

StorageTek Automated Cartridge System Library Software

Instalación, configuración y operación del cluster de High Availability

Versión 8.4

E69742-01

Diciembre de 2015

StorageTek Automated Cartridge System Library Software

Instalación, configuración y operación del cluster de High Availability

E69742-01

Copyright © 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 comunique 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 filiales 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 filiales. 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.

Tabla de contenidos

Prefacio	9
Destinatarios	9
Accesibilidad a la documentación	9
Convenciones	9
1. Introducción	11
Requisitos del sistema	12
Opciones de cliente	12
Opciones del servidor	12
Opciones de matriz de almacenamiento	13
Requisitos de la red	13
Requisitos de software	13
Lista de comprobación previa a la instalación para ACSLS HA	13
Personal de asistencia técnica de Oracle	14
Personal de asistencia técnica al cliente	14
Hardware para el sistema ACSLS HA	14
Información de red	15
Direcciones IP y nombres de host asignados a los dos servidores ACSLs HA	15
Comunicación con bibliotecas HLI	15
Firewalls	15
Cambiador de medios SCSI mediante fibra	16
Medios de instalación	16
Aplicaciones de clientes (copia de seguridad o ILM) que se comunican con ACSLs	16
Grupo e ID de usuario de ACSLS	16
Procedimiento de instalación de alto nivel	17
2. Configuración del sistema Solaris para ACSLS HA	19
Configuración de archivo <code>/etc/hosts</code>	19
Configuración de acceso para <code>root</code>	19
Configuración de red de rutas múltiples	20
Interfaz pública e IPMP	22
Interfaz de biblioteca	25
Configuración de disco de rutas múltiples	26

3. Configuración del sistema de archivos con ZFS	29
Creación de un sistema de archivos raíz reflejado	29
Creación de un sistema de archivos reflejado para la aplicación ACSLS	31
4. Descarga de paquetes de software	35
Descarga de paquetes de software	35
Descargando ACSLS 8.4	35
Descarga de PostgreSQL 8.4 (opcional)	36
Descarga de Oracle Cluster 4.2	36
Cómo descargar la imagen base de Solaris Cluster	36
Cómo determinar si necesita la actualización de parche de Solaris Cluster	37
Descarga de ACSLS HA 8.4	37
Descarga de parches	38
Descarga de la documentación del producto	38
5. Instalación de ACSLS 8.4	39
Instalación en el primer nodo	39
Instalación en el nodo adyacente	40
6. Instalación de Solaris Cluster 4.2	43
Instalación del paquete del cluster	43
Rutina <i>scinstall</i>	45
Ejecución de <i>scinstall</i>	46
Verificación de la configuración del cluster	47
7. Instalación y configuración de ACSLS HA 8.4	51
Procedimiento de instalación básico	51
Configuración de ACSLS HA	52
Supervisión de la operación del cluster de ACSLS	53
Utilidad <i>ha_console.sh</i>	54
Verificación de la operación del cluster	55
8. Ajuste de ACSLS HA	59
Definición de una política de failover para comunicaciones de la biblioteca	59
Bibliotecas con Redundant Electronics (RE)	60
Configuración de <i>Pingpong_interval</i> de failover	60
Registro de notificación por correo electrónico de eventos del sistema	61

9. Operación del cluster de ACSLS	63
Inicio del control del cluster de ACSLS	64
Configuración de la política de failover para acsls-storage	64
Operación y mantenimiento de ACSLS bajo el control del cluster	65
Suspensión del control del cluster	65
Apagado del cluster de ACSLS HA	66
Encendido de un sistema de cluster de ACSLS suspendido	67
Creación de un único cluster de nodo	67
10. Instalación, actualización y eliminación de componentes de software	69
Instalación de parches para ACSLS	69
Eliminación del paquete ACSLS	70
Instalación de versiones de actualización de ACSLS	71
Reinstalación de ACSLS HA o instalación de actualizaciones	71
Actualización de Solaris Cluster	73
Eliminación de Solaris Cluster	73
11. Registro, diagnóstico y prueba de cluster	75
Supervisión de la operación general del cluster	75
Utilidades de supervisión del cluster	76
Pruebas de recuperación y failover	77
Condiciones de recuperación	77
Supervisión de recuperación	77
Pruebas de recuperación	78
Condiciones de failover	79
Supervisión de failover	80
Pruebas de failover	80
Pruebas adicionales	81
12. Consejos de resolución de problemas	83
Verificación de que ACSLS se esté ejecutando	83
Control de la conexión con el recurso de disco compartido	84
Cuando no se puede hacer ping en el host lógico	85
Comprobación de la interconexión entre nodos	86
Índice	87

Lista de figuras

2.1. Tarjeta de interfaz de biblioteca HBRr única conectada a dos puertos Ethernet en cada nodo de servidor	21
2.2. Configuración de HBC dual en una biblioteca con Redundant Electronics	22
2.3. Dos conexiones de fibra por servidor a la matriz de almacenamiento compartido externo	26
7.1. Ejemplo de event_tail.sh	53
7.2. Organización de ventanas de terminal Gnome	54

Prólogo

Esta guía contiene directrices y procedimientos para la instalación y la configuración del software del cluster de StorageTek Automated Cartridge System Library Software High Availability (ACSLS HA) 8.4 de Oracle en los sistemas basados en SPARC y los sistemas basados en x86 de Solaris.

ACSLS HA 8.4 se ha diseñado específicamente para admitir ACSLS 8.4 en Solaris 11.2 con sistemas de archivos ZFS. Esta versión admite la instalación del software ACSLS en cualquier sistema de archivos definido por el usuario.

Destinatarios

Este documento está destinado a los administradores de sistemas UNIX con experiencia y suficiente conocimiento sobre el sistema operativo Solaris 11 con ZFS, además de conocimiento práctico de Solaris Cluster 4.x.

En este documento, se ofrece información básica moderada para la mayoría de las tecnologías utilizadas y proporciona indicaciones para los procedimientos de instalación anticipada estándar. Sin embargo, este documento solo no reemplaza el requisito implícito de experiencia y conocimientos del sistema UNIX.

Accesibilidad a la documentación

Para obtener información sobre el 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 My Oracle Support

Los clientes de Oracle que hayan contratado servicios de soporte electrónico pueden acceder a ellos mediante My Oracle Support. Para obtener información, visite <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> o, si tiene alguna discapacidad auditiva, visite <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs>.

Convenciones

Se han utilizado las siguientes convenciones en este documento:

Convención	Significado
Negrita	El formato de negrita indica elementos de la interfaz gráfica de usuario asociados a una acción, o bien términos definidos en el texto o en el glosario.
<i>Cursiva</i>	El formato de cursiva indica títulos de libros, énfasis o variables de pendientes de asignación para los que se proporcionan valores concretos.

Convención	Significado
<i>monospace</i>	El formato de monoespacio indica comandos en un párrafo, direcciones URL, código en los ejemplos, texto que aparece en la pantalla o texto que se introduce.

Capítulo 1. Introducción

ACSLs HA es una configuración de hardware y software que proporciona redundancia dual, recuperación automática y recuperación de failover automática para garantizar un servicio de control de bibliotecas de cintas ininterrumpido si se producen errores en un componente o subsistema. En este documento, se explican los procedimientos de configuración, instalación y prueba necesarios para brindar alta disponibilidad al software ACSLS.

Es conveniente consultar el proceso de instalación completo antes de comenzar con el procedimiento. El proceso de instalación de una aplicación en cluster implica varios pasos que requieren estricta atención a los detalles. Este procedimiento normalmente está a cargo de especialistas en integración de sistemas Unix.

Existen múltiples componentes de hardware y software asociados con el sistema ACSLS HA, y la totalidad del procedimiento de instalación puede tardar varios días. En el caso de los entornos de bibliotecas de producción, se recomienda a los clientes instalar un servidor ACSLS simple e independiente para manejar la producción de bibliotecas durante la instalación de ACSLS HA.

La configuración es un cluster de dos nodos. Incluye dos subsistemas completos (uno activo y otro en espera) con software de supervisión capaz de detectar errores graves del sistema. Puede conmutar el control del sistema primario al sistema en espera para cualquier error no recuperable del subsistema. La configuración proporciona fuentes de alimentación redundantes, redes redundantes e interconexiones de E/S que pueden recuperar los errores de comunicación del subsistema de manera instantánea sin necesidad de realizar un switchover general.

ACSLs HA aprovecha las funciones de supervisión y failover en Solaris Cluster y las funciones de rutas múltiples del sistema operativo Solaris para brindar operación de control flexible de bibliotecas con mínima inactividad. Solaris ofrece rutas múltiples de IP para garantizar conectividad de red ininterrumpida y E/S de disco de rutas múltiples con RAID1 para garantizar acceso ininterrumpido a los datos del sistema. Solaris Cluster observa el estado de los recursos del sistema, incluso el sistema operativo, el hardware interno y los recursos de E/S externos, y puede gestionar un switchover del sistema si es necesario. Además, el agente de ACSLS HA supervisa la aplicación ACSLS, la base de datos, el sistema de archivos y la conectividad con los recursos de la biblioteca StorageTek, invocando el servicio de failover de Solaris Cluster, si es necesario.

En esta configuración redundante, el servidor de control de bibliotecas ACSLS tiene una identidad de host lógico única que siempre es conocida dentro de la estructura del cluster y

para el resto del mundo. Esta identidad se transfiere automáticamente según las necesidades entre los nodos del cluster con mínima inactividad durante la transición.

Antes de comenzar el proyecto, revise el proceso completo de instalación y configuración de ACSLS HA tal como se documenta aquí. Si lo desea, se puede establecer que los servicios avanzados de atención al cliente de Oracle aconseje, asista o maneje toda la instalación.

Para obtener la documentación de ACSLS, consulte Oracle Technical Network (OTN) en:

<http://docs.oracle.com/>

Requisitos del sistema

Una configuración de servidor ACSLS-HA se compone de dos nodos de servidor Solaris que comparten una matriz de discos RAID externa.

Opciones de cliente

ACSLS HA admite todos los clientes de ACSLS que usan como interfaz de red la interfaz de programación de aplicaciones del sistema de cartuchos automatizado (ACSAPI). Una sola dirección IP de red se comparte entre los dos nodos de servidor, lo que permite a los clientes ACSAPI dirigirse a ACSLS con un ID de host virtual común.

En este producto, no se admiten bibliotecas lógicas presentadas a clientes de canal de fibra mediante SMCE (emulación del cambiador de medios de SCSI).

Opciones del servidor

ACSLS-HA 8.4 se debe ejecutar en cualquier sistema que cumpla con los requisitos mínimos de hardware para Solaris Cluster 4.2. Para conocer los requisitos específicos de plataformas de servidores, consulte el documento titulado *Requisitos del sistema de Oracle Solaris Cluster*.

<http://www.oracle.com/technetwork/server-storage/solaris-cluster/documentation/sysreq-cluster-166689.pdf>

Para evitar cualquier único punto de error, cada nodo de servidor ACSLS HA debe estar configurado con lo siguiente:

- Fuente de alimentación dual (redundante)
- Seis puertos Ethernet 10/100/1000 Base-T
- Dos puertos de canal de fibra (si se utiliza el almacenamiento con conexión a FC)
- Dos puertos SAS (si se utiliza el almacenamiento con conexión a SAS)

Si el sistema está destinado para uso con bibliotecas lógicas, se requiere al menos un puerto de canal de fibra adicional dedicado en configuraciones que admiten aplicaciones de clientes SCSI.

Se requiere un puerto de canal de fibra adicional para bibliotecas conectadas a fibra, como SL500 o SL150.

Opciones de matriz de almacenamiento

Para conocer los subsistemas de matriz de discos admitidos, consulte el documento titulado *Programa de socios de almacenamiento de Oracle Solaris Cluster*.

<http://www.oracle.com/technetwork/server-storage/solaris-cluster/partnerprogram-cluster-168135.pdf>

Requisitos de la red

Debe reservar siete direcciones IP en total.

1. Host lógico (IP virtual del cluster [VIP])
2. Dirección IP del nodo 1
3. Dirección IP del nodo 2
4. Dirección IP de origen de interfaz 1 de biblioteca (nodo 1)
5. Dirección IP de origen de interfaz 2 de biblioteca (nodo 1)
6. Dirección IP de origen de interfaz 1 de biblioteca (nodo 2)
7. Dirección IP de origen de interfaz 2 de biblioteca (nodo 2)

Lo ideal sería que la interfaz 1 de la biblioteca estuviera en una subred diferente de la interfaz 2 de la biblioteca (consulte la [Figura 2.1, “Tarjeta de interfaz de biblioteca HBRr única conectada a dos puertos Ethernet en cada nodo de servidor”](#)).

Requisitos de software

ACSLs HA 8.4 requiere los siguientes componentes de software:

- Oracle Solaris 11.2 (SPARC o X86)
- Oracle Solaris Cluster 4.2

Lista de comprobación previa a la instalación para ACSLS HA

Antes de instalar un nuevo sistema ACSLS HA o actualizar un sistema ACSLS HA a una nueva versión, determine y registre la información sobre el entorno del cliente en el que se instalará ACSLS HA.

Si finaliza esta lista de comprobación previa a la instalación, eliminará el riesgo. Esta lista de comprobación garantiza que la instalación se realice sin problemas y no se demore mientras espera recibir detalles sobre el entorno del cliente.

Personal de asistencia técnica de Oracle

- ¿Quién es el personal local de Oracle que brinda asistencia a este cliente?
- ¿Alguno de ellos tiene experiencia con la administración del sistema Solaris?
- ¿Alguno de ellos tiene experiencia con ACSLS?
- ¿Alguno de ellos tiene experiencia con ACSLS HA?

Personal de asistencia técnica al cliente

- ¿Quién es el personal de administración del sistema del cliente que brindará asistencia para actividades relacionadas con los servidores ACSLS HA y la red del cliente?
- ¿Alguno de ellos tiene experiencia con la administración del sistema Solaris?
- ¿Alguno de ellos tiene experiencia con ACSLS?
- ¿Alguno de ellos tiene experiencia con ACSLS HA?
- ¿Quiénes son los administradores de la red?

Hardware para el sistema ACSLS HA

- ¿Qué modelo de servidores Oracle Sun?
- ¿Qué nivel de versión y actualización de Solaris?
- Memoria (10 GB como mínimo).
- Se necesitan dos unidades de inicio en cada servidor para reflejar los discos.
- ¿De qué modelo es el disco compartido? ¿Es compatible con Solaris Cluster?
- Se utilizan SAS o HBA de fibra para conectar cada servidor ACSLS con la matriz de discos compartidos.
- Se requieren seis puertos Ethernet en cada servidor ACSLS.
- Si ACSLS gestiona bibliotecas conectadas a fibra (SL500 o SL150) o presenta bibliotecas lógicas que utilizan puertos de modo de destino de fibra, se necesita un HBA de fibra en cada servidor ACSLS.
- ¿Qué cables de alimentación se necesitan para conectar los servidores Solaris y la matriz de discos con el entorno del cliente? Por ejemplo, los conectores deben coincidir con los tomas de alimentación en el sitio del cliente para evitar demoras en la instalación de HA.
- Antes de comenzar una instalación de HA, asegúrese de que los servidores HA y la matriz de discos compartidos se hayan configurado correctamente:
 - Para satisfacer el requisito de los seis puertos para las conexiones Ethernet, cada servidor HA debe contar con una tarjeta de controlador de interfaz de red (NIC).
 - Debe conocer el tipo de interfaz de la matriz de discos compartidos externa y asegurarse de que cada servidor tenga configurado un HBA compatible.
 - Si ACSLS se comunicará con bibliotecas conectadas a fibra, como SL500s o SL150s, se requieren HBA de fibra.
 - Si ACSLS presenta bibliotecas lógicas mediante el modo de destino de fibra, se requieren HBA de fibra de Qlogic.

Información de red

Revise la siguiente información de la red.

Direcciones IP y nombres de host asignados a los dos servidores ACSLS HA

- En total, se necesitan nueve direcciones IP para la instalación:
 - Dirección local del nodo de servidor 1 de ACSLS
 - Dirección local del nodo de servidor 2 de ACSLS
 - Dirección del host lógico (dirección IP virtual compartida entre dos nodos HA)
 - Conexión a de biblioteca desde nodo 1
 - Conexión b de biblioteca desde nodo 1 (para dos TCP/IP o redundancia de TCP/IP múltiple)
 - Conexión a de biblioteca desde nodo 2
 - Conexión b de biblioteca desde nodo 2 (para dos TCP/IP o redundancia de TCP/IP múltiple)
 - ILOM en nodo 1
 - ILOM en nodo 2
- ¿Los clientes de ACSAPI se comunicarán con ACSLS?
 - Después un evento de failover, el nodo activo asume la dirección IP virtual. Los clientes de ACSLS pueden acceder a la dirección IP virtual, sin importar qué nodo esté activo.
 - ¿Sabe cómo configurar la dirección IP virtual de ACSLS HA o el nombre de host en los clientes ACSAPI? Esta configuración depende de la aplicación ISV que se está ejecutando en el cliente.
- Las direcciones IP que utiliza ACSLS para comunicarse con bibliotecas conectadas a TCP/IP (SL8500s, SL3000s y 9310s).
- Para evitar un único punto de error, es conveniente establecer cada conexión de biblioteca redundante por su propia subred independiente. Para evitar problemas relacionados con un alto volumen de tráfico de red, la subred se debe reservar para la comunicación de la biblioteca y no se debe someter a la interferencia de las conversaciones de red generales.
- Las direcciones IP y las contraseñas necesarias para tener acceso al procesador de servicios (por ejemplo, ILOM o ALOM) en cada nodo de ACSLS HA.

Comunicación con bibliotecas HLI

¿La comunicación entre bibliotecas conectadas a TCP/IP y ACSLS en una subred está protegida del tráfico de difusión?

Firewalls

- ¿Hay firewalls entre los clientes ACSAPI y el sistema ACSLS HA?

- ¿Hay firewalls entre el sistema ACSLS HA y las bibliotecas que gestiona?

Si existen firewalls, consulte el apéndice "Opción de seguridad de firewall" en la *Guía del administrador de ACSLS 8.4* a fin de obtener información sobre cómo configurar clientes ACSLS y ACSAPI para comunicarse a través de firewalls.

Cambiador de medios SCSI mediante fibra

- ¿Este sistema ACSLS tiene bibliotecas lógicas para clientes que utilizan puertos de modo de destino de canal de fibra? En caso afirmativo, requiere un HBA de fibra de QLogic.

Medios de instalación

- ¿Habrá un acceso directo o indirecto de los servidores HA a Internet para permitir descargas de software desde el sitio web Oracle eDelivery, incluso Oracle Solaris Cluster, ACSLS, ACSLS HA y otros paquetes o parches necesarios?

Si el acceso es indirecto, asegúrese de poder transferir archivos de Internet a servidores HA.

- Suponiendo que el software se descargará directamente desde Internet en máquinas locales, asegúrese de que la totalidad de la información del proxy para la configuración del explorador esté disponible en el momento de la instalación.

Aplicaciones de clientes (copia de seguridad o ILM) que se comunican con ACSLS

- ¿Los clientes ACSAPI (como aplicaciones de copia de seguridad o Information Lifecycle Management) se comunicarán con ACSLS?
 - Si los clientes ACSAPI se comunicarán con ACSLS, ¿cuáles son las aplicaciones de clientes (como NetBackup, Oracle SAM)?
 - ¿Qué versiones de estos clientes se utilizan?
 - Si los clientes se ejecutan en Windows y utilizan LibAttach, ¿qué versión de LibAttach ejecutan?
- ¿Las aplicaciones de clientes se comunican con bibliotecas lógicas de ACSLS mediante los puertos de modo de destino de canal de fibra?
 - ¿Cuáles son las aplicaciones de clientes (como NetBackup y Oracle SAM)?
 - ¿Qué versiones de estos clientes se utilizan?

Grupo e ID de usuario de ACSLS

ACSLs requiere los siguientes ID de usuario en el grupo *acsls*: *acsss*, *acsdb* y *acssa*.

¿Estos ID de usuario y el grupo *acsls* pueden configurarse localmente en los servidores ACSLS HA o deben integrarse al sistema de gestión de contraseñas y usuarios central del sitio?

Procedimiento de instalación de alto nivel

La instalación completa de ACSLS HA implica los siguientes pasos:

1. Instale dos servidores de plataformas Solaris conectados a un canal de fibra externo común o una matriz de discos SAS2. Instale Solaris 11.2 en cada servidor.

Consulte el documento *Instalación de sistemas Oracle Solaris 11* disponible en la biblioteca de Oracle Technology Network:

<http://www.oracle.com/technetwork/documentation/solaris-11-192991.html>

2. Configure el sistema Solaris básico.
 - Privilegios de acceso de usuarios
 - Acceso de red y E/S de disco de rutas múltiples

Consulte [Capítulo 2, Configuración del sistema Solaris para ACSLS HA \[19\]](#).

3. Configure los sistemas de archivos ZFS.
 - agrupación de almacenamiento raíz
 - agrupación de almacenamiento acsls

Consulte [Capítulo 3, Configuración del sistema de archivos con ZFS](#).

4. Descargue paquetes de software. Consulte [Capítulo 4, Descarga de paquetes de software \[35\]](#).
 - ACSLS 8.4.0
 - Solaris Cluster 4.2
 - ACSLS HA 8.4.0

Consulte [Capítulo 4, Descarga de paquetes de software \[35\]](#).

5. Instale ACSLS 8.4.0 y la actualización del parche (si corresponde). Consulte [Capítulo 5, Instalación de ACSLS 8.4 \[39\]](#).
6. Instale Solaris Cluster 4.2 y la actualización del parche (si corresponde). Consulte [Capítulo 6, Instalación de Solaris Cluster 4.2](#).
7. Instale ACSLS HA 8.4.0. Consulte [Capítulo 7, Instalación y configuración de ACSLS HA 8.4](#).
8. Ajuste la operación del cluster para ACSLS HA. Consulte [Capítulo 8, Ajuste de ACSLS HA \[59\]](#).

Capítulo 2. Configuración del sistema Solaris para ACSLS HA

Después de instalar el sistema Solaris 11.2 básico, existen tres contextos que contienen requisitos específicos de configuración para Solaris Cluster y ACSLS HA.

1. Configure */etc/hosts*.
2. Configure privilegios de acceso para el usuario *root*.
3. Configure la interfaz de red para obtener acceso a Internet mediante rutas múltiples.
4. Configure la E/S de disco de rutas múltiples.

Configuración de archivo */etc/hosts*

El archivo */etc/hosts* de cada nodo debe contener entradas para el host local, los dos nombres de nodo del cluster y sus direcciones IP, y el host lógico.

```
127.0.0.1          localhost  loghost
129.99.99.101     thisNode.domain.com  thisNode
129.99.99.102     sisterNode
129.99.99.100     logicalHost.domain.com  logicalHost
```

Configuración de acceso para *root*

Las operaciones de failover y supervisión de Solaris Cluster son manejadas por el usuario *root* que debe tener control sobre todo el cluster desde cualquier nodo. El usuario *root* se establece como usuario de confianza, lo que permite brindar acceso a la red privada entre los nodos con la autenticación de shell seguro (*ssh*).

1. Active el acceso root directo a cada nodo desde un sistema externo. Edite el archivo */etc/user_attr* y comente (o elimine) la línea que especifica un rol para *root*.

```
# root:::::type=role
```
2. Permita a *root* iniciar sesión en el sistema desde otros puntos diferentes de la consola del sistema.

Edite el archivo */etc/default/login* y comente la línea que especifica acceso solo a la consola.

```
# CONSOLE=/dev/console
```

3. Permita el acceso de inicio de sesión de shell seguro para *root*.

Edite el archivo */etc/ssh/sshd_config* y especifique **yes** (sí) para *PermitRootLogin*.

```
PermitRootLogin=yes
```

Repita los pasos de 1 a 3 en el nodo adyacente.

4. Establezca *root* como usuario de confianza. Esto define un protocolo de inicio de sesión para *root* a cualquier nodo desde el nodo hermano para el cual se establece la autenticación sin necesidad de contraseña.
 - a. Cree un par de claves RSA pública y privada. Para permitir el inicio de sesión de un nodo a otro sin contraseña, no introduzca una frase de contraseña.

```
# cd /root/.ssh
# ssh-keygen -t rsa
Enter file in which to save the key (//.ssh/id_rsa): ./id_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in ./id_rsa.
Your public key has been saved in ./id_rsa.pub.
The key fingerprint is:
1a:1b:1c:1d:1e:1f:2a:2b:2c:2d:2e:2f:ea:3b:3c:3d root@node1
```

De esta forma, se crean dos archivos en el directorio */root/.ssh*: *id_rsa* e *id_rsa.pub*.

- b. Copie *id_rsa.pub* en el directorio */root/.ssh* del nodo hermano:

```
# cat id_rsa.pub | ssh root@node2 /
'cat >> /root/.ssh/authorized_keys'
Password:
```

- c. Con la clave de autenticación en su lugar, pruebe la capacidad para confirmar comandos de manera remota sin contraseña.

```
# hostname
node1
# ssh root@node2 hostname
node2
```

Configuración de red de rutas múltiples

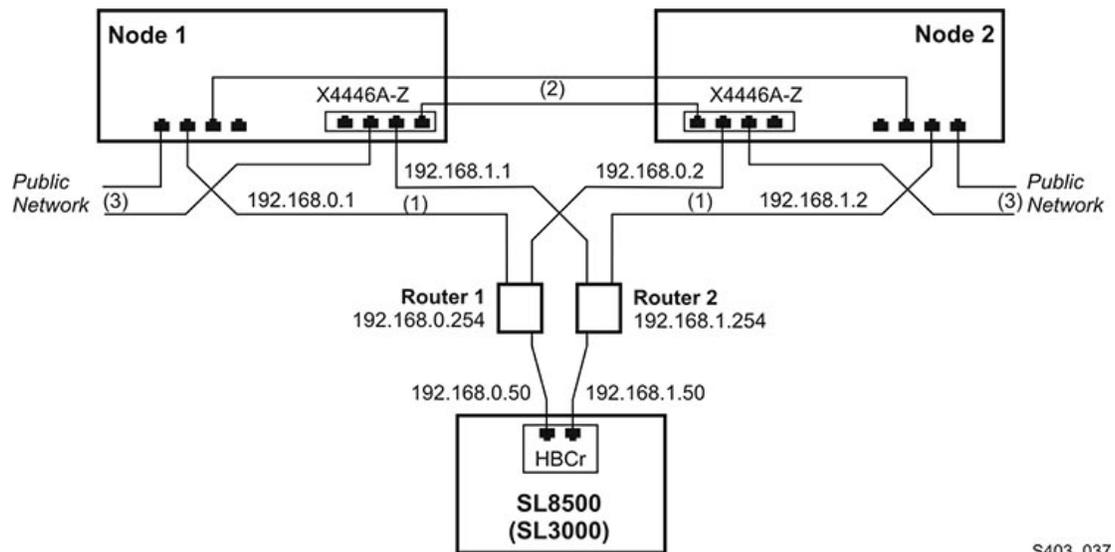
La redundancia es el esquema general para las soluciones informáticas de alta disponibilidad. La redundancia se aplica no solo a los servidores, sino a cada interfaz de comunicación en

cada servidor. Para la interfaz pública, esto significa utilizar rutas múltiples de protocolo de Internet (IPMP) en Solaris. Las rutas múltiples de protocolo de Internet proporcionan recuperación instantánea de NIC para comunicaciones de red con errores sin necesidad de realizar un failover del sistema general. Para la interfaz de la biblioteca, esto significa utilizar una conexión TCP/IP dual con dos interfaces de red en dos rutas independientes. Si se produce un error en algún elemento de una ruta, ACSLS continúa comunicándose por la interfaz alternativa.

ACSLS HA requiere conexiones de red redundantes para lo siguiente:

- comunicaciones públicas y de clientes
- comunicaciones de la biblioteca
- comunicaciones de cluster privadas dentro de nodos

Figura 2.1. Tarjeta de interfaz de biblioteca HBRr única conectada a dos puertos Ethernet en cada nodo de servidor

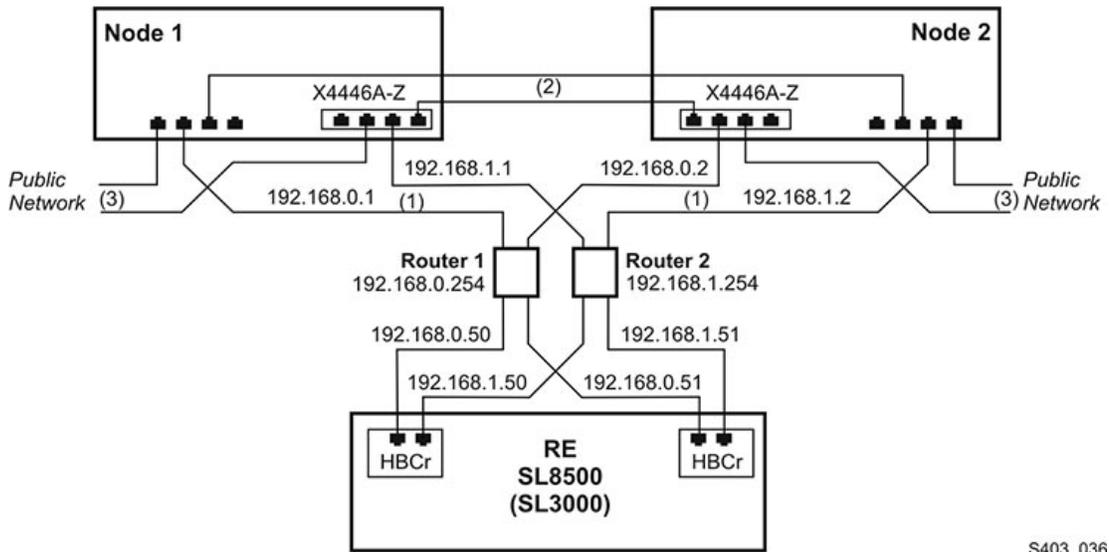


S403_037

En las figuras de esta sección, se muestran ocho puertos Ethernet accesibles con dos controladores separados en cada servidor. Seis puertos proporcionan las tres conexiones redundantes. Dos puertos en esta configuración permanecen sin utilizar. A pesar de la aparente complejidad, solo hay tres conexiones Ethernet de dos rutas desde cada servidor:

- comunicación entre servidor y biblioteca
- intercambio de latidos de servidor a servidor en una red privada
- comunicación de servidor a cliente en una red pública

Figura 2.2. Configuración de HBC dual en una biblioteca con Redundant Electronics



S403_036

En una biblioteca con Redundant Electronics, existen dos rutas independientes de cada nodo de servidor a cada controlador de biblioteca HBCr. Si se produce un error en la comunicación con ambos puertos en una interfaz HBCr, ACSLS HA invoca una conmutación automática a una tarjeta HBCr alternativa. Todo esto se lleva a cabo sin necesidad de realizar un failover del nodo de servidor alternativo.

Interfaz pública e IPMP

Solaris IPMP ofrece un mecanismo para desarrollar interfaces de red redundantes con el fin de proteger contra errores de NIC, cables, conmutadores u otro hardware de red. Cuando se configura IPMP en el host Solaris, se combinan dos o más interfaces de red físicas en un único grupo IPMP.

Para ver una asignación de nombres de interfaces de redes a dispositivos físicos, utilice el comando `dladm show-phys`:

Por ejemplo:

```
# dladm show-phys
LINK      MEDIA      STATE    SPEED  DUPLEX    DEVICE
net2      Ethernet  up       100    full     ixgbe1
net3      Ethernet  up       10000  full     ixgbe3
net0      Ethernet  up       10000  full     ixgbe2
net1      Ethernet  up       1000   full     ixgbe0
```

Para mostrar el estado de interfaces de redes configuradas, utilice `ipadm`.

Por ejemplo:

```
# ipadm
NAME          CLASS/TYPE STATE UNDER ADDR
lo0           loopback  ok    --    --
  lo0/v4      static    ok    --    127.0.0.1/8
  lo0/v6      static    ok    --    ::1/128
net1          ip        ok    --    --
  net1/v4     static    ok    --    129.99.99.99/24
  net1/v6     addrconf ok    --    fe99::999:999:ff23:ee02/10
net4          ip        ok    --    --
  net4/v4     static    ok    --    129.999.99.99/24
```

Las dos interfaces deben estar configuradas y asignadas a un ID de grupo común para ACSLS HA. Entre estas interfaces, podría estar la interfaz principal del servidor. En este caso, dado que la dirección *ip* ya está asignada a la interfaz (y no al grupo), será necesario anular la configuración de esta interfaz y, luego, volver a configurarla en el grupo *ipmp*.

Dado que se interrumpe la comunicación de red durante esta operación, es necesario realizar los siguientes pasos de la consola del servidor.

Para anular la configuración de la interfaz principal existente:

```
ipadm delete-addr <primary interface>
```

Por ejemplo:

```
# ipadm delete-addr net0/v4
```

```
ipadm delete-ip <primary interface>
```

Por ejemplo:

```
# ipadm delete-ip net0
```

Para volver a configurar la interfaz principal:

```
ipadm create-ip <primary interface>
```

Por ejemplo:

```
# ipadm create-ip net0
```

Para crear una segunda interfaz principal:

```
ipadm create-ip <primary_interface>
```

Por ejemplo:

```
# ipadm create-ip net5
```

Para crear el grupo *ipmp*:

```
ipadm create-ipmp <group_name>
```

Por ejemplo:

```
# ipadm create-ipmp ipmp0
```

Nota:

El nombre del grupo debe ser alfanumérico.

Para asignar el host *ip-address* al grupo:

```
ipadm create-addr -T static -a <ip-address> <group_name>
```

Por ejemplo:

```
# ipadm create-addr -T static -a 129.99.99.9 ipmp0
```

Para agregar la interfaz principal al grupo:

```
ipadm add-ipmp -i <primary_interface> <group_name>
```

Por ejemplo:

```
# ipadm add-ipmp -i net0 ipmp0
```

Para agregar una segunda interfaz al grupo:

```
ipadm add-ipmp -i <second_primary_interface> <group_name>
```

Por ejemplo:

```
# ipadm add-ipmp -i net5 ipmp0
```

Verifique la configuración de *ipmp* mediante *ipmp*:

```
# ipadm
NAME                CLASS/TYPE STATE    UNDER    ADDR
ipmp0               ipmp      ok      --        --
  ipmp0/v4          static    ok      --        123.45.67.89/8
lo0                 loopback  ok      --        --
  lo0/v4            static    ok      --        127.0.0.1/8
  lo0/v6            static    ok      --        ::1/128
net0                ip        ok      ipmp0     --
net5                ip        ok      ipmp0     --
```

Observe que las dos interfaces de red fueron configuradas en el grupo ipmp0. Observe que la dirección IP versión 4 fue asignada al grupo ipmp0.

Es posible que necesite reiniciar el sistema para confirmar estos cambios y establecer comunicaciones de red según la nueva configuración.

Repita la configuración de red en el nodo hermano.

La asignación entre el grupo *ipmp* y la dirección IP pública del cluster se establece cuando inicia el cluster con *start_acslsha.sh*. Consulte [Capítulo 9, Operación del cluster de ACSLS](#).

Interfaz de biblioteca

Se necesitan dos interfaces de red restantes para la configuración de la biblioteca. Para este ejemplo, se usan *net1* y *net6*. Observe (en la [Figura 2.1, “Tarjeta de interfaz de biblioteca HBRr única conectada a dos puertos Ethernet en cada nodo de servidor”](#) y la [Figura 2.2, “Configuración de HBC dual en una biblioteca con Redundant Electronics”](#)) que estas dos conexiones se enrutan en subredes separadas para eliminar un enrutador como punto único de error entre el servidor en cluster y la biblioteca.

1. Cree las dos interfaces de red en cada nodo.

```
# ipadm create-ip net1
# ipadm create-ip net6
```

2. Asigne *ip-address* para cada interfaz.

```
# ipadm create-addr -T static -a <ip-address> net1/v4
# ipadm create-addr -T static -a <ip-address> net6/v4
```

El objeto de la dirección normalmente se nombra mediante la interfaz y la versión del protocolo: *net1/v4*

3. Verifique la configuración de *ipmp*:

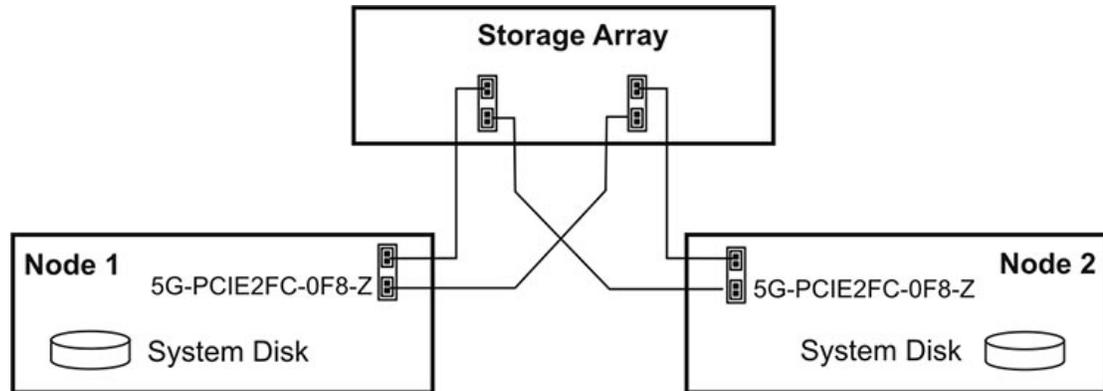
```
# ipadm
NAME                CLASS/TYPE STATE    UNDER    ADDR
ipmp0               ipmp      ok       --       --
  ipmp0/v4          static    ok       --       123.45.67.89/8
lo0                 loopback  ok       --       --
  lo0/v4            static    ok       --       127.0.0.1/8
  lo0/v6            static    ok       --       ::1/128
net0                 ip        ok       ipmp0    --
net1                 ip        ok       --       --
  net1/v4           static    ok       --       192.168.0.1/8
net5                 ip        ok       ipmp0    --
net6                 ip        ok       --       --
  net6/v4           ip        ok       --       192.168.1.1/8
```

- Reinicie cada nodo para que la configuración surta efecto.

Configuración de disco de rutas múltiples

La matriz de discos compartidos externa se conecta a los dos hosts; cada uno con conexiones de fibra o SAS redundantes entre el servidor y la matriz de discos.

Figura 2.3. Dos conexiones de fibra por servidor a la matriz de almacenamiento compartido externo



S403_038

La matriz se debe configurar para presentar dos unidades virtuales al host conectado.

Solaris 11.2 se ocupa de la configuración de rutas múltiples (MPXIO) automáticamente si detecta más de una ruta a un dispositivo de disco. Verifique que su sistema Solaris esté configurado correctamente con conexiones redundantes a cada disco virtual de la matriz.

```
# mpathadm list lu

/dev/rdsk/c0t600A0B800049EE1A0000840552D3E2F9d0s
  Total Path Count: 2
  Operational Path Count: 2
/dev/rdsk/c0t600A0B800049EDD60000DAD52D3DA90d0s2
  Total Path Count: 2
  Operational Path Count: 2
```

La pantalla *mpathadm* debe mostrar dos dispositivos de discos, cada uno con un recuento de rutas operativas de 2.

Si ejecuta ACSLS HA en un sistema SPARC, *mpathadm* no muestra nada hasta que se configure MPXIO. Si la pantalla no muestra nada o muestra una configuración incorrecta, continúe con este punto para configurar MPXIO mediante *stmsboot -e* en el sistema Solaris 11.2. Consulte el documento *Administración de Oracle Solaris: rutas múltiples y configuración de SAN* de la biblioteca de Oracle Technology Network: http://docs.oracle.com/cd/E23824_01/html/E23097.

Tenga en cuenta que los dispositivos con rutas múltiples de E/S de Solaris activadas reciben nombres nuevos que indican que están bajo el control de rutas múltiples de E/S de Solaris. Un dispositivo tiene un nombre diferente a su nombre original.

```
Original device name:    c1t0d0  
Name After stmds boot:  c0t600A0B800049EDD600000C9952CAA03Ed0
```

Capítulo 3. Configuración del sistema de archivos con ZFS

Solaris 11.2 se basa en un sistema de archivos ZFS. La E/S de disco, la partición de disco y el reflejo de disco (o RAID) son manejados completamente por ZFS. En consecuencia, no habría necesidad de realizar la partición del disco (como se hacía generalmente con los sistemas de archivos UFS). La totalidad del disco del sistema se debe presentar como una partición única.

Su matriz de almacenamiento ya está configurada con RAID; por lo tanto, no es esencial configurar un nivel adicional de RAID mediante ZFS para su sistema de archivos ACSLS. La RAID de ZFS es esencial si utiliza discos JBOD simples, pero la RAID adicional es opcional si emplea una matriz de discos completa. Los siguientes ejemplos muestran cada enfoque.

Creación de un sistema de archivos raíz reflejado

1. Su plataforma Solaris debe estar configurada con dos unidades de disco físicas. Particione el disco del sistema y su unidad reflejada para obtener un óptimo rendimiento de ZFS.

En un nuevo sistema, antes de la instalación del sistema operativo, puede particionar cada una de las unidades de disco del sistema de manera que la partición 0 contenga la mayoría (o la totalidad) del espacio en disco. ZFS opera más rápido y con mayor confiabilidad si tiene acceso a todo el disco. Asegúrese de que la partición que defina para ZFS en el segundo disco tenga el mismo tamaño que aquella definida en el disco principal.

En un sistema donde ya está instalado Solaris 11.2, utilice *format* o *fdisk* en el disco del sistema principal para ver el tamaño de la partición *root*. Luego, formatee el segundo disco del sistema con una partición que tenga el mismo tamaño. Etiquete el disco cuando haya finalizado el formateo.

2. Cuando el sistema esté en funcionamiento, verifique *rpool* con el comando *zpool status*.

```
# zpool status
pool: rpool
state: ONLINE
scan: none requested
config:
  NAME                STATE      READ WRITE CKSUM
  rpool                ONLINE    0     0     0
```

```
c0t5000C5000EA48903d0s0 ONLINE 0 0 0
```

- Identifique el segundo disco del sistema y determine el ID del dispositivo.

```
# echo | format
AVAILABLE DISK SELECTIONS:
 0. c0t5000C5000EA48893d0 <SUN146G cyl 14087 alt 2 hd 24 sec 848>
    /scsi_vhci/disk@g5000c5000ea48893
 1. c0t5000C5000EA48903d0 <SUN146G cyl 14087 alt 2 hd 24 sec 848>
    /scsi_vhci/disk@g5000c5000ea48903
```

Elija el dispositivo alternativo que tenga el tamaño más parecido al del dispositivo que se muestra en el paso 2. En este ejemplo, el ID del segundo disco es `c0t5000C5000EA48893d0s`.

- Agregue el segundo disco a *rpool*.

```
# zpool attach -f rpool /
    c0t5000C5000EA48903d0 /
    c0t5000C5000EA48893d0
```

El sistema comienza la reconstrucción de la unidad reflejada y copia los contenidos de la unidad de inicio en la segunda unidad. Esta operación tarda varios minutos y no debe ser interrumpida por un reinicio.

Puede supervisar el progreso mediante lo siguiente:

```
zpool status -v
```

Nota 1: Hasta finalizar la reconstrucción, cualquier pantalla de estado muestra el disco en modo degradado. El disco permanece en estado degradado mientras se copia la información del disco principal al reflejo.

Nota 2: Si se produce un error en *zpool attach* porque el disco está etiquetado como disco EFI, siga el proceso que se describe en el documento *Administración de Solaris: dispositivos y sistemas de archivos*: http://docs.oracle.com/cd/E23824_01/pdf/821-1459.pdf. Este proceso convierte el disco EFI a SMI de la siguiente manera:

```
# format -e
(select the drive to serve as the rpool mirror).
format> partition
partition> print
partition> label
    (specify label type "0")
Ready to label? y
```

```

partition> modify
(select "1" All free Hog)
Do you wish to continue ... yes
Free Hog Partition[6]? (specify partition "0")
(Specify a size of "0" to the remaining partitions)
Okay to make this current partition table? yes
Enter table name: "c1t1d0"
Ready to label disk? y
partition> quit
format> quit

```

5. Confirme la configuración de *rpool* reflejada.

```

# zpool status
pool: rpool
state: ONLINE
scan: resilvered 6.89G in 0h3m with 0 errors
config:

```

NAME	STATE	READ	WRITE	CKSUM
rpool	ONLINE	0	0	0
mirror-0	ONLINE	0	0	0
c0t5000C5000EA48903d0	ONLINE	0	0	0
c0t5000C5000EA48893d0	ONLINE	0	0	0

Repita esta operación en el nodo adyacente.

Creación de un sistema de archivos reflejado para la aplicación ACSLS

El sistema de archivos ACSLS reside en un *zpool* en la matriz de almacenamiento compartido externo. En los siguientes ejemplos, se utiliza una matriz reflejada simple (RAID1) que utiliza solo dos discos. Pueden ser unidades reales, pero es más probable que sean dispositivos virtuales presentados como unidades discretas de la matriz de almacenamiento conectado.

La matriz de almacenamiento ya está configurada con RAID; por lo tanto, no es esencial configurar un nivel adicional de RAID mediante ZFS para su sistema de archivos ACSLS. La RAID de ZFS es esencial si utiliza discos JBOD simples, pero la RAID adicional es opcional si emplea una matriz de discos completa. Los siguientes ejemplos muestran cada enfoque.

1. Prepare la matriz de almacenamiento compartido.

En las configuraciones estándar, utilice una única unidad virtual de su matriz de discos. De lo contrario, la configuración reflejada RAID de ZFS utiliza dos unidades virtuales del mismo tamaño. Puede utilizar la herramienta de administración con la matriz de discos o

la utilidad de formato Solaris para particionar las dos unidades virtuales con el fin de que tengan el mismo tamaño.

- Determine el directorio base que desea para la instalación de ACSLS.

ACSL 8.4 se puede instalar en cualquier sistema de archivos. El sistema de archivos base elegido no debe existir en el sistema *rpool*. Si ya existe, debe destruir el sistema de archivos existente antes de crearlo en el nuevo *zpool*.

Si se utiliza el directorio base */export/home* por defecto para ACSLS, es necesario destruir el sistema de archivos */export* de la agrupación *root* por defecto en Solaris 11.2.

Para confirmar si */export/home* está conectado a *rpool*, ejecute el siguiente comando:

```
# zfs list
```

Para separar */export/home* de *rpool*, primero, guarde los archivos o los directorios que desea preservar. Asegúrese de que no existan directorios de inicio de usuarios actualmente activos en */export/home*. Luego use *zfs destroy* para eliminar todo en */export*:

```
# zfs destroy -r rpool/export
```

Repita este paso para separar *rpool/export* en el nodo adyacente.

- Use *format* para identificar los nombres de dispositivos de las unidades en la matriz de discos conectados:

```
# echo | format
AVAILABLE DISK SELECTIONS:
  0. c0t5000C5000EA48893d0 <FUJITSU-MAY2073RCSUN72G-0501-68.37GB>
    /pci@0,0/pci1022,7450@2/pci1000,3060@3/sd@0,0
    /dev/chassis/SYS/HD0/disk
  1. c0t5000C5000EA48893d0 <FUJITSU-MAY2073RCSUN72G-0501-68.37GB>
    /pci@0,0/pci1022,7450@2/pci1000,3060@3/sd@1,0
    /dev/chassis/SYS/HD1/disk
  3. c0t600A0B800049EDD600000C9952CAA03Ed0 <SUN-LCSM100_F-50.00GB>
    /scsi_vhci/disk@g600a0b800049edd600000c9952caa03e
  4. c0t600A0B800049EE1A0000832652CAA899d0 <SUN-LCSM100_F-50.00GB>
    /scsi_vhci/disk@g600a0b800049ee1a0000832652caa899
```

En este ejemplo, hay dos discos del sistema y los dos discos virtuales presentados de la matriz de discos con nombres de dispositivos que comienzan con *c0t600A...*

- Cree el *acslspool*.

Para las configuraciones estándar que utilizan una matriz de discos completa, cree el *acslspool* de la siguiente manera:

```
# zpool create -m /export/home acslspool/
/dev/dsk/c0t600A0B800049EDD600000C9952CAA03Ed0
```

Si se agrega la RAID de ZFS, tal como se sugiere en el paso 1, cree una configuración reflejada de la siguiente manera:

```
# zpool create -m /export/home acslspool mirror /
/dev/dsk/c0t600A0B800049EDD600000C9952CAA03Ed0 /
/dev/dsk/c0t600A0B800049EE1A0000832652CAA899d0
```

5. Verifique el nuevo *acslspool*.

```
# zpool status acslspool
pool: acslspool
state: ONLINE
scan: none requested
config:
NAME                                STATE  READ  WRITE  CKSUM
acslspool                            ONLINE  0     0     0
  mirror-0                            ONLINE  0     0     0
    c0t600A0B800049EDD600000C9952CAA03Ed0  ONLINE  0     0     0
    c0t600A0B800049EE1A0000832652CAA899d0  ONLINE  0     0     0
```

Nota:

Cuando utiliza una matriz de discos RAID, la configuración de ZFS reflejada es opcional.

6. Cree un archivo de prueba en la nueva agrupación y verifíquelo.

```
# cd /export/home
# date > test
# ls
test
# cat test
Tue Jan  7 11:48:05 MST 2015
```

7. Exporte la agrupación.

```
# cd /
# zpool export acslspool
```

8. Inicie sesión en el nodo adyacente (al que se hará referencia como el nuevo nodo actual).

9. Desde el nuevo nodo actual, confirme que `/export/home` (o el sistema de archivos destinado para ACSLS) no esté montado en ningún lugar de la agrupación `root`.

```
# zfs list
```

Si el sistema de archivos existe en `rpool`, repita el paso 2 (anterior) en este nodo actual.

10. Desde el nuevo nodo actual, importe el `acslspool` y verifique que `acslspool` esté presente en este nodo.

```
# zpool import acslspool
# zpool status
  pool: acslspool
  state: ONLINE
    scan: none requested
config:
NAME                                STATE  READ WRITE CKSUM
acslspool                            ONLINE   0   0   0
  mirror-0
    c0t600A0B800049EDD600000C9952CAA03Ed0  ONLINE   0   0   0
    c0t600A0B800049EE1A0000832652CAA899d0  ONLINE   0   0   0
```

Si se produjo un error en `zpool import`, puede intentar la operación con `zpool import -f`.

Nota:

Cuando utiliza una matriz de discos RAID, la configuración de ZFS reflejada es opcional.

11. Verifique que el archivo de prueba esté presente en el nuevo nodo actual.

```
# cd /export/home
# ls
test
# cat test
Tue Jan 7 11:48:05 MST 2015
```

Capítulo 4. Descarga de paquetes de software

En este capítulo, se describen los procedimientos de descarga de los principales parches y paquetes de software necesarios para ACSLS HA, además de la documentación del producto.

Descarga de paquetes de software

Se necesitan tres paquetes de software principales para ACSLS HA.

- ACSLS 8.4
- Oracle Cluster 4.2
- ACSLS HA 8.4

Deberá descargar los paquetes de software en cada nodo de servidor. Recomendamos colocar los paquetes en el directorio */opt*.

Los paquetes están disponibles en Oracle Software Delivery Cloud.

<https://edelivery.oracle.com/>

Descargando ACSLS 8.4

1. Inicie un explorador web en el sistema y vaya al sitio web de Oracle Software Delivery Cloud, en la siguiente URL.

<https://edelivery.oracle.com>

2. Inicie sesión con el nombre de usuario y la contraseña proporcionados por el representante de soporte de Oracle.
3. Lea y acepte las restricciones de exportación.
4. Marque el cuadro Filter Products By Programs (Filtrar productos por programas).
5. Introduzca **acsls** para Product (Producto) y seleccione StorageTek Automated Cartridge System Library Software (ACSLs).
6. Haga clic en **Select Platform** (Seleccionar plataforma) y seleccione su plataforma de Solaris (Solaris o X86). Haga clic en **Select** (Seleccionar).
7. En la pantalla Selected Products (Productos seleccionados), haga clic en **Continue** (Continuar).
8. En Available Releases (Versiones disponibles), marque el cuadro correspondiente a la versión ACSLS 8.4.0.0.0 para especificar su plataforma de Solaris y haga clic en **Continue** (Continuar).

9. En la pantalla Oracle Terms and Restrictions (Condiciones y restricciones de Oracle), lea y acepte las condiciones de las licencias. Haga clic en **Continue** (Continuar).
10. Seleccione el paquete *V77685-xx* y guarde el archivo zip en la ubicación que desee.

Para conocer los procedimientos, consulte [Capítulo 5, *Instalación de ACSLS 8.4*](#).

Descarga de PostgreSQL 8.4 (opcional)

Los paquetes de PostgreSQL 8.3 se incluyen en la descarga de ACSLS 8.4. Estos funcionan y se instalan automáticamente al instalar ACSLS 8.4. Sin embargo, si prefiere instalar PostgreSQL 8.4, descargue el archivo *postgres 8.4 bz2* de <http://www.postgresql.org/> en el directorio */opt* de cada nodo. Cuando ACSLS se instala, busca el archivo *.bz* en */opt* e instala PostgreSQL 8.4 de forma automática. Para obtener instrucciones detalladas, consulte la sección "INSTALLING POSTGRESQL" (INSTALACIÓN DE POSTGRESQL) en el archivo README.txt que se incluye con el paquete de ACSLS 8.4.

Descarga de Oracle Cluster 4.2

Cuando se descarga Oracle Cluster 4.2, es necesario realizar dos pasos:

- Descargar la imagen base de Solaris Cluster.
- Determinar si necesita la actualización del parche de Solaris Cluster.

Para conocer los procedimientos, consulte [Capítulo 6, *Instalación de Solaris Cluster 4.2*](#).

Cómo descargar la imagen base de Solaris Cluster

1. Inicie un explorador web en el sistema y vaya al sitio web de Oracle Software Delivery Cloud, en la siguiente URL.

<https://edelivery.oracle.com>
2. Inicie sesión con el nombre de usuario y la contraseña proporcionados por el representante de soporte de Oracle.
3. Lea y acepte las restricciones de exportación.
4. Marque el cuadro Filter Products By Programs (Filtrar productos por programas).
5. Introduzca **Oracle Solaris Cluster** y seleccione **Enterprise Edition**.
6. Haga clic en **Select Platform** (Seleccionar plataforma), elija SPARC o x86 y haga clic en **Select** (Seleccionar).
7. En la pantalla Selected Products (Productos seleccionados), haga clic en **Continue** (Continuar).
8. En Available Releases (Versiones disponibles), seleccione **Alternate Release** (Versión alternativa) y **4.2.0.0 Enterprise Edition** para su plataforma Solaris. Haga clic en **Continue** (Continuar).
9. Lea y acepte las licencias de copyright, y haga clic en **Continue** (Continuar).

10. Seleccione el paquete *V46190-xx* y guarde el archivo zip en la ubicación que desee.

Cómo determinar si necesita la actualización de parche de Solaris Cluster

Consulte la versión de Solaris que tiene actualmente instalada.

```
# pkg info entire | grep Version
```

- Si la versión de Solaris es 11.2.12 o inferior, no es necesaria la actualización del parche de Oracle Solaris Cluster.
- Si la versión de Solaris es 11.2.13 o superior, es necesaria la actualización del parche del cluster.
 1. Vaya al sitio web de soporte de Oracle.

<http://support.oracle.com>

2. Haga clic en **Sign In** (Iniciar sesión) e introduzca el nombre de usuario y la contraseña proporcionados por el representante de soporte de Oracle.
3. Haga clic en **Patches & Updates** (Parches y actualizaciones).
4. En Patch Search (Búsqueda de parches), haga clic en **Product or Family (Advanced)** (Producto o familia [avanzada]).
5. En el cuadro Product (Producto), introduzca **Solaris Cluster**.
6. En el cuadro Release is (¿Cuál es la versión?), haga clic en la flecha hacia abajo y marque **Solaris Cluster 4.2.0**. Haga clic en **Search** (Buscar).
7. Busque la imagen ISO de ORACLE SOLARIS CLUSTER 4.2.5.x.x REPO que coincida con su plataforma (SPARC o X86) y seleccione ese parche. Haga clic en **Buscar** (Descargar).
8. En Patch Search (Búsqueda de parches), verifique la información y haga clic en **Download** (Descargar).
9. Seleccione el paquete del parche y guarde el archivo zip en la ubicación que desee.

Descarga de ACSLS HA 8.4

1. Inicie un explorador web en el sistema y vaya al sitio web de Oracle Software Delivery Cloud, en la siguiente URL.

<https://edelivery.oracle.com>

2. Inicie sesión con el nombre de usuario y la contraseña proporcionados por el representante de soporte de Oracle.
3. Lea y acepte las restricciones de exportación.
4. Marque Filter Products By **Programs** (Filtrar productos por programas).
5. Introduzca **acsls** y seleccione StorageTek Automated Cartridge System Library Software (ACSL) High-Availability Agent (HA).

6. Seleccione la plataforma (SPARC o x86) y haga clic en **Select** (Seleccionar).
7. En la pantalla Selected Products (Productos seleccionados), haga clic en **Continue** (Continuar).
8. Verifique ACSLS HA para su plataforma y haga clic en **Continue** (Continuar).
9. Lea y acepte las licencias de copyright, y haga clic en **Continue** (Continuar).
10. Seleccione el archivo zip y haga clic en **Download** (Descargar).
11. Lea y acepte las licencias de copyright, y haga clic en **Continue** (Continuar).
12. Seleccione el paquete v75269-xx y guarde el archivo zip en la ubicación que desee.

Para conocer los procedimientos, consulte [Capítulo 7, Instalación y configuración de ACSLS HA 8.4](#).

Descarga de parches

Es posible que haya parches disponibles para ACSLS 8.4, Solaris Cluster 4.2 y ACSLS HA 8.4. Compruebe si hay actualizaciones de parche en el sitio de soporte de Oracle:

<https://support.oracle.com>

1. Inicie sesión con su ID de Oracle y su contraseña.
2. Seleccione el separador **Patches and Updates** (Parches y actualizaciones).
3. En el separador **Search** (Buscar), haga clic en **Product or Family (Advanced)** (Producto o Familia [Avanzado]).
4. Siga los procedimientos que se describieron anteriormente para el paquete de software.

Descarga de la documentación del producto

Para descargar documentación del producto relacionada:

<http://docs.oracle.com>

Para ACSLS:

1. Ubique el almacenamiento y seleccione Storage Software (Software de almacenamiento).
2. Seleccione la documentación de StorageTek ACSLS Manager y, luego, Automated Cartridge System Library Software 8.4.
3. Seleccione View Library (Ver biblioteca).

Para Solaris Cluster:

1. Ubique los sistemas operativos y seleccione Operating Systems (Sistemas operativos).
2. En Oracle Solaris Cluster, seleccione Oracle Solaris Cluster 4.2.
3. Seleccione el idioma deseado para Cluster 4.2 y el documento.

Capítulo 5. Instalación de ACSLS 8.4

La instalación de ACSLS 8.4 se analiza en detalle en la *Guía de instalación de StorageTek Automated Cartridge System Library Software 8.4*. Para instalar ACSLS 8.4, realice el siguiente procedimiento de alto nivel.

Instalación en el primer nodo

1. Descargue ACSLS 8.4 en el directorio `/opt` en cada servidor.
2. Descomprima el archivo zip descargado.
3. Confirme que `acslspool` esté montado en el nodo actual

```
# zfs list
NAME                                USED  AVAIL  REFER  MOUNTPOINT
acslspool                            1.60G  47.4G  1.60G  /export/home
rpool                                 6.97G  60.0G  4.58M  /rpool
rpool/ROOT                            4.39G  60.0G   31K   legacy
rpool/ROOT/solaris                    4.39G  60.0G  3.17G  /
rpool/ROOT/solaris/var                1.22G  60.0G  1.21G  /var
rpool/VARSHARE                        95.5K  60.0G  95.5K  /var/share
rpool/dump                            1.55G  60.0G  1.50G  -
rpool/swap                            1.03G  60.0G  1.00G  -
node2:# clrg resume acsls-rg
```

4. Vaya al directorio de instalación de ACSLS y ejecute la secuencia de comandos de instalación de paquetes:

```
# cd /opt/ACSL_8.4.0
# ./pkg_install.sh
```

5. Observe `/etc/passwd` en este nodo. Tome nota de los números de ID de grupo y usuario asignados a los usuarios `acsss`, `acssa` y `acsdb`.

```
# tail -3 /etc/passwd
# grep acsls /etc/group
```

Cuando realice la instalación en el nodo adyacente, confirme que los números de ID de usuario asignados en el segundo nodo coincidan con los números de ID correspondientes incluidos aquí.

- Determine el origen del entorno ACSLS y ejecute la secuencia de comandos de instalación de paquetes.

```
# . /var/tmp/acsls/.acsls_env
# cd $ACS_HOME/install
# ./install.sh
```

Nota:

Cuando la secuencia de comandos de instalación solicite el directorio de copia de seguridad de la base de datos, especifique un directorio que esté montado en la matriz de discos compartidos. Utilice cualquier ruta en el directorio de instalación de ACSLS (*\$installDir*). Por ejemplo, si instala ACSLS en */export/home*, utilice */export/home/backup* para los archivos de copia de seguridad de la base de datos.

- Confirme que esté conectada la biblioteca.

```
# su - acsss
$ testlmutcp <library ip address>
```

- Ejecute la rutina de configuración de la biblioteca.

```
$ acsss_config
```

- Compruebe si hay alguna actualización del parche a ACSLS 8.4. Si hay un parche, descárguelo e instálelo como se indica.
- Exporte *acslspool* desde el nodo actual.

```
$ exit
# cd /
# zpool export acslspool
```

Esta operación falla si existen usuarios u operaciones que estén activos en el sistema de archivos ACSLS.

Instalación en el nodo adyacente

Mientras que la mayoría de los archivos en el paquete *STKacsls* se extrae en la matriz de discos compartidos (donde ya se han instalado esos archivos), sigue siendo necesario instalar ACSLS 8.4 en el nodo adyacente, dado que se agregarán usuarios de ACSLS a cada nodo y se deben instalar diversos archivos del sistema (como secuencias de comandos de inicio o detención de SMF, trabajos de cron) en cada nodo.

- Inicie sesión en el nodo adyacente e importe *acslspool*.

```
# zpool import acslspool
```

Si esta operación falla, pruebe con `zpool import -f acslspool`.

2. Vaya al directorio de instalación de paquetes ACSLS e instale el paquete.

```
# cd /opt/ACSLs_8.4.0
# ./pkg_install.sh
```

La rutina de instalación le indica que ya existen algunos archivos ACSLS en el directorio de instalación (en la unidad compartida). Puede optar por sobrescribirlos.

3. Observe los ID de grupo y usuario asignados en este nodo para los usuarios `acsss`, `acssa` y `acsdb`.

```
# tail -3 /etc/passwd
# grep acsls /etc/group
```

Confirme que estos números coincidan con los números asignados en el primer nodo. De forma predeterminada, el GID debe ser 100, pero este número cambiará si GID 100 ya está en uso.

Es importante que los números UID y GID coincidan en ambos nodos. Si los números son diferentes en el segundo nodo, edite el archivo `/etc/passwd`, de manera que los números UID y GID del segundo nodo coincidan con aquellos del primer nodo.

Ahora confirme que el ID de grupo de los archivos en `$ACS_HOME` tenga la propiedad de grupo de `acsls`. Si no la tienen, es necesario desinstalar y volver a instalar el paquete `STKacsls`.

```
# pkgrm STKacsls
# pkgadd STKacsls
```

4. Herede el entorno ACSLS y ejecute la secuencia de comandos del shell de instalación.

```
# . /var/tmp/acsls/.acsls_env
# cd $ACS_HOME/install
# ./install.sh
```

Nota 1: Cuando la secuencia de comandos de instalación solicite el directorio de copia de seguridad de la base de datos, especifique un directorio que esté montado en la matriz de discos compartidos. Utilice cualquier ruta en el directorio de instalación de ACSLS (`$installDir`). Por ejemplo, si instala ACSLS en `/export/home`, utilice `/export/home/backup` para los archivos de copia de seguridad de la base de datos.

Nota 2: Cuando ejecute `install.sh` en el segundo nodo, no es necesario volver a instalar la GUI de ACSLS. Cuando la secuencia de comandos de instalación le indica que

el dominio de *AcsIs GUI* ya existe para la GUI, simplemente indique **no** al indicador y vuelva a instalar la GUI, y asegúrese de indicar **no** a la petición de datos para eliminar la GUI.

5. Si se agregó un parche para ACSLS 8.4 en el primer nodo, repita la instalación del parche en este nodo.
6. Confirme que esté conectada la biblioteca.

```
# su - acsss
$ testlmutcp <library ip address>
```

7. Ejecute la rutina de configuración de la biblioteca.

```
$ acsss_config
```

Para activar la redundancia entre el servidor HA y la biblioteca, consulte la [Figura 2.1, “Tarjeta de interfaz de biblioteca HBRr única conectada a dos puertos Ethernet en cada nodo de servidor”](#) o la [Figura 2.2, “Configuración de HBC dual en una biblioteca con Redundant Electronics”](#). Cuando ejecute *acsss_config* (opción 8), asegúrese de definir dos conexiones para cada ACS e introduzca la dirección IP de la biblioteca para cada conexión.

Capítulo 6. Instalación de Solaris Cluster 4.2

La instalación de Solaris Cluster se explica en detalle en la *Guía de instalación del software Oracle Solaris Cluster*, que está disponible en el sitio [technetwork](#) de Oracle (consulte [Capítulo 4, Descarga de paquetes de software \[35\]](#) de este documento).

ACSLSHA 8.4 se admite en Solaris 11.2 con Oracle Solaris Cluster 4.2.

Instalación del paquete del cluster

Siga este procedimiento para instalar el software del cluster.

1. Cree un directorio, `/opt/OSC`.

```
# mkdir /opt/OSC
```

2. Es posible que haya descargado una o dos imágenes ISO para el paquete de Solaris Cluster, según la versión del sistema operativo que haya determinado en [“Descarga de Oracle Cluster 4.2”](#). Mueva cada paquete del cluster descargado al directorio `/opt/OSC`.
3. Descomprima los paquetes. Identifique una imagen ISO para cada paquete descomprimido.
4. Cree un pseudodispositivo a partir de cada imagen ISO.

```
# /usr/sbin/lofiadm -a /opt/OSC/V46190-01.iso
```

```
# /usr/sbin/lofiadm -a /opt/OSC/osc-4_2_5_1_0-repo-incr.iso
```

Realice un seguimiento de los números de instancia de `/dev/lofi` que creó para cada una de ellas.

5. En el directorio `/opt/OSC`, cree un punto de montaje para cada pseudodispositivo.

```
# mkdir mnt
```

```
# mkdir mnt1
```

6. Monte los pseudodispositivos en estos puntos de montaje.

```
# mount -F hsfs -o ro /dev/lofi/1 /opt/OSC/mnt
```

```
# mount -F hsfs -o ro /dev/lofi/2 /opt/OSC/mnt1
```

7. Seleccione uno de los siguientes:

- Si la versión de Solaris es 11.2.13 o superior, continúe con el paso 8.
- Si la versión de Solaris es 11.2.12 o inferior y se descargó solo la imagen base del cluster, ahora puede publicar el repositorio para esa imagen base.

```
# pkg set publisher -G '*' -g file:/opt/OSC/mnt/repo ha-cluster
```

Continúe con el paso 13 de esta sección para instalar el paquete.

8. En los siguientes pasos, copie el paquete de OSC base en un sistema de archivos de lectura y escritura para fusionar la actualización del parche con el paquete base.

Cree un sistema de archivos de lectura y escritura para fusionar los paquetes de OSC.

```
# cd /opt/OSC
```

```
# mkdir merged_iso
```

9. Copie el repositorio de imágenes de OSC base en el directorio creado.

```
# cp -r mnt/repo merged_iso
```

10. Sincronice las dos imágenes juntas en el directorio fusionado.

```
# rsync -aP mnt1/repo merged_iso
```

11. Vuelva a compilar los índices de búsqueda para el repositorio

```
# pkgrepo rebuild -s merged_iso/repo
```

12. Publique el repositorio *ha-cluster* de los paquetes fusionados.

```
# pkg set-publisher -g file:/opt/OSC/merged_iso/repo ha-cluster
```

13. Instale el paquete de Oracle Solaris Cluster.

```
# pkg install --accept ha-cluster-full
```

Repita los pasos de 1 a 13 en el nodo adyacente.

Rutina *scinstall*

La rutina de instalación de Solaris Cluster realiza una serie de comprobaciones entre los dos nodos para asegurarse de que puede supervisar la operación del sistema desde ambos servidores y puede controlar las acciones de inicio y failover.

Pasos preliminares:

1. Antes de ejecutar *scinstall*, es útil establecer un entorno para *root* que incluya la ruta a las utilidades del cluster que se acaban de instalar. Edite el archivo */root/.profile*. Cambie las instrucciones de la ruta e incluya */usr/cluster/bin*.

```
export PATH=/usr/cluster/bin:/usr/bin:/usr/sbin
```

Asegúrese de realizar este cambio en cada nodo. Para heredar la nueva ruta, cierre sesión y vuelva a iniciar sesión, o simplemente *su -*.

2. Confirme que la propiedad *config/local_only* para *rpc/bind* sea *false*.

```
# svccfg -s network/rpc/bind listprop config/local_only
```

Si la propiedad es *true*, debe establecerla en *false*.

```
# svccfg -s network/rpc/bind setprop config/local_only=false
```

Ahora confirme lo siguiente:

```
# svccfg -s network/rpc/bind listprop config/local_only
```

3. Un requisito de configuración de hardware esencial para el software del cluster es la existencia de dos conexiones de red privada, que están reservadas para garantizar la comunicación ininterrumpida de la operación del cluster entre los dos nodos.

La [Figura 2.1, “Tarjeta de interfaz de biblioteca HBRr única conectada a dos puertos Ethernet en cada nodo de servidor”](#) muestra estas conexiones físicas, etiquetadas como (2). Cada conexión se origina de un adaptador de red separado para asegurarse de que ningún punto único de error pueda interrumpir la comunicación interna del cluster. La rutina *scinstall* comprueba cada una de las dos conexiones para verificar que no se vea otro tráfico de red en el cable. Finalmente, *scinstall* verifica que la comunicación sea funcional entre las dos líneas. Después de verificar la conexión física, la rutina asocia cada interfaz con una dirección interna privada que comienza con 172.16.

Antes de ejecutar *scinstall*, verifique el ID del dispositivo de red asignado para los dos puertos de red de cada servidor que ha configurado para esta conexión privada. Ejecute *dladm show-phys* para ver las asignaciones de interfaces.

```
# dladm show-phys
```

4. Se debe establecer un nombre de host lógico y una dirección IP para representar el cluster de cualquier nodo. Este host lógico responde de manera confiable a la comunicación de red si el host activo se ejecuta desde el nodo 1 o el nodo 2.

Actualice el archivo */etc/hosts* en ambos nodos para incluir el nombre de host lógico y la dirección IP lógica. Este host se activa cuando inicia ACSLS HA (“[Configuración de ACSLS HA](#)”).

5. Para lograr una instalación correcta del cluster, debe tener activado Solaris Common Agent Container. Verifique que el contenedor de agentes esté activado.

```
# cacoadm status
```

Si la respuesta del estado indica que el contenedor de agentes está DESACTIVADO en el inicio del sistema, actívelo de la siguiente manera:

```
# cacoadm enable
```

Ejecución de *scinstall*

Desde uno de los dos nodos, ejecute el comando *scinstall* y luego siga este procedimiento:

1. Desde el menú principal, seleccione **Create a new cluster** (Crear un nuevo cluster).
2. Desde el submenú, seleccione **Create a new cluster** (Crear un nuevo cluster).
3. Acepte los valores por defecto iniciales.
4. Seleccione la instalación **Typical** (Típica).
5. Asigne un nombre al cluster, por ejemplo, *acsls_cluster*.
6. En la petición de datos Cluster Nodes (Nodos del cluster), introduzca el nombre de host del nodo adyacente. Acepte la lista de nodos si es correcta.
7. Defina las dos interconexiones de nodos privados que ha identificado con esta finalidad. Permita que la rutina de instalación asocie los enlaces TCP con las conexiones físicas.
8. Siga las indicaciones para crear el cluster. A menos que haya identificado un dispositivo específico para actuar como dispositivo de quórum, permita a la rutina *scinstall* seleccionar los dispositivos de quórum.
9. No se alarme si la utilidad informa que la comprobación del cluster *falló en ambos nodos*. Se informa un error incluso para las advertencias leves. Debe revisar el informe de cada nodo y buscar los errores graves o las violaciones que se pudieran devolver. La rutina muestra la ruta al archivo log que informa los detalles relacionados con errores o advertencias que se encuentran durante la operación. Revise el archivo log y corrija los problemas graves o moderadamente graves identificados.

La rutina *scinstall* se ejecuta desde un nodo e instala Solaris Cluster en ambos nodos. Observe la rutina al configurar un nodo, reiniciar ese nodo, configurar el segundo nodo y reiniciar ese segundo nodo.

Verificación de la configuración del cluster

1. Verifique que ambos nodos estén incluidos en el cluster.

```
# clnode list -v
Node           Type
----           ----
node1          cluster
node2          cluster
```

2. Visualice la lista de dispositivos disponibles para Solaris Cluster.

```
# cldevice list -v
DID Device    Full Device Path
d1           node1:/dev/rdisk/c0t600A0B800049EDD600000C9952CAA03Ed0
d1           node2:/dev/rdisk/c0t600A0B800049EDD600000C9952CAA03Ed0
d2           node1:/dev/rdisk/c0t600A0B800049EE1A0000832652CAA899d0
d2           node2:/dev/rdisk/c0t600A0B800049EE1A0000832652CAA899d0
d3           node1:/dev/rdisk/c1t0d0
d4           node1:/dev/rdisk/c1t1d0
d5           node2:/dev/rdisk/c1t0d0
d6           node2:/dev/rdisk/c1t1d0
```

En este ejemplo, los dispositivos de disco compartido son d1 y d2, mientras que d3 y d4 son los dispositivos de inicio del nodo 1, y d5 y d6 son los dispositivos de inicio del nodo 2. Tenga en cuenta que se puede acceder a d1 y d2 desde cualquier nodo.

3. Un quórum se compone de tres o más dispositivos. Se utiliza durante los eventos de inicio para determinar qué nodo será el nodo activo.

Confirme que se haya configurado un quórum completo.

```
# clquorum list -v
Quorum        Type
-----        ----
d1             shared_disk
node1          node
node2          node
```

Se puede agregar un segundo `shared_disk` a la lista de dispositivos de quórum.

```
# clquorum add d2
# clquorum list -v
Quorum          Type
-----
d1              shared_disk
d2              shared_disk
node1           node
node2           node
```

Si no aparecen los dispositivos de disco compartido, determine sus ID de dispositivo y, luego, agréguelos al quórum.

- a. Identifique el ID de dispositivo para cada disco compartido.

```
# cldevice list -v
```

- b. Ejecute *clsetup* para agregar los dispositivos de quórum.

```
# clsetup
```

```
Select '1' for quorum.
Select '1' to dd a quorum device.
Select 'yes' to continue.
Select 'Directly attached shared disk'
Select 'yes' to continue.
Enter the device id (d<n>) for the first shared drive.
Answer 'yes' to add another quorum device.
Enter the device id for the second shared drive.
```

- c. Ejecute *clquorum show* para confirmar la pertenencia al quórum.

```
# clquorum show
```

4. Revise la configuración general del cluster.

```
# cluster check -v | egrep -v "not applicable|passed"
```

Busque cualquier instancia violada en la lista.

5. Verifique la lista de tipos de recursos registrados.

```
# clrt list
SUNW.LogicalHostname:4
SUNW.SharedAddress:2
SUNW.gds:6
```

Si *SUNW.gds* no está en la lista, regístrelo.

```
# clrt register SUNW.gds
```

Confirme con *clrt list*.

Capítulo 7. Instalación y configuración de ACSLS HA 8.4

El paquete *SUNWscacsls* contiene un software de agentes ACSLS que se comunica con Oracle Solaris Cluster. Incluye parches y archivos de configuraciones especiales que garantizan la operación adecuada entre ACSLS y Solaris Cluster.

Procedimiento de instalación básico

1. Descomprima el archivo descargado *SUNWscacsls.zip* en */opt*.

```
# cd /opt
# unzip SUNWscacsls.zip
```

2. Instale el paquete *SUNWscacsls*.

```
# pkgadd -d .
```

3. Repita los pasos 1 y 2 en el nodo adyacente.
4. Verifique que *acslspool* permanezca montado en uno de los dos nodos.

```
# zpool status acslspool
```

Si *acslspool* no está montado, revise el otro nodo.

Si *acslspool* no está montado en ningún nodo, impórtelo en el nodo actual de la siguiente manera:

```
# zpool import -f acslspool
```

Verifíquelo con *zpool status*.

5. Vaya al directorio */opt/ACLSHA/util* en el nodo que posee *acslspool* y ejecute la secuencia de comandos *copyUtils.sh*. Esta operación actualiza o copia los archivos esenciales en ubicaciones adecuadas en ambos nodos. No es necesario repetir esta operación en el nodo adyacente.

```
# cd /opt/ACLSHA/util
```

```
# ./copyUtils.sh
```

- En el nodo donde *acslspool* está activo, como usuario *acsss*, inicie la aplicación ACSLS (*acsss enable*) y verifique que esté en funcionamiento. Resuelva los problemas que encuentre. Los problemas principales se pueden resolver mediante la eliminación y la reinstalación del paquete *STKacsls* en el nodo.

Si debe volver a instalar el paquete *STKacsls*, ejecute la secuencia de comandos */opt/ACSLSHA/util/copyUtils.sh* después de instalar el paquete.

- Cierre *acsls*.

```
# su - acsss
$ acsss shutdown
$ exit
#
```

- Exporte *acslspool* del nodo activo.

```
# zpool export acslspool
```

Nota:

Esta operación falla si el usuario *acsss* ha iniciado sesión, si hay un shell de usuario activo en algún lugar de *acslspool* o si algún servicio *acsss* continúa activo.

- Importe *acslspool* del nodo adyacente.

```
# zpool import acslspool
```

- Inicie la aplicación ACSLS en este nodo y verifique la operación correcta de la biblioteca. Resuelva los problemas que encuentre. Los problemas principales se pueden resolver mediante la eliminación y la reinstalación del paquete *STKacsls* en el nodo.

Si debe volver a instalar el paquete *STKacsls*, ejecute la secuencia de comandos */opt/ACSLSHA/util/copyUtils.sh* después de instalar el paquete.

Configuración de ACSLS HA

Este paso crea tres recursos ACSLS que, luego, gestiona y controla Solaris Cluster:

- acsls-rs* es la aplicación ACSLS en sí.
- acsls-storage* es el sistema de archivos ZFS en el cual reside ACSLS.
- <logical host>* es la dirección IP virtual (la identidad de red común para ambos nodos). Consulte [“Configuración de archivo /etc/hosts”](#).

Una vez que estos controles de recursos se crean, se asignan a un grupo de recursos común con el nombre *acsls-rg*.

Para configurar estos recursos, primero, verifique que *acslspool* esté montado (*zpool list*) y, luego, vaya al directorio */opt/ACLSHA/util* y ejecute *acsAgt configure*:

```
# cd /opt/ACLSHA/util
# ./acsAgt configure
```

La utilidad solicita el nombre del host lógico. Asegúrese de que el host lógico esté definido en el archivo */etc/hosts* y que las direcciones IP correspondientes estén asignadas en el grupo *imp* definido en el capítulo [Capítulo 2, Configuración del sistema Solaris para ACSLS HA](#). Además, antes de ejecutar *acsAgt configure*, use *zpool list* para confirmar que *acslspool* esté montado en el nodo de servidor actual.

Este paso de configuración puede tardar un minuto o más en terminar. Una vez que los controles de recurso se han creado, la operación intenta iniciar la aplicación ACSLS.

Supervisión de la operación del cluster de ACSLS

Hay varios puntos de vista desde los cuales se puede analizar la operación del cluster de ACSLS. Cuando Solaris Cluster sondea la aplicación ACSLS a cada minuto, puede resultar útil ver los resultados de los sondeos a medida que se obtienen. Cuando un sondeo devuelve un estado que dispara un evento de switchover del nodo, resulta útil ver la actividad de cierre en un nodo y la actividad de inicio en el nodo adyacente. En general, resulta útil tener una vista del estado operativo de la aplicación ACSLS a lo largo del tiempo.

El punto de vista operativo principal corresponde a la perspectiva de ACSLS. El final del archivo *acsss_event.log* puede brindar la mejor indicación del estado general del sistema en todo momento.

La herramienta *event_tail.sh* en el directorio */opt/ACLSHA/util/* brinda acceso directo a *acsss_event.log* desde cualquier nodo. La vista que se obtiene desde esta herramienta permanece activa, incluso cuando el control conmuta de un nodo a otro. Esta herramienta no solo realiza un seguimiento dinámico de la actividad normal de ACSLS, sino también de todos los cambios de estado del grupo de recursos del cluster de ACSLS (*acsls-rg*) y, de esa manera, permite obtener una vista en tiempo real del momento en el que un nodo se desconecta y el otro se conecta. Confirme esta herramienta desde el shell, como se muestra a continuación:

```
# /opt/ACLSHA/util/event_tail.sh
```

Figura 7.1. Ejemplo de *event_tail.sh*

```
event_tail.sh
2015-07-31 12:47:04 ACSLSA[0]:
1436 N sa_demux.c 1 296
Server system recovery complete.

2015-07-31 12:47:04 ACSLSA[0]:
1419 N sa_demux.c 1 296
Server system running.

--- Cluster Resource Groups ---
Group Name      Mode Name      Suspended      Status
-----
acsls-rg        acsls-ha1      Yes            Online
                acsls-ha2      Yes            Offline
```

Para ver la actividad de inicio y detención desde la perspectiva de un solo nodo, consulte *start_stop_log* desde ese nodo, como se muestra a continuación:

```
# tail -f /opt/ACSLSHA/log/start_stop_log
```

Para ver los resultados de los sondeos periódicos en el nodo activo:

```
# tail -f /opt/ACSLSHA/log/probe_log
```

El agente de Solaris Cluster y del cluster de ACSLS envía detalles de los eventos importantes al log del sistema Solaris (*var/adm/messages*). Para ver el log del sistema en un nodo determinado, se proporciona un enlace en el directorio */opt/ACSLSHA/log*:

```
# tail -f /opt/ACSLSHA/log/messages
```

Utilidad ha_console.sh

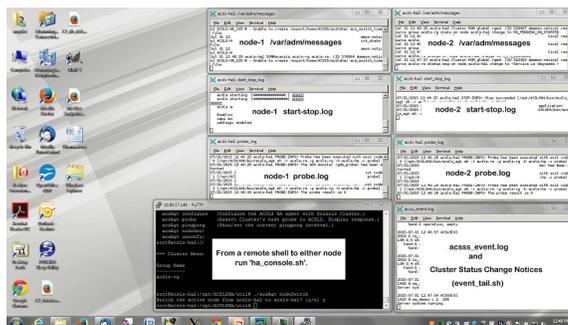
Dados los diferentes puntos de vista de una configuración en cluster y la migración del control del cluster de un nodo al otro a lo largo del tiempo, seguir la actividad operativa del sistema en todo momento desde una única perspectiva puede ser un verdadero desafío. La utilidad *ha_console.sh* permite ofrecer con más facilidad una vista completa.

Inicie sesión en cada nodo del sistema ACSLS HA desde el escritorio remoto y ejecute *ha_console.sh*. Esta utilidad busca su identidad de inicio de sesión (*who am i*) para determinar dónde enviar *DISPLAY*. Para ver la pantalla, inicie sesión directamente desde la consola local o el sistema del escritorio en el nodo HA. Si se presenta algún problema, busque los mensajes en *gnome-terminal.log* en el directorio */opt/ACSLSHA/log*.

```
# /opt/ACSLSHA/util/ha_console.sh
```

Esta utilidad supervisa todos los logs mencionados en esta sección desde ambos nodos. Inicia siete ventanas de terminal Gnome en la pantalla de la consola local. Puede resultar útil organizar las ventanas en la pantalla de la siguiente manera:

Figura 7.2. Organización de ventanas de terminal Gnome



En una sola pantalla del terminal, se muestra una vista completa de todo el complejo de clusters ACSLS.

Dado que el sistema remoto envía datos de la pantalla a la pantalla local, abra el acceso X-11 en el sistema local. En el caso de los sistemas UNIX, el comando que permite realizar esto es *xhost +*. En un sistema Windows, se debe instalar un software cliente X-11, como *xming* o *exceed*.

Si tiene alguna dificultad para usar *ha_console.sh*, se pueden abrir varias sesiones de inicio de sesión desde el sistema local en cada nodo para ver los diferentes logs mencionados en esta sección.

Verificación de la operación del cluster

1. Cuando *acs1sha* se haya iniciado y se haya registrado en Solaris Cluster, utilice los comandos del cluster para comprobar el estado del grupo de recursos ACSLS y sus recursos asociados.

```
# clrg status
=== Cluster Resource Groups ===
Group Name      Node Name      Suspended      Status
-----
acsls-rg        node1          No             Online
                  node2          No             Offline

# clr status
=== Cluster Resources ===
Resource Name    Node Name      State           Status Message
-----
acsls-rs         node1          Online          Online
                  node2          Offline         Offline
acsls-storage    node1          Online          Online
                  node2          Offline         Offline
<logical host>  node1          Online          Online
                  node2          Offline         Offline
```

2. Suspenda de manera temporal la preparación de failover del cluster para facilitar las pruebas iniciales.

```
# clrg suspend acsls-rg
# clrg status
```

3. Pruebe la operación de conmutación del cluster del nodo activo al nodo en espera.

```
# cd /opt/ACLSHA/util
# ./acsAgt nodeSwitch
```

La actividad de switchover se puede supervisar desde varias perspectivas mediante los procedimientos descritos en la sección anterior.

4. Verifique la conectividad de red del sistema cliente ACSLS mediante el nombre de host lógico del servidor ACSLS.

```
# ping acsls_logical_host
# ssh root@acsls_logical_host hostname
passwd:
```

Esta operación debe devolver el nombre de host del nodo activo.

5. Verifique la operación de ACSLS.

```
# su acsss
$ acsss status
```

6. Repita los pasos 3, 4 y 5 del nodo opuesto.
7. Reanude la preparación de failover del cluster.

```
# clrg resume acsls-rg
# clrg status
```

8. La siguiente serie de pruebas incluye la verificación del comportamiento de failover del nodo.

Para ejecutar varios escenarios de failover en secuencia, reduzca el intervalo de pingpong por defecto de veinte minutos a cinco minutos. (Para obtener más información, consulte el capítulo [Capítulo 8, Ajuste de ACSLS HA](#)). Para realizar pruebas, es conveniente reducir la configuración por defecto.

Para cambiar el intervalo de pingpong, vaya al directorio `/opt/ACSLSHA/util` y ejecute `acsAgt pingpong`.

```
# ./acsAgt pingpong
Pingpong_interval
  current value: 1200 seconds.
  desired value: [1200] 300
Pingpong_interval : 300 seconds
```

9. Reinicie el nodo activo y supervise la operación desde las dos consolas del sistema y desde los puntos de vista sugeridos en [“Supervisión de la operación del cluster de ACSLS”](#). Verifique la operación de failover automática en el nodo en espera.
10. Verifique el acceso de red al host lógico desde el sistema cliente como se indica en el paso 4.

11. Cuando la operación de ACSLS esté activa en el nuevo nodo, reinicie el nodo y observe la acción de failover en el nodo opuesto.

Si se supervisa la operación mediante `ha_console.sh`, se puede ver que las ventanas asociadas con el nodo que se reinicia desaparecen. Cuando el nodo esté nuevamente activo, ejecute el comando `ha_console.sh` una vez más en alguno de los nodos para restaurar las ventanas del nodo recién reiniciado.

12. Repita la verificación de la red como se indica en el paso 4.

En [Capítulo 9, Operación del cluster de ACSLS](#), se proporciona un conjunto completo de escenarios de failover. Se puede probar cualquier cantidad de estos escenarios antes de colocar el sistema ACSLS HA en producción. Antes de regresar el sistema a producción, restaure la configuración recomendada del intervalo de pingpong para evitar que la actividad de failover se repita constantemente.

Capítulo 8. Ajuste de ACSLS HA

En este capítulo, se explica cómo configurar una política óptima de failover en un complejo de bibliotecas, cómo ajustar el intervalo de pingpong por defecto para evitar eventos de failback no deseados y cómo registrarse para recibir notificaciones por correo electrónico de eventos de failover.

Definición de una política de failover para comunicaciones de la biblioteca

El agente de ACSLS HA constantemente supervisa la comunicación entre ACSLS y las bibliotecas conectadas. Dicha comunicación es crítica para la operación continua de ACSLS. Pero las medidas, si hubiera, que se deberían adoptar en caso de problemas de comunicación de la biblioteca dependen de una política determinada por el administrador local de ACSLS HA.

La tabla de políticas, `$ACS_HOME/acslsha/ha_acs_list.txt`, permite al administrador local definir la acción de failover deseada para cualquier ACS que necesita recuperación de HA. En caso de error de comunicación de la biblioteca, y según la directiva del administrador, el agente de ACSLS HA realiza un failover al nodo alternativo si se ha confirmado la comunicación correcta de ACS en ese nodo.

En entornos de varios ACS, es posible que se prefiera que el sistema ACSLS HA realice un failover en caso de que falle la comunicación con un único ACS. Pero debido a que cualquier acción de failover interrumpe la producción en todas las bibliotecas conectadas, es posible que el administrador prefiera limitar la acción de failover general a los ACS más críticos en el centro de datos. Se crea un registro de políticas en `ha_acs_list.txt` para cada ACS para el cual se requiere una acción de failover del cluster cuando se pierde la comunicación de la biblioteca. Cada registro tiene dos campos:

```
ACS Number    Fail-over Action (true or false)
```

El primer campo es el ID de ACS y el segundo campo es el valor booleano de *true* o *false*. La lógica de la configuración de la política es la siguiente:

- Cuando el segundo campo es *false*, el agente de ACSLS HA no inicia una acción de failover del cluster al nodo alternativo, incluso cuando se ha producido un error de comunicación con ACS y no se puede restaurar.

- Cuando el segundo campo es *true*, el agente de ACSLS HA confirma la acción de failover del cluster después de que ha fallado cada intento de restablecer la comunicación desde el nodo principal. Se produce un failover del sistema solo si se ha confirmado el contacto de la biblioteca en el nodo alternativo.

La acción por defecto es *false* para cualquier ACS no incluido en este archivo.

Bibliotecas con Redundant Electronics (RE)

En el caso de bibliotecas con Redundant Electronics (RE), el agente de ACSLS HA intenta conmutar la comunicación a la ruta alternativa de RE antes de recurrir a una acción de failover del cluster. Esta acción de conmutación de RE se aplica solamente a una biblioteca SL8500, SL3000 o 9310 anterior con LMU duales. La conmutación automática de RE no se intenta en ninguna biblioteca particionada.

Configuración de *Pingpong_interval* de failover

El *Pingpong_interval* de Solaris Cluster es una propiedad de timeout que evita una acción repetida de failover si no se puede restaurar la recuperación completa después del primer evento de failover del cluster.

Esta es una propiedad que el usuario puede modificar para el grupo de recursos ACSLS. El valor por defecto se configura en 20 minutos. Con esta configuración, el primer evento de failover se produce de inmediato cuando el agente de ACSLS HA solicita una acción de failover. Pero si la condición que podría disparar la acción de failover no se borra en el nuevo nodo de cluster, la acción de failover posterior se demora hasta que caduque el intervalo de pingpong definido. Esto evita la paginación excesiva innecesaria de control entre un nodo de cluster y el otro hasta resolver el problema de la raíz.

Para modificar la configuración por defecto de esta propiedad, modifique el número por defecto en el archivo `$ACS_HOME/acs1sha/pingpong_interval`. Ese número se expresa en segundos.

El valor por defecto de 1.200 segundos es una configuración razonable para la mayoría de las configuraciones de biblioteca medianas a grandes. El valor óptimo de timeout para esta propiedad depende del número real de LSM y de las unidades de cinta que existen en la configuración de la biblioteca. Las configuraciones de bibliotecas más grandes pueden tardar más tiempo en recuperarse después de un evento de failover, y, por lo tanto, este número se debe establecer en un intervalo más prolongado para los sistemas configurados con más de diez LSM o cuarenta unidades, o ambos.

Se recomienda una configuración de 1.800 (30 minutos) para una configuración de cuarenta LSM, mientras que se recomienda una configuración de 900 (15 minutos) para bibliotecas más pequeñas configuradas con uno a cuatro LSM.

Los cambios realizados aquí tienen efecto hasta que se vuelve a configurar ACSLS HA con el comando `acsAgt configure`.

```
# cd /opt/ACSLSHA/util  
# ./acsAgt configure
```

Este comando se puede confirmar incluso si el grupo de recursos *acsls-rg* ya está activo. Registra la nueva configuración por defecto sin afectar la operación normal de HA.

La configuración *pingpong_interval* se puede cambiar dinámicamente para realizar pruebas mediante *acsAgt pingpong*. El valor establecido con este comando permanece vigente hasta que se reinicia el grupo de recursos con *acsAgt configure*.

Registro de notificación por correo electrónico de eventos del sistema

Los usuarios con tareas administrativas se pueden registrar para recibir notificaciones automáticas por correo electrónico de eventos del sistema, incluso los eventos de inicio del sistema y los eventos de failover del cluster de ACSLS HA.

A fin de registrarse para dichos eventos, los usuarios deben agregar su dirección de correo electrónico en los archivos respectivos del siguiente directorio:

```
$ACS_HOME/data/external/email_notification/  
  boot_notification  
  ha_failover_notification
```

Coloque la dirección de correo electrónico de cada destinatario en una única línea debajo de los comentarios del encabezado. Posteriormente, cada vez que el sistema se inicie o el cluster de HA realice un failover al nodo en espera, cada usuario registrado recibirá una notificación por correo electrónico.

Esta capacidad asume que el servicio sendmail se ha activado en el servidor ACSLS y que las limitaciones del firewall de red permiten la comunicación por correo electrónico desde el centro de datos.

Capítulo 9. Operación del cluster de ACSLS

Solaris Cluster se diseñó para lograr la recuperación automática del sistema en diversos escenarios de error mediante la transferencia del control operativo de un nodo de servidor al nodo siguiente. Sin embargo, la mayoría de los errores en un sistema Solaris no requieren una acción de switchover de todo el sistema para recuperarse.

- Solaris IPMP maneja los errores relacionados con comunicaciones de redes de manera rápida y discreta.
- Solaris ZFS maneja los errores de discos del sistema de manera automática y discreta.
- Los errores con una única unidad de disco en la matriz de almacenamiento conectado son recuperados automáticamente por el firmware de matriz de almacenamiento. Y en aquellos casos donde la matriz de almacenamiento no tuviera la posibilidad de recuperarse de un error de disco, Solaris ZFS tiene el control para proporcionar E/S de disco ininterrumpida a la unidad alternativa en la configuración reflejada.
- Si se produce un error de un puerto HBA a la matriz compartida, Solaris conmuta automáticamente al puerto alternativo. Del mismo modo, si se produce un error en el módulo del controlador de la matriz compartida o si se desconecta un cable de interconexión, Solaris lo revierte instantáneamente a la ruta alternativa que se conecta al recurso del disco.
- El error de la ruta de comunicación de la biblioteca se recupera automáticamente mediante lógica TCP/IP dual en ACSLS. Además, las operaciones de una tarjeta de controlador de biblioteca con errores se recuperan automáticamente mediante la lógica ACSLS HA asociada con Redundant Electronics (RE) de la biblioteca.
- Si se produce un error en alguno de los procesos múltiples en ejecución en ACSLS, el daemon de ACSLS reinicia instantáneamente el proceso con errores.
- Si se produce un error en el daemon de ACSLS en sí mismo o si algunos de los servicios ACSLS restantes se dejan de ejecutar, la utilidad de gestión de servicios (SMF) de Solaris reiniciará de inmediato el servicio con errores.

Todos estos escenarios se manejan de manera rápida y automática sin participación de Solaris Cluster. Pero si cualquier otro fallo grave afecta la operación de ACSLS en el nodo de servidor activo, ACSLS HA indica a Solaris Cluster que conmute el control al nodo alternativo.

Una vez comenzado, ACSLS HA realiza sondeos del sistema una vez por minuto a fin de observar si se produce alguno de los siguientes eventos:

- Pérdida de comunicación con una biblioteca conectada+.

- Pérdida de contacto de red con el host lógico ACSLS.
- Pérdida de contacto con el puerto listener RPC para llamadas de clientes.
- Pérdida de acceso al sistema de archivos ACSLS.
- Estado de mantenimiento irrecuperable del servicio SMF acsls.

Cualquiera de estos eventos activa un failover del cluster. Solaris Cluster también sabe cómo realizar un failover si se producen condiciones fatales del sistema en el nodo de servidor activo.

Inicio del control del cluster de ACSLS

Para activar el control de failover del cluster:

```
# cd /opt/ACSLSHA/util
# ./acsAgt configure
```

La utilidad solicita el nombre del host lógico. Asegúrese de que el host lógico esté definido en el archivo */etc/hosts* y que las direcciones IP correspondientes estén asignadas en el grupo *ipmp* definido en el capítulo [Capítulo 2, Configuración del sistema Solaris para ACSLS HA](#). Antes de ejecutar *acsAgt configure*, use *zpool list* para confirmar que *acslspool* esté montado en el nodo de servidor actual.

Mediante esta acción, se inicia el control del cluster de ACSLS. Solaris Cluster supervisa el sistema realizando sondeos a cada minuto para verificar el estado de ACSLS específicamente y el sistema Solaris en general. Cualquier condición considerada fatal inicia una acción en el nodo alternativo.

Para controlar el estado de cluster del grupo de recursos ACSLS:

```
# clrg status
```

La pantalla:

- muestra el estado de cada nodo,
- identifica el nodo que es el nodo activo,
- y muestra si se debe suspender la acción de failover.

Configuración de la política de failover para acsls-storage

Se recomienda configurar una política en el recurso *acsls-storage* para reiniciar el nodo activo siempre que se pierda la comunicación entre ese nodo y el dispositivo de disco RAID compartido. Esta acción provoca que el nodo activo ceda el control cuando no puede conectarse al disco y, de esa manera, permite a Solaris Cluster transferir el control al nodo alternativo. La configuración de *Failover_mode* de SOFT a HARD garantiza un reinicio

del nodo activo siempre que se pierda la comunicación con el dispositivo de almacenamiento compartido.

Para ver el modo existente *Failover_mode*, ejecute el siguiente comando:

```
# clrs show -v acsls-storage | grep Failover
```

Se debe configurar *Failover_mode* en HARD de la siguiente manera:

```
# clrs set -p Failover_mode=HARD acsls-storage
```

Operación y mantenimiento de ACSLS bajo el control del cluster

Una vez que se ha activado el control del cluster, puede operar ACSLS de manera normal. Inicie y detenga ACSLS mediante la utilidad de control *acsss* estándar. Bajo el control del cluster, los usuarios inician y detienen los servicios ACSLS de la misma manera que iniciarían y detendrían la aplicación en un servidor ACSLS independiente. La operación se administra con los siguientes comandos *acsss* estándar:

```
acsss enable
acsss disable
acsss db
```

El inicio o la detención manual de los servicios *acsss* con estos comandos no hacen de ninguna manera que Solaris Cluster intervenga con la acción de failover. El uso de los comandos Solaris SMF (como *svcadm*) tampoco genera la intervención del cluster. Cada vez que los servicios *acsss* se cancelen o se interrumpan, SMF, no el cluster, será el principal responsable de reiniciar estos servicios.

Solaris Cluster solo interviene para restaurar el control en el nodo adyacente en las siguientes circunstancias:

- Pérdida de comunicación con el sistema de archivos ACSLS.
- Pérdida de comunicación con todos los puertos Ethernet públicos redundantes.
- Comunicación perdida e irrecuperable con la biblioteca especificada.

Suspensión del control del cluster

Si se sospecha que la actividad de mantenimiento puede activar un evento de failover del cluster no deseado, suspenda el control del cluster del grupo de recursos *acsls*.

Para suspender el control del cluster:

```
# clrg suspend acsls-rg
```

Mientras el grupo de recursos está suspendido, Solaris Cluster no intenta conmutar el control al nodo adyacente, independientemente de las condiciones que pudieran disparar dicha acción.

Esta suspensión permite realizar reparaciones más invasivas en el sistema, incluso cuando la producción de la biblioteca pudiera estar en plena operación.

Si el nodo activo se reinicia mientras está en modo suspendido, no monta *acslspool* después del reinicio, y la operación de ACSLS se detiene. Para eliminar esta condición, reanude el control del cluster.

Para reanudar el control del cluster:

```
# clrg resume acsls-rg
```

Si el recurso de disco compartido está montado en el nodo actual, la operación normal se reanuda. Pero si Solaris Cluster descubre en el momento de la activación que *zpool* no está montado, conmuta el control de inmediato al nodo adyacente. Si no se puede acceder al nodo adyacente, el control se conmuta nuevamente al nodo actual. El cluster intenta montar *acslspool* e iniciar los servicios ACSLS en este nodo.

Apagado del cluster de ACSLS HA

El siguiente procedimiento indica la secuencia segura de apagado en caso de ser necesario apagar el sistema ACSLS HA.

1. Determine el nodo activo en el cluster.

```
# clrg status
```

Busque el nodo en línea.

2. Inicie sesión como *root* en el nodo activo y detenga el control de Solaris Cluster del grupo de recursos ACSLS.

```
# clrg suspend acsls-rg
```

3. Conmute al usuario *acsss* y cierre los servicios *acsss*:

```
# su - acsss  
$ acsss shutdown
```

4. Cierre sesión como *acsss* y apague el nodo gradualmente.

```
$ exit
```

```
# init 5
```

5. Inicie sesión en el nodo alternativo y apáguelo con *init 5*.
6. Apague la matriz de discos compartidos mediante el interruptor de energía físico.

Encendido de un sistema de cluster de ACSLS suspendido

Para restaurar la operación de ACSLS en el nodo que estaba activo antes de un cierre controlado:

1. Encienda ambos nodos localmente mediante el interruptor de energía físico o remotamente mediante Sun Integrated Lights Out Manager.
2. Encienda la matriz de discos compartidos.
3. Inicie sesión en cualquier nodo como *root*.
4. Si intenta iniciar sesión como *acsss* o incluir el directorio *\$ACS_HOME*, puede notar que el recurso de discos compartidos no está montado en ningún nodo. Para reanudar la supervisión del cluster, ejecute el siguiente comando:

```
# clrg resume acsls-rg
```

Con esta acción, Solaris Cluster monta el disco compartido en el nodo que estaba activo cuando se cerró el sistema. Esta acción, además, debería reiniciar automáticamente los servicios *acsss*, y la operación normal debería reanudarse.

Creación de un único cluster de nodo

En ocasiones, ACSLS debe continuar con la operación desde un entorno de servidor independiente en un nodo mientras se repara el otro nodo. Esto se aplicaría en situaciones de mantenimiento del hardware, actualización del sistema operativo o actualización a Solaris Cluster.

Utilice los siguientes procedimientos para crear un servidor ACSLS independiente.

1. Reinicie el nodo deseado en un modo sin cluster.

```
# reboot -- -x
```

Para iniciar en un modo sin cluster desde Open Boot Prom (OBP) en servidores SPARC:

```
ok: boot -x
```

En servidores X86, es necesario editar el menú de inicio de GRUB.

- a. Encienda el sistema.

- b. Cuando aparezca el menú de inicio de GRUB, pulse **e** (editar).
 - c. Desde el submenú, utilizando las teclas de flecha, seleccione **kernel /platform/i86pc/multiboot**. Cuando lo haya seleccionado, pulse **e**.
 - d. En el modo de edición, agregue `-x` a la opción de inicio múltiple `kernel /platform/i86pc/multiboot -x` y haga clic en **Intro**.
 - e. Con la opción de inicio múltiple `-x` seleccionada, pulse **b** para realizar el inicio con esa opción.
2. Una vez que ha finalizado el ciclo de inicio, inicie sesión como root e importe la agrupación ACSLS Z.

```
# zpool import acslspool
```

Si fuera necesario, utilice la opción `-f` (forzar) cuando el recurso de disco se mantiene vinculado a otro nodo.

```
# zpool import -f acslspool
```

3. Abra los servicios acsss.

```
# su - acsss  
$ acsss enable
```

Capítulo 10. Instalación, actualización y eliminación de componentes de software

En este capítulo, se describen los procedimientos que se deben seguir al actualizar o eliminar diferentes componentes asociados con ACSLS HA.

Instalación de parches para ACSLS

Para instalar parches para el paquete STKacsls:

1. Suspenda el control del cluster.

```
# clrg suspend acsls-rg
```

2. Descargue el parche en su directorio `/opt` y descomprima el paquete.
3. Vaya al directorio `/opt/ACSL_8.x.x` y siga las instrucciones del archivo `README.txt` del parche.
4. Desactive la operación de ACSLS y conmute el control al nodo adyacente.

```
# su - acsss  
$ acsss shutdown  
$ exit  
# cd /opt/ACLSHA/util  
# acsAgt nodeSwitch
```

5. Instale el parche ACSLS en el nodo nuevo.
6. Aplique los cambios de ACSLS HA a la estructura de ACSLS actualizada.

```
# cd /opt/ACLSHA/util  
# ./copyUtils.sh
```

7. Active los servicios ACSLS.

```
# su - acsss  
# acsss enable
```

8. Reanude el control del cluster del grupo de recursos `acsls-rg`.

```
# clrg resume acsls-rg
```

Eliminación del paquete ACSLS

La eliminación del paquete ACSLS podría ser necesaria en casos de actualización de ACSLS. Para hacerlo, es necesario desactivar el control del cluster, detener los servicios ACSLS en ambos nodos y, luego, eliminar el paquete en cada nodo. Utilice el siguiente procedimiento:

1. Suspenda el control del cluster.

```
node1:# clrg suspend acsls-rg
```

2. En el nodo activo, cierre ACSLS.

```
node1:# su - acsss
node1:$ acsss shutdown
node1:$ exit
node1:#
```

3. Exporte el sistema de archivos en la matriz de discos compartidos.

```
node1:# cd /
node1:# zpool export acslspool
```

Esta operación falla si ha iniciado sesión como usuario *acsss*.

4. Inicie sesión en el nodo alternativo e importe la matriz de discos compartidos.

```
node1:# ssh <alternate node>
node2:# zpool import acslspool
```

5. Cierre ACSLS.

```
node2:# su - acsss
node2:$ acsss shutdown
node2:$ exit
node2:#
```

6. Elimine el paquete *STKacsls*.

```
node2:# pkgrm STKacsls
```

7. Regrese al nodo original y elimine el paquete *STKacsls*.

```
node2:# exit
node1:# pkgrm STKacsls
```

Instalación de versiones de actualización de ACSLS

Es necesario eliminar el paquete *STKacsls* en ambos nodos antes de instalar una nueva versión de ACSLS. Consulte el procedimiento detallado en la sección anterior. Para instalar un nuevo paquete, siga este procedimiento:

1. Descargue el paquete *STKacsls* en el directorio */opt* y descomprima el paquete. Repita este paso en el nodo alternativo.
2. Con Solaris Cluster suspendido, asegúrese de que la matriz de discos compartidos (*acslspool*) esté montada en el nodo actual.

```
node1:# zpool list
```

Si *acslspool* no está montada, inicie sesión en el nodo alternativo. Si no está montada en ningún nodo, importe *acslspool*.

3. Vaya al directorio */opt/ACSL_8.x.x* y siga las instrucciones del archivo *README.txt*.
4. Exporte *acslspool*.

```
node1:# zpool export acslspool
```

Esta operación falla si ha iniciado sesión como usuario *acsss*.

5. Inicie sesión en el nodo alternativo y repita los pasos de 1 a 3.
6. Vaya al directorio */opt/ACSLSHA/util* y ejecute *copyUtils.sh*.

```
node2:# cd /opt/ACSLSHA/util
node2:# ./copyUtils.sh
```

7. Inicie el control de la biblioteca ACSLS.

```
node2:# su - acsss
node2:$ acsss enable
node2:$ exit
node2:#
```

8. Reanude el control del cluster del grupo de recursos *acsls*.

```
node2:# clrg resume acsls-rg
```

Reinstalación de ACSLS HA o instalación de actualizaciones

Para reinstalar el paquete *SUNWscacsls*, se debe detener la operación de la biblioteca ACSLS y desconectar el grupo de recursos *acsls-rg*.

1. Cierre ACSLS.

```
# su - acsss
$ acsss shutdown
$ exit
#
```

2. Guarde los cambios personalizados que haya realizado en *ha_list.txt* y *pingpong_interval*.

```
# cd $ACS_HOME/acslsha
# cp ha_list.txt ha_list.save
# cp pingpong_interval pingpong_interval.save
```

3. Desconecte el grupo de recursos *acsls-rg*.

```
# clrg offline acsls-rg
```

Mediante esta acción, se desmonta *acslspool* del sistema de archivos ZFS.

4. Desconfigure el grupo de recursos *acsls-rg*.

```
# cd /opt/ACSLSHA/util
# ./acsAgt unconfigure
```

5. Descargue y descomprima el paquete *SUNWscacsls* actualizado en ambos nodos.

6. Vuelva a montar *acslspool* en alguno de los dos nodos.

```
# zpool import -f acslspool
```

7. Inicie ACSLS para verificar si funciona correctamente.

```
# su - acsss
$ acsss enable
$ exit
#
```

8. Ejecute la utilidad *copyUtils.sh*.

```
# cd /opt/ACSLSHA/uti
# ./copyUtils.sh
```

9. Restaure los archivos personalizados que guardó en el paso 2.

```
# cd $ACS_HOME/acslsha
# cp ha_list.save ha_list.txt
```

```
# cp pingpong_interval.save pingpong_interval
```

10. Configure el grupo de recursos *acs1s-rg*.

```
# cd /opt/ACSLSHA/util
# ./acsAgt configure
```

Mediante esta acción, se detiene y se reinicia ACSLS.

En unos minutos, el comando *clrg status* debería mostrar que el grupo de recursos *acs1s-rg* está nuevamente en línea y ACSLS está en funcionamiento.

Actualización de Solaris Cluster

Antes de eliminar o actualizar Solaris Cluster, desactive ACSLS y desconfigure el grupo de recursos *acs1s-rg*.

```
# su - acsss
$ acsss shutdown
$ exit
# cd /opt/ACSLSHA/util
# ./acsAgt unconfigure
```

Consulte la documentación actual de Solaris Cluster para obtener procedimientos de actualización específicos. El comando general para actualizar Solaris Cluster es el siguiente:

```
# scinstall -u
```

Una vez actualizada la instalación de Solaris Cluster, configure el grupo de recursos *acs1s-rg*:

```
# cd /opt/ACSLSHA/util
# ./acsAgt configure
```

Eliminación de Solaris Cluster

1. Desactive ACSLS y el grupo de recursos *acs1s-rg*.

```
# su - acsss
$ acsss shutdown
$ exit
# cd /opt/ACSLSHA/util
# ./acsAgt unconfigure
```

2. Reinicie ambos nodos en modo sin cluster.

```
# reboot -- -x
```

3. Cuando ambos nodos estén en funcionamiento, inicie sesión en alguno de ellos y elimine el paquete de Solaris Cluster.

```
# scinstall -r
```

Capítulo 11. Registro, diagnóstico y prueba de cluster

En este capítulo, se describen los diversos recursos disponibles para probar la instalación de ACSLS-HA y diagnosticar y solucionar problemas que pudieran surgir en el sistema.

Supervisión de la operación general del cluster

Las actividades que se realizan durante un evento de inicio o switchover están ampliamente distribuidas en los dos nodos. Como consecuencia, el punto de vista elegido para observar la operación general durante el proceso de prueba puede determinar la posibilidad de ver los eventos a medida que ocurren. “[Utilidad ha_console.sh](#)” describe los procedimientos para configurar una vista completa.

Una configuración del panel de control recomendada para observar el comportamiento general de HA durante el proceso de prueba incluiría ocho ventanas de shell, cuatro de cada nodo.

1. Se debería reservar un shell de comando *root* en cada nodo para confirmar varios comandos, si fuera necesario
2. Configure una ventana en cada nodo para visualizar el final del archivo `/var/adm/messages` del sistema.

```
# tail -f /var/adm/messages
```

Solaris Cluster imprime todos los mensajes informativos en este archivo log.

3. Configure otra ventana en cada nodo para visualizar el final del recurso `acsls-rs` `start_stop_log`.

```
# tail -f /var/cluster/logs/DS/acsls-rg/acsls-rs/start_stop_log.txt
```

Allí se muestran todos los mensajes publicados por la secuencia de comandos `acsls_agt.sh`.

4. Se debe configurar una tercera ventana en cada nodo para visualizar el final del log de sondeo `acsls-rs`.

```
# tail -f /var/cluster/logs/DS/acsls-rg/acsls-rs/probe_log.txt
```

Una vez iniciada la aplicación, Solaris Cluster sondea el recurso ACSLS a cada minuto. Cada sondeo devuelve un código numérico al cluster, y los resultados se imprimen en el archivo *probe_log.txt*. Después de cada sondeo, uno de los cinco valores estándar devueltos se ve publicado en este log:

```
0 - The probe found that ACSLS is healthy and functioning normally.
1 - The probe may not have completed due to a functional error.
2 - The probe reports that ACSLS is in a transitional state.
3 - The ACSLS application has been intentionally placed offline.
201 - A condition was detected that requires fail-over action.
```

Solaris Cluster inicia la acción de failover solo en respuesta al código *201*. Las condiciones que incitan tal acción se muestran en el capítulo [Capítulo 9, Operación del cluster de ACSLS](#). Todos los demás códigos que devuelve el sondeo del cluster se consideran informativos y no confirman ninguna acción en respuesta por parte del cluster.

