centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 889D

Guía de Configuración segura para Oracle OCI Database - Instancias VM

MARZO 2022

Catálogo de Publicaciones de la Administración General del Estado
https://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
2022.04.28 15:48:29 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-140-8

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

LIMITACIÓN DE RESPONSABILIDAD
El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

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 ORACLE OCI DATABASE - INSTANCIAS VM 5
1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA 5
1.2 DEFINICIÓN DEL SERVICIO OCI DATABASE 5
1.3 SERVICIOS PARA OCI DATABASE 6
1.3.1 SISTEMA DE BASE DE DATOS DE MÁQUINA VIRTUAL 6
1.3.2 BASE DE DATOS AUTÓNOMA 9
1.3.3 EXADATA CLOUD SERVICES 10
CONFIGURACIÓN SEGURA PARA ORACLE OCI DATABASE - INSTANCIAS VM 13
1.4 MARCO OPERACIONAL 13
1.4.1 CONTROL DE ACCESO 13
1.4.1.1 IDENTIFICACIÓN 13
1.4.1.2 REQUISITOS DE ACCESO 14
1.4.1.3 SEGREGACIÓN DE FUNCIONES Y TAREAS 15
1.4.1.4 PROCESO DE GESTIÓN DE DERECHOS DE ACCESO 16
1.4.2 EXPLOTACIÓN 20
1.4.2.1 INVENTARIO DE ACTIVOS 20
1.4.2.2 MANTENIMIENTO 21
1.4.2.3 GESTIÓN DE INCIDENTES 24
1.4.2.4 REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS 27
1.4.2.5 REGISTRO DE LA GESTIÓN DE INCIDENTES 31
1.4.2.6 PROTECCIÓN DE CLAVES CRIPTOGRÁFICAS 31
1.4.3 MONITORIZACIÓN DEL SISTEMA 33
1.4.3.1 DETECCIÓN DE INTRUSIÓN 33
1.4.3.2 SISTEMA DE MÉTRICAS 35
1.5 MEDIDAS DE PROTECCIÓN 43
1.5.1 PROTECCIÓN DE LAS COMUNICACIONES 43
1.5.1.1 PERÍMETRO SEGURO 44
1.5.2 PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN 47
1.5.2.1 ETIQUETADO 48
1.5.3 PROTECCIÓN DE LA INFORMACIÓN 49
1.5.3.1 DATOS DE CARÁCTER PERSONAL 49
1.5.3.2 CALIFICACIÓN DE LA INFORMACIÓN 50
1.5.3.3 CIFRADO 52
1.5.3.4 COPIAS DE SEGURIDAD (BACKUP) 53
2. GLOSARIO 58
3. RESUMEN Y APLICACIÓN DE MEDIDAS 60

1. GUÍA DE CONFIGURACIÓN SEGURA PARA ORACLE OCI DATABASE - INSTANCIAS VM

1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA

Esta guía muestra el despliegue y configuración de los servicios de Base de datos de Oracle Cloud Infrastructure (OCI) para 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 OCI Database y las instancias de base de datos en máquinas virtuales 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 los 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 OCI DATABASE

Oracle Cloud Infrastructure (OCI), es la nube de última generación diseñada para ejecutar cualquier aplicación de forma más rápida y segura por menos.

El marco de adopción de la nube de OCI ayuda a las organizaciones a facilitar su transición a la nube y proporciona a los clientes una metodología para utilizar eficiencias incorporadas de Oracle Cloud, como los servicios de Bases de datos en sus distintas modalidades que se describen a continuación.

Dentro de los Servicios que ofrece OCI, esta guía se centrará en el servicio Database que ofrece soluciones de base de datos en la nube gestionadas conjuntamente y autónomas.

a) Autonomous Databases.

b) Sistemas gestionados conjuntamente:

   i. Sistemas de base de datos con hardware dedicado y máquinas virtuales.

   ii. Exadata Cloud Service.

   iii. Exadata Cloud at Customer.

Las bases de datos autónomas (Autonomous Databases) son entornos preconfigurados y completamente gestionados que son adecuados para cargas transaccionales y data warehouse.

Las soluciones gestionadas conjuntamente son sistemas con hardware dedicado, de máquina virtual y de sistemas Exadata que se pueden personalizar con los recursos y la configuración que satisfagan las necesidades del cliente.

Nota: Los sistemas de Hardware dedicado en Base de datos de Oracle se encuentran en desuso y se mencionan por el hecho de que las organizaciones aún puedan seguir utilizándolos, pero no se abordarán medidas específicas por ello.

Puede aprovisionar rápidamente una instancia de Autonomous Database o un sistema de base de datos gestionado por el usuario. Tendrá acceso completo a las funciones y operaciones disponibles en la base de datos, pero será Oracle quien posea y gestione la infraestructura.

También puede ampliar los servicios de bases de datos gestionadas en su propio centro de datos mediante Exadata Cloud at Customer (C@C), que aplica la potencia combinada de Exadata y OCI al mismo tiempo que permite cumplir los requisitos de residencia de datos de la organización. También dispone de la opción de Autonomous Cloud at Customer (C@C).

Aparte de estos servicios, Oracle dispone del Servicio MySQL Database, que es un servicio nativo de OCI totalmente gestionado, desarrollado y respaldado por el equipo de MySQL en Oracle. Oracle automatiza todas las tareas, como la copia de seguridad y la recuperación, la aplicación de parches de bases de datos y sistemas operativos, etc. El cliente es el único responsable de gestionar sus datos, diseños de esquema y políticas de acceso.

Una característica que ofrece Oracle en los servicios de Database es que se pueden mover sistemas de base de datos, recursos de Autonomous Database y recursos de Exadata C@C de un compartimento a otro. Cuando se mueve un recurso de base de datos a un nuevo compartimento, sus recursos dependientes se mueven con él. Después de mover el recurso al nuevo compartimento, las políticas inherentes se aplican inmediatamente y afectan al acceso a ese recurso y a sus recursos dependientes a través de la consola.

Nota: Para mover recursos entre compartimentos, los usuarios del recurso deben tener permisos de acceso suficientes en el compartimento al que se está moviendo ese recurso, así como en el compartimento actual.

De los servicios de Oracle Database antes mencionados, esta guía comprende las medidas de seguridad que deberán ser aplicadas en el Servicio de Base de datos en la nube de Oracle. Para el resto de los servicios de base de datos relacionados con Cloud at Customer, deberá aplicar la correspondiente Guía de seguridad: "CCN-STIC-889F Guía de Configuración segura para C@C Sistemas Exadata-Autonomous DB".

1.3 SERVICIOS PARA OCI DATABASE

1.3.1 SISTEMA DE BASE DE DATOS DE MÁQUINA VIRTUAL

En relación con los sistemas de base de datos de instancias de máquinas virtuales, OCI ofrece sistemas de base de datos de nodo único o sistemas de base de datos RAC de dos nodos en máquinas virtuales. Se puede gestionar mediante la consola, la API, la CLI de OCI, la CLI de base de datos (DBCLI), Enterprise Manager o SQL Developer.

Todos los sistemas de base de datos Oracle de nodo único admiten las siguientes ediciones de Oracle Database:

a) Standard Edition.

b) Enterprise Edition.

c) Enterprise Edition - High Performance.

d) Enterprise Edition - Extreme Performance.

Sin embargo, para los sistemas de base de datos Oracle RAC de dos nodos requieren Oracle Enterprise Edition - Extreme Perfomance.

Para el aprovisionamiento estándar de sistemas de base de datos (con Oracle Automatic Storage Management (ASM) como software de gestión de almacenamiento), las versiones de base de datos admitidas son:

a) Oracle Database 21c

b) Oracle Database 19c

c) Oracle Database 18c (18.0)

d) Oracle Database 12c versión 2 (12.2)

e) Oracle Database 12c versión 1 (12.1)

Para más información relacionada con Oracle Automatic Storage Management (ASM), puede consultar el siguiente enlace en inglés de Oracle:

https://docs.oracle.com/en/database/oracle/oracle-database/19/ostmg/asm-intro.html

Por otro lado, para un rápido aprovisionamiento de sistemas de base datos de instancias de máquinas virtuales de nodo único (usando Logical Volume Manager como software de gestión del almacenamiento), las versiones de Database admitidas son:

a) Oracle Database 21c

b) Oracle Database 19c

c) Oracle Database 18c

d) Oracle Database 12c versión 2 (12.2)

Para más información relacionada con Logical Volume Manager, puede consultar el siguiente enlace en inglés de Oracle:

https://docs.oracle.com/en/database/oracle/oracle-database/19/admin/using-oracle-managed-files.html

Hay que tener en cuenta que para las bases de datos que utilizan infraestructura de máquinas virtuales, OCI utiliza la facturación por segundos. Esto significa que el uso de almacenamiento y OCPU se facturan por segundos, con un periodo de uso mínimo de un minuto para los sistemas de base de datos de instancias de máquinas virtuales.

Como se comentaba con anterioridad, hay dos tipos de sistemas de base de datos en máquinas virtuales:

a) Un sistema de base de datos de instancias de máquinas virtuales de un nodo que consta de una máquina virtual.

b) Un sistema de base de datos de instancias de máquinas virtuales de dos nodos que consta de dos máquinas virtuales.

Al iniciar un sistema de base de datos de instancias de máquinas virtuales, seleccione la edición y la versión de Oracle Database que se apliquen a la base de datos en ese sistema de base de datos. No se puede cambiar la edición seleccionada. Según la versión y edición de Oracle Database seleccionadas, el sistema de base de datos puede admitir varias bases de datos conectables (PDB).

Para obtener más información sobre las funciones, opciones y paquetes de gestión permitidos por la solución Oracle Database para las versiones 19c y 21c, consultar los siguientes enlaces en inglés:

a) Oracle Database 19c:

   https://docs.oracle.com/en/database/oracle/oracle-database/19/dblic/Licensing-Information.html

b) Oracle Database 21c:

   https://docs.oracle.com/en/database/oracle/oracle-database/21/dblic/Licensing-Information.html

Finalmente, a diferencia de un sistema de base de datos con hardware dedicado, un sistema de base de datos de instancias de máquinas virtuales solo puede tener un único directorio raíz de base de datos, que a su vez solo puede tener una sola base de datos. Las bases de datos tendrán la misma versión que el directorio raíz de Database.

Nota: Los sistemas de Hardware dedicado en Base de datos de Oracle se encuentran en desuso y se mencionan por el hecho de que las organizaciones aún puedan seguir utilizándolos, pero no se abordarán medidas específicas por ello.

Los sistemas de base de datos de instancias de máquinas virtuales también difieren de los sistemas con hardware dedicado de la siguiente manera:

a) Una base de datos del sistema de base de datos de instancias de máquinas virtuales utiliza el almacenamiento de bloques de OCI en lugar del almacenamiento local. Se especifica un tamaño de almacenamiento al iniciar el sistema de base de datos, pudiendo ampliar el almacenamiento según sea necesario en cualquier momento.

   Para obtener más información sobre el almacenamiento para sistemas de base de datos de instancias de máquinas virtuales, consultar el siguiente enlace de Oracle:

   https://docs.oracle.com/es-ww/iaas/Content/Database/Concepts/overview.htm

b) Para cambiar el número de núcleos de CPU en un sistema de base de datos de instancias de máquinas virtuales existente, debe cambiar la unidad de ese sistema de base de datos.

   Más información sobre el cambio de la unidad de un sistema de base de datos de instancias de máquinas virtuales, consultar el siguiente enlace de Oracle:

   https://docs.oracle.com/es-ww/iaas/Content/Database/Tasks/managingDBsystem.htm

Para obtener más información sobre cómo crear un sistema de base de datos de máquina virtual, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Database/Tasks/creatingDBsystem.htm

1.3.2 BASE DE DATOS AUTÓNOMA

La base de datos autónoma de OCI es un entorno de base de datos preconfigurado y totalmente administrado con cuatro tipos de carga de trabajo disponibles:

a) **Autonomous Transaction Processing:** diseñado para cargas de trabajo transaccionales. Ofrece alta simultaneidad para transacciones y consultas cortas.

   Puede obtener una visión general completa del producto a través del siguiente enlace en inglés de Oracle:

   https://docs.oracle.com/en/cloud/paas/atp-cloud/index.html

b) **Autonomous Data Warehouse:** ideado para cargas de trabajo de toma de decisiones y almacenes de datos.

   Puede obtener una visión general completa del producto a través del siguiente enlace en inglés de Oracle:

   https://docs.oracle.com/en/cloud/paas/autonomous-data-warehouse-cloud/

c) **Autonomous JSON Database:** diseñado para el desarrollo de aplicaciones centradas en JSON. Ofrece una API de documentos fáciles de usar para desarrolladores y almacenamiento de JSON nativo.

   Puede obtener una visión general del producto, consultando el siguiente enlace en inglés de Oracle:

   https://docs.oracle.com/en/cloud/paas/autonomous-json-database/ajdug/index.html

d) **Oracle APEX Application Development:** optimizado para desarrolladores de aplicaciones que necesitan una base de datos de procesamiento de transacciones para el desarrollo de aplicaciones median Oracle APEX, que permite crear y desplegar aplicaciones con poco código, incluidas las bases de datos.

   Puede obtener más información del producto consultando el siguiente enlace en inglés de Oracle:

   https://docs.oracle.com/en/cloud/paas/apex/index.html

No es necesario configurar ni gestionar ningún hardware ni instalar ningún software. Después del aprovisionamiento, puede escalar el número de núcleos de CPU o la capacidad de almacenamiento de la base de datos en cualquier momento sin que esto afecte a la disponibilidad o el rendimiento. Autonomous Database gestiona la creación de la base de datos y las siguientes tareas de mantenimiento:

a) Realizar una copia de seguridad de la base de datos.

b) Aplicar un parche en la base de datos

c) Actualizar la base de datos

d) Ajustar la base de datos

Por otro lado, Autonomous Database se puede usar sin abonar nada como parte del conjunto de recursos gratuitos de OCI. Los usuarios de las cuentas gratuitas y de pago de OCI tienen acceso a dos instancias gratis de Autonomous Database de manera permanente, en la que disponen de 8 GB de memoria fija, 20 GB de almacenamiento, 1 OCPU y se pueden configurar para cargas de trabajo Autonomous Transaction Processing o Autonomous Data Warehouse.

Para obtener más información relacionada con los recursos gratuitos de OCI Autonomous Database, consultar el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Database/Concepts/adbfreeoverview.htm

Para finalizar, las bases de datos de Autonomous Database tienen las siguientes opciones de infraestructura de Exadata:

a) **Infraestructura de Exadata compartida:** pensada para el aprovisionamiento y gestión de Autonomous Database sin que el usuario gestione la infraestructura. Es decir, Oracle despliega y gestiona la infraestructura de Exadata, permitiendo que ambos tipos de carga de trabajo (procesamiento de transacciones y almacén de datos) puedan ser aprovisionados en una infraestructura de Exadata compartida.

b) **Infraestructura de Exadata dedicada:** para el uso exclusivo del hardware de Exadata. Ofrece una arquitectura de base de datos multi tenant, lo que le permite crear y gestionar varias bases de datos autónomas en un único sistema de base de datos. Ambos tipos de carga de trabajo (procesamiento de transacciones y almacén de datos) se pueden aprovisionar en la infraestructura de Exadata dedicada.

   Consulte las opciones de hardware de la infraestructura de Exadata autónoma para obtener más información sobre la arquitectura, funciones y especificaciones de hardware a través del siguiente enlace de Oracle:

   https://docs.oracle.com/es-ww/iaas/Content/Database/Concepts/adbddoverview.htm

Para obtener más información relacionada con la creación de una instancia de Autonomous Database en una infraestructura de Exadata compartida, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Database/Tasks/adbcreating.htm

Para obtener más información relacionada con la creación de una instancia de Autonomous Database en una infraestructura de Exadata dedicada, consulte el siguiente enlace de Oracle:

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

1.3.3 EXADATA CLOUD SERVICES

Exadata Cloud Service permite aprovechar la potencia de Exadata en la nube. Puede aprovisionar Sistemas Exadata flexibles que le permitan agregar servidores de recursos de cómputo y servidores de almacenamiento de base de datos al sistema a medida que aumenten sus necesidades.

Los Sistemas Exadata, a partir del modelo X8M, ofrecen redes RDMA sobre Ethernet convergente (RoCE) para módulos de memoria persistente (PMEM) de gran ancho de banda y baja latencia, y software Exadata inteligente. Los sistemas X8M se pueden aprovisionar mediante una unidad equivalente a un sistema X8 de cuarto de rack y, a continuación, se pueden agregar servidores de base de datos y almacenamiento en cualquier momento, tras el aprovisionamiento.

Para obtener más información sobre los sistemas X8M, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Database/Concepts/exaflexsystem.htm

Las instancias de Exadata Cloud Service requieren Enterprise Edition - Extreme Performance. Esta edición proporciona todas las funciones de Oracle Database Enterprise Edition, además de todos los paquetes de gestión de base de datos de Enterpise Manager y todas las opciones de Enterprise Edition, como Oracle Database In-Memory y Oracle Real Application Clusters (RAC).

Las instancias de Exadata Cloud Service soportan las siguientes versiones de software:

a) Oracle Database 19c (19.0)

b) Oracle Database 18c (18.0)

c) Oracle Database 12c versión 2 (12.2)

d) Oracle Database 12c versión 1 (12.1)

Nota: Exadata Cloud Service ofrece suscripciones de tipo “Pay As You Go” y “Annual Universal Credits”. Para obtener más información relacionada con los precios y las suscripciones, consulte el siguiente enlace de Oracle en inglés: https://www.oracle.com/cloud/bring-your-own-license/faq/universal-credit-pricing.html

Los sistemas de Exadata Cloud Service integran el hardware de Exadata Database Machine de Oracle, con los recursos de red necesarios para conectarse de forma segura a la red local de su organización y a otros servicios en la nube de Oracle.

Para obtener una visión general de la arquitectura completa de los componentes de un sistema Exadata Cloud Service, consulte el siguiente enlace en inglés de Oracle:

https://docs.oracle.com/en/engineered-systems/exadata-cloud-service/ecsid/

Por otro lado, se soportan tres tipos de operaciones de escalado para Exadata Cloud Service:

a) Para todas las instancias de Exadata Cloud Service, puede escalar la potencia de procesamiento del nodo de cálculo dentro del sistema aprovisionado, agregando o restando núcleos de CPU según sea necesario.

b) Para sistemas Exadata a partir del X8M, la unidad flexible le permite agregar servidores de almacenamiento y base de datos adicionales al recurso de infraestructura de Exadata en la nube según las necesidades.

c) Para sistemas de base de datos X6, X7 y X8 de Exadata, puede escalar moviendo el sistema a una configuración de unidad diferente, como por ejemplo, de un cuarto a medio rack.

Para obtener más información sobre cada tipo de escalado, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Database/Tasks/exasystemscaling.htm

Además, cada instancia de Exadata Cloud Service consta de nodos de cálculo y servidores de almacenamiento. Cada nodo de cálculo se configura con una máquina virtual (VM). Tiene privilegios de raíz para las VM del nodo de cálculo, por lo que puede cargar y ejecutar software adicional en ellas. Sin embargo, no tiene acceso administrativo a los componentes de infraestructura de Exadata, incluido el hardware del nodo de cálculo físico, los conmutadores de red, las unidades de distribución de energía (PDU), el integrated lights-out management (ILOM) o los Exadata Storage Servers, que son administrados por Oracle.

Para sistemas X8M, el hardware de Exadata se administra mediante dos tipos de recursos, el recurso de infraestructura de Exadata en la nube y el clúster de VM en la nube y para sistemas X6, X7 y X8, el hardware de Exadata se administra mediante el recurso del sistema de base de datos.

Para obtener más información relacionada con las configuraciones de shapes disponibles, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Database/References/exashapes.htm

Finalmente, al iniciar una instancia de Exadata Cloud Service, Oracle Automatic Storage Management (ASM) configura el espacio de almacenamiento dentro de los servidores de almacenamiento Exadata para su uso. Por defecto, se crean los siguientes grupos de discos ASM:

a) El grupo de discos DATA está destinado al almacenamiento de archivos de datos de Oracle Database.

b) El grupo de discos RECO se utiliza principalmente para almacenar el área de recuperación rápida (FRA), que es un área de almacenamiento en la que Oracle Database puede crear y gestionar varios archivos relacionados con la copia de seguridad y la recuperación, como copias de seguridad de RMAN y archivos redo log archivados.

c) Los sistemas de archivos /acfs contienen archivos del sistema que admiten varias operaciones. No debe almacenar archivos personalizados, archivos de datos de Oracle Database ni copias de seguridad dentro de los grupos de discos de ACFS. Los montajes de ACFS personalizados se pueden crear mediante el grupo de discos DATA ASM para archivos que no están relacionados con el servicio.

