c) Los logs también se cifran cuando son archivados y mientras están en almacenamiento.

3. GLOSARIO

A continuación de describen una serie de términos, acrónimos y abreviaturas en materia de seguridad utilizados en esta guía.

Término	Definición
AJAX	Asynchronous JavaScript And XML (Javascript Asíncrono y XML).
Apdex	Application Performance Index (Índice de Rendimiento de Aplicaciones).
API	Application Programming Interfaces (Interfaz de Programación de Aplicaciones).
APM	Application Performance Monitoring (Supervisión del Rendimiento de la Aplicación).
Bucket	Cubo o almacén de datos ilimitado, de alto rendimiento, duradero y seguro.
C@C	Oracle Cloud at Customer (Nube de Oracle en el Cliente).
CCN	Centro Criptológico Nacional.
CLI	Command Line Interface (Interfaz de Línea de Comandos).
CNCF	Cloud Native Computing Foundation (Fundación de Computación Nativa en la Nube).
CPU	Central Processing Unit (Unidad de Procesamiento Central).
CRUD	Create, Read, Update and Delete (Crear, Leer, Actualizar y Eliminar).
DevOps	Development and Operations (Desarrollo y Operaciones).
ENS	Esquema Nacional de Seguridad.
Events	Servicio de eventos.
Functions	Servicio de funciones.
IA	Inteligencia artificial.
IaaS	Infrastructure as a Service (Infraestructura como Servicio).
IaC	Infrastructure as Code (Infraestructura como Código).
IoT	Internet of Things (Internet de las Cosas).
Java Management	Agente de Java.
JMS	Java Message Service (Servicio de Mensajes Java).
JSON	JavaScript Object Notation (Notación de Objeto de JavaScript).
KMS	Key Management Service (Servicio de Gestión de Llaves).
Logging	Servicio de registro de logs.
Logging Analytics	Servicio de análisis de registro.
Monitoring	Servicio para la supervisión.
MOS	My Oracle Support (Mi Soporte de Oracle).
Notifications	Servicio de notificaciones.
Object Storage	Servicio de almacenamiento de objetos.
OCI	Oracle Cloud Infrastructure (Infraestructura de Nube de Oracle).
OCI IAM	Identity and Access Management (Gestión de Identidad y Acceso).
OCID	Oracle Cloud Identifier (Identificador en la Nube de Oracle).
PaaS	Platform as a Service (Plataforma como Servicio).

Término	Definición
PII	Personally Identificable Information (Información Personal Identificable).
RBAC	Role Based Access Control (Control de Acceso Basado en Roles).
SDK	Software Development Kits (Kit de Desarrollo de Software).
SMS	Short Message Service (Servicio de Mensajes Cortos).
SQL	Structured Query Language (Lenguaje de Consulta Estructurado).
Tenant	Arrendamiento que contrata una organización y en el que Oracle presenta los servicios OCI contratados por el cliente.
TLS	Transport Layer Security (Seguridad de la capa de transporte).
VCN	Virtual Cloud Network (Red Virtual en la Nube).
VM	Virtual Machine (Máquina Virtual).

4. RESUMEN Y APLICACIÓN DE MEDIDAS

El siguiente cuadro, resume las medidas de seguridad a implementar para valorar el nivel de cumplimiento.

Control ENS	Medidas y Configuración	Estado	
OP	MARCO OPERACIONAL		
OP.ACC	CONTROL DE ACCESO		
op.acc.1	Identificación	Aplica	Cumple
	Se ha configurado el uso de cuentas de usuario de OCI IAM para la administración y gestión de los recursos de monitorización.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.acc.2	Requisitos de acceso	Aplica	Cumple
	Se han creado los grupos de seguridad necesarios en la organización para la gestión de los recursos de monitorización.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.acc.3	Segregación de funciones y tareas	Aplica	Cumple
	Se han creado grupos de seguridad basados en roles (RBAC) para los recursos de monitorización.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
op.acc.4	Proceso de gestión de derechos de acceso	Aplica	Cumple
	Se han gestionado los privilegios de acceso de los usuarios mediante la definición de políticas que cumplen los principios de mínimo privilegio, necesidad de conocer y capacidad para autorizar.	☐Si ☐No	☐Si ☐No
		Observaciones:	
OP.EXP	EXPLOTACIÓN		
op.exp.4	Mantenimiento	Aplica	Cumple
	Se está manteniendo el equipamiento lógico atendiendo a las especificaciones de los fabricantes en lo relativo a la instalación y mantenimiento de los agentes de gestión.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se está efectuando un seguimiento continuo de los anuncios de defectos.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se han actualizado los agentes Java de APM a la versión más reciente.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
op.exp.8	Registro de la actividad de los usuarios	Aplica	Cumple
	Se ha concedido permisos sobre el recurso audit-events.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se ha concedido permisos para realizar búsquedas de logs.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se está realizando un seguimiento de los eventos de auditoría.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se han revisado los registros de actividad buscando patrones anormales.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.exp.10	Protección de los registros de actividad	Aplica	Cumple
	El Servicio Audit de OCI implementa una retención de 365 días. Si necesita más retención, ha implementado el Servicio de Logs y creado un bucket para su almacenamiento.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
OP.MON	MONITORIZACIÓN DEL SISTEMA		
mp.eq.2	Sistema de métricas	Aplica	Cumple
	Se está supervisando de forma activa y pasiva los recursos del tenant a través de los servicios de monitorización de OCI como Supervisión.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se ha configurado la prioridad de las alarmas dependiendo de la importancia del recurso.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se han creado temas y suscripciones en el servicio de Notificaciones para la publicación de mensajes.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se ha configurado un dominio APM y los orígenes de datos para la gestión del servicio de Application Perfomance Monitoring.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se ha configurado el servicio de Logging Analytics (análisis de registro) para la supervisión de los datos de log.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
	Se han recopilado datos para valorar el sistema de gestión de incidentes.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se han recopilado datos de recursos consumidos para conocer la eficiencia del sistema de seguridad.	☐Si ☐No	☐Si ☐No
		Observaciones:	
MP	MEDIDAS DE PROTECCIÓN		
MP.INFO	PROTECCIÓN DE LA INFORMACIÓN		
mp.info.1	Datos de carácter personal	Aplica	Cumple
	Se han configurado reglas específicas en la configuración del agente de explorador APM para evitar mostrar la información de identificación personal en los datos.	☐Si ☐No	☐Si ☐No
		Observaciones:	
mp.info.1	Cifrado	Aplica	Cumple
	Se ha configurado el cifrado en tránsito en las instancias para la protección de los logs.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se ha configurado el cifrado estático en el almacenamiento de OCI.	☐Si ☐No	☐Si ☐No
		Observaciones:	

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL