

Oracle® Guía de seguridad de Solaris Cluster 4.3



Referencia: E62323
Octubre de 2015

Referencia: E62323

Copyright © 2000, 2015, Oracle y/o sus filiales. Todos los derechos reservados.

Este software y la documentación relacionada están sujetos a un contrato de licencia que incluye restricciones de uso y revelación, y se encuentran protegidos por la legislación sobre la propiedad intelectual. A menos que figure explícitamente en el contrato de licencia o esté permitido por la ley, no se podrá utilizar, copiar, reproducir, traducir, emitir, modificar, conceder licencias, transmitir, distribuir, exhibir, representar, publicar ni mostrar ninguna parte, de ninguna forma, por ningún medio. Queda prohibida la ingeniería inversa, desensamblaje o descompilación de este software, excepto en la medida en que sean necesarios para conseguir interoperabilidad según lo especificado por la legislación aplicable.

La información contenida en este documento puede someterse a modificaciones sin previo aviso y no se garantiza que se encuentre exenta de errores. Si detecta algún error, le agradeceremos que nos lo comuniqué por escrito.

Si este software o la documentación relacionada se entrega al Gobierno de EE.UU. o a cualquier entidad que adquiera las licencias en nombre del Gobierno de EE.UU. entonces aplicará la siguiente disposición:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Este software o hardware se ha desarrollado para uso general en diversas aplicaciones de gestión de la información. No se ha diseñado ni está destinado para utilizarse en aplicaciones de riesgo inherente, incluidas las aplicaciones que pueden causar daños personales. Si utiliza este software o hardware en aplicaciones de riesgo, usted será responsable de tomar todas las medidas apropiadas de prevención de fallos, copia de seguridad, redundancia o de cualquier otro tipo para garantizar la seguridad en el uso de este software o hardware. Oracle Corporation y sus subsidiarias declinan toda responsabilidad derivada de los daños causados por el uso de este software o hardware en aplicaciones de riesgo.

Oracle y Java son marcas comerciales registradas de Oracle y/o sus subsidiarias. Todos los demás nombres pueden ser marcas comerciales de sus respectivos propietarios.

Intel e Intel Xeon son marcas comerciales o marcas comerciales registradas de Intel Corporation. Todas las marcas comerciales de SPARC se utilizan con licencia y son marcas comerciales o marcas comerciales registradas de SPARC International, Inc. AMD, Opteron, el logotipo de AMD y el logotipo de AMD Opteron son marcas comerciales o marcas comerciales registradas de Advanced Micro Devices. UNIX es una marca comercial registrada de The Open Group.

Este software o hardware y la documentación pueden proporcionar acceso a, o información sobre contenidos, productos o servicios de terceros. Oracle Corporation o sus filiales no son responsables y por ende desconocen cualquier tipo de garantía sobre el contenido, los productos o los servicios de terceros a menos que se indique otra cosa en un acuerdo en vigor formalizado entre Ud. y Oracle. Oracle Corporation y sus filiales no serán responsables frente a cualesquiera pérdidas, costos o daños en los que se incurra como consecuencia de su acceso o su uso de contenidos, productos o servicios de terceros a menos que se indique otra cosa en un acuerdo en vigor formalizado entre Ud. y Oracle.

Accesibilidad a la documentación

Para obtener información acerca del compromiso de Oracle con la accesibilidad, visite el sitio web del Programa de Accesibilidad de Oracle en <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Acceso a Oracle Support

Los clientes de Oracle que hayan adquirido servicios de soporte disponen de acceso a soporte electrónico a través de My Oracle Support. Para obtener información, visite <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> o <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> si tiene problemas de audición.

Contenido

- Uso de esta documentación 7**
- 1 Introducción a la seguridad de Oracle Solaris Cluster 9**
 - Visión general de Oracle Solaris Cluster y de la seguridad 10
 - Descripción general de Geographic Edition y de la seguridad 10
 - Principios generales de seguridad 11
 - Instalación y configuración seguras de Oracle Solaris Cluster 11
 - Instalación y configuración seguras de Geographic Edition 12
 - Funciones de seguridad de Oracle Solaris Cluster 13
 - Funciones de seguridad de Geographic Edition 14
 - Consideraciones de seguridad para desarrolladores 15
- Índice 17**

Uso de esta documentación

- **Visión general:** proporciona una visión general de la seguridad en Oracle Solaris Cluster, información sobre instalaciones y configuración seguras, funciones de seguridad y consideraciones de seguridad para los desarrolladores.
- **Destinatarios:** técnicos, administradores de sistemas y proveedores de servicios autorizados.
- **Conocimiento requerido:** experiencia avanzada en la resolución de problemas y en el reemplazo de hardware.