Los nombres de los grupos de discos contienen una cadena de identificación breve asociada al entorno de la máquina de la base de datos Exadata. Por ejemplo, el identificador podría ser C2, en cuyo caso el grupo de discos DATA se denominaría DATAC2, el grupo de discos RECO se denominaría RECOC2, etc.

Además, puede crear un grupo de discos SPARSE. El grupo de discos SPARSE se necesita para admitir instantáneas de Exadata. Las instantáneas de Exadata permiten la creación y destrucción de forma muy rápida y sencilla de clones de bases de datos de Oracle eficientes en cuanto a espacio. Los clones de instantáneas se suelen utilizar con fines de desarrollo, prueba u otros propósitos que requieren una base de datos transitoria.

Para obtener más información relacionada con las operaciones de base de datos Exadata, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Database/Tasks/examanagingdatabases.htm

CONFIGURACIÓN SEGURA PARA ORACLE OCI DATABASE - INSTANCIAS VM

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.

1.4 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.

1.4.1 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).

1.4.1.1 IDENTIFICACIÓN

La identificación de los usuarios del sistema se realizará utilizando un identificador único para los sistemas de identificación previstos en la normativa de aplicación. Cuando el usuario tenga diferentes roles frente al sistema, por ejemplo, trabajador interno del organismo, administrador de los sistemas, o de los servicios, recibirá identificadores singulares para cada uno de los casos de forma que siempre queden delimitados privilegios y registros de actividad.

La configuración de cuentas federadas y locales para la administración y gestión de los recursos de las bases de datos se realiza desde el servicio OCI IAM, descrito de manera detallada en la guía de seguridad CCN-STIC-889A Guía de Configuración segura IAM y servicios de seguridad.

Por otro lado, dentro de esta medida, y en particular para Base de datos, es necesaria una protección especial para asignar complejidad al uso de contraseñas para los usuarios que se autentiquen en las bases de datos. Las bases de datos de Oracle proporcionan un script PL/SQL para verificar la complejidad de la contraseña de la base de datos. Este script se encuentra en:

```
$ORACLE_HOME/rdbms/admin/UTLPWDMG.SQL
```

Puede obtener instrucciones sobre la ejecución del script UTLPWDMG.SQL para verificar la complejidad de la contraseña, consultando el siguiente enlace en inglés:

https://docs.oracle.com/cd/B28359_01/network.111/b28531/authentication.htm

1.4.1.2 REQUISITOS DE ACCESO

Los recursos del sistema deben quedar protegidos y los requisitos de acceso es una medida de seguridad necesaria para la consecución de tal fin. Los mecanismos derivados de los requisitos de acceso deben impedir el uso de los recursos salvo que se asignen los privilegios adecuados.

Los privilegios son asignados a cuentas de usuario o grupos de usuario a través de políticas configuradas en el servicio de OCI IAM, atendiendo siempre a la política y normativa de seguridad de la organización y al principio del mínimo privilegio.

El principal objetivo de las medidas de seguridad aplicadas es el control de acceso a los componentes del sistema, sus ficheros o registros de configuración. Para ello, OCI dispone de compartimentos donde se ubican los recursos y limita el espacio de acción mediante permisos concedidos a determinados grupos de usuarios, asegurando que cada usuario solamente acceda a los recursos que necesita acceder.

Por otro lado, para determinar las necesidades de acceso a los recursos de un sistema de base de datos de instancias de máquinas virtuales, es necesario conocer qué permisos dotan de capacidad a un administrador o grupo de administradores para la construcción de un sistema de base de datos y los permisos necesarios para la gestión posterior.

Así pues, para la creación de un sistema de base de datos cualquiera, es necesario disponer de una red virtual en la nube (VCN) configurada correctamente y, al menos, una subred de VCN pública o privada. Los recursos de red relacionados con la VCN (gateways, tablas de rutas, listas de seguridad, DNS, etc.), deben quedar protegidos y controlados mediante políticas de acceso y limitados o separados por compartimentos respecto de otros recursos del entorno de producción.

A su vez, la gestión de acceso sobre los recursos permite la interacción sobre otros recursos de OCI como el almacenamiento de objetos, para guardar las copias de seguridad del sistema de base de datos a través de los tipos de servicio Gateway disponibles como Internet Gateway, para el acceso desde internet a una máquina en una subred pública, NAT Gateway para que una máquina de una subred privada pueda acceder a internet o el Service Gateway, para que una máquina pueda acceder a determinados servicios como Object Storage.

Finalmente, para la gestión de un sistema de base de datos de instancias de máquinas virtuales, es necesario dotar a un administrador o un grupo de administradores la capacidad de realizar todas las tareas relacionadas con los recursos asociados a un sistema de base de datos, cumpliendo siempre con el principio del mínimo privilegio.

1.4.1.3 SEGREGACIÓN DE FUNCIONES Y TAREAS

Esta medida tiene su aplicación con la funcionalidad de Oracle Database Vault, la cual implementa controles de seguridad de datos dentro de Oracle Database para restringir el acceso a los datos de aplicaciones por usuarios privilegiados, reduciendo el riesgo de amenazas internas y externas, y tratando los requisitos de cumplimiento, incluida la separación de tareas.

Oracle Database Vault protege los datos confidenciales frente a los ciberataques, bloqueando el acceso no autorizado creando entornos de aplicaciones restringidas dentro de Oracle Database.

Evita cambios no autorizados bloqueando cambios accidentales o maliciosos en las bases de datos de producción que intentan llevarse a cabo fuera de las ventanas de mantenimiento específicas, utilizando para ello factores como, la dirección IP del cliente, el programa, el nombre del usuario y la hora del día para controlar el acceso a los datos y las operaciones de datos.

Presenta separación de roles para la administración y la seguridad, permitiendo que los roles de seguridad definidos administren usuarios, perfiles y controles de seguridad, y limite a los administradores para que solo puedan administrar la base de datos.

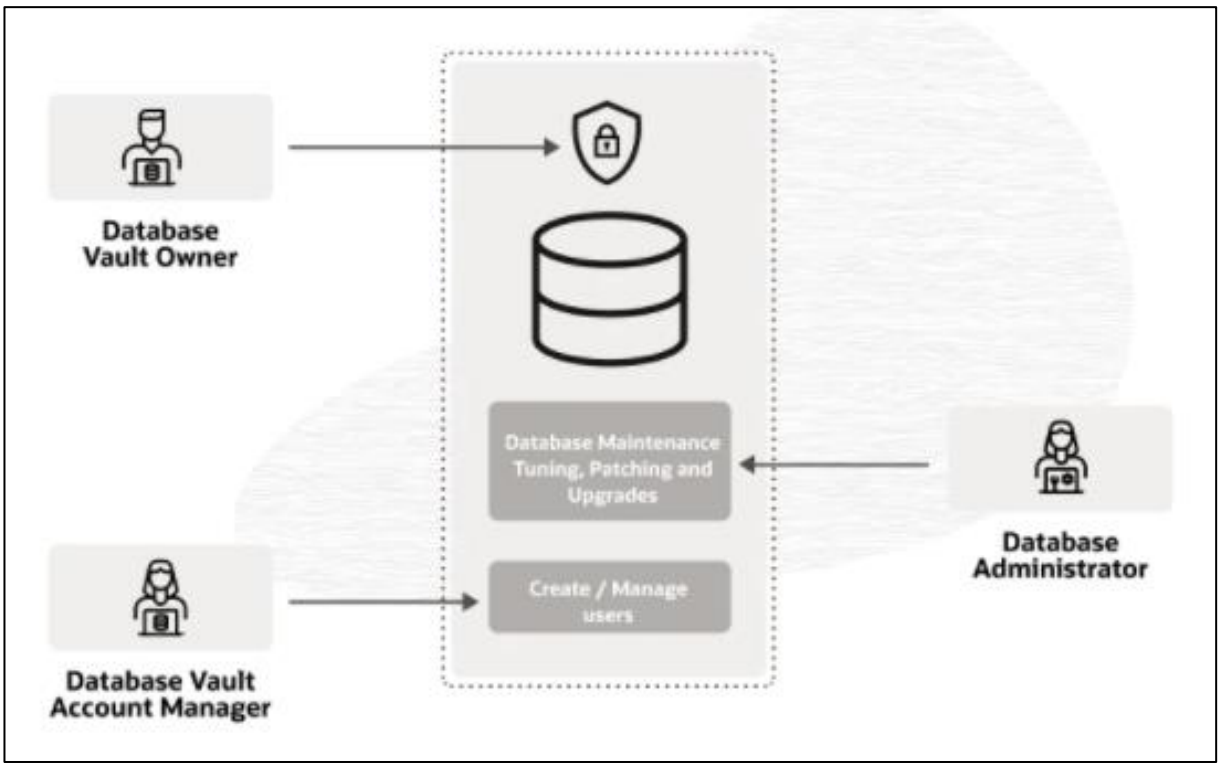


Imagen de la separación de roles en Oracle Database Vault.

Nota: La capacidad de Oracle Database Vault solamente está disponible para las ediciones Enterprise Database Service-High Performance y la Enterprise Database Service-Extreme Performance, para las bases de datos de instancias de máquinas virtuales.

Para configurar y activar Database Vault, en Autonomous Database, debe conectarse a la Base de datos como usuario “admin” y debe crear el propietario de Database Vault y los usuarios del gestor de cuentas, por ejemplo:

```
create user [dbv_owner] identified by <password>;
grant create session to [dbv_owner];
create user [dbv_acctmgr] identified by <password>;
grant create session to [dbv_acctmgr];
```

Después, debe configurar Database Vault, proporcionando los nombres de usuario del propietario y del gestor de cuentas mediante el comando; por ejemplo:

```
exec dvsys.configure_dv('[dbv_owner]','[dbv_acctmgr]');
```

Conéctese como propietario de Database Vault a la base de datos dedicada para habilitarlo:

```
exec dbms_macadm.enable_dv;
```

Reinicie el despliegue de Autonomous Database dedicado, deteniendo y volviendo a iniciar el proceso.

Nota: Estos comandos utilizan nombres de ejemplo. Debe asegurarse de sustituir los nombres entre corchetes por sus propios nombres dentro de la organización.

Para obtener información sobre la gestión de privilegios de Database Vault puede visitar el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/autonomous-database/doc/use-database-vault.html

Para obtener más información relacionada con Database Vault puede consultar el siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/database/oracle/oracle-database/19/dvadm/getting-started-with-oracle-database-vault.html

1.4.1.4 PROCESO DE GESTIÓN DE DERECHOS DE ACCESO

Cada servicio de OCI se integra con OCI IAM con fines de autenticación y autorización para todas las interfaces (la consola, el SDK o la CLI, y la API de REST).

Un administrador de la organización debe configurar grupos, compartimentos y políticas que controlen qué usuarios pueden acceder a qué servicios, qué recursos y el tipo de acceso. Por ejemplo, las políticas controlan quién puede crear nuevos usuarios, crear y gestionar la red en la nube, iniciar instancias, crear contenedores, descargar objetos, etc.

Creación de permisos por Grupos

En cuanto a los permisos de los usuarios de Oracle, se recomienda otorgar permisos para suprimir bases de datos “database_delete, db_system_delete” al mínimo posible de usuarios y grupos de OCI IAM.

Esto minimizará la pérdida de datos debido a supresiones involuntarias por un usuario autorizado o debido a supresiones maliciosas. Otorgue permisos “delete” solo a los grupos de administradores del tenant, de los compartimentos y al grupo de Administradores de Base de Datos.

Para evitar lo anterior, será necesario crear una política con las siguientes líneas:

Política	Descripción
Allow group [DBUsers] to manage db-systems in compartment [DBComparment] where request.permission!='DB_SYSTEM_DELETE' Allow group [DBUsers] to manage databases in compartment [DBCompartment] where request.permission!='DATABASE_DELETE' Allow group [DBUsers] to manage db-homes in compartment [DBCompartment] where request.permission!='DB_HOME_DELETE'	Permite al grupo DBUsers realizar todas las acciones de gestión excepto suprimir bases de datos y artefactos.

Nota: Estas políticas utilizan nombres de grupo y compartimento de ejemplo. Debe asegurarse de sustituir los nombres entre corchetes por sus propios nombres dentro de la organización. A su vez, se recomienda el uso de compartimentos a la hora de otorgar permisos, en lugar del término ‘tenancy’, para conceder mínimos privilegios.

Además de la complejidad de la contraseña de la base de datos, puede utilizar los grupos de seguridad de red de VCN o las listas de seguridad para aplicar el control de acceso de red a las instancias de base de datos. Oracle recomienda configurar los grupos de seguridad de Red de VCN o las listas de seguridad para permitir el acceso con el mínimo de privilegios a las bases de datos de clientes en OCI Database, y para ello se debe controlar el acceso a la configuración segura de los elementos de red para que los usuarios no puedan modificar las listas de seguridad y/o los grupos de seguridad de red.

Por otro lado, las zonas de seguridad de Oracle controlan cómo se gestionan los recursos del compartimento donde reside la base de datos, por lo que es importante controlar el acceso a este elemento de seguridad mediante la creación políticas de IAM, para controlar quién tiene acceso a las zonas y recetas de seguridad y controlar el tipo de acceso para cada grupo de usuarios. Por defecto, solo los usuarios del grupo “Administrators” tienen acceso a todos los recursos de la zona de seguridad.

A continuación, se definen algunas políticas base para la gestión de bases de datos, aunque es posible que el nivel de su organización requiera más detalle, el cual puede encontrar en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/database-management/doc/permissions-required-database-management.html

Aplicación de Políticas para Bases de datos

Política	Descripción
Allow group [CCNAdmins-BD] to manage database-family in compartment [DBCompartment]	Permitir que los administradores de bases de datos gestionen los sistemas de bases de datos de Oracle Cloud incluidos los sistemas de bases de datos de instancias de máquina virtual.
Allow group [CCNAdminsOnPrem-BD] to manage external-database-family in compartment [DBCompartment]	Permitir que los administradores de bases de datos gestionen los recursos de bases de datos externas de Oracle Cloud en un compartimento específico.
Allow group [CCNAdmins-BD] to manage autonomous-database-family in compartment [DBCompartment] Allow group [CCNAdmins-ABD] to manage autonomous-database in compartment [DBCompartment] Allow group [CCNAdmins-ABD] to manage autonomous-backup in compartment [DBCompartment]	Permitir a los administradores de bases de datos y de conjuntos gestionar Autonomous Databases en un compartimento específico.

Nota: Estas políticas utilizan nombres de grupo y compartimento de ejemplo. Debe asegurarse de sustituir los nombres entre corchetes por sus propios nombres dentro de la organización. A su vez, se recomienda el uso de compartimentos a la hora de otorgar permisos, en lugar del término 'tenancy', para conceder mínimos privilegios.

Puede ampliar información acerca de los detalles de estas políticas para Base de datos en el siguiente enlace de Oracle:

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

Aplicación de políticas IAM de zonas de seguridad

Política	Descripción
Allow group [CCNAdmins-Seg] to manage security-zone in compartment [DBCompartment]	Permite a los usuarios del grupo de los administradores de Seguridad crear, actualizar y suprimir zonas de seguridad para el compartimento específico donde resida el sistema de base de datos.
Allow group [CCNAudit-Seg] to read security-zone in compartment [DBCompartment]	Permite a los usuarios del grupo de los Auditores de Seguridad ver las zonas de seguridad en un compartimento específico.

Nota: Estas políticas utilizan nombres de grupo y compartimento de ejemplo. Debe asegurarse de sustituir los nombres entre corchetes por sus propios nombres dentro de la organización. A su vez, se recomienda el uso de compartimentos a la hora de otorgar permisos, en lugar del término 'tenancy', para conceder mínimos privilegios.

Aplicación de políticas para Zonas de seguridad

Política	Descripción
deny db_instance_move_to_compartment_not_in_security_zone	No puede mover una base de datos de una zona de seguridad a un compartimento estándar.
deny db_instance_subnet_not_in_security_zone	Una base de datos de una zona de seguridad debe utilizar subredes que también estén en una zona de seguridad.
deny db_resource_association_not_in_security_zone	Los recursos de infraestructura de Exadata en una zona de seguridad no se pueden asociar a bases de datos de contenedor o clústeres de VM que no están en zonas de seguridad.
deny db_instance_public_access	Las bases de datos de una zona de seguridad no se pueden asignar a subredes públicas. Deben utilizar subredes privadas.
deny buckets_without_vault_key	Los bucket de almacenamiento de objetos de una zona de seguridad deben utilizar una clave maestra de cifrado gestionada por el cliente en el servicio de almacén de claves. No pueden utilizar la clave de cifrado por defecto gestionada por Oracle.
deny database_without_backup	Las bases de datos de una zona de seguridad se deben configurar para realizar copias de seguridad automáticas.
deny database_not_in_security_zone_create_from_backup_in_security_zone	No puede utilizar una copia de seguridad de base de datos en una zona de seguridad para crear una base de datos que no esté en una zona de seguridad.
deny database_in_security_zone_create_clone_not_in_security_zone	No puede clonar una base de datos en una zona de seguridad para crear una base de datos que no esté en una zona de seguridad.
deny free_database_creation	No puede crear una base de datos siempre libre en una zona de seguridad.

Nota: Estas políticas definen denegaciones de acciones que quizás puedan ser necesarias en su entidad. Aplique las que corresponda según su organización.

Puede ampliar la información acerca de las Zonas de Seguridad de Oracle en el siguiente enlace:

https://docs.oracle.com/es-ww/iaas/security-zone/using/security-zone-policies.htm

Por último, puede consultar el siguiente enlace de Oracle para consultar los permisos necesarios para la gestión de bases de datos en función del despliegue del tipo de bases de datos de su organización en la nube de Oracle:

https://docs.oracle.com/es-ww/iaas/database-management/doc/permissions-required-database-management.html

Para el proceso de gestión de la seguridad, OCI dispone del servicio Data Safe (Seguridad del Dato) con el que dispone de una gestión de evaluación de los usuarios con acceso a datos confidenciales en las Bases de Datos y que se detallará en el siguiente punto 1.4.2.4 REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS de este documento.

1.4.2 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.

1.4.2.1 INVENTARIO DE ACTIVOS

En cuanto a la medida de etiquetado de los soportes de información, OCI dispone del Servicio Tagging (Etiquetas) que permite agregar metadatos a los recursos, lo que brinda la posibilidad de definir claves y valores y asociarlos a recursos.

Se pueden utilizar las etiquetas para organizar y visualizar los recursos según las necesidades de la organización, pudiendo utilizar las etiquetas de base de datos para una clasificación más detallada del tipo: Entornos, Departamentos, Contenidos, Accesos, etc., con los que posteriormente gestionar un inventario de las bases de datos o incluso poder segregar aún más los permisos de acceso a las mismas, mediante políticas que cumplan con ciertos valores predefinidos en las etiquetas establecidas cuando se crea una base de datos.

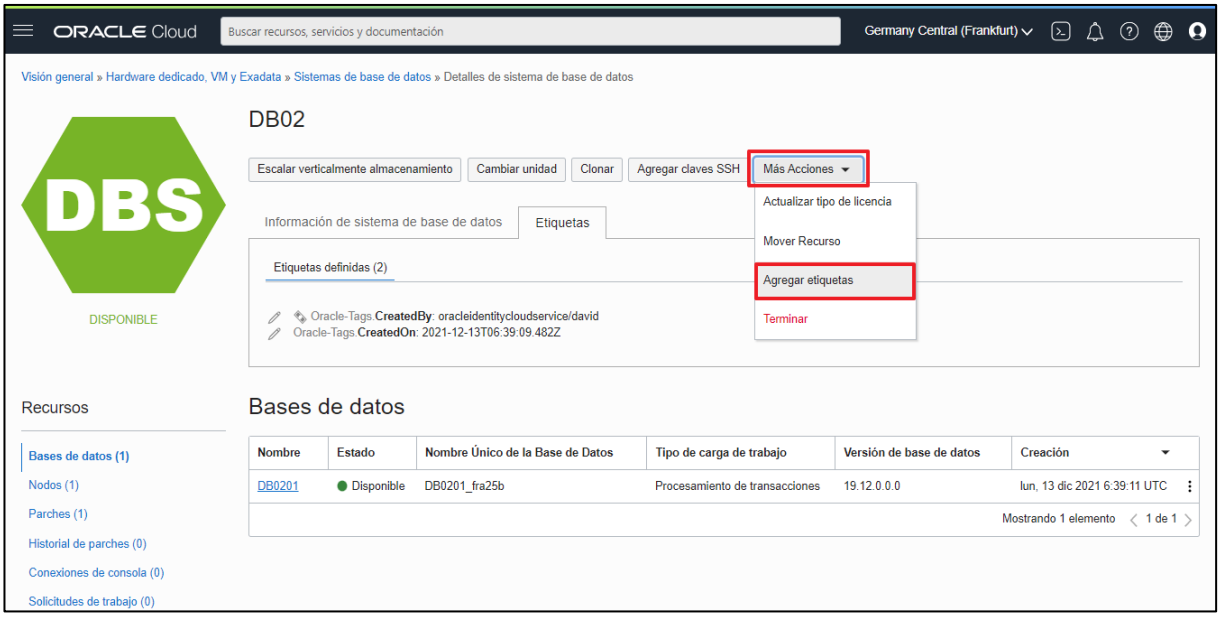


Imagen de un Sistema de base de datos donde se pueden ver las etiquetas por defecto y cómo crear nuevas

Imagen de una base de datos donde se pueden ver las etiquetas por defecto y cómo crear nuevas

1.4.2.2 MANTENIMIENTO

La medida establece una seguridad mínima que debe aplicarse para el nivel alto del ENS. Se debe atender siempre a las especificaciones de los fabricantes en lo relativo a la instalación y mantenimiento de los sistemas de bases de datos. Además, es necesario el seguimiento continuo de los anuncios de defectos y se debe disponer de un procedimiento que analice, priorice y determine cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones.

Nota: para sistemas de base de datos Autonomous DB, Oracle programa y lleva a cabo todas las aplicaciones de parches y demás operaciones de mantenimiento en todos los recursos de la infraestructura de Exadata dedicada y Exadata compartida. Puede especificar cuándo se pueden producir dichas operaciones de mantenimiento y qué tipo de aplicación de parches de base de datos se realiza.

Al contrario que los sistemas de base de datos Autonomous Database, para los sistemas de base de datos de instancias de máquina virtual, es necesario la intervención del usuario para mantener los sistemas operativos actualizados. Sin embargo, existen ciertos requisitos que deben tenerse en cuenta a la hora de actualizar el sistema operativo de una instancia.

a) Es recomendable disponer de un sistema redundante y de alta disponibilidad. Para ello, Oracle dispone del servicio Data Guard, que se tratará en detalle en este apartado.

b) No se debe eliminar ni modificar las reglas esenciales del firewall para un sistema de base de datos como las siguientes en /etc/sysconfig/iptables:

   i. Reglas del firewall para los puertos 1521, 7070 y 7060, porque permite al servicio de base de datos gestionar el sistema de base de datos. Si se elimina la regla o se modifica, el servicio de base de datos puede dejar de funcionar correctamente.

   ii. Reglas del firewall para 169.254.0.2:3260 y 169.254.0.3:80, impide que los usuarios que no sean root escalen privilegios o manipulen el volumen de inicio y el proceso de inicio del sistema.

c) Copia de seguridad de las bases de datos del sistema de base de datos antes de la actualización del sistema operativo. Para obtener más información sobre la copia de seguridad de una base de datos, consultar el punto 1.5.3.4 COPIAS DE SEGURIDAD (BACKUP) de este documento.

d) No se debe eliminar los paquetes del sistema de base de datos. No obstante, es posible que se deba eliminar los RPM personalizados para que la actualización se complete correctamente.

e) Testear previamente las actualizaciones en sistemas de preproducción.

f) Configuración de la VCN para permitir el acceso al repositorio de YUM.

Para obtener más información sobre la actualización de un sistema de base de datos paso a paso, consultar el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Database/Tasks/updatingDB.htm

Por otro lado, la aplicación de parches se realiza sobre la base de datos, directorio raíz de base de datos y sobre el sistema de base de datos de instancias de máquinas virtuales.

Oracle recomienda siempre realizar una planificación y preparación para la aplicación de parches a un sistema de base de datos, entre las cuales, se citan las siguientes:

a) Realice una copia de seguridad de la base de datos.

b) Pruebe el parche en un sistema de base de datos de preproducción.

c) Aplique siempre un parche a un sistema de base de datos antes de aplicar el parche a las bases de datos de ese sistema.

Se recomienda usar el parche más reciente cuando sea posible.

d) Use la acción de comprobación previa, para asegurarse de que el sistema de base de datos o el directorio raíz de base de datos cumple los requisitos del parche que se desea aplicar.

Para obtener más información sobre cómo aplicar un parche de sistema de base de datos de máquina virtual, visualización del historial de parches o el uso de la API, consultar el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Database/Tasks/patchingDB.htm

Para obtener más información sobre cómo aplicar un parche a una base de datos de un sistema de base de datos de máquina virtual consultar el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Database/Tasks/patchingDatabase.htm

Finalmente, Oracle dispone del servicio Data Guard que proporciona un conjunto de servicios que crean, mantienen, administran y monitorean una o más bases de datos en espera para conseguir que las bases de datos de producción sobrevivan frente a desastres y corrupción de los datos. Oracle Data Guard mantiene estas bases de datos en espera como copias de la base de datos de producción y, en consecuencia, habilitando la alta disponibilidad.

Una implantación de Oracle Data Guard requiere dos sistemas de base de datos, uno que contenga la base de datos principal y otro que contenga la base de datos en espera. Cuando se activa el servicio de Oracle Data Guard para una base de datos del sistema de base de datos de instancias de máquinas virtuales, se crea un nuevo sistema de base de datos con la base de datos en espera y se asocia a la base de datos principal.

No obstante, antes de implementar Oracle Data Guard, se debe conocer los detalles de los requisitos previos como los siguientes:

a) Ambos sistemas de base de datos deben estar en el mismo compartimento.

b) Los sistemas de base de datos deben ser del mismo tipo de unidad (por ejemplo, si la unidad de la base de datos principal es una máquina virtual, la unidad de la base de datos en espera puede ser cualquier otra unidad de máquinas virtuales).

c) Las versiones y ediciones de la base de datos deben ser idénticas.

d) Cada base de datos de una asociación de Data Guard debe tener un valor de nombre único [DB_UNIQUE_NAME] que no esté en uso por otras bases de datos en los sistemas de base de datos que alojan la asociación de Data Guard. Sin embargo, la base de datos primaria y en espera pueden utilizar el mismo valor DB_NAME del nombre de la base de datos.

e) La edición de la base de datos determina si Active Data Guard está disponible, estando disponible solo en la edición Enterprise Edition-Extreme Performance. Si se utiliza el modelo de licencia BYOL y el cliente no dispone de licencia de Active Data Guard, se deberá utilizar Enterprise Edition o superior (EE-Hp y EE-EP) y configurar Data Guard manualmente.

f) Si las bases de datos principal y en espera están en la misma región, ambas deben utilizar la misma red virtual en la nube (VCN).

g) Si las bases de datos principal y en espera están en regiones diferentes, se debe emparejar las redes virtuales en la nube (VCN) de cada base de datos.

h) Se debe configurar las reglas de entrada y salida de la lista de seguridad para las subredes de ambos sistemas de base de datos en la asociación de Oracle Data Guard, para permitir que el tráfico TCP fluya entre los puertos aplicables.

Además, Oracle recomienda que el sistema de base de datos de la base de datos en espera esté en un dominio de disponibilidad diferente que el sistema de base de datos de la base de datos principal, para mejorar la disponibilidad y la recuperación ante desastres.

Oracle Data Guard mantiene la base de datos en espera mediante la transmisión y la aplicación de datos redo desde la base de datos principal. Si la base de datos principal deja de estar disponible, puede utilizar Oracle Data Guard para cambiar o realizar un failover de la base de datos en espera al rol principal.

Para obtener más información relacionada con el uso y configuración de Data Guard para sistemas de base de datos de instancias de máquina virtual, consultar el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Database/Tasks/usingdataguard.htm

1.4.2.3 GESTIÓN DE INCIDENTES

Esta medida implica la necesidad en las organizaciones de disponer de procesos frente a incidentes con un alto impacto en la seguridad de los sistemas, incluyendo:

a) Procedimiento de reporte de incidentes reales o sospechosos, detallando el escalado de la notificación.

b) Procedimiento de toma de medidas urgentes, incluyendo la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros, según convenga al caso.

c) Procedimiento de asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente.

d) Procedimientos para informar a las partes interesadas, internas y externas.

e) Procedimientos para prevenir la repetición de un incidente, así como, incluir en los procedimientos de usuario la identificación y forma de tratar el incidente y actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidentes.

Aunque es una medida más procedimental que técnica, OCI tiene disponibles servicios que apoyan, reportan y previenen estos incidentes para minimizar los riesgos al unir los servicios de Data Safe y Cloud Guard.

Cloud Guard ya monitoriza las configuraciones de la base de datos con detectores que verifican el acceso público a las bases de datos, bases de datos sin copias de seguridad automáticas o posibles problemas cuando las bases de datos no tienen los últimos parches.

Hay aspectos adicionales que se deben considerar para fortalecer aún más la seguridad de sus bases de datos. Debe asegurarse de que las bases de datos estén configuradas de manera segura, monitorizar las actividades críticas de la base de datos y proteger cualquier información confidencial que se almacenan en las bases de datos.

Oracle ayuda a abordar estos desafíos con el Servicio Data Safe, que proporciona capacidades de seguridad esenciales para sus bases de datos de Oracle.

Oracle Data Safe permite a las organizaciones evaluar los riesgos de configuración, evaluar a los usuarios de la base de datos, administrar la configuración de auditoría, analizar la actividad de la base de datos, descubrir datos confidenciales almacenados en bases de datos y enmascarar datos confidenciales para su uso en copias de bases de datos que no son de producción, todo en una única consola unificada.

Los nuevos detectores llamados "Database not registered with Data Safe (Base de datos no registrada con Data Safe)" y "Data Safe is not enabled (Data Safe no está habilitado)", permiten a los clientes confirmar que Data Safe está habilitado y que sus bases de datos están siendo monitorizadas por Data Safe.

El primer detector de Cloud Guard indicará la lista de bases de datos en la nube que aún no están registradas en Data Safe.

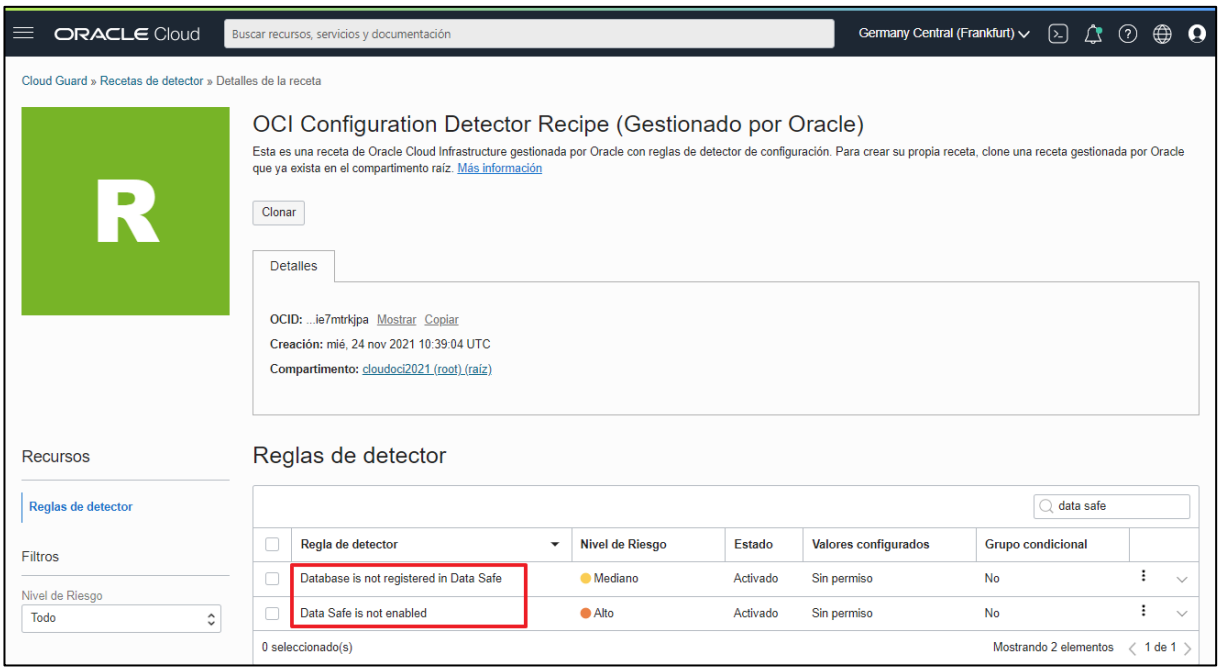
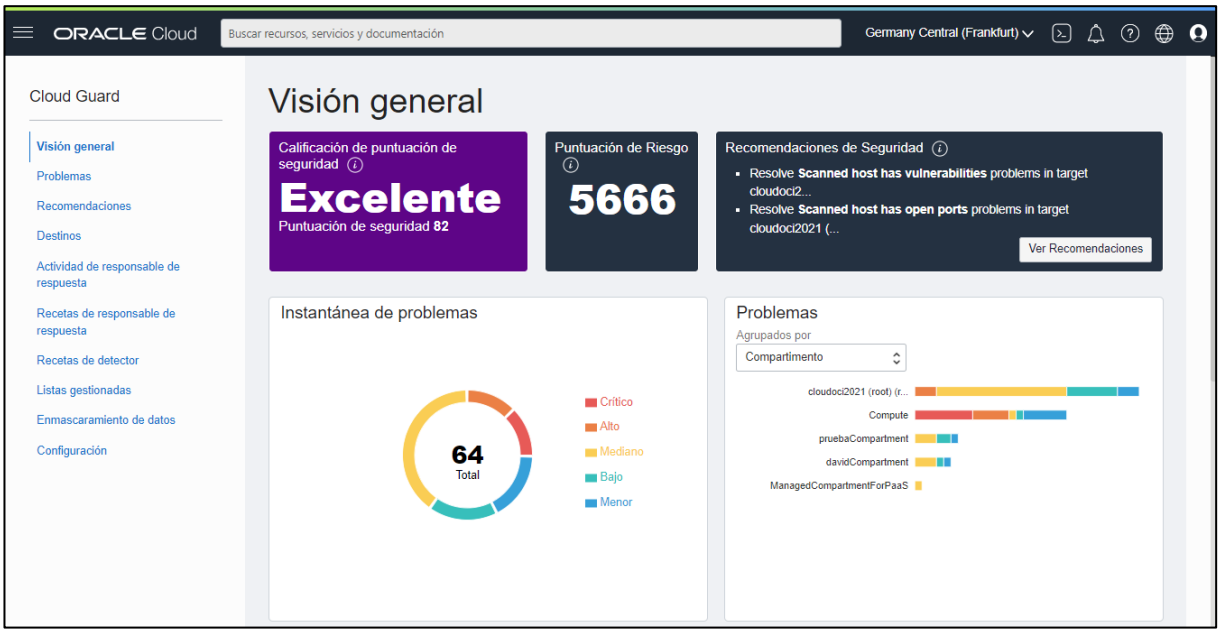


Imagen del detalle de la receta de Cloud Guard que contiene las reglas para verificar que Data Safe está activado y monitorizando las Bases de datos.

Por tanto, Cloud Guard ofrece un panel de control con una visión general del estado de seguridad a través de una calificación de puntuación de seguridad y de riesgos, por los que realiza posteriormente recomendaciones al respecto.



Ejemplo de dashboard del servicio de Cloud Guard con el estado y puntuación del nivel de seguridad del tenant.

Desde la opción del menú Problemas de Cloud Guard, puede supervisar los problemas y localizar incidentes de seguridad, como los ya mencionados que se integran con Data Safe para su gestión desde el menú de "Recomendaciones".

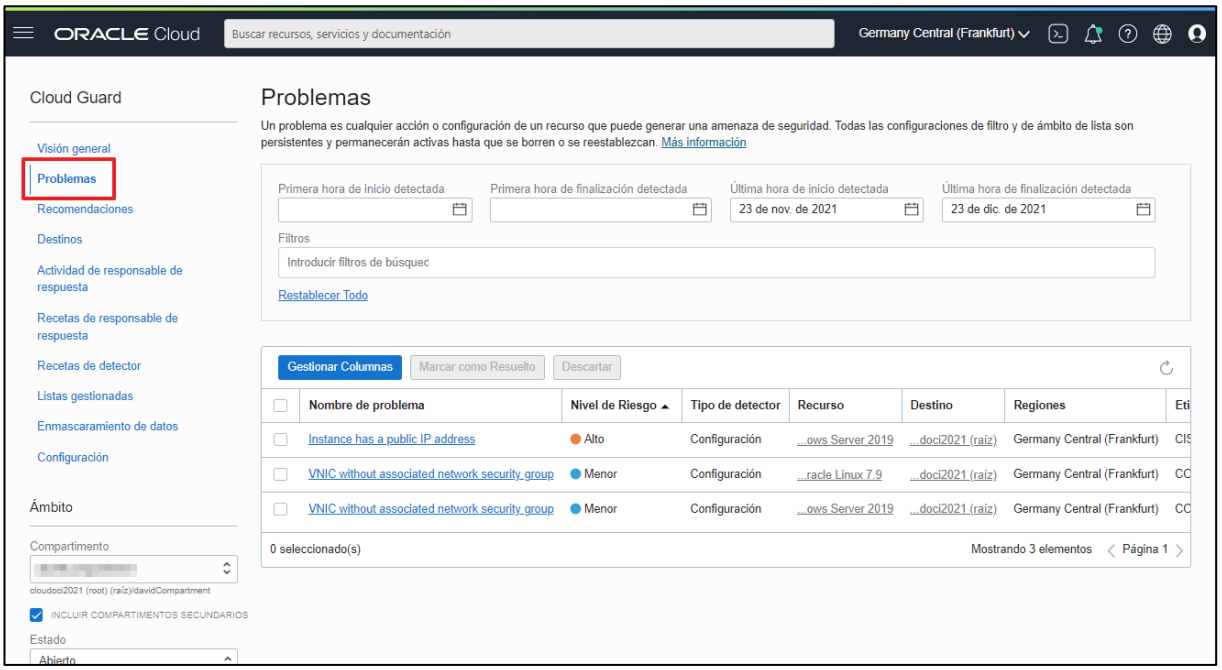


Imagen del menú Problemas en Cloud Guard.

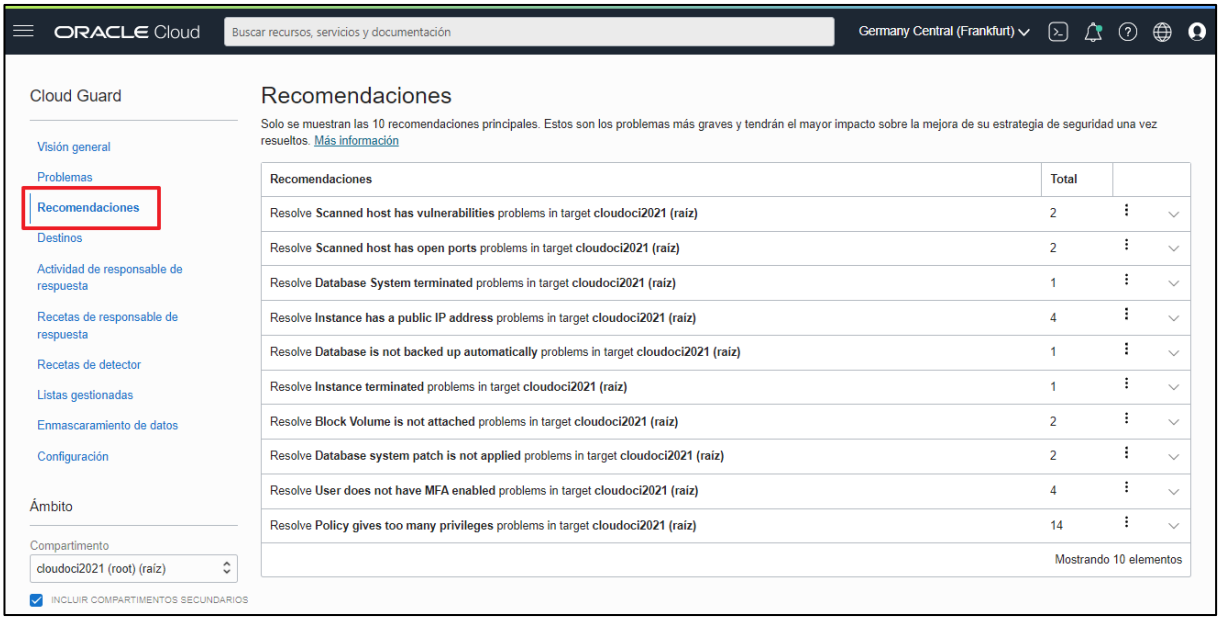


Imagen del menú Recomendaciones en Cloud Guard.

Puede ampliar la información acerca de la gestión de problemas desde el servicio de Cloud Guard a través del siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/cloud-guard/using/part-problems.htm

1.4.2.4 REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS

Oracle Data Safe es un servicio en la nube completamente integrado que se centra en la seguridad de los datos. Proporciona un conjunto de funciones completo e integrado para proteger los datos confidenciales y regulados de las bases de datos de Oracle Cloud. Las funciones incluyen Evaluación de seguridad, Evaluación de usuarios, Detección de datos, Enmascaramiento de datos y Auditoría de actividad.

Los datos de auditoría de una base de datos se almacenan en una tabla de base de datos llamada pista de auditoría. El servicio Data Safe aprovecha y copia dichos datos a su propia tabla de auditoría para mostrar, mediante las funciones descritas con anterioridad, toda la información necesaria para ayudar al usuario en la protección de los datos confidenciales y en el cumplimiento de la medida de seguridad.

Para poder utilizar el servicio, es necesario activarlo primero, accediendo desde el menú de OCI → Oracle Database → Seguridad de los datos, y pulsando el botón de “Activar Data Safe”.

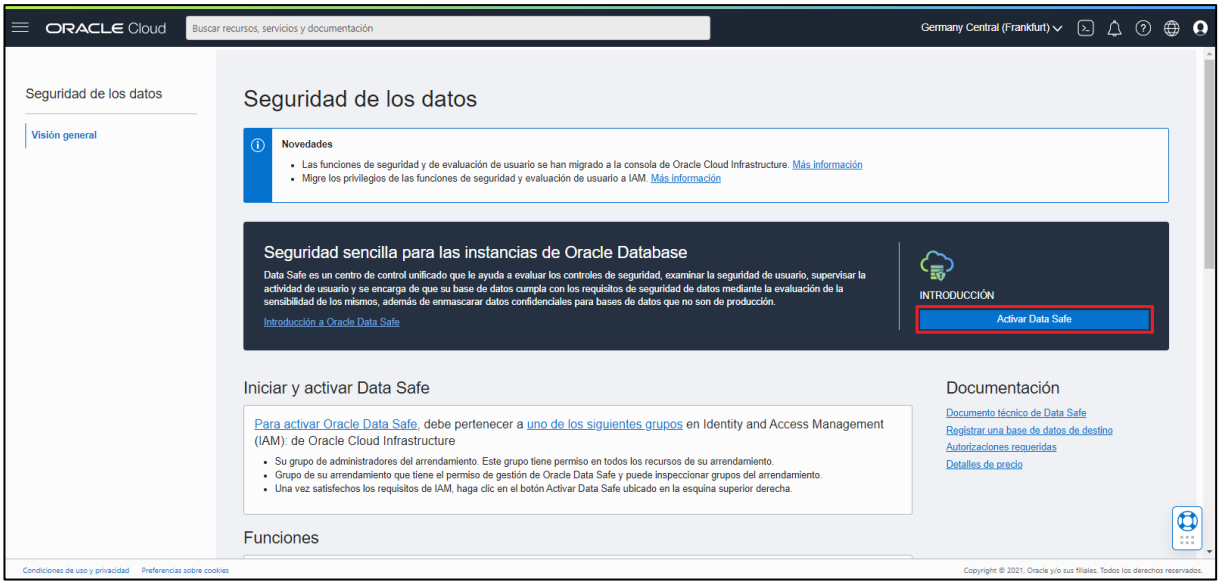


Imagen del Servicio de Seguridad de los datos y su activación.

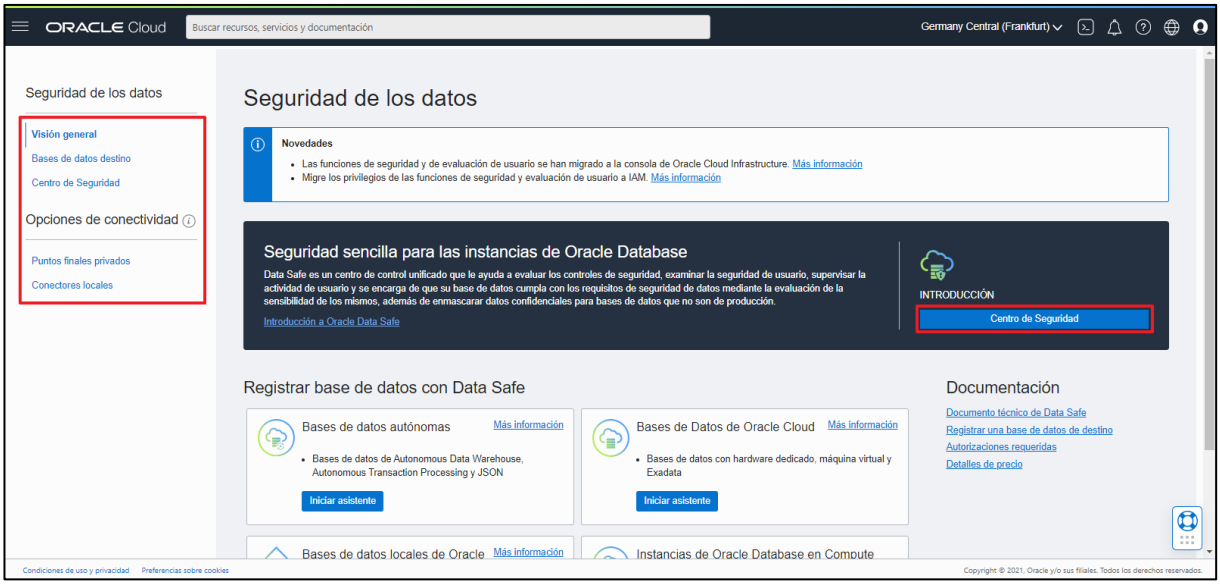


Imagen de los menús del Servicio de Seguridad de los datos tras su activación.

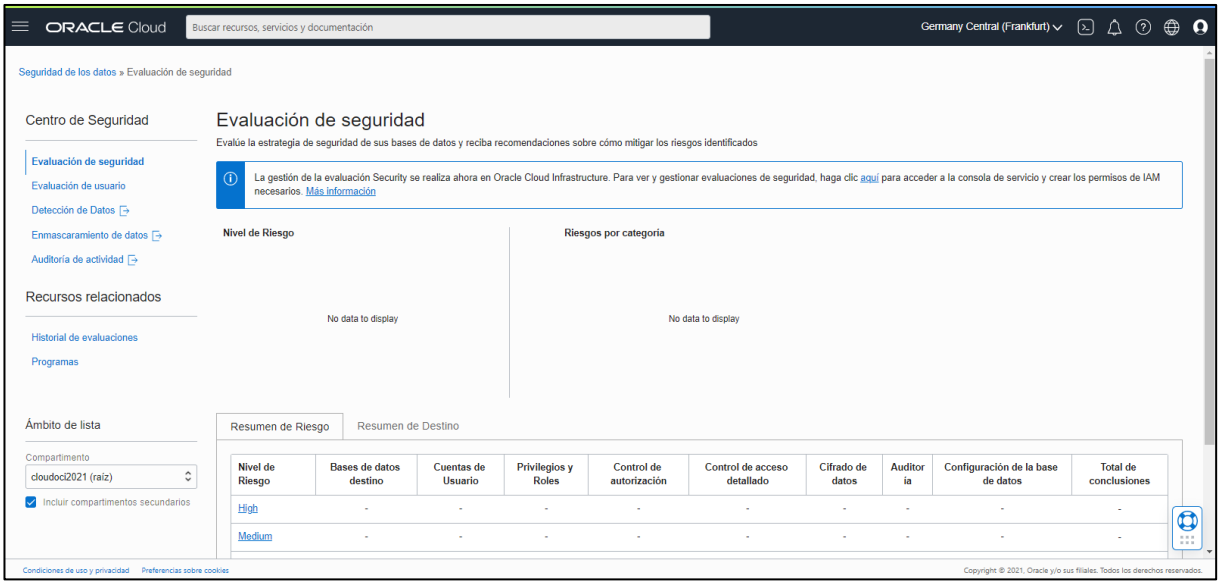


Imagen del Centro de Seguridad tras la activación.

Con el servicio activado y tras disponer de bases de datos y usuarios con acceso a las mismas, las consolas comenzarán a evaluar los datos y se presentarán de la siguiente forma.

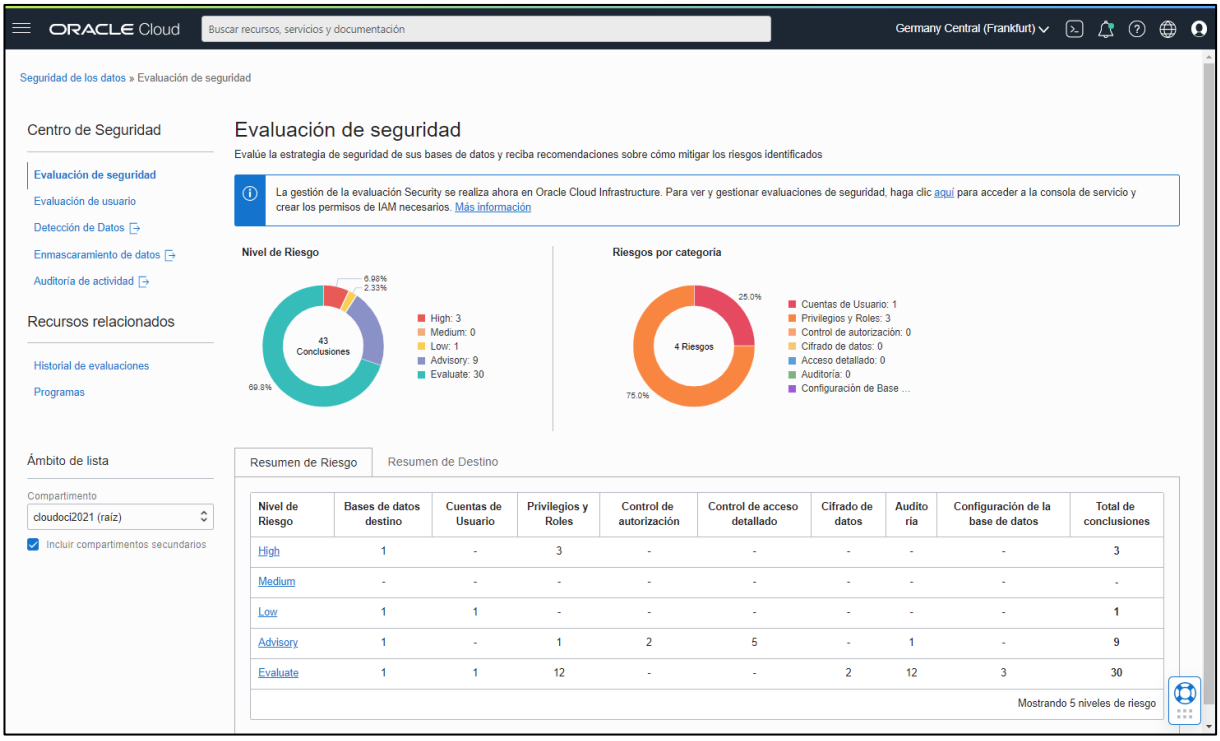


Imagen de la Evaluación de seguridad y los resultados sobre los riesgos detectados.

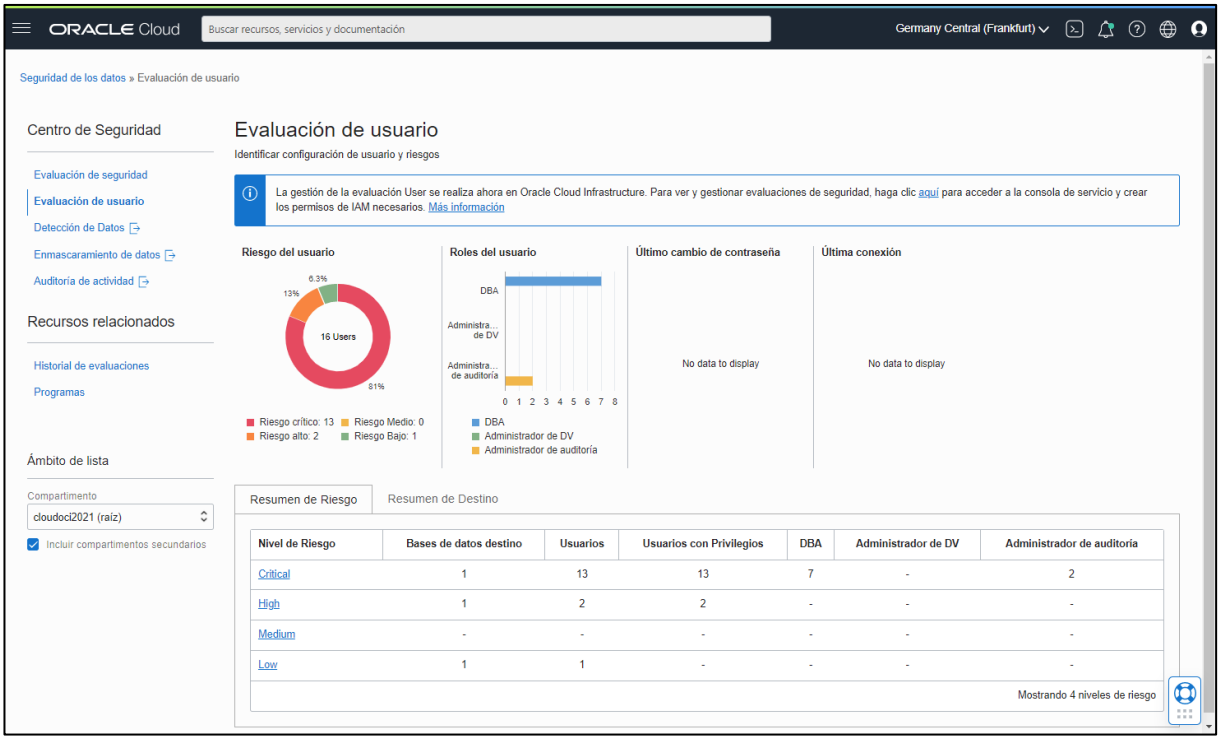


Imagen de la Evaluación de usuario y los resultados sobre los riesgos detectados.

En el siguiente enlace en inglés, encontrará información acerca de la comparación entre la evaluación de los usuarios y la evaluación de seguridad para poder interpretar los resultados:

https://docs.oracle.com/en/cloud/paas/data-safe/udscs/user-assessment-overview.html

El último menú, Auditoría de actividad, se enlaza a una consola externa en inglés, donde podrá localizar los registros sobre la actividad con las bases de datos.

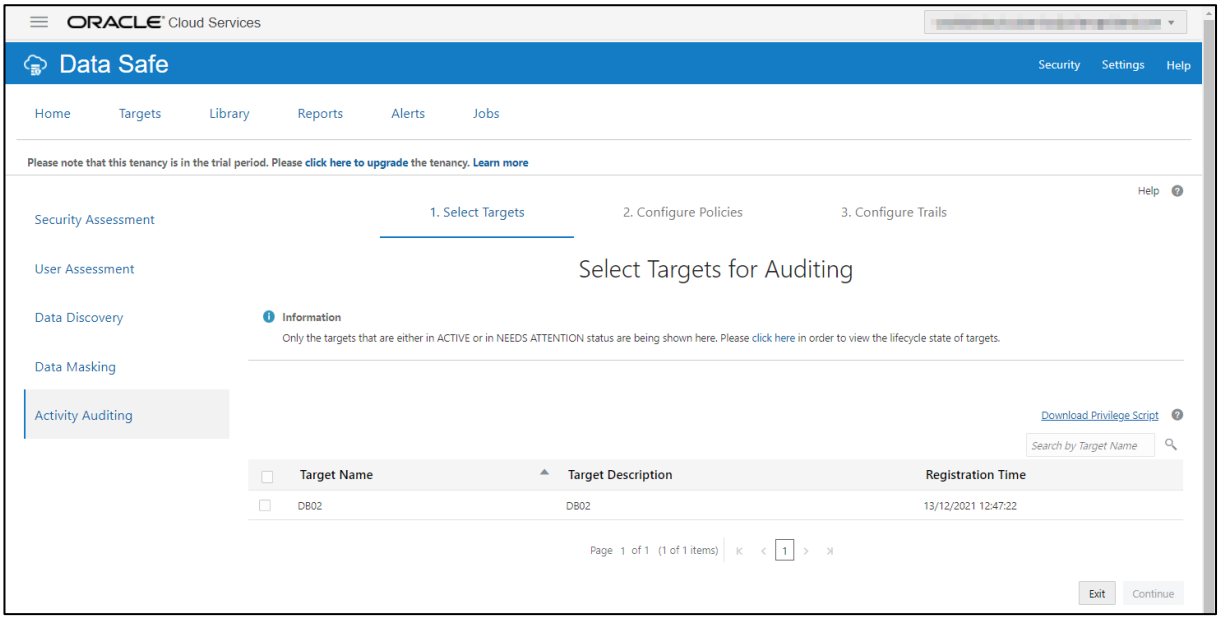


Imagen de la Auditoría de actividad de las Bases de datos.

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

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

1.4.2.5 REGISTRO DE LA GESTIÓN DE INCIDENTES

Esta medida indica la necesidad de registrar todas las actuaciones relacionadas con la gestión de incidentes, de forma que se registren las acciones realizadas tras un incidente, así como las evidencias para sustentar una posterior demanda judicial o hacer frente a ella y se determinará los eventos a auditar.

OCI conserva los registros de auditoría por 365 días y no se borra ninguna acción realizada en la gestión de los problemas desde Cloud Guard, garantizando las evidencias de las acciones realizadas frente a los problemas detectados a la hora de ejecutar la correspondiente recomendación que realiza a cada problema detectado.

En cuanto a los eventos que recoge a nivel de base de datos, puede seguir el siguiente enlace para ampliar la información:

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

1.4.2.6 PROTECCIÓN DE CLAVES CRIPTOGRÁFICAS

El ENS establece que el uso de claves criptográficas debe estar asegurado durante todo su ciclo de vida, desde la generación, transporte, custodia, archivado (tras su retirada) y su destrucción final, indicando para esta categoría básica que en su generación estarán aislados de los medios de explotación y en su posterior archivado lo serán en medios aislados de los de explotación.

Para la categoría alta, el ENS establece que se emplearán programas, algoritmos evaluados y certificados para ello.

OCI Database, dispone del Servicio Vault (Almacén) para la gestión de claves y secretos por parte de la organización, cumpliendo con la medida establecida por el ENS, siendo posible utilizar la gestión de claves propias como gestionadas por Oracle. Por defecto, Oracle mantiene las claves de TDE de forma interna, obligatoria y no se puede deshabilitar. El uso del servicio Vault es una opción solo si el usuario necesita gestionar las claves manualmente.

Para acceder al menú del servicio Vault, debe dirigirse al menú principal de OCI → Identidad y seguridad → Almacén.

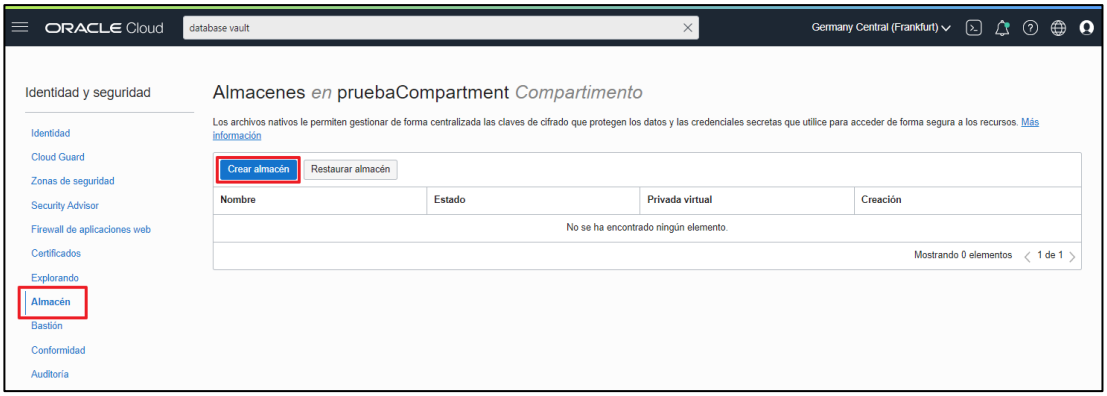


Imagen del Servicio Vault de OCI (Almacén).

Debe crear un "Almacén" para contener las claves de uso personal que vaya a utilizar para el cifrado de las Bases de datos. Su creación debe estar asociada al compartimento donde se encuentre la Base de datos o las Bases en general, para poderla utilizar en todas ellas.

Para este ejemplo, se ha creado un Almacén denominado "databaseVault", asociado al Compartimento "database" del que cuelgan el resto de los compartimentos que contienen las bases de datos: "DB-Desarrollo" y "DB-Produccion".

Dentro de este Almacén, debe crear la clave o claves y secretos que vaya a utilizar en las Bases de datos, pudiendo discriminar si crearlas en el Compartimento raíz de "database" o en los compartimentos internos que este contiene para los entornos de desarrollo o producción.

Nota: Preste atención al ejemplo propuesto, ya que es posible que contenga más o menos entornos de los que utilice en su entidad, teniendo que adaptarlo al modelo de su organización.

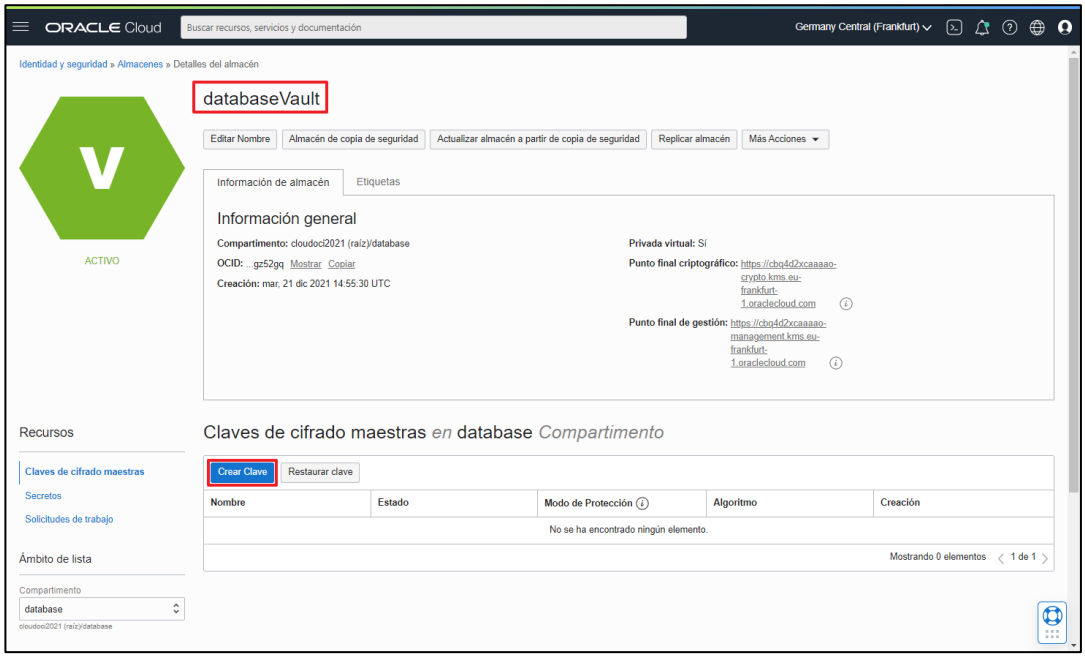


Imagen de la creación de una clave de cifrado en un Almacén, asociado a un compartimento concreto.

Puede ampliar la información acerca de las claves gestionadas por el cliente en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Database/Concepts/exaoverview.htm

1.4.3 MONITORIZACIÓN DEL SISTEMA

El ENS establece al respecto de esta norma que los sistemas estarán 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.

1.4.3.1 DETECCIÓN DE INTRUSIÓN

El ENS establece que el sistema estará sujeto a medidas de monitorización de su actividad, apuntando a la existencia de herramientas de detección o de prevención de intrusión, como necesidad para el cumplimiento de la norma.

OCI, al respecto de esta norma, dispone de varios servicios propios y herramientas de terceros a disposición de los clientes desde el Marketplace para la detección de intrusión. Los Servicios de Monitoring, Cloud Guard y Detección de anomalías son algunos con los que cuenta OCI para ello.

a) Servicio Monitoring (Supervisión):

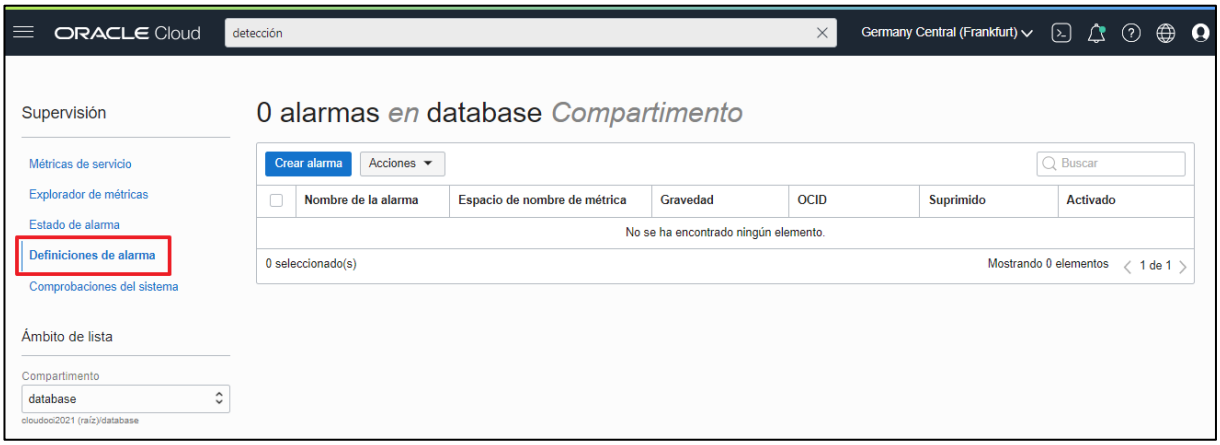


Imagen donde se definen las alarmas de supervisión en OCI.

Puede ampliar la información acerca de la definición de alarmas del sistema de Monitoring (Supervisión) desde el siguiente enlace de Oracle:

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

b) Servicio Cloud Guard:

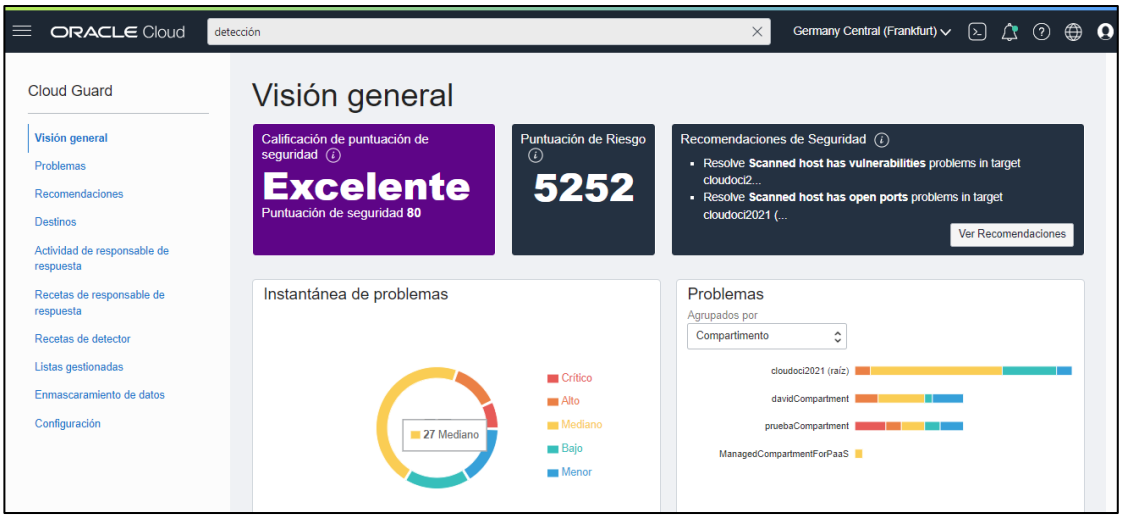


Imagen de la visión general de la consola de Cloud Guard.

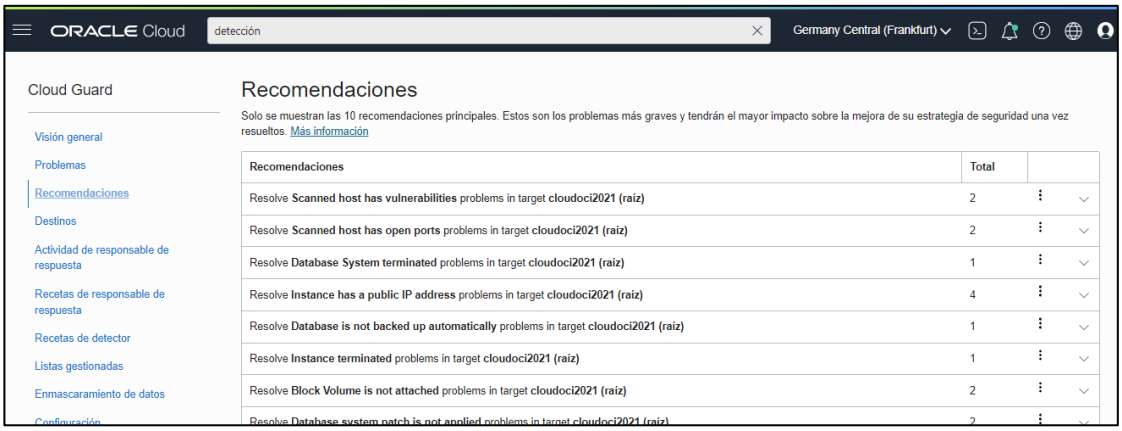


Imagen de las Recomendaciones de Cloud Guard a fallos detectados en un Compartimento.

Puede ampliar la información sobre Cloud Guard en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/cloud-guard/using/problems-page.htm

c) Detección de anomalías:

La detección de anomalías le ayuda a identificar anomalías en un conjunto de datos multivariante aprovechando la interrelación entre las señales, identificando los elementos, eventos u observaciones raros en los datos que difieren significativamente de la expectativa. El servicio está diseñado para ayudar a analizar grandes cantidades de datos correlacionados e identificar las anomalías lo antes posible con la máxima precisión.

El servicio de detección de anomalías se puede utilizar para identificar incidentes y observaciones no deseadas, y proporcionar la magnitud de la anomalía como la diferencia entre el valor esperado y el real.

Este servicio ayuda a definir alertas y acciones específicas de la organización. Le ayuda a identificar anomalías en un conjunto de datos multivariante aprovechando la interrelación entre señales. Cuando el servicio construye un modelo de aprendizaje automático para cada una de las señales como una función de interrelación entre señales, maximiza la precisión de las anomalías identificadas. Esta precisión ayuda a monitorear sistemas complejos con una gran cantidad de señales.

El servicio de detección de anomalías utiliza un método estadístico innovador que ayuda a identificar anomalías lo antes posible. Además, produce métodos de estimación de estado invariados y multivariados, con técnicas de prueba de razón de probabilidad secuencial.

Al servicio de Detección de anomalía se accede a través del menú de OCI → Análisis y AI → Detección de anomalías.

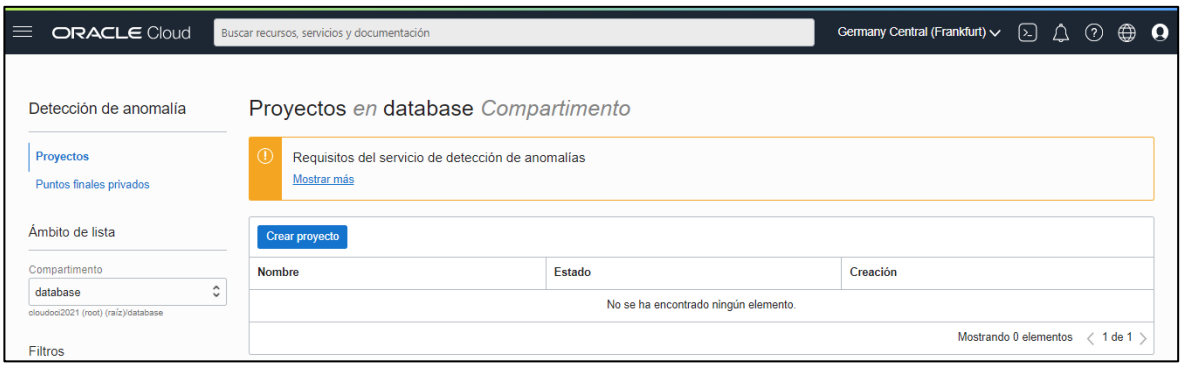


Imagen del Servicio Detección de anomalía y los proyectos.

Para comenzar a utilizar el servicio debe crear una nueva política en el tenant para permitir el uso y gestión del Servicio a los miembros del grupo Administradores de Base de datos:

allow group [DBAdmins] to use ai-service-anomaly-detection-family in tenancy

Nota: Estos comandos utilizan nombres de ejemplo. Debe asegurarse de sustituir los nombres entre corchetes por sus propios nombres dentro de la organización.

Puede ampliar la información acerca del Servicio de Detección de anomalía a través del siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/anomaly/using/overview.htm

1.4.3.2 SISTEMA DE MÉTRICAS

En cuanto al sistema de métricas, el ENS establece que se recopilarán 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.

La aplicación técnica de esta medida se basa en el uso de métricas de servicio de base de datos, para supervisar el estado, la capacidad y el rendimiento de los recursos del servicio de base de datos.

Las métricas de servicio de base de datos ayudan a medir datos cuantitativos útiles, como la utilización de la CPU y del almacenamiento, el número de intentos de conexión a la base de datos correctos y con fallos, las operaciones de base de datos, las consultas SQL, las transacciones, etc.

Dependiendo del tipo de base de datos, OCI dispone de distintas métricas que se ajustan a una base de datos autónoma, métricas de la base de datos externa o métricas de sistemas Exadata y máquinas virtuales.

Para el análisis del rendimiento de bases de datos en máquinas virtuales es necesario la disposición y uso de métricas. El servicio de base de datos emite métricas en el espacio de nombres *oracle_oci_database* para bases de datos Oracle que se ejecutan en sistemas de bases de datos de instancias de máquinas virtuales.

A continuación, las métricas de servicio de base de datos para instancias de máquina virtual incluyen las siguientes dimensiones:

a) **Displayname:** nombre sencillo de la base de datos.

b) **Region:** en la que reside la base de datos.

c) **Resourceid:** de la base de datos.

d) **Resourcename:** el nombre de la base de datos.

Para continuar, las métricas emitidas por el servicio de base de datos en el espacio de nombre *oci_autonomous_database* están disponibles automáticamente para cualquier Autonomous Database que se cree, sin necesidad de activar la supervisión en el recurso de instancias de Autonomous Database.

Las métricas de servicio de base de datos para Autonomous Database incluyen las siguientes dimensiones:

a) **Autonomousdbtype**: tipo de Autonomous Database, Autonomous Data Warehouse (ADW) o Autonomous Transaction Processing (ATP).

b) **DeploymentType**: tipo de infraestructura de Exadata, compartida o dedicada. Al utilizar la consola para visualizar gráficos de métricas por defecto de varias bases de datos de Autonomous Database, debe especificar esta dimensión.

c) **Displayname**: nombre fácil de recordar de la Autonomous Database.

d) **Region**: en la que se encuentra la Autonomous Database.

e) **Resourceid**: OCID de la Autonomous Database.

f) **Resourcename**: nombre de la Autonomous Database.

Todas las métricas de servicio se pueden filtrar por las dimensiones descritas anteriormente. Para obtener más información sobre las distintas métricas de una Autonomous Database puede consultar el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Database/References/databasemetrics_topic-Overview_of_the_Database_Service_Autonomous_Database_Metrics.htm

Por último, las métricas emitidas por el servicio de base de datos en el espacio de nombre *oracle_external_database* están disponibles automáticamente para cualquier base de datos externa que se cree.

Las métricas de servicio de base de datos para bases de datos externas incluyen las siguientes dimensiones:

a) **Displayname**: nombre fácil de recordar de la base de datos externa.

b) **Region**: en la que reside el recurso de base de datos externa de OCI.

c) **Resourceid**: OCID de la base de datos externa.

d) **Resourcename**: nombre de la base de datos externa.

Puede encontrar más información relacionada con las métricas de Base de datos en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Database/References/databasemetrics.htm

Para visualizar las métricas y realizar un seguimiento de cualquier base de datos creada, OCI dispone, entre otras herramientas, del servicio de Gestión de base de datos.

El servicio de Gestión de base de datos proporciona funciones completas de diagnóstico y gestión del rendimiento de la base de datos para supervisar y gestionar bases de datos Oracle.

Con el servicio de Gestión de base de datos se puede supervisar bases de datos de instancia única y RAC, que incluyen bases de datos de contenedor (CDB), bases de datos conectables (PDB) y bases de datos de tipo no contenedor (no CDB). Gestión de base de datos soporta Oracle Database versión 11.2.0.4 y posterior, y aquí se muestran las tareas más importantes que se pueden realizar con este servicio:

a) Controlar las métricas clave de rendimiento y configuración de la flota de bases de datos Oracle. También se puede comparar y analizar las métricas de la base de datos durante un período de tiempo seleccionado.

b) Utilizar el hub de rendimiento para obtener una vista de un único panel del rendimiento de la base de datos, que permite diagnosticar rápidamente los problemas de rendimiento.

c) Utilizar AWR Explorer para visualizar los datos históricos de rendimiento de las instantáneas de AWR en gráficos fáciles de interpretar.

d) Agrupar las bases de datos Oracle esenciales, que residen en compartimentos en un grupo de bases de datos para su supervisión.

e) Crear y programar trabajos SQL para realizar operaciones administrativas en un único grupo de bases de datos o Oracle Database.

Sin embargo, antes de activar y usar Gestión de base de datos, se debe revisar y completar las tareas de requisitos previos, teniendo en cuenta que, para bases de datos autónomas, solo es necesario realizar las tareas de requisitos generales:

a) Tareas de requisitos generales:

   i. Crear grupos de usuarios de OCI IAM

ii. Crear políticas que asignen los permisos necesarios para dichos grupos de usuarios. Para obtener más información sobre los permisos necesarios para gestión de base de datos, puede consultar el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/database-management/doc/permissions-required-database-management.html

b) Tareas de requisitos previos relacionados con la base de datos externa:

i. Instalar agentes de gestión. Para obtener más información relacionada con la instalación de agentes de gestión, puede consultar el siguiente enlace de Oracle:

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

ii. Registrar ORACLE Database con el servicio Base de datos externas. Para obtener información sobre cómo crear un manejador de Base de datos externa, puede consultar el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Database/Tasks/externalcreating.htm

iii. Conectar Oracle Database al gestor de Base de datos externas. Para obtener más información relacionada con la conexión de Oracle Database a un gestor de Base de datos externa, puede consultar el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Database/Tasks/externalconnection.htm

c) Tareas de requisitos previos relacionados con la base de datos Oracle Cloud (Sistemas de base de datos en máquinas virtuales y Exadata Cloud Service):

i. Definir las credenciales de usuario de supervisión de base de datos Oracle Cloud y guardar la contraseña de usuario de base de datos como un secreto en el servicio de Vault. Para obtener más información relacionada con el servicio Vault, puede consultar el siguiente enlace de Oracle:

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

ii. Crear un punto final privado de Gestión de base de datos. Para obtener más información al respecto, puede consultar el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/database-management/doc/perform-database-management-prerequisite-tasks.html

iii. Activar la comunicación entre Gestión de base de datos y Oracle Cloud Database. Para obtener más información sobre la activación de la comunicación descrita, puede consultar el siguiente enlace de Oracle:

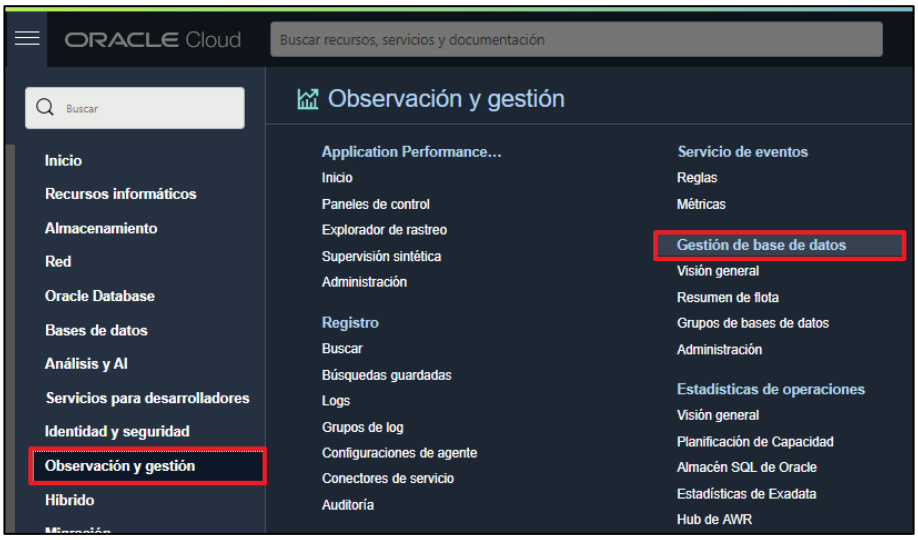
https://docs.oracle.com/es-ww/iaas/database-management/doc/perform-database-management-prerequisite-tasks.html

Una vez completado los requisitos previos, según el tipo de base de datos que se disponga, para la activación del servicio de gestión de base de datos, puede consultar la siguiente documentación de Oracle:

https://docs.oracle.com/es-ww/iaas/database-management/doc/enable-database-management.html

Finalmente, una vez activada la Gestión de base de datos puede acceder a la página del Servicio como se muestra a continuación:

a) Abra el menú de navegación OCI → Observación y gestión → Gestión de base de datos.



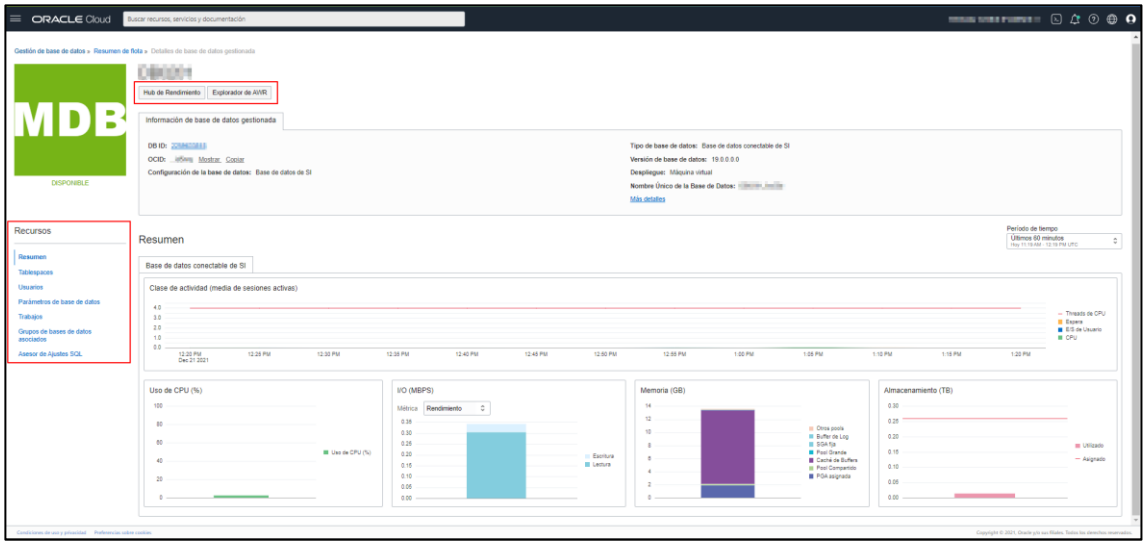
b) En el panel izquierdo de la página Visión general, seleccione el compartimento que contiene las bases de datos Oracle para las que está activada la gestión de base de datos.

Página de Visión general de Gestión de base de datos.

En la página Visión General, se puede obtener una visión general de las funciones de Gestión de base de datos, precios y documentación para navegar a la información sobre los precios y funciones de Gestión de base de datos, visualizar el número de bases de datos Oracle activadas y usar Resumen de conjunto y Grupos de bases de datos para usar las funciones de Gestión de base de datos que supervisan y gestionan las bases de datos Oracle.

Asimismo, el servicio de Gestión de base de datos permite supervisar el estado de la flota de Oracle Database, controlando la disponibilidad y el rendimiento de las bases de datos Oracle.

Desde el apartado de Administración de bases de datos gestionadas de la página de Visión general, se puede encontrar un resumen de conjunto que supervisa varias bases de datos Oracle, permitiendo detectar e identificar de forma proactiva la causa raíz de los problemas de rendimiento en una flota de base de datos y responder a alertas relacionadas con el rendimiento y la configuración.



Página de detalles de base de datos gestionada.

Desde la página de detalles de base de datos gestionada, se puede ver información variada y mosaicos diversos seleccionando, desde el apartado de recursos, la información relacionada con resumen, tablespaces, usuarios, parámetros de base datos, trabajos, grupos de base de datos asociados o el Asesor de Ajustes SQL.

Por otro lado, se puede usar la herramienta hub para el análisis y ajustes del rendimiento de las bases de datos de instancias de máquinas virtuales. Mediante esta herramienta, es posible visualizar datos de rendimiento históricos y en tiempo real. No obstante, para utilizar el hub de rendimiento para máquinas virtuales, es necesario que esté activado para la base de datos. Al activar una base de datos, el administrador de la base de datos puede elegir entre dos opciones de gestión de base de datos: gestión básica o gestión completa. Dependiendo del tipo de gestión escogida, el número de apartados mostrados en el hub de rendimiento varía. Así pues, para una gestión básica, solo se muestran los apartados de Análisis ASH y Supervisión SQL del hub de rendimiento, mientras que, si se escoge la gestión completa, se muestran todos los apartados disponibles del hub de rendimiento.

Para obtener más información relacionada con las funciones del hub de rendimiento, consultar el siguiente enlace de Oracle:

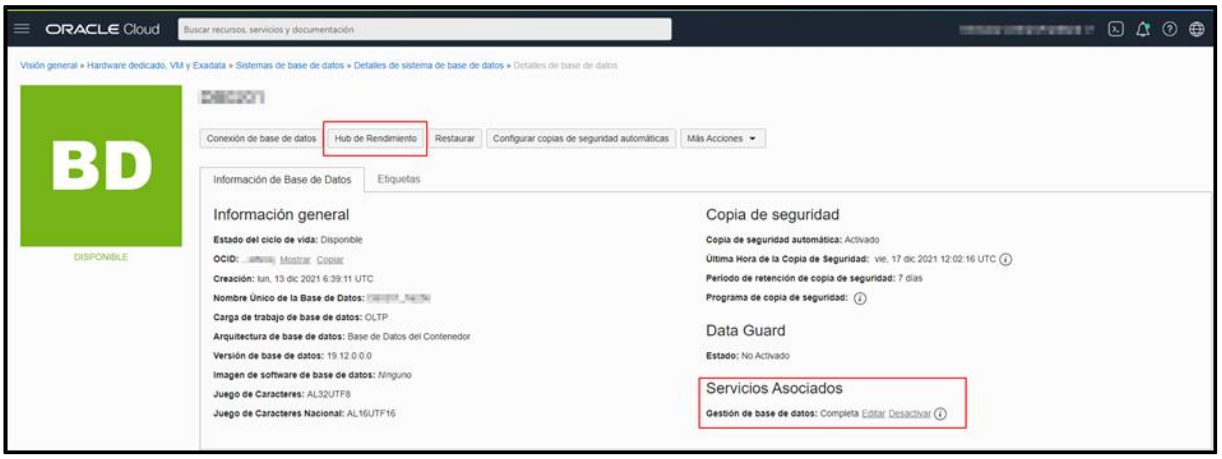
https://docs.oracle.com/es-ww/iaas/Content/Database/Tasks/perfhub.htm

Para navegar por el hub de rendimiento para las bases de datos de instancias de máquinas virtuales desde la consola, se debe hacer lo siguiente desde el menú de OCI → Oracle Database → Hardware dedicado, VM y Exadata:

a) Seleccione un compartimento.

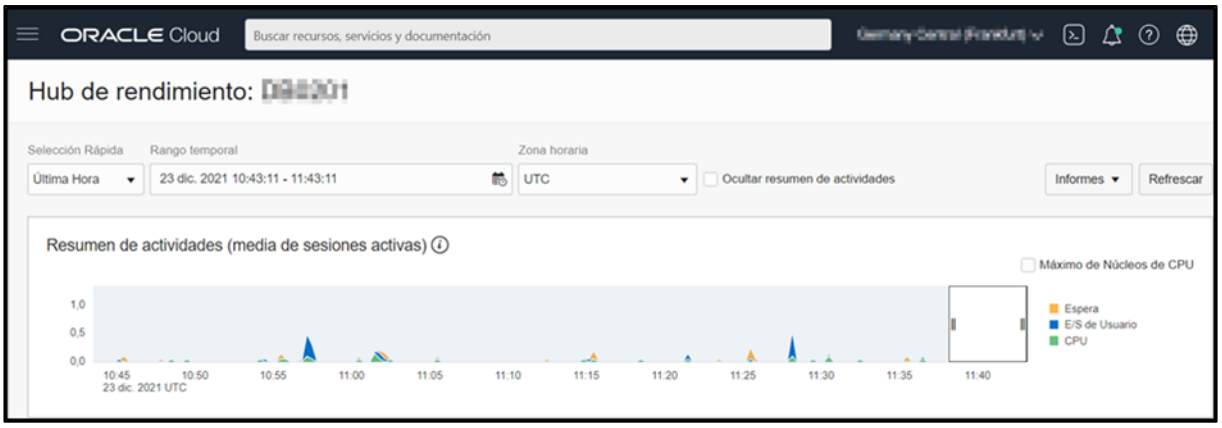
b) Haga clic en el nombre del sistema de base de datos que muestra la lista de bases de datos en el sistema de base de datos seleccionado.

c) Seleccione el nombre de la base de datos y haga clic en hub de rendimiento.

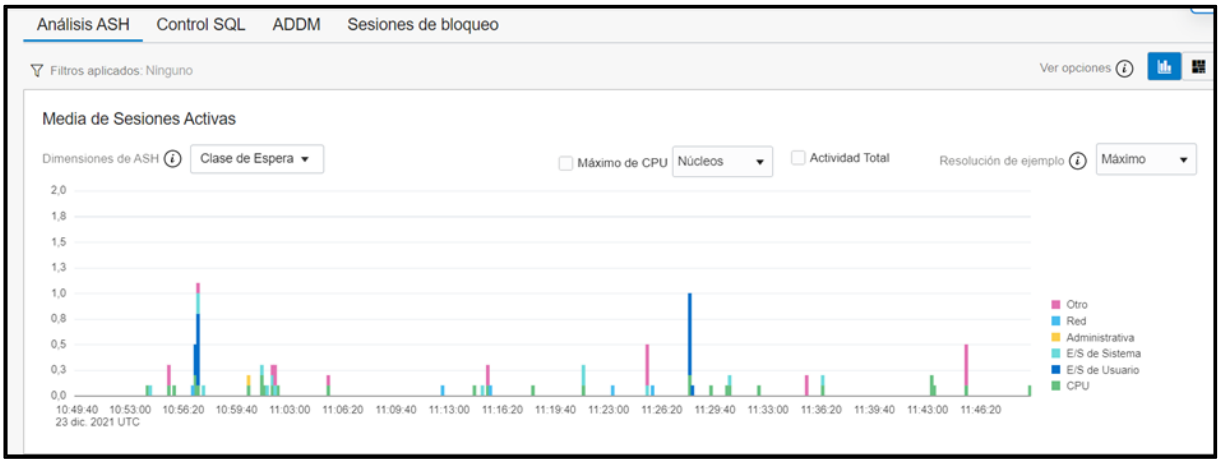


Panel de detalles de la base de datos.

d) Configure las funciones del hub de rendimiento.



Panel de Hub de rendimiento.

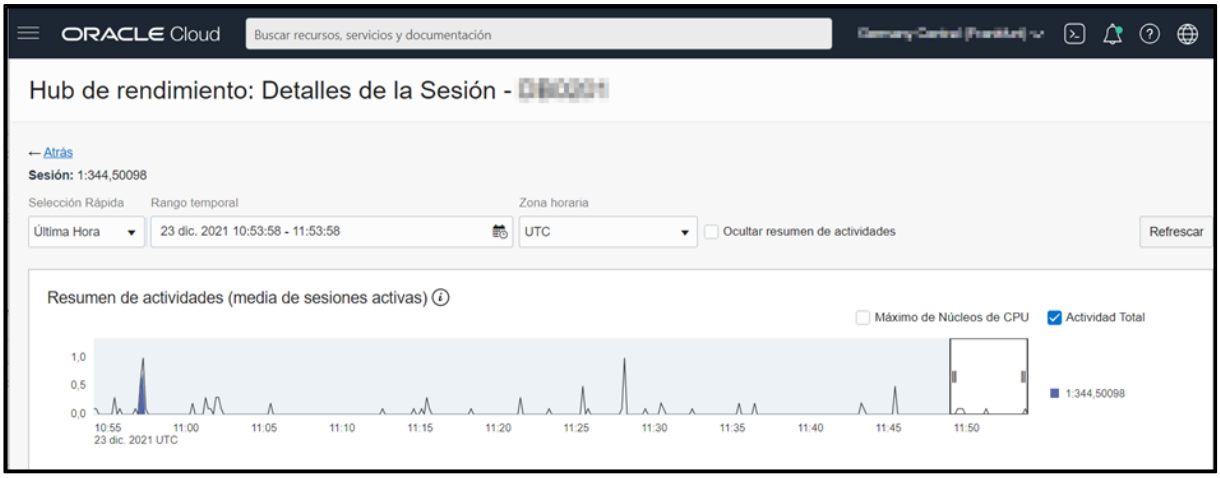


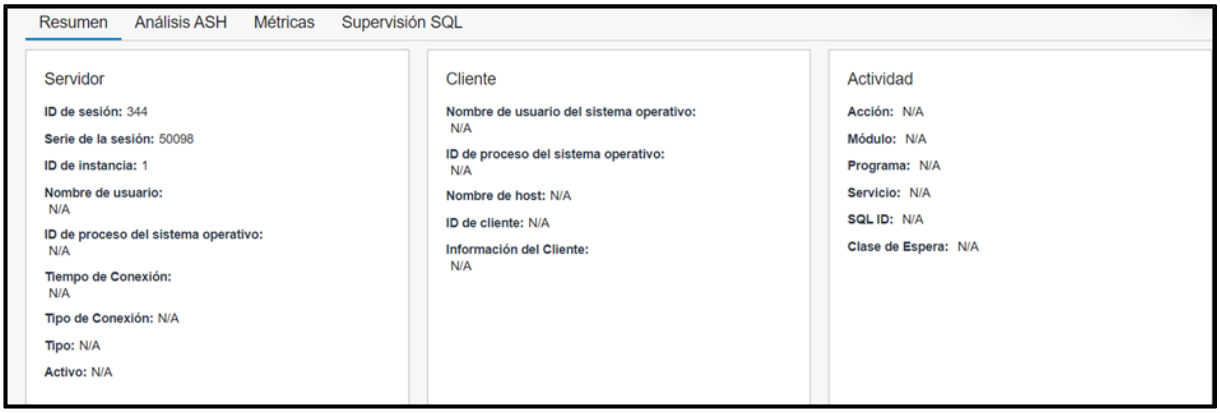
Panel de visualización de las funciones del hub. Actualmente se encuentra seleccionado Análisis ASH.

e) En el apartado de Análisis ASH, se puede configurar diferentes funciones que lanzan diversos datos que muestran el rendimiento de la base de datos. Por ejemplo, se puede seleccionar Sesión de Usuario por clase de espera y escoger una sesión concreta para analizar más datos.

Tabla de Sesión de Usuario.

f) Seleccione una sesión de usuario para ver más detalles.





Panel de detalles de la sesión escogida para analizar.

Además, dentro de las funciones del hub de rendimiento que pueden ser configuradas en cada apartado del panel principal, en concreto, en el Análisis ASH, es posible utilizar el ajuste SQL.

El ajuste SQL es un aspecto importante del ajuste del rendimiento del sistema de base de datos. El asesor de ajustes SQL es un mecanismo que resuelve problemas relacionados con sentencias SQL de rendimiento subóptimo.

El Asesor de Ajustes SQL puede tomar una o más sentencias SQL como entrada y llamar al optimizador de ajuste automático para analizar las sentencias. Los resultados se presentan en forma de conclusiones y recomendaciones.

Para obtener más información relacionada con el asesor de ajustes SQL, consultar el siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/database/oracle/oracle-database/19/tgsql/sql-tuning-advisor.html

Nota: El Asesor de Ajustes SQL solo está disponible para Oracle Database Enterprise Edition versión 12.2 y posteriores.

Para finalizar, también se puede utilizar el explorador de AWR para la supervisión de la base de datos. En el visor AWR se podrá ver, analizar y usar los datos como un repositorio central para la importación, análisis y comparación de datos AWR de otras bases de datos.

Para obtener más información relacionada con el Explorador de AWR, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/database-management/doc/use-awr-viewer-analyze-database-performance.html

1.5 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.

1.5.1 PROTECCIÓN DE LAS COMUNICACIONES

El conjunto de medidas orientadas a la protección de las comunicaciones tiene como objetivo proteger la información en tránsito, así como dotar de los mecanismos necesarios para la detección y bloqueo de intrusos en una red.

Aunque fundamentalmente tienen un alcance mayor en cuanto a la implementación de sistemas de electrónica de red y control perimetral que aporta la infraestructura en la nube de Oracle, determinadas medidas pueden ser aplicables y gestionadas desde alguno de los servicios que ofrece OCI.

1.5.1.1 PERÍMETRO SEGURO

El ENS establece que se debe disponer de un sistema cortafuegos que separe la red interna del exterior. Todo el tráfico deberá atravesar dicho cortafuegos, que sólo dejará transitar los flujos previamente autorizados. Además, en la categoría alta debe disponer de dos o más equipos, de distinto fabricante y estar redundados, tal y como dispone Oracle en su infraestructura de Nube.

Los sistemas de base de datos de OCI, creados en una subred pública pueden enviar tráfico saliente directamente a Internet a través de un Internet Gateway. Los sistemas de base de datos creados dentro de una subred privada no tienen conectividad a Internet, a menos que se configure el servicio NAT Gateway, que permite la salida a Internet, pero deniega el acceso desde el exterior a la instancia de la base de datos.

En una red virtual en la nube (VCN), puede utilizar reglas de seguridad junto con una subred privada para restringir el acceso a un sistema de base de datos. En despliegues de varios niveles, se pueden utilizar una subred privada y reglas de seguridad de VCN para restringir el acceso al sistema de base de datos desde los niveles de aplicaciones.

Las comunicaciones a base de datos se pueden reforzar mediante protocolos de seguridad como NNE o TLS/mTLS y certificados o wallets. El protocolo de seguridad de la capa de transporte mutua (mTLS) es la opción por defecto en una base de datos Autónoma.

En el siguiente enlace de Oracle dispone de información acerca de la configuración de red necesaria para sistemas de bases de datos, así como diagramas sobre las diferentes opciones de configuración según disponga la organización:

https://docs.oracle.com/es-ww/iaas/Content/Database/Tasks/network.htm

Para realizar la aplicación de parches y las copias de seguridad del sistema operativo para un sistema de base de datos en una subred privada, puede utilizar un gateway de servicio o un gateway de NAT para conectarse a los puntos finales de aplicación de parches o copia de seguridad.

