centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 889F

Guía de Configuración segura para Oracle C@C Sistemas Exadata - Autonomous DB

ABRIL 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 15:52:50 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-137-4

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.

abril de 2022

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

TABLA DE ILUSTRACIONES

1. GUÍA DE CONFIGURACIÓN SEGURA PARA ORACLE C@C SISTEMAS EXADATA - AUTONOMOUS DB

1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA

Esta guía muestra el despliegue y configuración de los servicios de Oracle Cloud at Customer (O-C@C) para cargas de trabajo en la nube privada de Oracle siguiendo las exigencias del Esquema Nacional de Seguridad (ENS).

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

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

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

1.2 DEFINICIÓN DEL SERVICIO C@C SISTEMAS EXADATA - AUTONOMOUS DB

O-C@C, es la nube de última generación diseñada para ejecutar cualquier aplicación de forma más rápida y segura por menos.

El marco de adopción de C@C 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 Sistemas Exadata y Autonomous DB para la infraestructura de la nube de Oracle, la cual dispone de la Certificación de Conformidad con el Esquema Nacional de Seguridad.

Por otro lado, existen escenarios por los cuales una nube pública no es una opción viable para la soberanía de los datos o para mantener un control total de la infraestructura de red y seguridad de una organización.

O-C@C es la solución en la nube que permite a las organizaciones el aislamiento completo de su infraestructura, cumpliendo con los principales marcos de seguridad. El hardware, propiedad de Oracle, se despliega en el propio centro de datos del cliente, brindando el control de los datos y los sistemas de una organización que puede usar sus propios firewalls, balanceadores de carga y VPN, cumpliendo con los SLA específicos en sus propios centros de datos.

Además, las organizaciones se aseguran de que no están lidiando con problemas de latencia o bien que cumplan con el deseo de disponer una infraestructura dedicada en su propio centro de datos, o si la actividad económica de la organización se desarrolla en un país distinto al país donde reside su propio centro de datos.

Finalmente, dentro de los modelos que ofrece C@C, esta guía se centrará en el modelo de Plataforma como Servicio (PaaS).

a) **PaaS**: es un conjunto de servicios que permite crear y gestionar aplicaciones modernas en la era digital, on-premises o en la nube. Proporciona la infraestructura y los componentes que permiten a los desarrolladores, administradores de TI y usuarios crear, integrar, migrar, implementar, proteger y administrar sistemas y aplicaciones. Para ayudar a mejorar la productividad, PaaS ofrece componentes de programación listos para usar que permiten a los desarrolladores integrar nuevas características en sus aplicaciones, incluidas tecnologías innovadoras como artificial Intelligence (AI) (Inteligencia artificial), chatbots, blockchain y el Internet of Things (IoT). Esto también incorpora suites de herramientas de desarrollo de aplicaciones, lo que incluye servicios nativos en la nube, Kubernetes, Docker, motores de contenedor y mucho más.

También se recogen las medidas de aplicación técnica que marca el ENS para la Categoría Alta, según las medidas a establecer en cada una de las tareas de Sistemas Exadata de las que trata este documento, disponiendo para ello de varios servicios que se detallan a continuación.

1.3 SERVICIOS DE SISTEMAS EXADATA

Exadata Cloud at Customer (E-C@C) es uno de los servicios de base de datos que se ofrecen en Oracle Cloud Infrastructure (OCI) para soluciones de Oracle Database gestionadas conjuntamente y autónomas.

C@C permite mantener el control absoluto sobre los datos al tiempo que se aprovecha las capacidades combinadas de Oracle Exadata y OCI gestionadas por Oracle. También, permite aplicar toda la potencia combinada en su propio centro de datos, donde tendrá acceso completo a las funciones y capacidades de Oracle Database junto con el rendimiento inteligente y la escalabilidad de Oracle Exadata, pero con Oracle como propietario y gestor de la infraestructura de Exadata.

Cada configuración del sistema Oracle E-C@C contiene servidores Oracle Exadata Database y Oracle Exadata Storage Servers que se interconectan mediante una red de tejido RDMA de alta velocidad, baja latencia y software inteligente.

Por un lado, Oracle E-C@C usa tecnología de virtualización para separar los componentes gestionados por el cliente y los componentes gestionados por Oracle en cada servidor de base de datos. Además, se dispone de privilegio *root* para las máquinas virtuales del servidor de base de datos Oracle Exadata, por lo que puede gestionar el software del sistema Oracle Database, Oracle Grid Infrastructure y Oracle Exadata. Sin embargo, no se dispondrá de acceso administrativo para el hardware del servidor de base de datos física, el cual administra exclusivamente Oracle.

Por otro lado, Oracle E-C@C utiliza servidores Oracle Exadata Storage Server para el almacenamiento de las bases de datos. El almacenamiento se asigna a grupos de discos gestionados por Oracle Automatic Storage Management (Oracle ASM). Al igual que el software del sistema de Oracle Exadata citado anteriormente, se tendrá acceso administrativo completo a los grupos de discos de Oracle ASM, pero siendo Oracle quien administre el hardware y el software de Oracle Exadata Storage Server.

Finalmente, Oracle también se encarga de gestionar otros componentes de infraestructura como switches de red, unidades de distribución de energía (PDU) y la interfaz de gestión integrada de apagado (ILOM).

Para obtener más información relacionada con las licencias de software de Oracle Database necesarias, la facturación por segundos para el uso de OCPU y las versiones y ediciones disponibles de base de datos de E-C@C, consultar el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/exadata/doc/ecc-system-config-options.html

1.4 SERVICIOS AUTONOMOUS DB EN SISTEMAS EXADATA

Oracle Autonomous Database E-C@C combina los beneficios de un sistema de gestión de bases de datos autogestionado, autoprotegido y autorreparable con la seguridad y el control que ofrece durante el despliegue de forma segura y local tras un cortafuegos.

Una vez adquirido Autonomous DB en Oracle E-C@C y aprovisionado el hardware de la infraestructura de Exadata y el recurso de Oracle Cloud, varios tipos de recursos adicionales comenzarán a estar disponibles en OCI → Exadata Cloud at Customer → Clusters de VM de Exadata autónomos → Bases de datos de contenedor autónomas y bases de datos autónomas.

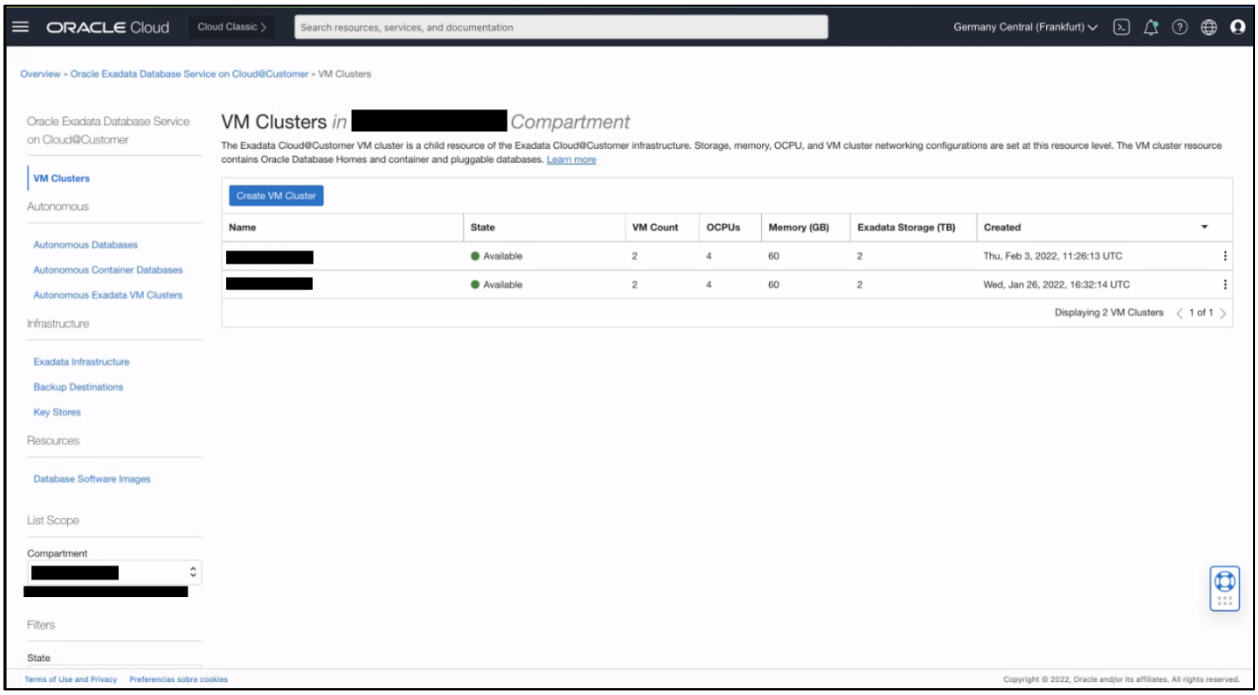

Fig. 1-VM Clústers en Oracle Exadata Database Service C@C

Oracle Autonomous Database E-C@C cuenta con un modelo de arquitectura de base de datos de cuatro niveles que utiliza la arquitectura de multitenant de la base de datos de Oracle.

Cada nivel de modelo de arquitectura se corresponde con uno de los siguientes tipos de recursos:

a) **Infraestructura de Oracle E-C@C:** rack de hardware que incluye nodos de recursos de cómputo para base de datos y servidores de almacenamiento unidos por una red RoCE de alta velocidad, baja latencia y software inteligente de Exadata.

b) **Clústeres de VM autónomos:** en la infraestructura de E-C@C, un clúster de máquina virtual (VM) es un juego de VM simétricas en todos los nodos de recursos de cómputo. La base de datos y el contenedor autónomos ejecutan todas las VM en todos los nodos, lo que posibilita una configuración de alta disponibilidad. También se permite el Node subsetting para crear clústeres VM en un subconjunto de los nodos.

   Para poder crear bases de datos autónomas en la infraestructura de E-C@C, se debe crear una red de clústeres de VM autónomos, que deben asociarse a un clúster de VM.

   Para obtener más información sobre la gestión de clústeres de VM de Exadata autónomos, consultar el siguiente enlace de Oracle:

   https://docs.oracle.com/es-ww/iaas/exadata/doc/adb-manage-aevmc.html

c) **Base de datos de contenedor autónoma:** proporciona un contenedor para varias bases de datos autónomas.

   Para obtener más información relacionada con la gestión de bases de datos de contenedor autónomas, consultar el siguiente enlace de Oracle:

   https://docs.oracle.com/es-ww/iaas/exadata/doc/adb-managing-acd.html

d) **Base de datos autónoma:** puede crear varias bases de datos autónomas dentro de la misma base de datos de contenedor autónoma, pudiendo configurarse Oracle Autonomous Database para cargas de trabajo transaccionales o analíticas de Data Warehouse.

   Para obtener más información sobre la gestión de bases de datos autónomas, consultar el siguiente enlace de Oracle:

   https://docs.oracle.com/es-ww/iaas/exadata/doc/adb-managing-adb.html

1.5 MODELO DE SEGURIDAD COMPARTIDO

Oracle ofrece la mejor tecnología de seguridad y procesos operativos para la protección de los servicios en la nube empresarial. Sin embargo, para que ejecute de forma segura las cargas de trabajo en sistemas E-C@C, debe conocer las responsabilidades de seguridad y conformidad del modelo de seguridad compartido y gestionado conjuntamente por el cliente y Oracle. El despliegue de E-C@C se divide en dos áreas principales de responsabilidades:

a) Servicios accesibles al cliente:

   i. Máquinas virtuales (VM) accesibles al cliente.

   ii. Servicios de base de datos accesibles al cliente.

b) Infraestructura gestionada por Oracle:

i. Unidades de distribución de energía (PDU).

ii. Switches de gestión fuera de banda (OOB) → Switches RoCE.

iii. Servidores de base de datos de Exadata físicos.

Los clientes controlan y supervisan el acceso a los servicios del cliente, incluido el acceso de red a sus VM (a través de firewalls y VLAN de capa 2 implementados en la VM del cliente), la autenticación para acceder a la VM y la autenticación para acceder a las bases de datos que se ejecutan en las VM. Oracle controla y supervisa el acceso a los componentes de infraestructura gestionados por Oracle. El personal de Oracle no está autorizado para acceder a los servicios del cliente, incluidas las VM y las bases de datos del mismo.

A su vez, los clientes acceden a las bases de datos de Oracle que se ejecutan en E-C@C a través de una conexión de capa 2 (VLAN etiquetada) que va desde el equipo del cliente hasta las bases de datos que se ejecutan en la VM del cliente que utiliza métodos de conexión estándar de Oracle Database, como Oracle Net en el puerto 1521. Los clientes acceden a la VM que ejecuta las bases de datos de Oracle a través de métodos estándar de Oracle Linux, como el SSH basado en token en el puerto 22.

A continuación, se muestra una tabla resumen de las responsabilidades tanto de Oracle como del cliente en las siguientes categorías, tanto para la plataforma de Oracle Cloud, como en las instancias de cliente:

Categorías	Sujeto	Oracle Cloud Platform	Instancias de cliente/inquilino
Supervision.	Operaciones de Oracle Cloud.	Infraestructura, control plane, fallos de hardware, disponibilidad y capacidad.	Disponibilidad de infraestructura para soportar la supervisión por parte del cliente de los servicios del cliente.
	Cliente.	Proporcionar acceso de red para soportar la supervisión y la recopilación de logs de infraestructura de Oracle.	Supervisión del sistema operativo, las bases de datos y las aplicaciones del cliente.
Gestión y resolución de incidentes.	Operaciones de Oracle Cloud.	Gestión y solución de incidentes. Piezas de recambio y envío de servicios de campo.	Soporte para cualquier incidente relacionado con la plataforma subyacente.
	Cliente.	Ayuda de diagnóstico in situ.	Gestión y resolución de incidentes de las aplicaciones del cliente.

Categorías	Sujeto	Oracle Cloud Platform	Instancias de cliente/inquilino
Gestión de parches.	Operaciones de Oracle Cloud.	Aplicación proactiva de parches de hardware, pila de control de IaaS/PaaS.	Ubicación temporal de los parches disponibles, por ejemplo, el juego de parches de Oracle Database.
	Cliente.	Proporcionar acceso de red para soportar la prestación de los parches.	Testear y aplicar parches en instancias de inquilino.
Copia de Seguridad y restauración.	Operaciones de Oracle Cloud.	Copia de Seguridad y recuperación de control plane y la infraestructura, recreación de VM del cliente.	Proporcionar VM en ejecución y a las que pueda acceder el cliente.
	Cliente.	Proporcionar acceso de red para soportar la prestación de automatización en la nube.	Instantáneas/copia de seguridad y recuperación de datos de IaaS y PaaS del cliente con capacidad nativa de Oracle o de terceros.
Soporte en la nube.	Operaciones de Oracle Cloud.	Respuesta y resolución de solicitudes de Servicio relacionadas con problemas de la infraestructura o la suscripción.	Respuesta y resolución de solicitudes de servicio.
	Cliente.	Enviar solicitudes de Servicio a través de My Oracle Support (MOS).	Enviar solicitudes de servicio a través del portal de soporte.

2. DESPLIEGUE SEGURO PARA ORACLE C@C

2.1 APROVISIONAMIENTO DE SISTEMAS ORACLE EXADATA C@C

El aprovisionamiento de un sistema Oracle E-C@C es un proceso colaborativo entre el cliente y Oracle. El hardware necesario para ejecutar Oracle Cloud en la organización es instalado y configurado por los ingenieros de Oracle Field Service en el propio centro de datos de la organización.

No obstante, antes de la entrega del hardware contratado para el servicio de C@C, se deben realizar las siguientes tareas para garantizar que el centro de datos esté listo para albergar la infraestructura. Se puede consultar los requisitos en el siguiente enlace de la documentación oficial de Oracle en inglés:

https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmin/exadata-site-requirements.html

Una vez revisados los requisitos necesarios, el proceso de configuración del sistema se realiza en la siguiente secuencia:

a) Se crea la infraestructura de Oracle E-C@C una vez llegue el hardware a su centro de datos. Para ello, un equipo de ingenieros de Oracle Customer Support realizará labores de instalación y configuración tanto del hardware como el software y el gateway de la infraestructura C@C.

b) Se genera un archivo que será proporcionado al fabricante Oracle y reunirá los detalles de configuración de la infraestructura.

c) El sistema Oracle E-C@C se instala físicamente en el centro de datos.

d) Oracle utiliza el archivo de configuración de la infraestructura para realizar la configuración inicial del sistema. Al finalizar esta tarea, Oracle proporciona un archivo de activación.

e) La infraestructura de E-C@C se activa mediante el archivo de activación suministrado por Oracle.

Una vez finalizado el proceso de aprovisionamiento, el sistema de O-C@C estará listo para su uso.

Nota: Evite introducir información confidencial al asignar descripciones, etiquetas o nombres fáciles de recordar a los recursos en la nube mediante la consola de OCI, las API o la interfaz de línea de comandos.

Por un lado, puede usar el asistente de despliegue de Oracle E-C@C para recopilar los detalles de configuración y crear el archivo de configuración de la infraestructura de Oracle E-C@C. El archivo de configuración controla los procesos de instalación y configuración automáticos de la infraestructura de Oracle E-C@C.

Para obtener más información relacionada con el asistente de despliegue de Oracle E-C@C, consultar el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/exadata/doc/ecc-deployment-assistant.html

Por otro lado, puede usar la consola para aprovisionar la infraestructura de E-C@C. Para ello, puede consultar el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/exadata/doc/ecc-provisioning.html

Finalmente, puede aumentar de manera dinámica la capacidad de almacenamiento para satisfacer los crecientes requisitos de carga de trabajo. La ampliación de la capacidad de almacenamiento a demanda se corresponde con una ampliación de la infraestructura de servidores de almacenamiento adicionales, sin afectar a las cargas de trabajo en ejecución actuales de los servidores de almacenamiento recién agregados al clúster de VM ya desplegado.

Para obtener más información relacionada con la expansión de almacenamiento flexible, puede consultar el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/exadata/doc/ecc-overview-elastic-storage.html

2.2 APROVISIONAMIENTO DEL PRIMER CLÚSTER DE VM EN EXADATA C@C

El clúster de VM proporciona el enlace necesario entre la infraestructura de E-C@C y las bases de datos Oracle que vayan a ser desplegadas.

La red de clúster de VM especifica los recursos de red, tales como direcciones IP y nombres de host, que residen en su centro de datos corporativo y están asignados a E-C@C. La red de clúster de VM incluye definiciones para la red de cliente de Exadata y la red de copia de seguridad de Exadata. La red de cliente y la red de copia de seguridad contienen las interfaces de red que utiliza para conectarse a las máquinas virtuales de clúster de VM y, en última instancia, las bases de datos que residen en esas máquinas virtuales.

Para obtener más información relacionada con la creación de la primera red de clúster de VM en E-C@C a través de la consola, consultar el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/exadata/doc/ecc-setting-up-the-network.html

El clúster de VM contiene una instalación de Oracle Clusterware, que soporta bases de datos en el clúster. En la definición del clúster de VM también se especifica el número de núcleos de CPU activados, lo que determina la cantidad de recursos de CPU disponibles para las bases de datos.

Por otro lado, existe un requisito en los clústeres de VM de E-C@C que debe cumplirse para conectarse a la máquina virtual del clúster de VM. Este requisito no es otro que utilizar una clave pública SSH en formato OpenSSH.

Para obtener más información relacionada con la creación de un clúster de VM a través de la consola, consultar el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/exadata/doc/ecc-first-vm-cluster.html

Finalmente, para obtener más información relacionada con la gestión de una infraestructura E-C@C, consultar el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/exadata/doc/ecc-manage-infrastructure.html

2.3 CREACIÓN DE LA PRIMERA BASE DE DATOS DE ORACLE DATABASE EN UN SISTEMA EXADATA DE C@C

Después de aprovisionar un clúster de VM, es necesario crear el primer directorio raíz de Oracle Database E-C@C mediante el uso de la consola de OCI, la API o la CLI.

Un directorio dbhome (raíz) de base de datos es una ubicación de directorio en las máquinas virtuales de la base de datos Exadata que contiene archivos binarios de software de Oracle Database.

Para obtener más información relacionada con la creación de un directorio raíz de Oracle Database E-C@C mediante la consola de OCI, consultar el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/exadata/doc/ecc-creating-first-db-home-on-exacc.html

A continuación, después de crear un directorio raíz de Oracle Database E-C@C y previo a la creación de la primera base de datos, es necesario crear destinos de copia de seguridad para la base de datos E-C@C.

E-C@C proporciona una utilidad de copia de seguridad que puede configurar de manera individual en cada base de datos. Para almacenar las copias de seguridad en una aplicación de recuperación o en una ubicación de archivos de red (NFS) que gestione, primero se debe crear un destino de copia de seguridad.

Cada destino de copia de seguridad define las propiedades necesarias para conectarse a la aplicación de recuperación o a la ubicación NFS, y se debe poder acceder a cada destino de copia de seguridad en el centro de datos desde los nodos de clúster de VM. También puede almacenar las copias de seguridad mediante el servicio de almacenamiento de objetos de OCI o en el almacenamiento local de Exadata.

Para obtener más información relacionada con los requisitos de los destinos de copia de seguridad de E-C@C y cómo se configuran mediante el uso de la consola, consultar el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/exadata/doc/ecc-create-bkup-dest.html

Por otro lado, una vez aprovisionado un directorio raíz de Oracle Database y cualquier destino de copia de seguridad necesario, puede avanzar para la creación de la primera base de datos en E-C@C.

Revise los requisitos necesarios y limitaciones para la creación de bases de datos de Oracle en E-C@C y los distintos tipos de versión soportadas a través del siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/exadata/doc/ecc-create-first-db.html

Finalmente, una vez aprovisionado la primera base de datos en E-C@C, debe conectarse a la máquina virtual de clúster de VM mediante SSH y a la base de datos aprovisionada mediante Oracle Net Services (SQL*Net).

Para obtener más información relacionada con la conexión a un sistema E-C@C y los requisitos necesarios que debe cumplir, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/exadata/doc/ecc-connecting-to-exacc-system.html

2.4 APROVISIONAMIENTO DE UNA BASE DE DATOS AUTONOMOUS DB EN EXADATA C@C

Si decide aprovisionar una base de datos Autonomous DB debe crear los recursos de la infraestructura de Exadata dedicada en el siguiente orden:

a) **Infraestructura de Exadata:** puede consultar el siguiente enlace de Oracle para revisar los requisitos de sitio, red y almacenamiento, así como preparar y desplegar E-C@C en su centro de datos:

https://docs.oracle.com/es-ww/iaas/exadata/doc/ecc-preparing-for-deployment.html

b) **Clúster de VM de Exadata autónomo:** un clúster de VM de Exadata autónomo es un juego de VM simétricas en todos los nodos de recursos de cómputo para base de datos o bien en algunos nodos mediante la funcionalidad de Node subsetting. La base de datos y el contenedor autónomo ejecutan las VM, lo que posibilita la alta disponibilidad.

Puede consultar el siguiente enlace de Oracle para obtener más información relacionada con la gestión de clústeres de VM de Exadata autónomos:

https://docs.oracle.com/es-ww/iaas/exadata/doc/adb-manage-aevmc.html

c) **Base de datos de contenedor autónoma:** un recurso de base de datos de contenedor autónomo proporciona un contenedor para las bases de datos autónomas. Puede crear varios recursos de base de datos de contenedor autónoma en un único recurso de clúster de VM de Exadata autónomo. Sin embargo, debe crear al menos uno para poder crear bases de datos autónomas.