Biblioteca de documentación del producto

La documentación y los recursos para este producto y los productos relacionados se encuentran disponibles en <http://www.oracle.com/pls/topic/lookup?ctx=E62278>.

Comentarios

Puede dejar sus comentarios sobre esta documentación en <http://www.oracle.com/goto/docfeedback>.

Introducción a la seguridad de Oracle Solaris Cluster

El producto Oracle Solaris Cluster es una solución de hardware y software integrada que se utiliza para crear servicios escalables y de alta disponibilidad. Esta guía proporciona una visión general de la seguridad en Oracle Solaris Cluster, además de información sobre instalaciones y configuración seguras, funciones de seguridad y consideraciones de seguridad para los desarrolladores. Utilice este manual con todo el conjunto de documentación de Oracle Solaris Cluster para proporcionar una vista completa del software Oracle Solaris Cluster.

El software Geographic Edition es una extensión en capas del software Oracle Solaris Cluster. El marco de Geographic Edition brinda protección para aplicaciones contra interrupciones imprevistas mediante el uso de varios clusters que están separados geográficamente por largas distancias. Estos clusters incluyen copias de la infraestructura de Geographic Edition, que administran datos replicados entre los clusters.

Este capítulo incluye las secciones siguientes:

- “Visión general de Oracle Solaris Cluster y de la seguridad” [10]
- “Descripción general de Geographic Edition y de la seguridad” [10]
- “Principios generales de seguridad” [11]
- “Instalación y configuración seguras de Oracle Solaris Cluster” [11]
- “Instalación y configuración seguras de Geographic Edition” [12]
- “Funciones de seguridad de Oracle Solaris Cluster” [13]
- “Funciones de seguridad de Geographic Edition” [14]
- “Consideraciones de seguridad para desarrolladores” [15]

Para obtener más información sobre la seguridad del sistema operativo (SO) Oracle Solaris, consulte [Directrices de seguridad y refuerzo de Oracle Solaris 11](#) y [Protección de sistemas y dispositivos conectados en Oracle Solaris 11.3](#).

Visión general de Oracle Solaris Cluster y de la seguridad

El entorno de Oracle Solaris Cluster extiende el sistema operativo Oracle Solaris en un sistema operativo de cluster. Un cluster es una colección de uno o más nodos que pertenecen exclusivamente a esa colección.

Las ventajas del software Oracle Solaris Cluster incluyen lo siguiente:

- Reduce o elimina el tiempo de inactividad del sistema debido a errores de software o de hardware.
- Garantiza a los usuarios finales la disponibilidad de los datos y las aplicaciones, independientemente del tipo de fallo que normalmente inutilizaría un sistema de un único servidor.
- Aumenta el rendimiento de las aplicaciones al permitir que los servicios se amplíen con procesadores adicionales agregando nodos al cluster y equilibrando la carga.
- Proporciona una mayor disponibilidad del sistema, ya que permite realizar el mantenimiento sin cerrar todo el cluster.

Un cluster ofrece varias ventajas en comparación con los sistemas de servidor único. Estas ventajas incluyen compatibilidad con failover y servicios escalables, la capacidad para crecimiento modular, la capacidad de establecer los límites de carga en los nodos y un precio de entrada bajo respecto a sistemas de tolerancia a fallos de hardware tradicionales.

En un cluster que se ejecuta en el sistema operativo Oracle Solaris, un *cluster global* y un *cluster de zona* son tipos de clusters. Los clusters pueden ser clusters globales, clusters de zona o una combinación de ambos. Para conocer más ventajas de la configuración de un cluster de zona, consulte [Oracle Solaris Cluster 4.3 Concepts Guide](#).

Descripción general de Geographic Edition y de la seguridad

El software Geographic Edition es una extensión en capas del software Oracle Solaris Cluster. El software de replicación de datos permite que las aplicaciones que se ejecutan en un cluster de Geographic Edition toleren desastres mediante la migración de servicios a un cluster secundario separado geográficamente. Un desastre, tal como un terremoto, incendio o tormenta, puede desactivar el cluster en el sitio primario.

En el caso de un desastre, el cluster de Geographic Edition puede continuar proporcionando servicios mediante el uso de los siguientes niveles de redundancia:

- Un cluster secundario
- Configuración de aplicaciones duplicadas en el cluster secundario
- Datos replicados en el cluster secundario

El software Geographic Edition proporciona un conjunto de herramientas para gestionar y configurar clusters separados geográficamente con una migración de los servicios entre los sitios. Los clusters pueden ser cluster globales, clusters de zona o una combinación de ambos. El software Geographic Edition puede administrar la disponibilidad entre múltiples ubicaciones físicas a través de seguridad robusta, migración de servicios de aplicaciones y replicación de datos para tolerar desastres en un sistema empresarial.

Principios generales de seguridad

Los siguientes principios son fundamentales para el uso de la aplicación Oracle Solaris Cluster de manera segura.

- Mantener el software actualizado
- Restringir acceso de red a servicios críticos
- Seguir el principio del menor privilegio
- Supervisar la actividad del sistema
- Mantenerse actualizado acerca de la última información de seguridad de Oracle

Instalación y configuración seguras de Oracle Solaris Cluster

En esta sección, se proporcionan enlaces para planificar y ejecutar una instalación y una configuración seguras de Oracle Solaris Cluster.

- **Instalación:** puede instalar el software Oracle Solaris con Automated Installer (AI) de Oracle Solaris 11. Para obtener más información, consulte [“Instalación del software” de Guía de instalación del software de Oracle Solaris Cluster 4.3](#).
- **Paquetes de cluster:** los paquetes de cluster de Oracle Solaris usan los nombres de paquetes Oracle Solaris Image Packaging System (IPS).
Para ver una lista de los paquetes núcleo, de servicios de datos y Geographic Edition de Oracle Solaris Cluster, consulte [Oracle Solaris Cluster 4.3 Package Group Lists](#).
- **Configuración:** puede configurar y administrar un cluster global y un cluster de zona. Para obtener más información, consulte [Capítulo 3, “Establecimiento del cluster global” de Guía de instalación del software de Oracle Solaris Cluster 4.3](#), [Capítulo 6, “Creación de clusters de zona” de Guía de instalación del software de Oracle Solaris Cluster 4.3](#) y [Capítulo 1, “Introducción a la administración de Oracle Solaris Cluster” de Guía de administración del sistema de Oracle Solaris Cluster 4.3](#).

En todos los métodos para establecer un nodo de cluster global, se requiere la autorización previa de un nodo del patrocinador designado, que solamente le permita al sistema designado el acceso al nodo que configurará. Si lo desea, puede utilizar el cifrado DES

para una configuración más segura. Para obtener más información, consulte la página del comando `man clauth(1CL)`.

- **Vulnerabilidad del contenedor de agentes común:** la combinación del contenedor de agentes común y algunas versiones antiguas de Java poseen una vulnerabilidad de seguridad en el software Oracle Solaris Cluster. Para obtener información sobre cómo identificar si el sistema tiene esta vulnerabilidad y cómo corregirla, consulte el documento de referencia de My Oracle Support, [CVE-2014-3566 Instrucciones para mitigar la vulnerabilidad de SSL v3.0 \(también conocida como "Poodle Attack"\) en Oracle Solaris Cluster \(ID de documento 1999997.1\)](https://support.oracle.com/epmos/faces/DocumentDisplay?id=1999997.1&displayIndex=1) (<https://support.oracle.com/epmos/faces/DocumentDisplay?id=1999997.1&displayIndex=1>). Este documento requiere que inicie sesión en My Oracle Support.
- **HA para NFS seguro con Kerberos V5:** si necesita asegurar el acceso a los servicios NFS que gestiona el servicio de datos HA para NFS, puede configurar un cliente Kerberos V5 para asegurar el servicio de datos HA para NFS. Esto incluye agregar un principal de Kerberos para NFS sobre los nombres de host lógicos en todos los nodos de cluster. Para obtener más información, consulte [“Securing HA for NFS With Kerberos V5” de Oracle Solaris Cluster Data Service for NFS Guide](#).

Instalación y configuración seguras de Geographic Edition

En esta sección, se proporcionan vínculos para planificar y ejecutar una instalación y una configuración seguras del software Geographic Edition.

- **Instalación:** el software Geographic Edition debe instalarse en un cluster que ejecute el sistema operativo Oracle Solaris y el software Oracle Solaris Cluster. Utilice Automated Installer (AI) de Oracle Solaris para instalar el software Geographic Edition al mismo tiempo que instala el software Oracle Solaris Cluster o en cualquier momento futuro. La configuración del marco de Geographic Edition es idéntica a la configuración del software Oracle Solaris Cluster. Consulte [Capítulo 2, “Installing and Configuring the Geographic Edition Software” de Oracle Solaris Cluster 4.3 Geographic Edition Installation and Configuration Guide](#).
- **Paquetes de Geographic Edition:** los paquetes de Geographic Edition usan los nombres de paquetes Oracle Solaris Image Packaging System (IPS). Para ver una lista de paquetes, consulte [Oracle Solaris Cluster 4.3 Package Group Lists](#).
- **Configuración:** puede realizar todas las tareas de administración en un cluster que ejecuta el marco de Geographic Edition sin provocar la falla de nodos o del cluster. Puede instalar, configurar, iniciar, usar, detener y desinstalar el software Geographic Edition en un cluster operacional. Consulte [Capítulo 4, “Administering RBAC” de Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide](#).

Funciones de seguridad de Oracle Solaris Cluster

Esta sección contiene información sobre determinados mecanismos de seguridad que ofrece Oracle Solaris Cluster.

Una instalación segura utiliza las siguientes funciones de seguridad críticas:

- **Control de acceso basado en roles (RBAC):** utilice las autorizaciones del RBAC de `solaris.cluster.modify`, `solaris.cluster.admin` y `solaris.cluster.read` para acceder al cluster. Debe convertirse en un administrador con el perfil de derechos de seguridad de usuario asignado para cambiar la mayoría de los atributos de seguridad de un rol. Para obtener más información, consulte [“Gestión del uso de los derechos” de Protección de los usuarios y los procesos en Oracle Solaris 11.3](#) y [“Perfiles de derechos de RBAC de Oracle Solaris Cluster” de Guía de administración del sistema de Oracle Solaris Cluster 4.3](#).
- **Nuevos nodos:** utilice el comando `claccess` o la utilidad `clsetup` con privilegios para agregar un nodo a un cluster. Para obtener más información, consulte [Capítulo 8, “Administración de nodos del cluster” de Guía de administración del sistema de Oracle Solaris Cluster 4.3](#).

La configuración predeterminada para el estado de acceso es `claccess deny-all`. Debe cambiarla solo cuando desee realizar una operación privilegiada, como agregar un nuevo nodo. Debe restaurar el estado `deny-all` cuando haya finalizado. Si pretende realizar cambios frecuentes a las configuraciones del cluster, puede asegurar una máxima confianza para los nuevos sistemas seleccionando un protocolo de autenticación seguro con el comando `/usr/cluster/bin/claccess -p protocol=authentication-protocol`. Para obtener más información, consulte la página del comando `man claccess(1CL)` y [Capítulo 10, “Configuración de autenticación de servicios de red” de Gestión de Kerberos y otros servicios de autenticación en Oracle Solaris 11.3](#).

- **Trusted Extensions:** se puede activar la función Trusted Extensions de Oracle Solaris para usarla en un cluster de zona. Para obtener más información, consulte [“Directrices para Trusted Extensions en un cluster de zona” de Guía de instalación del software de Oracle Solaris Cluster 4.3](#) y [“Cómo instalar y configurar Trusted Extensions” de Guía de instalación del software de Oracle Solaris Cluster 4.3](#).
- **Clusters de zona:** un cluster de zona comprende una o más zonas no globales de la marca `solaris`, la marca `solaris10` o el conjunto de marcas `labeled` con el atributo `cluster`. El cluster de zona con la marca `labeled` solo se utiliza con la función Trusted Extensions del software de Oracle Solaris.

Para crear un cluster de zona, debe emplear el comando `clzonecluster` o la utilidad `clsetup`. Puede ejecutar servicios compatibles en el cluster de zona del mismo modo que en un cluster global, con el aislamiento proporcionado por las zonas de Oracle Solaris. Para obtener más información, consulte [“Creación y configuración de un cluster de zona” de Guía de instalación del software de Oracle Solaris Cluster 4.3](#) y [“Trabajo con un cluster de zona” de Guía de administración del sistema de Oracle Solaris Cluster 4.3](#).

- **Conexiones seguras para consolas de cluster:** debe establecer conexiones de shell seguras para las consolas de los nodos del cluster. Para obtener más información sobre la utilidad `pconsole`, consulte [“Conexión segura a las consolas del cluster” de Guía de administración del sistema de Oracle Solaris Cluster 4.3](#).
- **Common Agent Container:** la GUI de Oracle Solaris Cluster Manager usa sólidas técnicas de cifrado para garantizar una comunicación segura entre las pilas de gestión de Oracle Solaris Cluster en cada nodo del cluster. Para obtener más información, consulte [“Resolución de problemas de Oracle Solaris Cluster Manager” de Guía de administración del sistema de Oracle Solaris Cluster 4.3](#).
- **Conexión:** el software Oracle Solaris Cluster usa el comando `syslogd` para registrar mensajes de error y estado. Asegúrese de configurar el archivo `/etc/syslog.conf` para controlar dónde se almacenan los mensajes. También debe proteger de manera segura los archivos de registro, como el archivo `/var/adm/messages`. Para obtener más información, consulte [“Administración del cluster” de Guía de administración del sistema de Oracle Solaris Cluster 4.3](#).
- **Auditoría:** Oracle Solaris Cluster está activado de manera predeterminada, de la misma forma que en el SO Oracle Solaris. La auditoría almacena todos los comandos ejecutados en el archivo `/var/cluster/logs/commandlog`, y debe definir las protecciones en el archivo según corresponda. Para obtener más información, consulte [“Cómo ver el contenido de los logs de comandos de Oracle Solaris Cluster” de Guía de administración del sistema de Oracle Solaris Cluster 4.3](#).
- **Endurecimiento del SO Oracle Solaris:** Oracle Solaris Cluster usa técnicas de endurecimiento de seguridad para volver a configurar el SO Oracle Solaris en un estado endurecido. Además, puede activar la auditoría del sistema de Oracle Solaris.

Funciones de seguridad de Geographic Edition

En esta sección, se incluye información sobre mecanismos de seguridad específicos ofrecidos por Geographic Edition.

Una instalación segura utiliza las siguientes funciones de seguridad críticas:

- **Control de acceso basado en roles (RBAC):** el software Geographic Edition basa sus perfiles de RBAC en los perfiles de derechos de RBAC que se usan en el software Oracle Solaris Cluster. Debe convertirse en un administrador con el perfil de derechos de seguridad de usuario asignado para cambiar la mayoría de los atributos de seguridad de un rol. Asuma el rol `root` y utilice los roles de RBAC de `solaris.cluster.geo.modify`, `solaris.cluster.geo.admin` y `solaris.cluster.geo.read` para acceder al cluster. Para obtener más información, consulte [Protección de los usuarios y los procesos en Oracle Solaris 11.3](#) y [“Modifying a User’s RBAC Properties” de Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide](#).
- **Certificados de seguridad:** durante la instalación, el cluster se configura para la comunicación segura con el cluster mediante el uso de certificados de seguridad (los

nodos dentro del mismo cluster comparten los mismos certificados de seguridad). La comunicación entre los clusters en una asociación de Geographic Edition se asegura gracias al puerto Java Management Extensions (JMX) con capa de conexión segura (SSL) utilizando los certificados de seguridad. Para obtener más información, consulte [“Configuring Trust Between Partner Clusters” de Oracle Solaris Cluster 4.3 Geographic Edition Installation and Configuration Guide](#).

- **Contenedor de agente común:** para activar un cluster de zona para que funcione como miembro de una asociación de Oracle Solaris Cluster, el contenedor de agente común debe configurarse manualmente dentro del cluster de zona. Para obtener más información, consulte [“Preparing a Zone Cluster for Partner Membership” de Oracle Solaris Cluster 4.3 Geographic Edition Installation and Configuration Guide](#).
- **IP Security Architecture (IPsec):** utilice IPsec para configurar comunicaciones de latido TCP/UDP seguras entre los clusters asociados. Para obtener más información, consulte [“Securing Inter-Cluster Communication” de Oracle Solaris Cluster 4.3 Geographic Edition Installation and Configuration Guide](#).

Consideraciones de seguridad para desarrolladores

En esta sección, se proporciona información útil para los desarrolladores que crean aplicaciones que utilizan Oracle Solaris Cluster. Los desarrolladores utilizan la API de Oracle Solaris Cluster. Para obtener más información, consulte [Capítulo 3, “Key Concepts for System Administrators and Application Developers” de Oracle Solaris Cluster 4.3 Concepts Guide](#).