El punto final privado es una representación de Gestión de bases de datos en la VCN en la que se puede acceder a la base de datos de Oracle Cloud y actúa como una VNIC con direcciones IP privadas en una subred de su elección. El punto final privado no tiene que estar en la misma subred que Oracle Cloud Database, aunque debe estar en una subred que se pueda comunicar con Oracle Cloud Database. En la Gestión de bases de datos, puede crear los siguientes tipos de puntos finales privados:

a) **Punto final privado para bases de datos Oracle Cloud de instancia única**: puede crear un máximo de cinco puntos finales privados de Gestión de bases de datos en su tenant para conectarse a bases de datos Oracle Cloud de instancia única en los sistemas de base de datos con máquina virtual. No hay ninguna restricción en el número de bases de datos de instancia única para las que puede activar Gestión de bases de datos mediante un único punto final privado. El punto final privado para bases de datos de Oracle Cloud de instancia única solo tiene una dirección IP privada.

b) **Punto final privado para bases de datos de Oracle Cloud RAC**: puede crear solo un punto final privado de Gestión de bases de datos en su tenant para conectarse a bases de datos de Oracle Cloud RAC en el sistema de base de datos de máquina virtual y el servicio de Exadata Cloud. Un punto final privado para bases de datos RAC de Oracle Cloud puede soportar hasta 15 listeners de red de acceso de cliente único (SCAN). En el caso de los sistemas de base de datos de máquina virtual, un SCAN es igual a un sistema de base de datos de máquina virtual RAC. En el caso del servicio Exadata Cloud, es igual a un clúster de VM de servicio de Exadata Cloud, independientemente del número de bases de datos RAC individuales alojadas en el clúster de VM de servicio de Exadata Cloud. El punto final privado para bases de datos Oracle Cloud de RAC tiene dos direcciones IP privadas.

c) **Punto final privado para bases de datos autónomas en infraestructura dedicada y compartida**: puede especificar que Autonomous Database utilice un punto final privado y configure una red virtual en la nube (VCN) en el tenant para usarla con el punto final privado. Además, puede configurar un punto final privado durante el aprovisionamiento o la clonación de la base de datos autónoma, o puede cambiar a un punto final privado en una base de datos existente que utilice un punto final público. La especificación de una lista de control de acceso impide el acceso a la base de datos de todas las direcciones IP que no estén en la lista de ACL. Después de especificar una lista de control de acceso, la base de datos autónoma solo aceptará conexiones desde direcciones de la lista ACL y rechazará todas las demás conexiones de cliente.

Debe tener en cuenta que puede crear un punto final privado de cada tipo en una VCN, lo que significa que puede crear un punto final privado para bases de datos de instancia única y otro para bases de datos RAC.

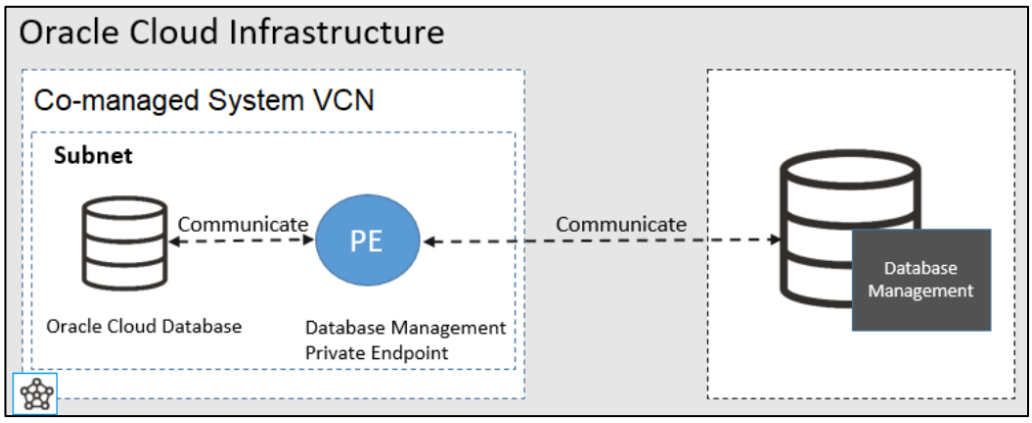


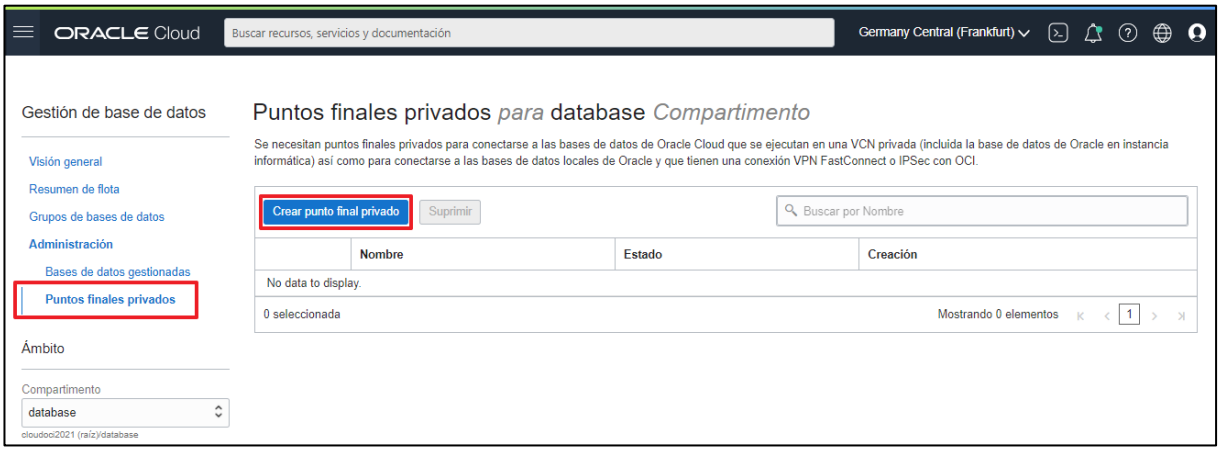
Diagrama de una visión general de cómo se comunica un punto final privado de Database Management con Oracle Cloud Database.

Para crear un punto final privado de Gestión de bases de datos, debe dirigirse al menú de OCI → Observación y gestión → Gestión de base de datos.

a) Seleccione “Administración” en el menú de la izquierda.

b) En el panel izquierdo de Administración, haga clic en “Puntos finales privados” y seleccione el compartimento de base de datos en el que desea crear el punto final privado.

c) Haga clic en “Crear punto final privado”.



d) En el cuadro de diálogo Crear punto final privado:

i. Nombre: introduzca un nombre para el punto final privado.

ii. Descripción: introduzca una descripción opcional para el punto final privado.

iii. Elegir compartimento: seleccione el compartimento en el que desea que resida el punto final privado.

iv. Utilice este punto final privado para bases de datos RAC: seleccione esta casilla de control si desea crear un punto final privado de Gestión de bases de datos para bases de datos RAC de Oracle Cloud en el sistema de base de datos de máquina virtual y el servicio Exadata Cloud.

El punto final privado de Gestión de bases de datos para bases de datos Oracle Cloud RAC es un recurso limitado y solo puede crear un punto final privado en su tenant.

v. Red virtual en la nube en [Compartimento]: seleccione la VCN en la que se puede acceder a la base de datos de Oracle Cloud. Por defecto, se muestra el compartimento seleccionado en la página "Puntos finales privados", seleccione otro compartimento, si es necesario.

vi. Subred en [Compartimento]: seleccione una subred dentro de la VCN seleccionada. En función de si el nuevo punto final privado de Gestión de bases de datos es para bases de datos de Oracle Cloud de instancia única o RAC, tomará una o dos direcciones IP privadas, respectivamente, en la subred seleccionada. Tenga en cuenta que la subred puede estar en un compartimento diferente al de la VCN; sin embargo, debe tener acceso a la subred de la base de datos en la VCN. Por defecto, se muestra el compartimento seleccionado en la página "Puntos finales privados", seleccione otro compartimento, si es necesario.

vii. Grupo de seguridad de red: opcionalmente, seleccione un NSG agregado al sistema de base de datos de máquina virtual o al clúster de máquina virtual de Exadata. También puede hacer clic en "+ Otro grupo de seguridad" para seleccionar otro NSG.

viii. Haga clic en Crear punto final privado.

Nota: NSG es obligatorio para los puntos finales privados de una base de datos Autónoma.

La opción de asociar los NSG existentes en el sistema de base de datos o clúster de VM al punto final privado de Database Management garantiza que el punto final privado pueda acceder a la base de datos. Con el NSG, puede agregar reglas de seguridad de entrada y salida para permitir la comunicación entre el punto final privado de Database Management y la base de datos de Oracle Cloud. Puede obtener más información sobre los NSG en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Network/Concepts/networksecuritygroups.htm

Puede ampliar la información sobre la realización de tareas requeridas en la gestión de base de datos en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/database-management/doc/perform-database-management-prerequisite-tasks.html

1.5.2 PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN

La protección de los soportes de la información está supeditada al uso de estos medios en la nube, bien como servicios ofrecido desde OCI (repositorios, almacenes) o recursos (VM como FileServer, backups).

El ENS establece una serie de medidas de seguridad para que las organizaciones puedan implementarlas. A continuación, se describen las siguientes medidas de seguridad y criterios de aplicación.

1.5.2.1 ETIQUETADO

Oracle Database también dispone de una opción de etiquetado de seguridad (Label Security) que permite a las organizaciones consolidar datos con diferentes requisitos de acceso (incluidos datos clasificados gubernamentales) en la misma base de datos. Implementa controles de acceso multinivel basados en la clasificación de los datos y la etiqueta de acceso del usuario de la aplicación. Esta capacidad permite el acceso a datos confidenciales asociados del tipo, proyectos de I + D, información financiera no pública o información de salud, que se aplicará dentro de Oracle Database.

Nota: Label Security está disponible en el servicio PaaS de Oracle Database en Exadata Cloud Service, Exadata Cloud at Customer para bases de datos autónomas. Para bases de datos de instancias de máquina virtual, el servicio está disponible con las licencias DBCS EE-High Perfomance y DBCS EE-Extreme Performance.

Con Label Security, los proyectos sensibles son accesibles para diferentes personas según su necesidad de conocerlos. Los compartimentos de etiquetas pueden autorizar a las personas adecuadas a ver solo los proyectos a los que tienen acceso, lo que elimina la necesidad de desarrollar o volver a codificar aplicaciones para cumplir con los requisitos de control de acceso a nivel de fila.

Los datos se pueden organizar por grupos utilizando Label Security. Todos los datos pueden residir de forma segura en las mismas tablas de una base de datos, sin la necesidad de crear tablas y bases de datos independientes para el acceso desde otras ubicaciones, oficinas, departamentos, etc. Se simplifican los informes, la gestión de datos y la seguridad de los datos.

Por último, Label Security puede consolidar datos con diferentes niveles de sensibilidad en un solo conjunto de tablas de base de datos. Por ejemplo, los niveles de sensibilidad de los datos se pueden definir como "Públicos", "Sensibles" y "Más sensibles", con la capacidad de definir más niveles según sea necesario. Dependiendo del nivel de acceso del usuario (público, empleado, gerente, ejecutivo, etc.), un usuario puede acceder a los datos hasta el nivel al que tiene acceso. De esta forma, no es necesario mantener tablas separadas para administrar los mismos datos; cada fila de datos está etiquetada con niveles. La gestión de la confidencialidad de los datos simplifica y mejora la seguridad de los datos a lo largo de su vida útil.

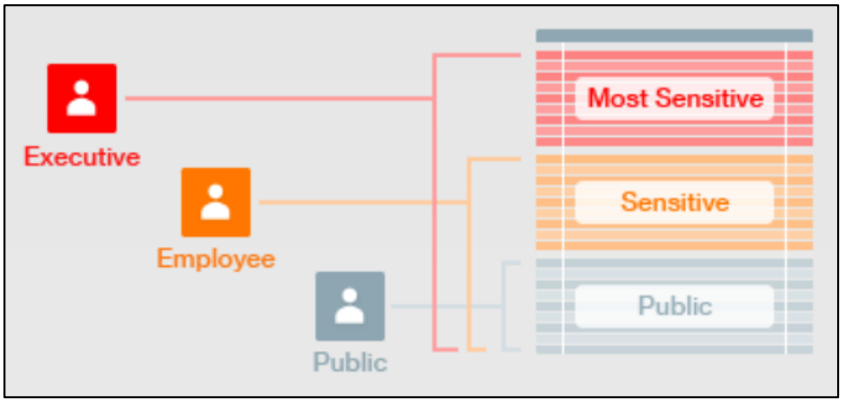


Imagen de niveles de sensibilidad asociados al acceso según tipos de usuarios.

En los sistemas de nivel alto, debe primar la seguridad por encima de la comodidad.

Puede ampliar información acerca de las Etiquetas de Seguridad de Oracle en el siguiente enlace:

https://www.oracle.com/es/database/technologies/security/label-security.html

1.5.3 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.

1.5.3.1 DATOS DE CARÁCTER PERSONAL

Esta medida se aplica cuando el sistema trate datos de carácter personal, y se estará a lo dispuesto a lo que establece las diferentes leyes, tanto a nivel nacional como dentro de la Unión Europea, competentes en protección de datos personales.

Oracle ofrece diversos servicios para la protección de la información y el tratamiento de los datos sensibles que puede almacenar una base de datos. En primer lugar, el servicio en la nube Data Safe, dispone de la función llamada enmascaramiento de datos y consiste en la sustitución permanente de los datos confidenciales por datos ficticios. Este proceso ayuda a generar datos realistas y funcionales con características similares a las de los datos originales para sustituir la información confidencial.

Esta función, pensada para entornos no relacionados con la producción, permite proteger los datos confidenciales y cumplir con las normativas de privacidad de datos. El enmascaramiento de datos confidenciales es un proceso de uso antes de utilizar los datos en entornos no relacionados con la producción, es decir, enmascara los datos en su almacenamiento. De esta forma, esta función soluciona la necesidad de compartir datos confidenciales o regulados para entornos de preproducción.

Para obtener más información relacionada con la función del enmascaramiento de datos del servicio Oracle Data Safe, consultar el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/data-safe/doc/data-masking-overview.html

Por otro lado, existen servicios a nivel de base de datos como Oracle Data Redaction y Data Masking. Oracle Data Redaction es la capacidad de transformar o enmascarar datos confidenciales en tiempo real. Permite enmascarar dinámicamente los datos que se devuelven de las consultas emitidas por las aplicaciones utilizando varios estilos de redacción diferentes.

La capacidad de Oracle Data Redaction es ideal para situaciones en las que se debe enmascarar caracteres específicos, del conjunto de resultados de consultas de información de identificación personal (PII), devueltas a ciertos usuarios de la aplicación. Aunque se recomienda tener especial cuidado con aquellas aplicaciones que realizan actualizaciones en la base de datos, ya que los datos enmascarados, se pueden volver a escribir en la base de datos.

El enmascaramiento de los datos es transparente para los usuarios de la aplicación, porque conserva el tipo de datos original y opcionalmente el formato. Los datos siguen siendo los mismos en los búferes, las cachés y el almacenamiento, por lo que también es transparente para la base de datos. Los datos que van a ser enmascarados cambian en el último minuto, justo antes de que los resultados de la consulta SQL se devuelvan a la persona que realiza dicha consulta.

Puede especificar qué usuarios de la aplicación deben ver solo los datos enmascarados al verificar la información del usuario de la aplicación, que se pasa a la base de datos a través de la función *SYS_CONTEXT*. Aunque el objetivo principal sea el enmascaramiento de los datos provenientes de entornos de producción, Oracle Data Redaction también puede ser utilizado en combinación con Data Masking, una funcionalidad que sirve para la protección de datos confidenciales en entornos de prueba y desarrollo, similar a la función de enmascaramiento de datos del servicio en la nube Data Safe.

Para obtener más información relacionada con Oracle Data Redaction, consultar el siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/database/oracle/oracle-database/19/asoag/introduction-to-oracle-data-redaction.html

Para obtener más información relacionada con Oracle Data Masking, consultar el siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/database/oracle/oracle-database/19/asoag/oracle-data-redaction-use-with-oracle-database-features.html

1.5.3.2 CALIFICACIÓN DE LA INFORMACIÓN

Para calificar la información se estará a lo establecido legalmente sobre la naturaleza de la misma. La política de seguridad establecerá quién es el responsable de cada información manejada por el sistema y recogerá, directa o indirectamente, los criterios que en cada organización determinarán el nivel de seguridad requerido.

El responsable de cada información seguirá los criterios determinados para asignar a cada información el nivel de seguridad requerido, y será responsable de su documentación y aprobación formal. El responsable de cada información en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad requerido.

Además del Servicio de Etiquetas, para cumplir con los niveles de seguridad establecidos por el ENS para la categoría alta, OCI dispone, dentro del servicio en la nube Oracle Data Safe, de la función “Detección de datos”, para detectar datos confidenciales en bases de datos de destino para su calificación.

En la protección de los datos confidenciales, el responsable de los datos primero debe conocer qué datos confidenciales posee y dónde se encuentran. La función Detección de datos inspecciona los metadatos y los datos reales de las bases de datos de Oracle para detectar datos confidenciales y proporciona resultados completos que incluyen columnas confidenciales e información relacionada.

La función Detección de datos utiliza tipos confidenciales que definen los tipos de datos que se deben buscar. Oracle Data Safe proporciona más de 125 tipos confidenciales predefinidos que puede utilizar para buscar datos confidenciales. Los tipos confidenciales abarcan datos personales que pertenecen a información biográfica, financiera, académica y de identificación, TI, asistencia sanitaria y empleo. También puede crear sus propios tipos confidenciales. Los tipos confidenciales predefinidos se organizan en categorías, lo que facilita la búsqueda y el uso de tipos confidenciales relevantes. Se indica a la función Detección de datos qué buscar y esta encuentra las columnas confidenciales que cumplen los criterios.

Para su aplicación, debe seguir un flujo de trabajo establecido en Oracle:

a) Debe tener registrada su base de datos en Data Safe o proceder al registro de la base de datos de destino en la que desea detectar datos confidenciales.

b) Recopile estadísticas de esquema en la base de datos de destino antes de ejecutar el trabajo de detección de datos para garantizar resultados precisos. Para ello, ejecute el procedimiento “dbms_stats.gather_schema_stats”.

   Puede consultar el siguiente enlace para para obtener información sobre los parámetros que puede incluir en el procedimiento “gather_schema_stats”.

   https://docs.oracle.com/en/database/oracle/oracle-database/19/arpls/DBMS_STATS.html

   El siguiente ejemplo recopila estadísticas sobre el esquema HCM1:

```
exec dbms_stats.gather_schema_stats(ownname => 'HCM1');
```

c) Cree un trabajo de detección de datos mediante el asistente de Detección de datos para detectar los datos confidenciales en la base de datos de destino y generar un modelo de datos confidenciales (MDC). En el asistente, siga estos pasos generales:

   i. Especifique la base de datos de destino y los esquemas que desea que busque la detección de datos.

   ii. Especifique los tipos confidenciales que se utilizarán para la detección de datos. Puede seleccionar tipos confidenciales individuales y/o categorías de tipos confidenciales. Opcionalmente, puede indicar a la Detección de datos que busque relaciones referenciales que no estén en el diccionario.

   iii. Ejecute el trabajo de detección de datos. La función Detección de datos identifica las columnas confidenciales examinando los nombres de las columnas, los comentarios, los ejemplos de datos, las relaciones entre objetos, etc. Además, genera un MDC.

   iv. Revise las columnas confidenciales en el MDC. Si es necesario, puede agregar y eliminar columnas confidenciales.

v. (Opcional) Antes de salir del asistente, haga clic en Atrás, modifique la selección de tipos confidenciales y vuelva a ejecutar el trabajo de detección de datos. Vuelva a revisar el MDC generado. Repita este paso hasta que considere que el MDC es preciso y está completo.

d) Analice los datos confidenciales en la base de datos de destino mediante la visualización del informe de Detección de datos.

e) Gestione el MDC:

i. Verifique el MDC con las bases de datos de destino con las que planea utilizarlo. La verificación garantiza que las bases de datos de destino tengan los esquemas y las columnas confidenciales que se muestran en el MDC.

ii. Actualice el MDC cuando sea necesario. Puede utilizar el asistente de Detección de datos para realizar actualizaciones incrementales. También puede agregar y eliminar columnas confidenciales manualmente.

iii. Para utilizar el MDC con otras bases de datos de destino, descargue y cargue el MDC en una biblioteca de Oracle Data Safe diferente.