Para obtener más información relacionada con la gestión de bases de datos de contenedor autónomas, consultar el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/exadata/doc/adb-managing-acd.html

d) **Autonomous Database:** un recurso de base de datos autónoma es una base de datos de usuario. Al crear una base de datos autónoma se selecciona la base de datos de contenedor autónoma para la misma y se especifica como “Data Warehouse” o “Procesamiento de transacciones” como su tipo de carga de trabajo para crear una base de datos de Autonomous Data Warehouse (ADW) o una base de datos de Autonomous Transaction Processing (ATP).

Para obtener más información relacionada con la gestión de bases de datos autónomas, consultar el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/exadata/doc/adb-managing-adb.html

2.5 MÚLTIPLES VM AUTONOMOUS DB EN EXADATA C@C

Multiple-VM Autonomous DB permite a las organizaciones crear y ejecutar instancias de base de datos autónomas aisladas y de alta disponibilidad en Sistemas E-C@C, que también están ejecutando bases de datos Oracle no autónomas.

La arquitectura de implementación original de E-C@C requería que los clientes dedicaran toda la plataforma a clústeres de máquinas virtuales de Exadata autónomo o a clústeres de máquinas virtuales de base de datos de Exadata.

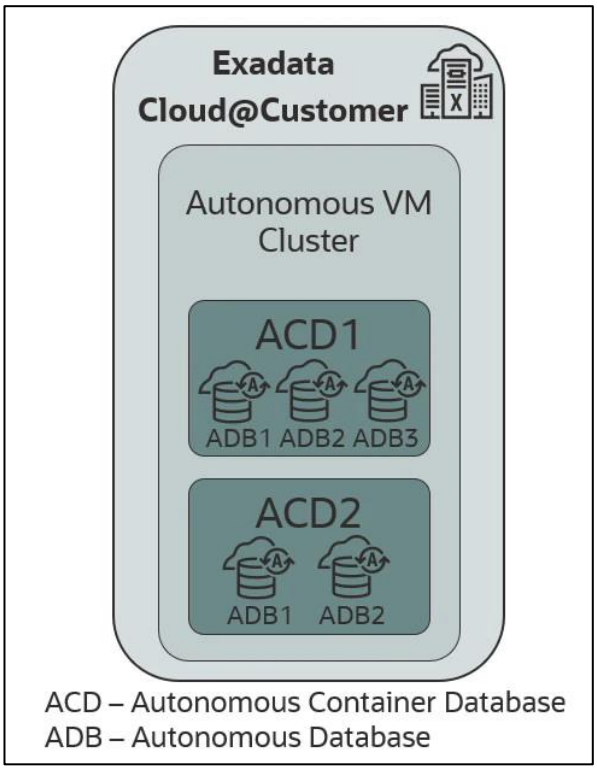

Fig. 2-Esquema de la arquitectura original de un Autonomous DB en E-C@C

Sin embargo, con la disponibilidad general de Multiple-VM Autonomous DB, las organizaciones pueden crear múltiples clústeres de máquinas virtuales Exadata autónomos y clústeres de máquinas virtuales Exadata Database en un mismo E-C@C.

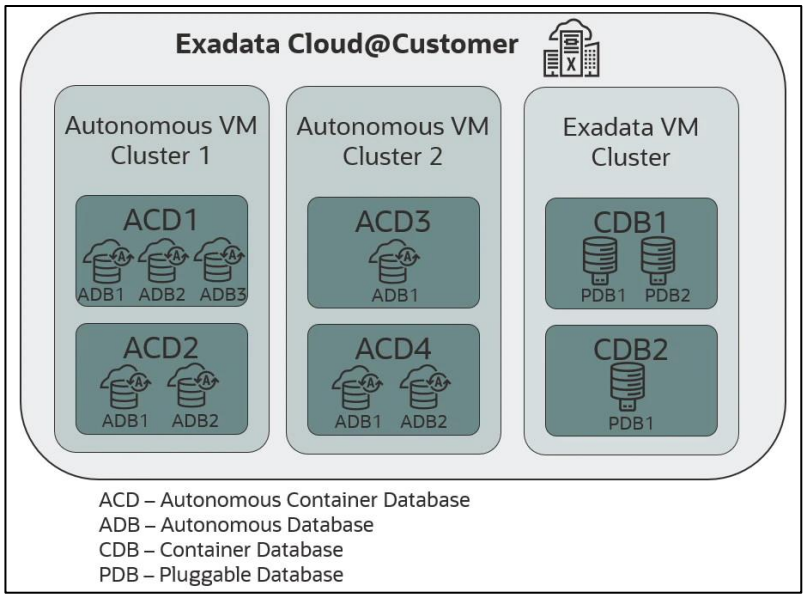

Fig. 3-Esquema de la arquitectura actual E-C@C

La base de datos autónoma de múltiples máquinas virtuales se ejecuta en un grupo de máquinas virtuales simétricas que aíslan instancias de servicio de base de datos autónomas de alta disponibilidad y se pueden implementar junto con clústeres de máquinas virtuales de base de datos Exadata, ejecutándose en una única infraestructura E-C@C.

Cada clúster de máquinas virtuales autónomas admite una configuración de red independiente, programación de mantenimiento, selección de tipo de licencia (BYOL y licencia incluida) y asignaciones personalizables de memoria, almacenamiento y cómputo en E-C@C para crear y ejecutar bases de datos autónomas.

La base de datos autónoma de varias máquinas virtuales permite a los clientes aprovisionar entornos operativos aislados, como desarrollo y pruebas, ensayo y producción, con sus propias reglas de acceso, cuotas y SLO de rendimiento. Esto, a su vez, permite a las organizaciones no solo migrar y modernizar las bases de datos existentes para obtener beneficios de la nube, sino también crear una plataforma de desarrollo de aplicaciones de bases de datos de autoservicio que cumpla con los estándares de gobierno corporativo. Esto permite a los desarrolladores internos crear nuevas aplicaciones utilizando bases de datos autónomas que se ajustan, escalan y administran automáticamente.

Para obtener más información, consulte el siguiente enlace de Oracle en inglés:

https://www.oracle.com/news/announcement/multiple-vm-autonomous-database-on-exadata-cloud-at-customer-2022-03-16/

3. CONFIGURACIÓN SEGURA PARA ORACLE C@C SISTEMAS EXADATA

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.

3.1 MARCO OPERACIONAL

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

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

3.1.1 CONTROL DE ACCESO

El conjunto de medidas que establece el control de acceso cubre todas las acciones que, bien preparatorias o ejecutivas, están orientadas a determinar qué o quién puede o no acceder a un recurso del sistema mediante una determinada acción. Con el cumplimiento de todas las medidas, se garantizará que nadie accederá a recursos sin la debida autorización.

Adicionalmente, se establecerá la necesidad de que el uso del sistema quede registrado para detectar y reaccionar ante una incidencia de seguridad o fallo del sistema.

3.1.1.1 IDENTIFICACIÓN

La identificación de los usuarios del sistema debe tener un identificador único, para conocer quién recibe y qué derechos de acceso recibió o bien saber quién y qué ha hecho algo. Además, cuando existan diferentes roles frente al sistema, las cuentas de usuario recibirán identificadores singulares para cada uno de los casos de forma que siempre queden delimitados los privilegios y registros de actividad.

Por un lado, las cuentas de usuario deben gestionarse de tal manera que puedan ser inhabilitadas en los casos que el usuario deje la organización o es cesado de sus funciones. También es imprescindible retener el tiempo suficiente y necesario para asegurar o garantizar la trazabilidad de los registros de actividad asociados a las cuentas de usuario.

Por otro lado, independientemente de las cuentas de usuario que se generen tras el aprovisionamiento de una base de datos Oracle Database o Autonomous Database y que deben cumplir con lo establecido por el ENS en la presente medida de seguridad, se ha de tener en cuenta, también, la existencia de varias cuentas de usuario por defecto que gestionan regularmente los componentes de Oracle E-C@C y en todas las máquinas de E-C@C.

No obstante, Oracle utiliza únicamente la conexión basada en SSH y ningún usuario o proceso de Oracle utiliza un sistema de autenticación basado en contraseña. A continuación, se describen los distintos tipos de usuarios que se crean por defecto:

Tipo	Cuentas	Función
Usuarios por defecto.	exawatch	Se encarga de recopilar y archivar estadísticas del sistema tanto en los servidores de base de datos como en los servidores de almacenamiento.
	dbmsvc	Se utiliza para Management Server en el servicio de nodos de base de datos del sistema Oracle Exadata.
Usuarios NOLOGIN.	Cuentas del Sistema para los servicios de proceso como bin, daemon, shutdown, etc.	Cualquier operación de proceso en los sistemas Linux deben tener una identidad de usuario. Sin embargo, las cuentas del sistema o pseudo usuarios generalmente no pueden iniciar sesión en el sistema.
Usuarios por defecto con acceso de shell restringido.	dbmmonitor	Estos usuarios se utilizan para realizar una tarea definida con una conexión de Shell restringida. En concreto, para la utilidad DBMCLI.
Usuarios por defecto con permisos de	root	Requisito de Linux para utilizar con moderación la ejecución de comandos locales con privilegios.

Tipo	Cuentas	Función
conexión y privilegios.	oracle	Para la ejecución de los procesos de Oracle Database.
	grid	Para la ejecución de los procesos Grid Infrastructure.
	opc	Para tareas de automatización de Oracle Cloud. Tiene la capacidad de ejecutar determinados comandos con privilegios sin autenticación adicional. Además, ejecuta el agente local "Agente DCS", que realiza operaciones de ciclo de vida para el software de Oracle Database y Oracle Grid Infrastructure.
	dbmadmin	Se utiliza para la utilidad de interfaz de línea de comandos de Oracle VM Exadata Database (DBMCLI). Se debe utilizar para ejecutar todos los servicios en el servidor de base de datos.

Para obtener más información relacionada con la utilidad de DBMCLI, consultar el siguiente enlace en inglés de Oracle:

https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmmn/exadata-dbmcli.html

Finalmente, para la gestión del control de acceso y la identificación de los usuarios sobre los recursos de OCI mediante políticas, grupos de usuarios y cuentas de usuario, consultar la guía de seguridad "CCN-STIC-889A Guía de Configuración segura para IAM y servicios de seguridad" para obtener más información".

3.1.1.2 REQUISITOS DE ACCESO

La presente medida de seguridad establecida por el ENS establece que los recursos del sistema deben protegerse mediante algún mecanismo que impida su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes. Los derechos de acceso de cada recurso se establecerán según las decisiones de la persona responsable del recurso, ateniéndose a la política y normativa de seguridad del sistema.

La aplicación técnica de la medida de seguridad se establece en el control de acceso sobre los recursos que pueda necesitar una organización en la nube de Oracle y el control de acceso sobre Oracle VM Exadata Database.

En primer lugar, para los recursos de la nube, OCI dispone de compartimentos donde se ubican los recursos. Un compartimento es un espacio lógico para la administración y aislamiento de los recursos mediante políticas a determinados grupos de usuarios, asegurando que cada usuario solamente acceda a los recursos que necesita acceder.

Así pues, los recursos implicados en la gestión de una base de datos de Oracle Database como de Autonomous Database en un sistema E-C@C, son similares a los recursos que puede necesitar una instancia de cómputo: dominio, recursos de red, almacenamiento y, en especial, para este caso, establecer un control de acceso a la propia base de datos aprovisionada:

a) **Control de acceso a la red:** más allá del simple aislamiento a nivel de red, se pueden instituir políticas de control de acceso detalladas a nivel de dispositivo. Todos los componentes de Oracle VM Exadata Database incluyen la capacidad de limitar el acceso a la red a los servicios, ya sea mediante métodos arquitectónicos, como el aislamiento de red, o mediante el filtrado de paquetes y las listas de control de acceso para limitar la comunicación hacía, desde y entre componentes y servicios.

b) **Control de acceso al almacenamiento:** admite los modos de control de acceso de seguridad abierta, seguridad con alcance de Oracle ASM y seguridad con alcance de base de datos.

   i. La seguridad abierta permite que cualquier base de datos acceda a cualquiera de los discos del grid.

   ii. La seguridad en el ámbito de Oracle ASM permite que varias bases de datos se asignen a uno o más clústeres de Oracle ASM para compartir discos del grid específicos.

   Además de su modo de control de acceso general, Oracle ASM admite controles de acceso a nivel de archivo y grupo de discos para garantizar que el acceso al contenido almacenado en el disco solo esté disponible para los usuarios autorizados.

   iii. La seguridad en el ámbito de la base de datos, el nivel más detallado de control de acceso garantiza que solo las bases de datos específicas puedan acceder a discos del grid específicos.

   La seguridad en el ámbito de la base de datos funciona a nivel de contenedor. Esto significa que el almacenamiento que proporciona ASM está asociado a la base de datos de contenedor (CDB) o no CDB. Debido a esto, no es posible tener seguridad en el ámbito de la base de datos por base de datos conectable (PDB).

Nota: Solo debe configurar la seguridad en el ámbito de la base de datos después de configurar y probar la seguridad en el ámbito de Oracle ASM.

c) **Control de acceso a la base de datos:** además de la autenticación basada en contraseña, Oracle Database también admite credenciales de clave pública, RADIUS y Kerberos. Usando Oracle Enterprise User Security, la base de datos se puede integrar con los repositorios LDAP existentes para autenticación y autorización. Estas capacidades brindan una mayor seguridad de la identidad de los usuarios que se conectan a la base de datos.

   Oracle Database Vault se puede utilizar para administrar el acceso de usuarios administrativos y privilegiados, controlando cómo, cuándo y dónde se puede acceder a los datos de la aplicación. Oracle Database Vault protege contra el uso indebido de credenciales de inicio de sesión robadas, omisión de aplicaciones y cambios no autorizados en aplicaciones y datos, incluidos los intentos de realizar copias de datos de aplicaciones. Oracle Database Vault es transparente para la mayoría de las aplicaciones y tareas diarias. Admite políticas de autorización de múltiples factores, lo que permite la aplicación segura de la política sin interrumpir las operaciones comerciales.

Por otro lado, puede utilizar una lista de control de acceso (ACL) para bases de datos autónomas en E-C@C. Una lista de control de acceso proporciona protección adicional a la base de datos al permitir que solo los clientes con direcciones IP específicas se conecten la misma. Puede agregar las direcciones IP de forma individual o en bloques de CIDR.

Opcionalmente, puede crear una ACL durante el aprovisionamiento de la base de datos o en cualquier momento posterior. También puede editar una ACL en cualquier momento. La activación de una lista de control de acceso con una lista de direcciones IP vacía hace que no se pueda acceder a la base de datos.

No obstante, tenga en cuenta lo siguiente en cuanto al uso de una ACL con Autonomous Database:

a) La consola del servicio de Autonomous Database no está sujeta a las reglas de la ACL.

b) En la versión actual, Oracle Application Express (APEX), los servicios RESTful y SQL Developer Web no están sujetos a las ACL. Si se activa una ACL, se desactivarán estas funciones automáticamente.

c) El hub de rendimiento no está sujeta a las reglas de la ACL.

d) Al crear una base de datos, si la definición de un ACL falla, también fallará el aprovisionamiento de la base de datos.

e) Se permite actualizar la ACL si la base de datos se encuentra en el estado Available (Disponible) o AvailableNeedsAttention (disponible, necesita atención).

f) La restauración de una base de datos no sobrescribe las ACL existentes.

g) La clonación de una base de datos, completa y con metadatos, tendrá la misma configuración de control de acceso que la base de datos de origen. Podrá realizar los cambios que sean necesarios.

h) Durante la actualización de la ACL, se permiten todas las operaciones de CBD. Sin embargo, las operaciones de ADB no se permiten durante la actualización de la ACL.

Finalmente, para obtener más información relacionada con la activación y gestión de una lista de control de acceso en una base de datos autónoma de E-C@C, consultar el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/exadata/doc/adb-managing-adb.html

3.1.1.3 SEGREGACIÓN DE FUNCIONES Y TAREAS

El sistema de control de acceso se organizará de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas, anulando la posibilidad de que un solo individuo autorizado pueda abusar de sus derechos para cometer alguna acción ilícita. En concreto, deben separarse las funciones de desarrollo de operaciones, mantenimiento y configuración del sistema y la auditoria o supervisión de cualquier otra función.

La organización puede optar por dividir la administración de Oracle Autonomous Database E-C@C entre los siguientes roles:

a) **Administrador de flotas:** los administradores de flotas crean, supervisan y gestionan los recursos de la infraestructura de Exadata C@C y del contenedor de base de datos autónoma. También deben configurar los destinos de copia de seguridad gestionados por el cliente, como la aplicación de recuperación y el NFS, para que los utilicen las bases de datos autónomas. Un administrador de flotas debe tener permisos para utilizar los recursos de red que requiera la infraestructura de Oracle E-C@C, así como permisos para gestionar los recursos de la base de datos de contenedor y la infraestructura.

b) **Administrador de bases de datos:** los administradores de bases de datos crean, supervisan y gestionan las bases de datos autónomas. También se encargan de crear y gestionar los usuarios en la base de datos. Los administradores de bases de datos deben tener permisos para utilizar las bases de datos de contenedor, para gestionar las bases de datos autónomas y las copias de seguridad y para utilizar los recursos de red relacionados. Al aprovisionar una base de datos autónoma, el administrador proporciona las credenciales de usuario para la cuenta *ADMIN* creada automáticamente, que proporciona derechos administrativos en la nueva base de datos.

c) **Usuario de bases de datos:** los usuarios de bases de datos son los desarrolladores que escriben aplicaciones que se conectan y utilizan una base de datos autónoma para almacenar y acceder a los datos. Los usuarios de bases de datos no necesitan cuentas de OCI, obtienen la conectividad de red y la información de autorización de conexión para la base de datos del administrador de bases de datos.

d) **Auditor:** la contabilidad y la auditoría mantienen un registro de la actividad de un usuario en el sistema. Las funciones de software y hardware de la VM de Exadata Database, permiten a los administradores monitorizar la actividad de inicio de sesión y mantener inventarios de hardware.

   i. Los inicios de sesión de los usuarios se controlan a través de los registros del sistema. Los administradores del sistema y las cuentas de servicio tienen acceso a los comandos que, si se usan incorrectamente, podrían causar daños y pérdida de datos. El acceso y los comandos deben monitorizarse cuidadosamente a través de los registros del sistema.

   ii. Los activos de hardware se rastrean a través de números de serie. Los números de pieza de Oracle se registran electrónicamente en todas las tarjetas, módulos y placas base, y se pueden utilizar para fines de inventario.

3.1.1.4 PROCESO DE GESTIÓN DE DERECHOS DE ACCESO

Los derechos de acceso de cada usuario deben limitarse atendiendo a los principios de mínimo privilegio, necesidad de conocer y capacidad de autorizar. Los privilegios de cada usuario se reducirán al mínimo estrictamente necesario para cumplir con sus obligaciones. De esta forma se acotan lo daños que pueda causar una entidad, de forma accidental o intencionada.

Además, los privilegios deben limitarse de forma que los usuarios accedan al conocimiento de aquella información que requieren para el cumplimiento de sus obligaciones. Por último, solamente el personal con competencia para ello podrá conceder, anular o modificar la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable.

Para garantizar que los procesos de las máquinas virtuales de Oracle Exadata Database tengan acceso a los privilegios que necesitan, los estándares de codificación segura de Oracle requieren el paradigma de los privilegios mínimos, asegurando que las aplicaciones, servicios y usuarios tengan acceso a las capacidades que necesitan para realizar sus tareas.

Cada proceso y Daemon se debe ejecutar con un usuario normal sin privilegios, a menos que pueda demostrar un requisito de un nivel superior de privilegios. Esto ayudará a contener cualquier problema imprevisto en un espacio de usuario sin privilegios y a no poner en peligro todo un sistema.

Este principio también se aplica a los miembros del equipo de operaciones de Oracle que utilizan cuentas con nombre individuales para acceder a la infraestructura de Oracle E-C@C con fines de mantenimiento o solución de problemas. El acceso auditado a niveles superiores de privilegio solo lo utilizarán cuando sea necesario para resolver un problema. La mayoría de los problemas se resuelven mediante automatización, por lo que también se emplean los privilegios mínimos al no permitir que los operadores humanos accedan a un sistema a menos que la automatización no sea capaz de resolver el problema.

Por otro lado, el principio de privilegio mínimo debe cumplirse también en el proceso de gestión de derechos de acceso para los recursos de la nube de OCI, que puede consultar para obtener más información a través de la guía de seguridad “CCN-STIC-889A Guía de Configuración segura para IAM y servicios de seguridad”.

Finalmente, Oracle VM Exadata Database promueve el principio de privilegio mínimo garantizando que el acceso a servidores individuales, almacenamiento, sistema operativo, bases de datos y otros componentes se pueda otorgar según el rol de cada usuario y administrador.

3.1.1.5 ACCESO LOCAL

Se considera acceso local al realizado desde puestos de trabajo de las propias instalaciones de la organización. Estos accesos deben tener en cuenta el nivel de las dimensiones de seguridad.

Por un lado, se debe prevenir ataques que puedan revelar información del sistema sin llegar a acceder al mismo. El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez efectuados un cierto número de fallos consecutivos. Además, se registrarán los accesos con éxito y los fallidos.

Para el nivel alto, el acceso debe estar limitado por horario, fechas y lugar desde donde se accede. Además, se definirán aquellos puntos en los que el sistema requerirá una renovación de la autenticación del usuario, mediante identificación singular, no bastando con la sesión establecida.

Por otro lado, existen dos tipos de conexiones posibles para conectarse al servicio de base de datos E-C@C. Puede conectarse a las máquinas virtuales en un servicio de base de datos E-C@C mediante una conexión SSH, o bien puede conectarse al servicio de base de datos.

Esta última es la recomendada para los accesos generales a la base de datos y sus datos, siendo necesario la limitación de acceso a la base de datos solo a los usuarios privilegiados para tareas de administración.

Para obtener más información relacionada con la conexión al servicio de base de datos de E-C@C, consultar el siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-connect-to-the-service.html

Finalmente, para obtener más información relacionada con el acceso local y remoto para la nuble pública de Oracle, consultar la guía de seguridad "CCN-STIC-889A Guía de Configuración segura para IAM y servicios de seguridad".

3.1.2 EXPLOTACIÓN

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

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

3.1.2.1 INVENTARIO DE ACTIVOS

La medida de seguridad establecida por el ENS dice que debe mantenerse un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a su responsable.

Oracle dispone del servicio de etiquetado para la aplicación técnica de la presente medida de seguridad para los recursos de OCI. El servicio de etiquetado permite agregar metadatos a los recursos, brindando la posibilidad de definir claves, valores y asociarlos a los recursos.

En consecuencia, al agregar valores y claves a los recursos permite llevar una contabilidad de usuarios, grupos, políticas, compartimentos, instancias de base de datos, bases de datos, recursos de almacenamiento etc.

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

https://docs.oracle.com/es-ww/iaas/Content/Tagging/Concepts/taggingoverview.htm

Finalmente, para los recursos de la infraestructura de C@C, se deberá inventariar e identificar a los responsables de dichos recursos en el propio centro de datos de la organización.

3.1.2.2 MANTENIMIENTO

Según establece el ENS, para mantener el equipamiento físico y lógico que constituye el sistema, se debe aplicar el mantenimiento de los sistemas atendiendo a las especificaciones de los fabricantes y efectuando un seguimiento continuo de los anuncios de defectos. Además, se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo se debe aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones.

Sin embargo, hay que tener en cuenta que Oracle aplica parches y actualizaciones a todos los componentes del sistema gestionados por Oracle de E-C@C.

Entre los parches y actualizaciones de Oracle se incluyen los hosts del servidor de base de datos físico, los servidores de Exadata Storage Servers, los switches de red, el switch de gestión, las unidades de distribución de energía (PDU), las interfaces de gestión de iluminación integrada (ILOM) y los servidores del control plane. A esto se le denomina el mantenimiento de la infraestructura de E-C@C.

Salvo en circunstancias excepcionales, recibirá una comunicación por adelantado que le informará de estas actualizaciones para ayudarle a planificarlas. Si hay actualizaciones recomendadas para las VM del clúster, Oracle proporciona notificaciones sobre ellas.

Siempre que sea posible, las actualizaciones programadas se llevan a cabo en modo rolling, de tal manera que se mantiene la disponibilidad del servicio durante el proceso de actualización. Sin embargo, puede que se perciba cierto impacto en el rendimiento mientras los distintos componentes del sistema no estén disponibles durante el proceso de actualización.

Por ejemplo, la aplicación de parches del servidor de base de datos normalmente requiere un reinicio. En esos casos, siempre que sea posible, los servidores de base de datos se reinician de forma sucesiva, de uno en uno, para garantizar que el servicio permanece disponible durante el proceso. Sin embargo, cada servidor de base de datos no estará disponible durante un corto periodo de tiempo mientras se reinicia, y la capacidad general del servicio disminuye en consecuencia. Si sus aplicaciones no toleran los reinicios, tome las medidas de atenuación que sean necesarias. Por ejemplo, cierre una aplicación mientras se produce la aplicación de parches del servidor de base de datos.

Además, puede elegir el mantenimiento no rolling, para actualizar los servidores de almacenamiento y base de datos. El método de mantenimiento no rolling actualiza primero los servidores de almacenamiento al mismo tiempo y, a continuación, los servidores de base de datos al mismo tiempo. Aunque el mantenimiento no rolling minimiza el tiempo de mantenimiento, genera tiempo de inactividad completo del sistema mientras se actualizan los servidores de almacenamiento y los servidores de base de datos.

Hay que tener en cuenta que las comprobaciones previas se realizan en los componentes de infraestructura de E-C@C antes del inicio de la ventana de mantenimiento. El objetivo de los controles previos es identificar problemas que puedan impedir que el mantenimiento de la infraestructura tenga éxito. La infraestructura de Exadata y todos los componentes permanecen en línea durante las comprobaciones previas. Una comprobación previa inicial se ejecuta aproximadamente dos semanas antes del inicio del mantenimiento y otra comprobación previa se ejecuta aproximadamente 24 horas antes del inicio del mantenimiento. Si los chequeos previos identifican una incidencia que requiere reprogramación, la notificación de mantenimiento se envía a los contactos de mantenimiento.

Nota: el estado de ciclo de vida del recurso de infraestructura de Exadata, permite controlar cuándo comienza y finaliza el mantenimiento del recurso de infraestructura. Puede obtener más información en el siguiente enlace de Oracle: https://docs.oracle.com/es-ww/iaas/exadata/doc/ecc-config-infra-maintenance.html

Por otro lado, el mantenimiento de un sistema E-C@C seguro y asegurarse del estado de funcionamiento óptimo del sistema, implica la realización de las siguientes tareas con regularidad y por parte del cliente:

a) Aplicación de parches al software Oracle Grid Infrastructure y Oracle Database y Autonomous DB en las VM de clúster y en las instancias autónomas.

b) Actualización del sistema operativo en las VM del clúster o en las instancias autónomas si tiene aprovisionado un Autonomous DB en instancias de clúster de VM autónomo.

Para obtener más información relacionada con la aplicación de parches y actualización del servicio de base de datos en los sistemas E-C@C, consultar el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/exadata/doc/ecc-update-exacc-system.html

Finalmente, para la aplicación de parches en Autonomous DB en infraestructura de E-C@C, consultar el siguiente enlace de Oracle para obtener más información:

https://docs.oracle.com/es-ww/iaas/exadata/doc/adb-patching.html

Además, puede consultar el siguiente enlace de Oracle para la gestión de imágenes de software de Oracle Database para la aplicación de parches en bases de datos:

https://docs.oracle.com/es-ww/iaas/exadata/doc/ecc-oracle-database-software-images.html

Oracle recomienda la configuración y gestión de asociaciones de Data Guard en el clúster de VM para el mantenimiento del servicio de base de datos en sistemas E-C@C, que puede consultar en el siguiente enlace:

https://docs.oracle.com/es-ww/iaas/exadata/doc/ecc-using-data-guard.html

3.1.2.3 PROTECCIÓN FRENTE A CÓDIGO DAÑINO

El ENS establece que se debe disponer de mecanismos de prevención y reacción frente a código dañino, realizando el mantenimiento necesario de acuerdo con las recomendaciones del fabricante.

En primer lugar, E-C@C ofrece una serie de controles que garantizan la confidencialidad, la integridad y la responsabilidad en todo el servicio. E-C@C se crea a partir de la imagen reforzada del sistema operativo proporcionada por Exadata Database Machine. Para obtener más información, consulte Descripción general de Oracle Exadata Database Machine Security en el siguiente enlace en inglés:

https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmsq/exadata-security-overview.html

Debido a que E-C@C se crea a partir de la imagen reforzada del sistema operativo de Exadata Database Machine, asegura la protección del entorno operativo principal al restringir la imagen de instalación a solo los paquetes de software necesarios, deshabilitando los servicios innecesarios e implementando parámetros de configuración seguros en todo el sistema.

No obstante, el cliente puede usar OpenSCAP para escanear la máquina virtual del cliente en busca de vulnerabilidades de seguridad. Una herramienta basada en el protocolo de automatización de contenido de seguridad que proporciona una metodología estandarizada y automatizada para la administración de seguridad del sistema, incluida la medición y administración de vulnerabilidades y evaluación del cumplimiento de políticas frente a estándares de seguridad como FISMA.

Puede obtener más información a través del siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-scap-sec.html

Además, el cliente puede utilizar el entorno de detección de intrusos avanzado (AIDE) de Oracle Linux para comprobar la integridad de archivos y directorios. AIDE es una pequeña herramienta de detección de intrusos que se instala automáticamente con el sistema operativo de Linux y utiliza reglas predefinidas para comprobar la integridad de archivos y directorios. Su objetivo es proteger el sistema internamente, proporcionando una capa de protección contra virus, rootkits, malware y detección de actividades no autorizadas.

Puede obtener más información sobre la herramienta a través del siguiente enlace de Oracle en inglés:

https://support.oracle.com/knowledge/Oracle%20Linux%20and%20Virtualization/26162821.html

Por otro lado, el cliente dispone de control para la instalación de software de terceros, incluido el software de escaneo en las VM del sistema E-C@C. Hay que tener en cuenta que Oracle no proporciona soporte técnico para este tipo de herramientas.

Finalmente, para los recursos de la nube de OCI, puede usar el servicio de Cloud Guard. Para obtener más información puede consultar la guía de seguridad “CCN-STIC-889A Guía de Configuración segura para IAM y servicios de seguridad”.

3.1.2.4 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, puede ayudarse de las herramientas para monitorizar la integridad de los sistemas de archivos como AIDE, que genera informes diarios para la monitorización de los cambios del sistema.

A su vez, puede usar el Daemon de OpenSCAP para evaluar continuamente su infraestructura para el cumplimiento de la seguridad o las vulnerabilidades. OpenSCAP es un servicio que se ejecuta en segundo plano, asegurando que las máquinas y contenedores se evalúen de acuerdo con el cronograma que especifique.

Puede obtener más información sobre el servicio OpenScap a través del siguiente enlace de Github en inglés:

https://github.com/OpenSCAP/openscap-daemon/blob/master/README.md

Finalmente, puede consultar la guía de seguridad "CCN-STIC-889D Guía de Configuración segura para OCI Database-Instancias VM" para obtener más información de las herramientas de seguridad como Oracle Data Safe para bases de datos de Oracle Cloud.

Nota: el cliente y Oracle trabajan juntos para asegurar y monitorizar el acceso a los servicios del cliente, bases de datos, datos de bases de datos, máquinas virtuales e infraestructura. Si cualquiera de las partes detecta una acción no autorizada, esa parte puede tomar medidas de respuesta de inmediato según la política de seguridad y los detalles y circunstancias en torno a la acción no autorizada, antes de notificar a la otra parte. Si el cliente detecta una acción no autorizada, debe notificar a Oracle sobre la acción y la respuesta a través del proceso Oracle SR. Oracle notificará al cliente las acciones no autorizadas detectadas y las respuestas llevadas a cabo por parte de Oracle.

3.1.2.5 REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS

El ENS establece que se deben registrar las actividades de los usuarios en el sistema de forma que el registro indique quién realiza la actividad, cuándo ha sido realizada y sobre qué recurso ha sido realizada. Además, se debe incluir la actividad de todos los usuarios, registrando las actividades realizadas con éxito y los intentos fracasados. Por último, para el nivel alto, se debe disponer de un sistema automático de recolección de registros y correlación de eventos en una consola de seguridad centralizada.

El sistema E-C@C proporciona sólidos controles de detección de auditoría y registro para los servicios de atención al cliente y la infraestructura gestionada por Oracle. El cliente controla la configuración del registro de los servicios al cliente y Oracle controla la configuración de registro de infraestructura gestionada por Oracle.

E-C@C proporciona 3 áreas para auditar y registrar las acciones de los clientes:

a) **Servicio de auditoría de OCI:** registros de auditoría para acciones de control plane como la interfaz de usuario web, CLI de OCI, API REST de OCI, etc., iniciadas mediante las credenciales proporcionadas por el servicio de OCI IAM de un cliente.

Puede obtener más información relacionada con el servicio de OCI IAM en la guía de seguridad "CCN-STIC-889A Guía de Configuración segura para IAM y servicios de seguridad".

b) **Auditoría de la base de datos de Oracle:** registros de auditoría para las acciones de la base de datos iniciadas a través de credenciales de base de datos de Oracle de un cliente.

Puede obtener más información relacionada con la auditoría de las bases de datos de Oracle en la guía de seguridad "CCN-STIC-889D Guía de Configuración segura para OCI Database-Instancias VM".

c) **Registro de auditoría del sistema operativo de la máquina virtual del cliente:** para las acciones iniciadas en la máquina virtual del cliente a través de las credenciales del sistema operativo.

3.1.2.6 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.

Finalmente, puede consultar el siguiente enlace de Oracle para ver los eventos emitidos por los recursos de Oracle Database en el sistema E-C@C:

https://docs.oracle.com/es-ww/iaas/exadata/doc/eventsproducers.html

3.1.2.7 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.

Para empezar, existen dos formas de administrar y almacenar las claves de cifrado para las bases de datos Oracle en los sistemas E-C@C: la primera, almacenarlas en la propia máquina virtual desplegada en la infraestructura de Exadata y la segunda, a través de un dispositivo de gestión de claves externo llamado Oracle Key Vault (OKV).

Oracle Key Vault es un dispositivo de software que almacena de forma segura las claves de cifrado y objetos de seguridad en un clúster multi maestro escalable, tolerante a fallos y separado de los propios datos cifrados.

Nota: Oracle Key Vault es un sistema administrado y proporcionado por el cliente y no forma parte de los servicios gestionados de OCI.

La integración de OKV permite tomar el control completo de sus claves de cifrado y almacenarlas de forma segura en un dispositivo externo de gestión de claves centralizado.

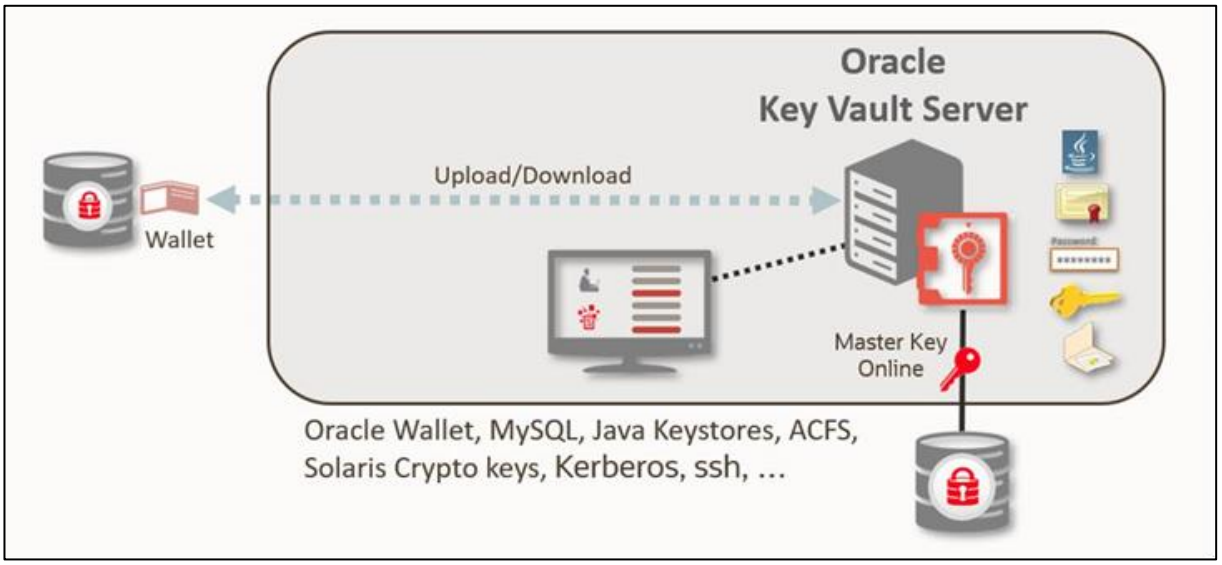

Fig. 4-Esquema del funcionamiento de Oracle Key Vault

OKV está optimizado para wallets de Oracle, almacenes de claves de Java y claves maestras de cifrado de datos transparente (TDE) de Advanced Security de Oracle. Oracle Key Vault es compatible con el estándar OASIS KMIP, que utiliza la tecnología Oracle Linux y Oracle Database para seguridad, disponibilidad y escalabilidad, y se puede implementar en el hardware compatible que elija.

OKV también proporciona una interfaz REST para que los clientes inscriban automáticamente puntos finales y configuren wallets y claves. Para que las bases de datos en los sistemas E-C@C se conecten a la interfaz REST de OKV, cree un almacén de claves en el tenant para almacenar la dirección IP y las credenciales de administrador de su OKV. E-C@C no almacenará la contraseña de administrador requerida para conectarse al dispositivo OKV. Asegúrese de crear un secreto con el servicio de Oracle Vault, que almacenará la contraseña requerida para que las bases de datos se conecten a OKV y pueda administrar las claves.

Finalmente, para obtener más información relacionada con Oracle Key Vault, consulte el siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/database/oracle/key-vault/index.html

3.1.3 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.

3.1.3.1 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.

La aplicación técnica de la medida de seguridad se centra en el sistema operativo de la máquina virtual invitada de la infraestructura E-C@C mediante registros, eventos y herramientas de protección frente a código dañino y auditoría.

Por otro lado, puede usar los servicios que ofrece OCI para la monitorización de las bases de datos como Cloud Guard y Monitoring.

Para obtener más información relacionada con los servicios de OCI Cloud Guard y Monitoring, puede consultar las guías de seguridad “CCN-STIC-889D Guía de Configuración segura para OCI Database-Instancias VM” y “CCN-STIC-889B Guía de Configuración segura para Monitorización y gestión”

3.1.3.2 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 la medida de seguridad que permite gestionar y supervisar los recursos de E-C@C, es proporcionada por el servicio de Oracle Enterprise Manager Cloud Control.

Oracle Enterprise Manager Cloud Control detecta los servicios Exadata Cloud y E-C@C como un único destino e identifica y organiza automáticamente todos los componentes dependientes para realizar las siguientes actividades:

a) Supervisar y gestionar todos los sistemas Exadata, junto con cualquier otro destino, desde una sola interfaz.

b) Visualizar datos de cómputo y almacenamiento.

c) Ver métricas de rendimiento de los componentes de Exadata.

Las funciones de Enterprise Manager Cloud Control sirven para gestionar y supervisar los recursos de Exadata Cloud y E-C@C:

a) Destino de Enterprise Manager para E-C@C.

   i. Identifica y organiza automáticamente los destinos relacionados.

   ii. Proporciona un punto de integración de alto nivel para las funciones del marco de Enterprise Manager, como las reglas de incidentes, los grupos, las notificaciones y las plantillas de supervisión.

b) Supervisión de rendimiento mejorada.

   i. Agrega destinos de Exadata Storage Server y Exadata Storage Grid.

   ii. Ofrece la visualización del rendimiento de los recursos de cómputo y almacenamiento de E-C@C.

   iii. Permite utilizar los mismos indicadores clave de rendimiento (KPI) de la arquitectura de máxima disponibilidad (MAA) desarrollados por Oracle Exadata Database Machine.

c) Detección basada en CLI con scripts.

   Enterprise Manager Cloud Control utiliza scripts para detectar recursos de OCI Exadata. Los scripts rastrean los hosts, clústeres, ASM, las bases de datos y los destinos relacionados existentes y también agregan los destinos del servidor de almacenamiento.

d) Panel único de los recursos locales de OCI Exadata.

e) Visualización.

   Enterprise Manager Cloud Control permite visualizar la base de datos y los destinos relacionados asociados a cada sistema Exadata Cloud y E-C@C.

Para obtener más información relacionada con Enterprise Manager Cloud Control, consulte el siguiente enlace de Oracle:

https://www.oracle.com/es/enterprise-manager/technologies/

3.2 MEDIDAS DE PROTECCIÓN

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

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

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

3.2.1 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 y C@C.

3.2.1.1 PERÍMETRO SEGURO

Se debe disponer de un sistema de cortafuegos que separe la red interna de la red externa. Todo el tráfico deberá atravesar dicho cortafuegos que dejará transitar solo los flujos previamente autorizados. Además, para la categoría alta de la presente medida de seguridad, el sistema de cortafuegos constará de dos o más equipos de diferente fabricante dispuestos en cascada y se dispondrán de sistemas redundantes.

El servicio de E-C@C no requiere una conexión TCP entrante para fines de administración, soporte o entrega del servicio. Sin embargo, sí requiere conexiones TCP salientes en el puerto 443 a los puntos finales de Oracle para fines de servicio remoto. Si está utilizando reglas de firewall basadas en el filtrado de direcciones IP, debido a la naturaleza dinámica de las interfaces de la nube, debe permitir el tráfico con todos los rangos CIDR de IP relevantes asociados con su región OCI.

La configuración de iptables y las reglas de firewall se almacenan en archivos /etc/sysconfig/iptables. Para obtener más detalles sobre qué puertos pueden ser necesarios en la VM invitada, consulte el siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-secguide.html

Para configurar el firewall manualmente, cree comandos como el siguiente ejemplo, teniendo en cuenta que es posible bloquear el sistema bloqueando los puertos a través de los cuales se conecta.

Se recomienda probar en un sistema de prueba y/o disponer de un administrador de iptables experimentado si es posible.

a) En el símbolo del sistema, ingrese el comando apropiado para cada puerto que se abrirá:

```
# iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 7002 -j ACCEPT
# iptables -A INPUT -m state --state NEW -m udp -p udp --dport 123 -j ACCEPT
```

b) Guarde la configuración de iptables.

```
# service iptables save
```

Para finalizar, consulte la guía de seguridad “CCN-STIC-889A Guía de Configuración segura para IAM y servicios de seguridad” para obtener más información relacionada con otros cortafuegos de terceros en el servicio de Marketplace y el servicio OCI WAF para la protección del tráfico de internet en la capa de aplicación del modelo de OSI.

3.2.1.2 PROTECCIÓN DE LA CONFIDENCIALIDAD

Esta medida indica que se emplearán redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad, empleando algoritmos acreditados por el CCN, preferentemente, con dispositivos hardware en el establecimiento y utilización de la red privada virtual y productos certificados conforme a lo establecido en el ENS.

OCI dispone, dentro del servicio Networking (Red), para implementar redes privadas virtuales en las comunicaciones para conectar la infraestructura de la nube con la red local de la organización, mediante VPN de sitio a sitio u OCI FastConnect.

Para obtener toda la información relacionada con las conexiones VPN de Sitio a Sitio o conexiones OCI FastConnect, consulte la guía de seguridad "CCN STIC 889C Guía de Configuración segura para Arquitecturas Híbridas"

Para obtener más información sobre la conexión FastConnect en E-C@C, consultar el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/exadata/doc/ecc-network-requirements.html

3.2.1.3 SEGREGACIÓN DE REDES

La segregación de redes acota el acceso a la información y propagación de los incidentes de seguridad, que quedan restringidos al entorno donde ocurren. Así pues, para la categoría alta, la red de la organización debe segmentarse de tal forma que exista un control de entrada y salida de los usuarios que llegan a cada segmento y que las redes puedan ser segmentadas por dispositivos físicos o lógicos. El punto de interconexión debe quedar asegurado, mantenido y monitorizado.

Para proporcionar una conectividad de red segura y fiable para diferentes funciones de gestión y aplicaciones, el servicio Database E-C@C utiliza diferentes redes. En la siguiente lista se describen las redes de un sistema E-C@C para el servicio de Database:

a) **Red de servicio de E-C@C:** estas redes se configurarán según las especificaciones de Oracle y el cliente no debe modificarlas sin el consentimiento de Oracle.
   i. **Red control plane:** esta red privada virtual (VPN) conecta los dos servidores de control plane ubicados en el rack y conecta el servicio Database E-C@C con OCI.
   ii. **Red de administración:** esta red conecta los servidores y los switches del servicio Database E-C@C con los dos servidores de control plane.
   iii. **Red de RoCE o RDMA sobre Ethernet convergente (RoCE):** esta red conecta los servidores de base de datos, los servidores Exadata Storage Server y los servidores de control plane mediante switches de RoCE del rack.

b) **Red de cliente:** redes gestionadas por el cliente y de su propiedad necesarias para que el plano de datos de E-C@C acceda a los sistemas relacionados.
   i. **Red de cliente:** conecta los servidores de base de datos E-C@C a la red cliente existente y se utiliza para el acceso de cliente a las máquinas virtuales.

ii. **Red de copia de seguridad:** similar a la red de acceso de cliente, ya que conecta los servidores Oracle Database E-C@C a la red existente. Se puede utilizar para acceder a las máquinas virtuales con distintos fines, incluidas copias de seguridad y transferencias de datos masivas.

Para revisar los requisitos de red de las distintas redes aprovisionadas para el servicio de Oracle Database E-C@C en el centro de datos de una organización, consultar el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/exadata/doc/ecc-network-requirements.html

3.2.2 PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN

La protección de los soportes de la información está supeditada al uso de estos medios en la nube. 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.

3.2.2.1 ETIQUETADO

Según el ENS, los soportes de información se etiquetarán de forma que, sin revelar su contenido, se indique el nivel de seguridad de la información contenida de mayor calificación. Los usuarios han de estar capacitados para entender el significado de las etiquetas, bien mediante simple inspección o bien mediante el recurso a un repositorio que lo explique.

Oracle Database y Autonomous DB disponen de una opción de etiquetado de seguridad llamado Label Security, que permite a las organizaciones consolidar los datos cumpliendo con los diferentes requisitos de acceso en la misma base de datos.

Nota: Label Security está disponible en el servicio PaaS de Oracle Database E-C@C y Autonomous DB E-C@C.

Para obtener más información sobre Label Security, consultar la guía de seguridad “CCN-STIC-889D Guía de Configuración segura para OCI Database-Instancias VM”

3.2.3 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.

3.2.3.1 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 servicios a nivel de base de datos para la aplicación técnica de la presente medida de seguridad. Estos servicios, Oracle Data Redaction, Oracle Data Masking, Oracle Data Safe y Oracle Database Vault permite la protección de los datos a través de técnicas como el enmascaramiento o el control de acceso.

Puede utilizar Oracle Data Redaction en un entorno de Oracle Database Vault. Por ejemplo, si hay un dominio de Oracle Database Vault alrededor de un objeto, un usuario que no pertenezca a la lista autorizada de propietarios o participantes del dominio no puede ver los datos del objeto.

Puede obtener más información relacionada con el servicio de Oracle Database Vault a través del siguiente enlace de Oracle:

https://www.oracle.com/es/security/database-security/database-vault/

Por otro lado, Oracle Data Redaction le permite redactar (enmascarar) los datos de la columna utilizando varios tipos de redacción en vuelo, disponiendo del dato almacenado sin modificación.

Los tipos de redacción que puede realizar son los siguientes:

a) **Redacción completa:** redacta todo el contenido de los datos de la columna. El valor redactado que se devuelve al usuario que realiza la consulta depende del tipo de datos de la columna. Por ejemplo, las columnas del tipo NUMBER de datos se redactan con un cero (0) y los tipos de datos de caracteres se redactan con un espacio en blanco.

b) **Redacción parcial:** redacta una parte de los datos de la columna. Por ejemplo, puede redactar la mayor parte de un número de Seguro Social con asteriscos (*), excepto los últimos 4 dígitos.

c) **Expresiones regulares:** puede utilizar expresiones regulares tanto en redacción completa como parcial. Esto le permite redactar datos en función de un patrón de búsqueda de datos. Por ejemplo, puede usar expresiones regulares para redactar números de teléfono o direcciones de correo electrónico específicos en sus datos.

d) **Redacción aleatoria:** los datos redactados presentados al usuario que realiza la consulta aparecen como valores generados aleatoriamente cada vez que se muestran, según el tipo de datos de la columna.

e) **Sin redacción:** esta opción le permite probar el funcionamiento interno de sus políticas de redacción, sin efecto en los resultados de consultas contra tablas con políticas definidas en ellas. Puede usar esta opción para probar las definiciones de políticas de redacción antes de aplicarlas a un entorno de producción.

Finalmente, puede consultar la guía de seguridad “CCN-STIC-889D Guía de Configuración segura para OCI Database-Instancias VM”, para obtener más información sobre los servicios y herramientas como Oracle Data Safe, Oracle Data Redaction y Oracle Data Masking, para la protección de los datos personales y confidenciales.

3.2.3.2 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.

A través del servicio de Data Safe y su función de "Detección de datos", es posible la aplicación técnica de la presente medida de seguridad. La función de Detección de datos de Oracle Data Safe permite detectar datos confidenciales en bases de datos de destino para su calificación.

Puede obtener más información relacionada con la herramienta de protección de los datos confidenciales a través de la guía de seguridad "CCN-STIC-889D Guía de Configuración segura para OCI Database-Instancias VM"

3.2.3.3 CIFRADO

La información con un nivel alto de confidencialidad se debe cifrar durante su almacenamiento, así como durante su transmisión. Solamente estará en claro mientras se está haciendo uso de ella.

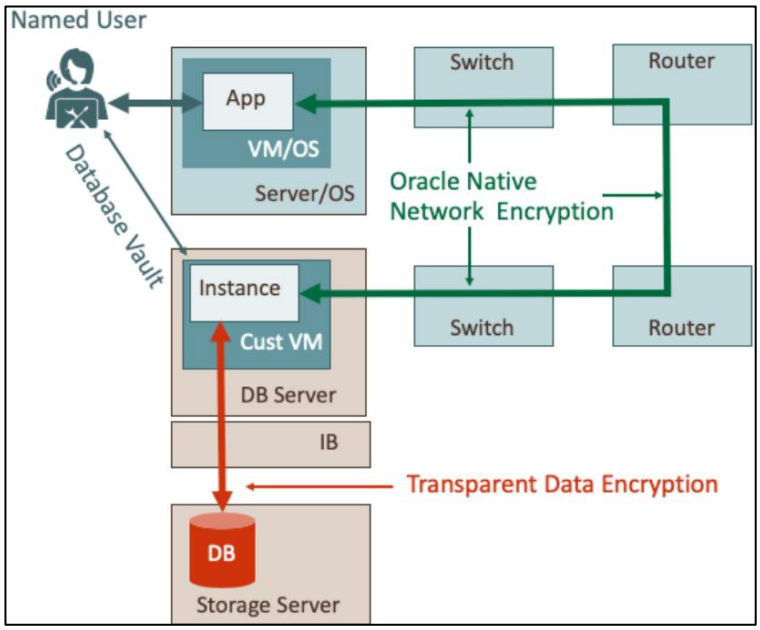

Fig. 5-Esquema del control y protección del dato en tránsito y en reposo para bases de datos E-C@C

Oracle Database proporciona integridad y cifrado de red de datos nativos para garantizar que los datos estén seguros mientras viajan por la red.

El propósito de un criptosistema seguro es convertir datos de texto sin formato en texto cifrado ininteligible basado en una clave, de tal manera que sea muy difícil convertir el texto cifrado de nuevo en su texto sin formato correspondiente sin conocer la clave correcta.

En un criptosistema simétrico, se utiliza la misma clave tanto para el cifrado como para el descifrado de los mismos datos. Oracle Database proporciona el sistema criptográfico simétrico Advanced Encryption Standard (AES) para proteger la confidencialidad del tráfico de Oracle Net Services.

Además, puede elegir dos formas de cifrar datos en tránsito: cifrado de red nativo de Oracle y el cifrado TLS. Puede consultar en el siguiente enlace de Oracle en inglés, las ventajas y desventajas en el uso de un cifrado u otro:

https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-network-data-encryption-and-integrity.html

Por otro lado, los controles de seguridad de Oracle Database Vault, protegen los datos de la aplicación del acceso no autorizado y cumplen con los requisitos reglamentarios y de privacidad. Puede implementar controles para bloquear el acceso de cuentas privilegiadas a los datos de la aplicación y controlar las operaciones confidenciales dentro de la base de datos mediante la autorización de rutas de confianza. A través del análisis de privilegios y roles, puede aumentar la seguridad de las aplicaciones existentes mediante el uso de mejores prácticas de privilegios mínimos. Oracle Database Vault protege los entornos de bases de datos existentes de forma transparente, eliminando los costosos y lentos cambios de aplicaciones.

Puede obtener más información acerca del servicio de Oracle Database Vault en el siguiente enlace de Oracle:

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

A su vez, TDE cifra las tablas de usuario y los espacios de tabla de la base de datos de Oracle. El cifrado es transparente para las aplicaciones y los usuarios autorizados, porque la base de datos cifra automáticamente los datos antes de ser almacenados. En sentido inverso, los datos son descifrados automáticamente cuando los datos son consultados desde el almacenamiento.

TDE evita que los usuarios privilegiados del sistema operativo, red o administradores del almacenamiento, puedan eludir los controles de la base de datos para acceder a los datos directamente en los ficheros de almacenamiento (datafiles). Los usuarios y aplicaciones de bases de datos autorizados no necesitan presentar la clave de descifrado cuando procesan datos cifrados. En su lugar, la base de datos aplica las reglas de control de acceso y deniega el acceso si el usuario no está autorizado a ver los datos.

Puede obtener más información de la integración de Oracle Database Vault con otros productos como Oracle TDE en el siguiente enlace en inglés:

https://docs.oracle.com/en/database/oracle/oracle-database/19/dvadm/integrating-database-vault-with-other-oracle-products.html

Finalmente, la integración del servicio OKV en las instalaciones E-C@C, permite la administración y almacenamiento de claves en las wallets de Oracle, incluido las claves maestras de cifrado de datos transparente.

Puede consultar la administración de claves de cifrado en dispositivos externos para las bases de datos aprovisionadas en el servicio E-C@C en el siguiente enlace en inglés de Oracle:

https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/adb-manage-keys-on-ext-dev.html

3.2.3.4 COPIAS DE SEGURIDAD (BACKUP)

Según establece el ENS, se realizarán copias de seguridad que permitan la recuperación de los datos perdidos con una antigüedad determinada. Estas copias poseerán el mismo nivel de seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad. Además, las copias de seguridad deben estar cifradas para garantizar la confidencialidad.

Para las copias de seguridad, puede utilizar la utilidad de copia de seguridad del servicio de Oracle Database E-C@C o puede configurar una ubicación de copia de seguridad en una ubicación que gestione.

Si se desea almacenar las copias de seguridad en una aplicación de recuperación o en una ubicación de un sistema de archivos de red (NFS) que gestione, primero debe crear un destino de copia de seguridad. Cada destino de copia de seguridad define las propiedades necesarias para conectarse a la aplicación de recuperación o a la ubicación de NFS, y se debe poder acceder a cada destino de copia de seguridad en el centro de datos desde los nodos de clúster de VM.

También puede almacenar copias de seguridad en el almacenamiento de objetos de OCI o en el almacenamiento local de Exadata del sistema Exadata Database C@C. Sin embargo, no es necesario crear un destino de copia de seguridad para ninguna de estas otras ubicaciones. En su lugar, las opciones aplicables para la copia de seguridad en el almacenamiento de objetos en la nube o en el almacenamiento local de Exadata están disponibles directamente al crear una base de datos.

No obstante, para configurar destinos de copia de seguridad en una ubicación de Zero Data Loss Recovery Appliance o una ubicación de copia de seguridad de NFS, revise los siguientes requisitos:

a) Para un destino de copia de seguridad Zero Data Loss Recovery Appliance:

   i. La aplicación se debe configurar con un usuario de catálogo privado virtual (VPC), que se utiliza para realizar las copias de seguridad.

   ii. La aplicación se debe configurar con el nombre único de base de datos de la base de datos de la que se está realizando la copia de seguridad y con una asignación al usuario de VPC.

   iii. El dispositivo debe ser accesible desde el sistema Exadata Database C@C con la cadena de conexión de Oracle Net Services proporcionada por el administrador de Zero Data Loss Recovery Appliance.

Nota: Zero Data Loss Recovery Appliance es un sistema innovador que protege las bases de datos y proporciona copias de seguridad en tiempo real desde la memoria del sistema, por lo que los datos se pueden recuperar hasta el último segundo. Para obtener más información, consulte el siguiente enlace de Oracle en inglés: https://docs.oracle.com/en/engineered-systems/zero-data-loss-recovery-appliance/index.html

b) Para un destino de copia de seguridad de NFS. Bases de datos no autónomas del servicio Database E-C@C:

   i. Se debe montar la ubicación del servidor NFS en un directorio de punto de montaje local en cada nodo del clúster de VM.

   ii. El directorio de punto de montaje local y el servidor NFS deben ser idénticos en todos los nodos del clúster.

   iii. Debe asegurarse de que el montaje de NFS se mantenga continuamente en todos los nodos del clúster de VM.

   iv. El usuario *oracle* del sistema operativo debe poder leer y escribir en el sistema de archivos montado en NFS en todos los nodos de clúster de VM.

c) Para un destino de copia de seguridad de NFS. Bases de datos autónomas del servicio Database E-C@C:

   i. Para garantizar que el clúster de VM autónomo pueda acceder al servidor NFS a través de la red de copia de seguridad, introduzca direcciones IP de la red de copia de seguridad válidas al configurar la red de clúster de VM.

   ii. El usuario *oracle* del sistema operativo debe poder leer y escribir en el sistema de archivos montado en NFS en todos los nodos de clúster de VM.

   iii. Si los permisos se controlan en el nivel de usuario, el uid:gid del usuario *oracle* para el clúster de VM autónomo es 1001:1001.

Por otro lado, Oracle E-C@C ofrece dos enfoques para configurar y realizar copias de seguridad:

a) **Copia de seguridad gestionada por Oracle:** una vez configurada, no necesita realizar ningún mantenimiento, como la programación de copias de seguridad y la supresión de las copias de seguridad. Oracle gestiona las copias de seguridad mediante flujos de trabajo bien definidos. Sin embargo, existen determinados parámetros de configuración de copias de seguridad que no están completamente integrados con el flujo de trabajo de copia de seguridad gestionada por Oracle. Si desea definir cualquiera de esos parámetros para las copias de seguridad, consulte el siguiente enlace de Oracle:

   https://docs.oracle.com/es-ww/iaas/exadata/doc/ecc-manage-db-backup-and-recovery.html#GUID-8D1DDFAE-E214-4714-90B1-9F680184E64F

b) **Copia de seguridad configurada por el cliente:** es responsabilidad del cliente configurar y ejecutar operaciones de copia de seguridad mediante el comando *dbaascli* según sus

preferencias. Puede consultar el siguiente enlace de Oracle para obtener más información sobre cómo realizar una copia de seguridad mediante *dbaascli*:

https://docs.oracle.com/es-ww/iaas/exadata/doc/ecc-manage-db-backup-and-recovery.html#GUID-0166B820-7E99-4649-9EF5-8D8F127B6AA3

Finalmente, existen medios alternativos para realizar las copias de seguridad para bases de datos del servicio Database E-C@C, además de la consola de OCI.

En general, es preferible utilizar la consola de OCI, la API de OCI o la línea de comandos de OCI sobre métodos de gestión alternativos. Sin embargo, si las acciones necesarias no se pueden completar mediante los métodos preferidos, hay otras dos opciones disponibles para configurar manualmente las copias de seguridad: *bkup_api* y Oracle Recovery Manager (RMAN).

Nota: bkup_api quedará en desuso en una versión futura. Utilice los comandos *dbaascli database backup*, *dbaascli pdb backup*, *dbaascli database recover* y *dbaascli pdb recover* para realizar copias de seguridad y recuperar bases de datos de contenedor y bases de datos de conexión.

Para obtener más información relacionada con la herramienta RMAN, consulte la guía de seguridad "CCN-STIC-889D Guía de Configuración segura para OCI Database-Instancias VM".

Para obtener más información relacionada con la gestión de copias de seguridad y recuperación de bases de datos del servicio de Oracle Database E-C@C, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/exadata/doc/ecc-manage-db-backup-and-recovery.html

4. GLOSARIO

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

Término	Definición
ACD	Autonomous Container Database (Base de Datos de Contenedores Autónomos).
ACL	Access Control List (Lista de Control de Acceso).
ADB	Autonomous DB (Base de Datos Autónoma).
ADW	Autonomous Data Warehouse.
AES	Advanced Encryption Standard (Estándar de Cifrado Avanzado).
AIDE	Advanced Intrusion Detection Environment (Entorno de Detección Avanzada de Intrusos).
APEX	Oracle Application Express (Aplicaciones Express de Oracle).
API	Application Programming Interface (Interfaz de Programación de Aplicaciones).
ASM	Automatic Storage Management (Gestión Automática de Almacenamiento).
ATP	Autonomous Transaction Processing.
BYOL	Bring-Your-Own-License (Incorpore Su Propia Licencia).
C@C	Oracle Cloud at Customer.
CCN	Centro Criptológico Nacional.
CDB	Container DataBase (Bases de Datos de Contenedor).
CIDR	Classless Inter-Domain Routing (Enrutamiento Entre Dominios sin Clases).
CLI	Command Line Interface (Interfaz de Línea de Comandos).
DBMCLI	Database Manager CLI (Interfaz de Línea de Comandos para la Administración de Bases de Batos).
E-C@C	Exadata Cloud at Customer (Nube de Exadata en el Cliente).
ENS	Esquema Nacional de Seguridad.
FISMA	Federal Information Security Management Act (Ley Federal de Seguridad de la Información).
IA	Inteligencia Artificial.
ILOM	Integrated Lights-Out Management (Administrador Integrado de Luces Apagadas).
IoT	Internet of Things (Internet de las Cosas).
KMIP	Key Management Interoperability Protocol (Protocolo de Interoperabilidad de Administración de Claves).
KPI	Key performance indicator (Indicador Clave de Rendimiento).
LDAP	Lightweight Directory Access Protocol (Protocolo Ligero de Acceso a Directorio).
MAA	Maximum Availability Architecture (Arquitectura de Máxima Disponibilidad).
MOS	My Oracle Support.

Término	Definición
NFS	Network File System (Sistema de Archivos de Red).
OASIS	Organization for the Advancement of Structured Information Standards (Organización para el Avance de los Estándares de Información Estructurada).
O-C@C	Oracle Cloud at Customer (Nube de Oracle en el Cliente).
OCI	Oracle Cloud Infrastructure.
OCI IAM	Oracle Cloud Identity and Access Management (Gestión de Identidad y Acceso).
OCPU	Oracle CPU.
OKV	Oracle Key Vault (Servicio de Almacenamiento de Claves de Oracle).
OOB	Out of Band (Fuera de Banda).
OSI	Open Systems Interconnection (Modelo de Interconexión de Sistemas Abiertos).
PDB	Production DataBase (Bases de Datos de Conexión).
PDU	Power Distribution Unit (Unidades de Distribución de Energía).
RADIUS	Remote Authentication Dial-In User Service (Protocolo de Autenticación y Autorización para el Acceso a la Red).
RDMA	Remote Direct Memory Access (Acceso Remoto Directo a Memoria).
REST	Representational State Transfer (Transferencia de Estado Representacional).
RMAN	Oracle Recovery Manager.
RoCE	RDMA over Ethernet Converged (RDMA Sobre Ethernet Convergente).
SLA	Service Level Agreement (Acuerdo de Nivel de Servicio).
SLO	Service Level Objectives (Objetivos de Nivel de Servicio).
SQL*Net	Oracle Net Services (Servicios de Red de Oracle).
SSH	Secure Shell.
TCP	Transmission Control Protocol (Protocolo de Control de Transmisión).
TDE	Transparent Data Encrypted (Cifrado de Datos Transparente).
TLS	Transport Layer Security (Seguridad de la Capa de Transporte).
Vault	Almacén.
VM	Virtual Machine (Máquina Virtual).
VPC	Virtual Private Catalog (Catálogo Privado Virtual).
WAF	Web Application Firewall (Firewall de Aplicaciones Web).

5. 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
	Las cuentas de usuario para las bases de datos de Oracle o Autonomous DB son únicas para cada usuario y usan la conexión SSH para el acceso a las bases de datos.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.acc.2	Requisitos de acceso	Aplica	Cumple
	Se han gestionado los requisitos de acceso mediante políticas y grupos de usuarios para el acceso a la red.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se han gestionado los requisitos de acceso mediante políticas y grupos de usuarios para el acceso al almacenamiento.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se han gestionado los requisitos de acceso mediante políticas y grupos de usuarios para el acceso a la base de datos.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
	Se ha configurado una lista de control de acceso (ACL para bases de datos autónomas en E-C@C.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.acc.3	Segregación de funciones y tareas	Aplica	Cumple
	Se han creado los grupos de seguridad basados en roles para la administración de Oracle Autonomous DB E-C@C.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.acc.4	Proceso de gestión de derechos de acceso	Aplica	Cumple
	Los procesos se están ejecutando con cuentas de usuario normales sin privilegios, a menos que se pueda demostrar disponer de un requisito de nivel superior de privilegios.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.acc.6	Acceso local	Aplica	Cumple
	Se está limitando el acceso a las bases de datos por horario, fechas y lugar. Además, se ha limitado el número de intentos de acceso permitidos.	☐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 según la clasificación o calificación de cada recurso o servicio.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.exp.4	Mantenimiento	Aplica	Cumple
	Se está aplicando los parches al software Oracle Grid Infrastructure, Oracle Database y Autonomous DB en las VM de clúster y en las instancias autónomas.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se está actualizando el sistema operativo en las VM del clúster o en las instancias autónomas.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.exp.6	Protección frente a código dañino	Aplica	Cumple
	Se está escaneando con frecuencia la máquina virtual del cliente en busca de vulnerabilidades de seguridad con herramientas como OpenSCAP, AIDE o herramientas de terceros.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
op.exp.7	Gestión de incidentes	Aplica	Cumple
	Se está usando las herramientas pertinentes para la monitorización de la integridad de los sistemas de archivos y detección de intrusos o búsqueda de vulnerabilidades.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.exp.8	Registro de la actividad de los usuarios	Aplica	Cumple
	Se está auditando el acceso y las acciones mediante registros proporcionados por el servicio de auditoría de OCI para los recursos del tenant, registros de auditoría para las acciones de la base de datos y los registros de auditoría del sistema operativo de la máquina virtual del cliente.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.exp.9	Registro de la gestión de incidentes	Aplica	Cumple
	Se dispone de un sistema de registro de todas las actuaciones relacionadas con la gestión de incidentes para las bases de datos y el sistema operativo de la máquina virtual invitada. A su vez, se han verificado los problemas registrados de los recursos de OCI una vez activado el servicio Cloud Guard.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
op.exp.11	Protección de claves criptográficas	Aplica	Cumple
	Se está haciendo uso del servicio Oracle Key Vault (OKV) para el almacenamiento y administración de las claves de cifrado para las bases de datos Oracle y Autonomous DB.	☐Si ☐No	☐Si ☐No
		Observaciones:	
OP.MON	MONITORIZACIÓN DEL SISTEMA		
op.mon.1	Detección de intrusión	Aplica	Cumple
	Se está haciendo uso de herramientas de detección de intrusos para el sistema operativo de la máquina virtual y se está monitorizando las bases de datos a través de los servicios de Cloud Guard y Monitoring.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.mon.2	Sistema de métricas	Aplica	Cumple
	Se ha configurado el servicio Oracle Enterprise Manager Cloud Control para la supervisión y gestión de todos los sistemas Exadata.	☐Si ☐No	☐Si ☐No
		Observaciones:	
MP	MEDIDAS DE PROTECCIÓN		
MP.COM	PROTECCIÓN DE LAS COMUNICACIONES		
mp.com.1	Perímetro seguro	Aplica	Cumple
	Se ha configurado las reglas de firewall para la protección del flujo de comunicaciones autorizados.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
mp.com.2	Protección de la confidencialidad	Aplica	Cumple
	Se está empleando los servicios de VPN y FastConnect para la protección de la confidencialidad en las VCN de OCI.	☐Si ☐No	☐Si ☐No
		Observaciones:	
mp.com.4	Segregación de redes	Aplica	Cumple
	Se dispone de dispositivos físicos o lógicos que segmentan las redes seguras para el servicio Database E-C@C y las redes VCN en OCI.	☐Si ☐No	☐Si ☐No
		Observaciones:	
MP.SI	PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN		
mp.si.1	Etiquetado	Aplica	Cumple
	Se ha configurado el servicio de etiquetado de seguridad Label Security para Oracle Database y Autonomous DB.	☐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:	

Control ENS	Medidas y Configuración	Estado	
mp.info.2	Calificación de la información	Aplica	Cumple
	Se está utilizando la función de Oracle Data Safe "Detección de datos" para la detección de los datos confidenciales en bases de datos de destino para la calificación de la información.	☐Si ☐No	☐Si ☐No
		Observaciones:	
mp.info.3	Cifrado	Aplica	Cumple
	Se está usando el servicio de Oracle Database Vault para la protección de los entornos de bases de datos existentes.	☐Si ☐No	☐Si ☐No
		Observaciones:	
mp.info.9	Copias de seguridad (Backup)	Aplica	Cumple
	Se ha configurado y ejecutado operaciones de copia de seguridad mediante dbaascli.	☐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