Las aplicaciones del agente que los desarrolladores crean deberían funcionar dentro del marco de seguridad del producto y tener en cuenta las siguientes funciones de seguridad:

- **Métodos de devolución de llamadas de agentes:** Oracle Solaris Cluster admite un amplio rango de agentes de aplicaciones, que se implementan como un conjunto de métodos de devolución de llamadas para controlar el inicio, detención, sondeo y validación de la aplicación. Los métodos de devolución de llamada como Start, Stop o Validate siempre se ejecutan como root. Si uno de estos archivos de método ejecutables puede ser modificado por un usuario que no sea root, esto crea una vulnerabilidad en la que un usuario que no es root puede alcanzar un incremento no autorizado de privilegios mediante la inserción de código en el método de devolución de llamada. Oracle Solaris Cluster comprueba la propiedad y los permisos de dichos ejecutables de método de devolución de llamada. La comprobación es controlada por la configuración de propiedad de cluster resource_security. Si resource_security se establece en SECURE y resulta que el código de método puede ser modificado por un usuario no root, la ejecución del método falla.

Los métodos del agente, en cambio, ejecutan programas externos con frecuencia, como comandos administrativos específicos de la aplicación. Los métodos del agente deberían ejecutar todos esos programas externos con un envoltorio para asegurarse de que el programa externo se ejecute con el menor privilegio posible. Oracle Solaris Cluster proporciona las propiedades application_user y resource_security y

la API `scha_check_app_user` para activar los servicios de datos y asegurar que la aplicación se ejecute de manera segura. El comando `scha_check_app_user` se puede llamar en secuencias de comandos para verificar el nombre de usuario con los ajustes de `Application_user` y `Resource_security` establecidos. Consulte las páginas del comando `man scha_check_app_user(1HA)`, `r_properties(5)` y `cluster(1CL)` para obtener más información.

- **Acceso seguro a una aplicación:** algunos casos requerirán el acceso seguro a una aplicación cuando ejecute comandos de gestión o configuración. Este acceso seguro debería realizarse con un método basado en credenciales, como el Oracle Wallet Manager. Si debe proporcionar una contraseña, la contraseña se debe utilizar de manera segura y almacenar de forma oculta. Por ejemplo, no debe transportarse en la línea de comandos donde está visible para un usuario a través del comando `ps`. Oracle Solaris Cluster proporciona el comando `clpstring` para permitirle crear cadenas privadas que pueden utilizarse para almacenar contraseñas cifradas de manera segura en el cluster y recuperar a las mismas cuando las contraseñas deben utilizarse para realizar tareas de gestión. Consulte la página del comando `man clpstring(1CL)` para obtener información sobre este comando.

Consulte la [Oracle Solaris Cluster Data Services Developer's Guide](#) para obtener más información acerca de cómo utilizar estas funciones de seguridad al desarrollar servicios de datos.

Índice

A

- acceso seguro a una aplicación, 16
- adición de nodos, 13
- auditoría, 14
- Automated Installer, 11, 12

C

- cluster
 - configuración, 11
 - funciones de seguridad, 13
 - instalación, 11
- cluster global, 10, 11
- clusters de zona
 - Trusted Extensions, 13
- clusters de zona de marca labeled, 13
- clusters de zonas, 10
 - Geographic Edition, 11
 - marca labeled, 13
- comando claccess , 13
- comando clauth , 11
- conexión, 14
- conexiones seguras para consolas de cluster, 14
- configuración, 11, 12
- contenedor de agente común, 15

D

- desarrolladores
 - consideraciones de seguridad para, 15

E

- endurecimiento del SO, 14

F

- funciones de seguridad, 14

I

- instalación, 11
- IPsec, 15

O

- Oracle Solaris Cluster
 - seguridad, 10
 - visión general, 10
- Oracle Solaris Cluster Geographic Edition
 - beneficios, 10
 - configuración, 12
 - instalación, 12
 - visión general, 10

P

- paquetes
 - Oracle Solaris Cluster, 11
 - Oracle Solaris Cluster Geographic Edition, 12

R

- RBAC, 13, 14
- recuperación ante desastres, 10
- replicación de datos, 10

S

- seguridad

- certificados, 14
- consideraciones para desarrolladores, 15
- instalación de Geographic Edition, 12
- principios generales, 10

T

- Trusted Extensions, 13

U

- utilidad `clsetup`, 13
- utilidad `pconsole` , 14

V

- visión general
 - Oracle Solaris Cluster, 10
 - Oracle Solaris Cluster Geographic Edition, 10