Puede ampliar la información acerca de la función de Detección de datos en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/data-safe/doc/data-discovery.html

1.5.3.3 CIFRADO

La medida de seguridad establecida por el ENS indica que la información con un nivel alto en confidencialidad se debe cifrar tanto durante su almacenamiento como durante su transmisión. Solo debe estar en claro mientras se esté haciendo uso de ella.

Todas las bases de datos creadas en OCI se cifran utilizando el cifrado de datos transparente (TDE) a nivel de TABLESPACE. Hay que tener en cuenta que, si migra una base de datos no cifrada desde la ubicación local a OCI mediante RMAN, la base de datos migrada no se cifrará. Oracle necesita cifrar dichas bases de datos después de migrarlas a la nube.

Para obtener más información sobre cómo cifrar la base de datos con un tiempo de inactividad mínimo durante la migración, puede consultar el siguiente documento técnico, en inglés sobre la Arquitectura de máxima disponibilidad de Oracle:

https://www.oracle.com/technetwork/database/availability/tde-conversion-dg-3045460.pdf

Tenga en cuenta que los sistemas de base de datos de máquina virtual utilizan el almacenamiento de bloques de OCI en lugar del almacenamiento local. El almacenamiento de bloques está cifrado por defecto.

Los tablespaces creados por el usuario se cifran por defecto en OCI Database. En estas bases de datos, el parámetro *ENCRYPT_NEW_TABLESPACES* se establece en *CLOUD_ONLY*, donde los tablespaces creados en una base de datos de Database Cloud Service (DBCS) se cifran de forma transparente con el algoritmo AES128 a menos que se especifique un algoritmo diferente.

El administrador de Database crea una instancia local de Oracle Wallet en una instancia de base de datos creada recientemente e inicializa la clave maestra de cifrado de datos transparente (TDE).

A continuación, Oracle Wallet se configura para que sea de apertura automática. Sin embargo, puede elegir definir una contraseña para Oracle Wallet. Se recomienda utilizar una contraseña segura en la medida que establece el ENS para esta categoría alta, contemplando un mínimo de doce caracteres, y estableciendo en el tenant la complejidad para el uso al menos de letras mayúscula, letras minúsculas, números y símbolos especiales.

Oracle recomienda rotar periódicamente la clave maestra de TDE. El período de rotación establecido por el ENS es de 45 días o menos. Puede rotar la clave maestra de TDE mediante comandos de base de datos nativa ("administrar gestión de claves" en 12c, por ejemplo) o dbaascli. Todas las versiones anteriores de la clave maestra de TDE se conservan en Oracle Wallet.

El cliente puede establecer su propia clave maestra de cifrado o dejarlo en manos de Oracle mediante el servicio OCI Vault, que es una aplicación de gestión de claves que se utiliza para gestionar claves maestras de cifrado de datos transparente en los servicios de OCI públicos.

Para obtener más información relacionada con el servicio de OCI Vault, consultar el siguiente enlace de Oracle:

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

Nota: El servicio Oracle Key Vault permite la gestión de claves, claves maestras de cifrado de datos transparente para el entorno de Exadata Cloud at Customer. Para obtener más información consultar el siguiente enlace de Oracle: https://docs.oracle.com/es-ww/iaas/autonomous-database/doc/manage-encryption-keys.html

1.5.3.4 COPIAS DE SEGURIDAD (BACKUP)

Según establece el ENS, se deben realizar copias de seguridad que permitan la recuperación de datos perdidos de manera accidental o intencionadamente, con una antigüedad determinada. Estas copias deben poseer el mismo nivel de seguridad que los datos originales en lo que se refiere a la integridad, confidencialidad, autenticidad y trazabilidad.

La realización de copias de seguridad del sistema de base de datos es un aspecto clave de cualquier entorno de base de datos Oracle. Todas las copias de seguridad de Oracle se cifran con la misma clave maestra utilizada para el cifrado de datos transparente (TDE). Puede almacenar copias de seguridad en la nube o en el almacenamiento local. Cada destino de copia de seguridad tiene ventajas, desventajas y requisitos que debe tener en cuenta, como se describe a continuación:

a) Object Storage (recomendado):
   i. Las copias de seguridad se almacenan en OCI Object Storage.
   ii. Durabilidad: alta
   iii. Disponibilidad: alta
   iv. Ratio de copia de seguridad y recuperación: media

v. Ventajas: alta durabilidad, rendimiento y disponibilidad.

b) Almacenamiento local:

i. Las copias de seguridad se almacenan localmente en el área de recuperación rápida del sistema de base de datos.

ii. Durabilidad: baja

iii. Disponibilidad: media

iv. Ratio de copia de seguridad y recuperación: alta

v. Ventajas: copia de seguridad optimizada y rápida recuperación a un momento dado.

vi. Desventajas: si el sistema de base de datos deja de estar disponible, la copia de seguridad también deja de estar disponible.

A la hora de realizar las copias de seguridad, Oracle ofrece la posibilidad de realizarlas de forma gestionada o no gestionada. La diferencia entre ellas es que las copias gestionadas se realizan desde la propia base de datos en OCI como una funcionalidad más de la misma, y las no gestionadas se realizan mediante Oracle Recovery Manager (RMAN).

Nota: No se puede usar RMAN para las bases de datos autónomas.

A continuación, se detallan brevemente los requisitos y las funciones básicas de cada una de ellas.

Gestión de copias de seguridad "gestionadas" por Oracle

Para la gestión de copias de seguridad gestionadas en una base de datos se requiere lo siguiente:

a) Permisos de seguridad mediante una política para el acceso a los recursos y el compartimento de la base de datos a gestionar.

b) Acceso al servicio OCI Object Storage, incluida la conectividad al punto final Swift correspondiente de Object Storage. Oracle recomienda utilizar un gateway de servicio con VCN para activar este acceso. Esta información puede encontrarla en el punto 1.5.1.1 PERÍMETRO SEGURO de este documento.

Al activar la función Copia de seguridad automática de una base de datos, el servicio crea lo siguiente de forma continua:

a) Copia de seguridad semanal de nivel 0, creada generalmente en un día específico del fin de semana. Una copia de seguridad de nivel 0 equivale a una copia de seguridad completa.

b) Copias de seguridad diarias de nivel 1, que son copias de seguridad incrementales creadas cada día durante los seis días siguientes al día de la copia de seguridad de nivel 0.

Nota: Las copias de seguridad de nivel 0 y nivel 1 se almacenan en Object Storage y tienen asignado un OCID.

c) Copias de seguridad de redo log archivadas en curso (con una frecuencia mínima de cada 60 minutos). Esta copia de seguridad difiere de las copias de seguridad automáticas de nivel 0 y nivel 1, ya que se basa en datos de log y no tiene asignado un OCID.

Las copias de seguridad incrementales automáticas (nivel 0 y nivel 1) se mantienen en Object Storage durante 30 días por defecto, aunque puede modificar ese valor para predefinir 7, 15, 30, 45 o 60 días. El sistema suprime automáticamente las copias de seguridad incrementales al final del período de retención seleccionado. Una vez al día, un trabajo de Oracle Scheduler descarta los archivos de auditoría y rastreo de más de 30 días (o el intervalo especificado por el usuario si procede). También puede desactivar el trabajo de Scheduler si desea conservar estos archivos de forma permanente utilizando los siguientes comandos DBCLI para ello:

Si su organización tiene establecido un periodo diferente de retención al establecido por la categoría del ENS, puede cambiar el periodo de retención del valor por defecto de 30 días mediante el siguiente comando:

```
dbcli update-database -in <dbName> -lr <number_of_days_to_retain_files>
```

Ejemplo:

```
dbcli update-database -in inventorydb -lr 15
```

También puede desactivar el trabajo de descarte diario de Scheduler para archivos de auditoría y rastreo antiguos para realizar un trabajo manual de retención de estas copias mediante el siguiente comando:

```
dbcli update-schedule -i <schedulerID> -d
```

Ejemplo:

```
dbcli update-schedule -i 5678 -d
```

Puede crear una copia de seguridad completa de la base de datos en cualquier momento, a menos que la base de datos asuma el rol en espera en una asociación de Data Guard.

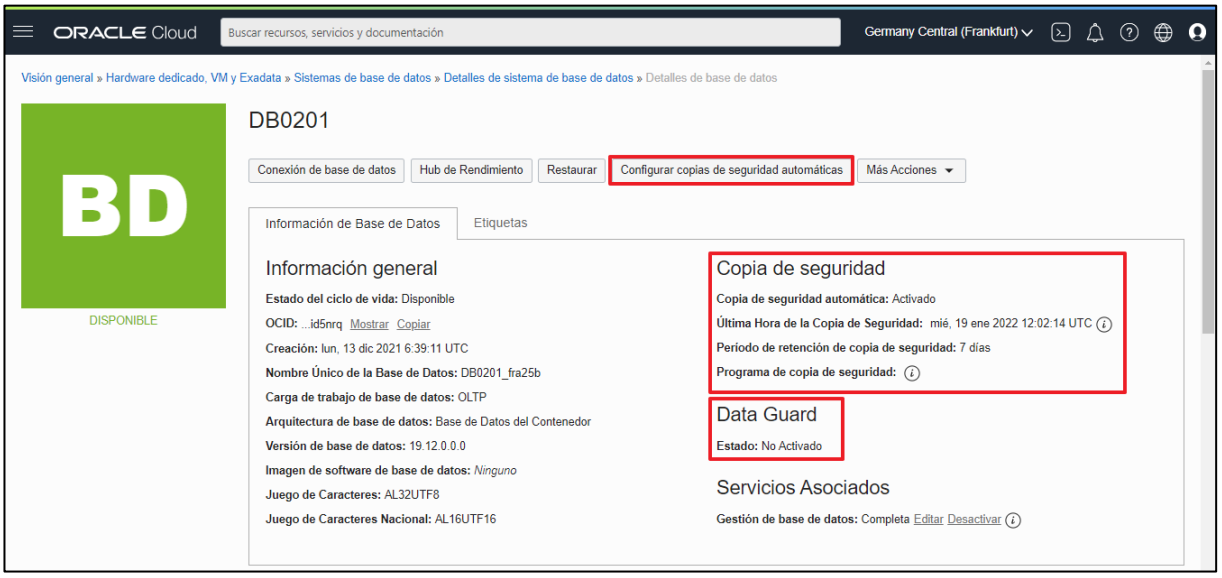


Imagen BD con la información de la activación de la copia de seguridad automática y el estado en Data Guard.

Imagen de la Configuración de copia de seguridad automática en OCI.

Puede ampliar la información de las copias de seguridad en bases de datos mediante el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Database/Tasks/backingupOS.htm

Con los servicios PaaS de bases de datos, también se pueden gestionar las copias de seguridad de forma automática (gestionada) en los sistemas de Exadata Cloud Service y Autonomous DB. Puede encontrar información al respecto mediante los siguientes enlaces en inglés de Oracle:

Para Exadata Cloud Service:

https://docs.oracle.com/en/cloud/paas/exadata-cloud/csexa/backing.html

Para Autonomous DB:

https://docs.oracle.com/en/cloud/paas/autonomous-database/adbsa/backup-intro.html

Gestión de copias de seguridad "no gestionadas" mediante RMAN y Oracle Data Pump

Dentro de los servicios de OCI, puede utilizar Oracle Recovery Manager (RMAN) para realizar copias de seguridad periódicas de las bases de datos de Database. Estas copias también pueden ser almacenadas en el almacenamiento local (volúmenes en bloque, por ejemplo) o en OCI Object Storage. RMAN cifra cada copia de seguridad de una base de datos con una clave de cifrado única. En el modo transparente, la clave de cifrado se almacena en Oracle Wallet. Las copias de seguridad de RMAN de Object Storage requieren que se configure el Servicio Gateway (SGW) y los grupos de seguridad de red de VCN o las listas de seguridad para permitir el acceso seguro a Object Storage.

Para ampliar la información acerca de la realización de copias de seguridad mediante RMAN, puede seguir el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Database/Tasks/backingupOSrman.htm

Si desea utilizar la consola de comandos CLI de Oracle, puede encontrar información en el siguiente enlace:

https://docs.oracle.com/es-ww/iaas/Content/Database/Tasks/backingupFRA.htm

Para finalizar, la tecnología de Oracle Data Pump permite el movimiento de datos y metadatos a muy alta velocidad de una base de datos a otra. Los backups manuales pueden realizarse mediante DataPump de manera artesanal, usando las utilidades de exportación e importación de Data Pump, para descargar la información estructural (metadatos) en el archivo de volcado.

Para obtener más información relacionada con la tecnología de Oracle Data Pump, consultar el siguiente enlace en inglés:

https://docs.oracle.com/en/database/oracle/oracle-database/19/sutil/oracle-data-pump-overview.html

2. GLOSARIO

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

Término	Definición
ACFS	ASM Cluster File System.
ACL	Access Control Lists (Listas de control de acceso).
ADW	Autonomous Data Warehouse.
AES	Advanced Encryption Standard (Estándar de cifrado avanzado).
APEX	Oracle Application Express (Aplicaciones express de Oracle).
API	Application Programming Interface (Interfaz de Programación de Aplicaciones).
ASH	Active Session History (Historial de sesiones activas).
ASM	Automatic Storage Management (gestión automática de almacenamiento).
ATP	Autonomous Transaction Processing.
Bucket	Cubo o almacén de datos ilimitado, de alto rendimiento, duradero y seguro.
CCN	Centro Criptológico Nacional.
CDB	Container DataBase (Bases de Datos de Contenedor).
CLI	Command Line Interface (Interfaz de Línea de Comandos).
DB	Database (Base de datos).
DBCS	Database Cloud Service (Servicio de Base de datos en la Nube).
E-C@C	Exadata Cloud at Customer (Nube de Exadata para Clientes).
ENS	Esquema Nacional de Seguridad.
FRA	Fast Recovery Area (Área de recuperación rápida).
Hub	Concentrador.
IaaS	Infrastructure as a Service (Infraestructura como Servicio).
ILOM	Integrated Lights-Out Management (administrador integrado de luces apagadas).
JSON	Javascript Object Notation.
KMS	Key Management Service (Servicio de Gestión de Claves).
MDC	Modelo de datos confidenciales.
mTLS	Mutual TLS.
MySQL	Sistema de base de datos relacional.
NNE	Native Network Encryption (Cifrado de red nativo).
NSG	Network Security Group (Grupo de seguridad de red).
O-C@C	Oracle Cloud at Customer (Nube de Oracle para Clientes).
OCI	Oracle Cloud Infrastructure (Infraestructura de Nube de Oracle).
OCI IAM	Oracle Cloud Identity and Access Management (Gestión de Identidad y Acceso).
OCID	Oracle Cloud Identifier (Identificador de Oracle en la nube).
OCPU	Oracle CPU.

Término	Definición
OKV	Oracle Key Vault (Almacén de Claves de Oracle).
PaaS	Platform as a Service (Plataforma como Servicio).
PDB	Production DataBase (Bases de Datos de Conexión).
PDU	Power Distribution Unit (Unidades de distribución de energía).
PMEM	Módulos de memoria persistente.
RAC	Real Application Clusters (Clúster de Aplicación Real).
RDMA	Remote Direct Memory Access (Acceso remoto directo a memoria).
RMAN	Oracle Recovery Manager.
RoCE	RDMA over Ethernet Converged (RDMA sobre ethernet convergente).
RPM	Red Hat Package Manager (Herramienta de administración de paquetes para GNU/Linux).
SDK	Software Development Kits (Paquetes de Desarrollo de Software).
Shape	Unidad o Forma de una plantilla que determina la cantidad de CPU, memoria y otros recursos que se asignan a una instancia.
TDE	Transparent Data Encryption (Cifrado de Datos Transparente).
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 de Nube Virtual).
VM	Virtual Machine (Máquina Virtual).
VNIC	Virtual Network Interface Card (Tarjeta de Interfaz de Red Virtual).
YUM	Yellow dog Updater, Modified (Herramienta libre de gestión de paquetes para sistemas Linux basados en RPM).

3. 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 federadas y locales de OCI IAM para la administración y gestión de los recursos de las bases de datos.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se ha verificado la complejidad de la contraseña de la base de datos a través del script PL/SQL proporcionado por la base de datos de Oracle.	☐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 Database para instancias de máquinas virtuales.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.acc.3	Segregación de funciones y tareas	Aplica	Cumple
	Se han creado las cuentas de los usuarios administradores y gestores de las bases de datos.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
	Se ha habilitado Database Vault en las bases de datos para los usuarios propietarios y gestores.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.acc.4	Proceso de gestión de derechos de acceso	Aplica	Cumple
	Se ha definido el grupo de gestión de las bases de datos y su política para ello sin posibilidad de eliminación.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se han aplicado las políticas para los administradores de las bases de datos.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se han definido las políticas de los grupos Administradores de Seguridad y Auditores de Seguridad para gestionar las zonas de seguridad en los compartimentos de bases de datos.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se han aplicado las políticas para las Zonas de seguridad.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
OP.EXP	EXPLOTACIÓN		
op.exp.1	Inventario de activos	Aplica	Cumple
	Se han configurado etiquetas personalizadas para todos los servicios de OCI Database.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.exp.4	Mantenimiento	Aplica	Cumple
	Se ha comprobado el nivel de parcheado de las bases de datos.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.exp.7	Gestión de incidentes	Aplica	Cumple
	Se han registrado las bases de datos en Data Safe.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.exp.8	Registro de la actividad de los usuarios	Aplica	Cumple
	Se ha activado Data Safe para registrar las bases de datos en el servicio.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
	Se han revisado los registros de la Auditoría de actividad para verificar que no hubiera accesos no autorizados a las bases de datos.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.exp.9	Registro de la gestión de incidentes	Aplica	Cumple
	Se han revisado los Problemas identificados en Cloud Guard relacionados con las bases de datos.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.exp.11	Protección de claves criptográficas	Aplica	Cumple
	Se ha creado algún Almacén de claves específico para Base de datos.	☐Si ☐No	☐Si ☐No
		Observaciones:	
OP.MON	MONITORIZACIÓN DEL SISTEMA		
op.mon.1	Detección de intrusión	Aplica	Cumple
	Se han definido Alarmas en el Servicio Monitoring (Supervisión) para las bases de datos.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se han revisado las Recomendaciones relacionadas con los problemas de base de datos del servicio de Cloud Guard, para su aplicación.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
	Se ha configurado el Servicio Detección de anomalías con la Política de permisos a usuarios y/o grupos.	☐Si ☐No	☐Si ☐No
		Observaciones:	
mp.eq.2	Sistema de métricas	Aplica	Cumple
	Se han revisado las métricas de cada base de datos para detectar anomalías.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se ha activado el Servicio de Gestión de Base de datos.	☐Si ☐No	☐Si ☐No
		Observaciones:	
MP	MEDIDAS DE PROTECCIÓN		
MP.COM	PROTECCIÓN DE LAS COMUNICACIONES		
mp.com.1	Perímetro seguro	Aplica	Cumple
	Se han gestionado los puntos finales en las VNC destinadas a las bases de datos.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
MP.SI	PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN		
mp.si.1	Etiquetado	Aplica	Cumple
	Se han configurado etiquetas de seguridad (Label Security) para los datos sensibles de la base de datos.	☐Si ☐No	☐Si ☐No
		Observaciones:	
MP.INFO	PROTECCIÓN DE LA INFORMACIÓN		
mp.info.1	Datos de carácter personal	Aplica	Cumple
	Se ha configurado la función de enmascaramiento de datos del servicio Data Safe de Oracle, previo registro de las bases de datos en el servicio.	☐Si ☐No	☐Si ☐No
		Observaciones:	
mp.info.2	Calificación de la información	Aplica	Cumple
	Se ha configurado la Detección de datos en el Servicio Data Safe de Oracle, previo registro de las bases de datos en el servicio.	☐Si ☐No	☐Si ☐No
		Observaciones:	
mp.info.3	Cifrado	Aplica	Cumple
	Se ha configurado el cifrado en tránsito en las instancias de OCI.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
	Se ha configurado el cifrado estático en el almacenamiento de OCI.	☐Si ☐No	☐Si ☐No
		Observaciones:	
mp.info.9	Copias de seguridad	Aplica	Cumple
	Se han activado las copias de seguridad en todas las bases de datos. • Gestionadas. • No gestionadas (RMAN).	☐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