Se pueden realizar sondeos de prueba en cualquier momento desde la línea de comandos. Utilice el comando *acsAgt probe*:

```
#!/opt/ACSLSHA/util/acsAgt probe
```

Todos los logs mencionados anteriormente reflejan una vista del sistema como la visualiza Solaris Cluster. Dos logs adicionales del directorio *\$ACS_HOME/log/* ofrecen una vista del nivel de la aplicación ACSLS. El archivo *acsss_event.log* informa todos los eventos importantes encontrados por ACSLS desde el momento en el que se inició la aplicación. Cualquier dificultad de inicio de ACSLS que encuentre SMF se registra en *acsls_start.log*.

Utilidades de supervisión del cluster

Las utilidades de Solaris Cluster se encuentran en el directorio */usr/cluster/bin*.

- Para ver el estado actual del grupo de recursos ACSLS: *clrg list -v*.
- Para ver el estado actual de los dos nodos del cluster: *clrg status*.
- Para ver el estado de los grupos de recursos: *clrs status*.
- Para obtener el estado detallado de los nodos, los dispositivos del quórum y los recursos del cluster: *cluster status*.
- Para obtener una lista de componentes detallada en la configuración del cluster: *cluster show*.
- Para ver el estado de cada nodo Ethernet en el grupo de recursos: *clnode status -m*.
- Para ver el estado de los diferentes recursos *acsls-rg* en cada nodo: *scstat -g*.
- Para ver el estado de los enlaces de red de latidos: *clintr status*.

- Para ver el estado de IPMP: `scstat -i`.
- Para ver el estado del nodo: `scstat -n`.
- Para ver el estado y la configuración del quórum: `scstat -q` o `clq status`.
- Para mostrar recursos del cluster detallados, incluso los valores de timeout: `clresource show -v`.

Pruebas de recuperación y failover

En esta sección, se explican las condiciones, la supervisión y las pruebas de recuperación y failover.

Condiciones de recuperación

Existen diversas condiciones fatales del sistema que se pueden recuperar sin necesidad de un evento de failover del sistema. Por ejemplo, con IPMP, se puede producir un error en una conexión Ethernet en cada grupo por cualquier motivo, pero la comunicación se debe reanudar de manera ininterrumpida mediante la ruta alternativa.

La matriz de discos compartidos se debe conectar a los servidores con dos puertos diferentes en cada servidor. Si se interrumpe una ruta, la operación de E/S de disco se debe reanudar sin interrupción en la ruta alternativa.

ACSLs se compone de varios servicios de software supervisados por la utilidad de gestión de servicios (SMF) de Solaris. Como usuario `acsss`, muestre cada servicio `acsss` con el comando `acsss status`. Entre estos servicios, se encuentra la base de datos de PostgreSQL, el servidor de aplicaciones web de WebLogic y el software de la aplicación ACSLS. Si se produce un error en un servicio del sistema Solaris, la SMF debe reiniciar automáticamente ese servicio sin necesidad de realizar un failover del sistema.

El servicio `acsls` en sí mismo se compone de diversos procesos secundarios que son supervisados por el proceso principal `acsss_daemon`. Para mostrar los subprocesos de ACSLS, utilice el comando `psacs` (como usuario `acsss`). Si alguno de los procesos secundarios se cancela por algún motivo, el proceso principal debe reiniciar de inmediato ese proceso secundario y recuperar la operación normal.

Supervisión de recuperación

La mejor ubicación para visualizar la recuperación de los recursos del sistema (como E/S de disco y conexiones Ethernet) es el log del sistema, `/var/adm/messages`.

La SMF mantiene un log específico para cada servicio de software que supervisa. Este log muestra eventos de inicio, reinicio y cierre. Para obtener la ruta completa al log de servicio, ejecute el comando `svcs -l service-name`. Los servicios ACSLS se pueden mostrar mediante el comando `acsss: $ acsss status`. Los subprocesos se pueden mostrar con el comando

```
$ acsss p-status.
```

Para ver la recuperación de algún subproceso de ACSLS, puede supervisar *acsss_event.log* (*\$ACS_HOME/ACSSS/log/acsss_event.log*). Este log muestra todos los eventos de recuperación que incluyen alguno de los subprocesos de ACSLS.

Pruebas de recuperación

La lógica de Solaris IPMP debe reiniciar automáticamente las conexiones de red redundantes. Cualquier conexión de datos interrumpida a la matriz de discos compartidos debe ser reiniciada automáticamente por Solaris en la ruta de datos redundante. SMF debe reiniciar automáticamente los servicios controlados por la utilidad de gestión de servicios de Solaris.

En el caso de las pruebas que incluyen un evento de failover real, debe conocer la configuración de propiedades definida en el archivo: *\$ACS_HOME/acslsha/pingpong_interval*. A pesar de las condiciones que pueden disparar un evento de failover, Solaris Cluster no inicia una acción de failover si se produce un evento de failover anterior dentro del *pingpong_interval* especificado.

Para ver o modificar dinámicamente el intervalo de pingpong, vaya al directorio */opt/ACSLSHA/util* y ejecute *acsAgt pingpong*:

```
# ./acsAgt pingpong
Pingpong_interval
  current value: 1200 seconds.
  desired value: [1200] 300
Pingpong_interval : 300 seconds.
```

Use alguna de las siguientes técnicas o todas ellas para evaluar la resiliencia de la instalación de HA:

1. Mientras ACSLS esté en funcionamiento, anule una conexión Ethernet de cada grupo IPMP en el nodo activo. Supervise el estado con *# scstat -i*.

Observe la reacción en */var/adm/messages*. La operación de ACSLS no debe ser interrumpida por este procedimiento.

2. Asegúrese de que el cluster *Failover_mode* esté configurado en **HARD**. Mientras ACSLS está en funcionamiento, anule una conexión SAS o de fibra del servidor activo con el recurso de discos compartidos.

Observe la reacción en */var/adm/messages*. La operación de ACSLS no debe ser interrumpida por este procedimiento.

Repita esta prueba con cada conexión de E/S redundante.

3. Cierre repentinamente ACSLS mediante la terminación de *acsss_daemon*. Use *kill acsss_daemon*.

Ejecute *svcs -l acsls* para ubicar el log de servicio.

Vea el final del log una vez que *acsss_daemon* se detenga. Observe que SMF reinicia el servicio automáticamente. Se debe visualizar una acción similar al detener *acsIs* con *acsIs shutdown*.

4. Desactive el servicio *acsIs* mediante SMF.

Esto se puede realizar como usuario *root* con *svcadm disable acsIs* o se puede realizar como usuario *acsss* con *acsss disable*.

Debido a que SMF se encarga de este evento de cierre, no se intenta reiniciar el servicio *acsIs*. Este es el comportamiento deseado. El servicio *acsIs* se debe reiniciar mediante SMF. Como usuario *root*, use el comando *svcadm enable acsIs*. De lo contrario, como usuario *acsss*, use el comando *acsss-enable*.

5. Desactive el servicio *acsdb*.

Como usuario *acsdb*, obtenga el archivo *.acsIs_env*.

```
$ su acsdb
$ . /var/tmp/acsIs/.acsIs_env
```

Ahora, desactive repentinamente la base de datos de PostgreSQL con el siguiente comando:

```
pg_ctl stop /
-D $installDir/acsdb/ACSDb1.0/data /
-m immediate
```

Esta acción debe desactivar la base de datos y, además, interrumpir los procesos *acsIs*. Ejecute *svcs -l acsdb* para ubicar el log de servicio *acsdb*.

Visualice el final del log de servicio *acsdb* y el log de servicio *acsIs* de la base de datos que se desactivó. Observe que, cuando se detiene el servicio *acsdb*, también se desactiva el servicio *acsIs*. Ambos servicios deben ser reiniciados automáticamente por SMF.

6. Mientras ACSLS está en funcionamiento, ejecute *psacs* como usuario *acsss* para obtener una lista de los subprocesos en ejecución en *acsss_daemon*.

Detenga cualquiera de los siguientes subprocesos. Observe *acsss_event.log* para confirmar que se ha reiniciado el subproceso y que se ha invocado un procedimiento de recuperación.

Condiciones de failover

El software Solaris Cluster supervisa el sistema Solaris y busca condiciones fatales que podrían necesitar un evento de failover del sistema. Estas condiciones incluyen failover iniciado por el usuario (*acsAgt nodeSwitch* o *clrg switch -n*), reinicio del sistema

del nodo activo, bloqueo del sistema, fallo fatal de la memoria o comunicaciones de E/S irreuperables en el nodo activo. Solaris Cluster, además, supervisa los agentes de HA que han sido diseñados para aplicaciones específicas. El agente de ACSLS HA solicita un evento de failover del sistema en los siguientes casos:

- Se ha perdido la comunicación TCP/IP entre el nodo activo y el host lógico.
- El sistema de archivos `$ACS_HOME` no está montado.
- El sistema de archivos de copia de seguridad de base de datos (`$ACS_HOME/. . . /backup`) no está montado.
- Se ha perdido la comunicación con la biblioteca correspondientes a un ACS incluido en el archivo `$ACS_HOME/acslsha/ha_acs_list.txt` cuyo estado deseado es en línea y donde `switch lmu` no se puede realizar con éxito.

Supervisión de failover

En todo momento, puede supervisar el estado de failover de los respectivos nodos mediante el comando `# clrg status`.

También puede supervisar la actividad de failover observando el final de `start_stop_log`:

```
# tail -f /var/cluster/logs/DS/acsls-rg/acsls-rs/start_stop_log.txt
```

Podría resultar útil visualizar (`tail -f`) el archivo `/var/adm/messages` en ambos nodos cuando realiza operaciones de failover de diagnóstico. Consulte [“Supervisión de la operación del cluster de ACSLS”](#).

Pruebas de failover

1. El comando simple para iniciar un evento de failover del cluster es `acsAgt nodeSwitch`.

```
# acsAgt nodeSwitch
```

De lo contrario, use el comando equivalente del cluster:

```
# clrg switch -n <node name> acsls_rg
```

Esta acción debe desactivar la aplicación ACSLS y conmutar la operación del servidor activo al sistema en espera. Las opciones `-M -e` indican al servidor del cluster que active los servicios SMF en el nuevo nodo. Consulte [“Supervisión de la operación del cluster de ACSLS”](#).

2. El reinicio del sistema en el nodo activo debe iniciar una conmutación de HA inmediata al nodo alternativo.

Con esta operación, ACSLS se debe ejecutar en el nuevo nodo activo. En el nodo en espera, observe el final del archivo `/var/adm/messages` mientras el sistema en espera asume su nuevo rol como nodo activo. También puede ejecutar periódicamente el comando `# clrg status`.

3. Mediante `init 5`, apague el nodo de servidor activo y verifique el failover del sistema.
4. Desconecte ambas líneas de datos entre el nodo de servidor activo y la matriz de almacenamiento de discos compartidos, y verifique la conmutación del sistema al nodo en espera.
5. Suponiendo que una biblioteca dada está incluida en el archivo de política `ha_acs_list.txt`, desconecte las líneas de comunicación Ethernet entre el nodo de servidor activo y esa biblioteca.

Verifique el failover del sistema al nodo en espera.

Pruebas adicionales

Si las unidades de inicio reflejadas se pueden conectar en caliente, puede desactivar una de las unidades de inicio y confirmar que el sistema sigue funcionando. Con una unidad de inicio desactivada, reinicie el sistema para verificar que el nodo proviene de la unidad de inicio alternativa. Repita esta acción para cada unidad de inicio en cada uno de los dos nodos.

Retire la fuente de alimentación del nodo activo, y el sistema debe permanecer en pleno funcionamiento con la fuente de alimentación alternativa.

Capítulo 12. Consejos de resolución de problemas

ACSLs HA 8.4 es la integración de la aplicación ACSLS que funciona en un sistema de dos nodos en Solaris 11.2 con IPMP y ZFS bajo el control de Solaris Cluster 4.2.

Verificación de que ACSLS se esté ejecutando

Para verificar que los servicios ACSLS se ejecuten en el nodo activo, utilice el siguiente comando como usuario *acsss*:

```
# su - acsss
$ acsss status
```

Si hay uno o más servicios desactivados, actívelos con `$ acsss enable`.

Si la pantalla de estado muestra que hay uno o más servicios ACSLS en modo de mantenimiento, ejecute el comando `$ acsss l-status`.

Busque la ruta al archivo log del servicio defectuoso y consulte ese log para comprender el motivo por el cual el servicio se colocó en modo de mantenimiento.

Si hay uno o más servicios *acsls* en modo de mantenimiento, se pueden eliminar desactivándolos y luego activándolos con el comando *acsss*.

```
$ acsss shutdown
$ acsss enable
```

Como usuario *root*, use `# svcadm clear <service name>` para eliminar un servicio individual.

El servicio no se elimina hasta que se corrija el fallo subyacente.

También se deben revisar los logs operativos específicos como medio para revelar el origen del problema. La mayoría de ellos se encuentran en el directorio `$ACS_HOME/log`.

El log principal que se revisará es `acsss_event.log`. Este log registra la mayoría de los eventos relacionados con la operación general de ACSLS.

Si el problema se relaciona con la GUI de ACSLS o con la operación de la biblioteca lógica, los logs relevantes se encuentran en el directorio `$ACS_HOME/log/ss1m`.

Para la GUI de ACSLS y WebLogic, busque *AcslsDomain.log*, *AdminServer.log* y *gui_trace.logs*.

Los problemas de instalación relacionados con WebLogic se encuentran en *weblogic.log*.

Para los problemas de la biblioteca lógica, después de configurar la biblioteca lógica, puede consultar *slim_event.logs* y *smce_stderr.log*.

Control de la conexión con el recurso de disco compartido

1. Verifique que el recurso *acsls-storage* esté en línea en el nodo de cluster activo.

```
# clrs status acsls-storage
```

2. Si el recurso *acsls-storage* no está en línea, verifique que el recurso esté montado en ZFS en el nodo activo:

```
# zpool status
```

Si *acslspool* no está montado en el nodo activo, verifique que esté montado en el nodo en espera.

```
# ssh standby hostname zpool status
```

Si el recurso de disco compartido está montado en el nodo en espera, conmute el control del cluster a ese nodo.

```
# clrg switch -n standby hostname acsls-rg
```

3. Si *acslspool* no está montado en el nodo activo y el recurso *acsls-storage* está fuera de línea, verifique que *acslspool* esté visible para el nodo activo.

```
# zpool import (no argument)
```

Nota:

Esta operación solamente funciona si *acsls-storage* está fuera de línea. Para ponerlo fuera de línea, utilice el comando *clrs disable acsls-storage*.

Si *acslspool* está visible para el nodo activo, intente importarlo:

```
# zpool import -f acslspool
```

Si la operación *import* funciona correctamente, coloque el recurso *acsls-storage* en línea para Solaris Cluster:

```
# clrs enable acsls-storage
```

Si *acslspool* no está visible para el nodo activo, es necesario resolver el problema de conexión física con la unidad compartida.

Cuando no se puede hacer ping en el host lógico

1. Verifique que el nombre de host lógico esté registrado en Solaris Cluster.

```
# clrslh list
```

2. Determine el nodo activo:

```
# clrg status | grep -i Online
```

3. Verifique si se puede hacer ping en el nodo activo.

```
# ping <node name>
```

4. Verifique que el recurso de nombre *logical-host* esté en línea para el nodo activo.

```
# clrslh status
```

Si el host lógico no está en línea, actívelo.

```
# clrs enable <logical host>
```

5. Verifique el estado de las interfaces IP asignadas al grupo público.

```
# ipadm
```

En la pantalla de salida, verifique el estado *ok* de cada miembro del grupo público *ipmp*.

6. Para cada interfaz del grupo público (*ipmp0*), verifique el estado físico.

```
# dladm show-phys
```

7. Verifique que el host lógico esté asociado con una de las dos interfaces del grupo *ipmp* público (que se muestra en el paso 5).

```
# arp <logical-hostname>
```

```
# ifconfig net0
```

```
# ifconfig net4
```

En este ejemplo, se supone que net0 y ne4 fueron asignados al grupo público *imp*.

La dirección MAC de una de las dos interfaces debe coincidir con la dirección MAC asignada al nombre de host lógico.

Comprobación de la interconexión entre nodos

Si sospecha que hay un error en el control del cluster debido a la pérdida de comunicación del cluster entre los dos nodos, puede comprobar la interconexión privada del cluster de la siguiente manera:

```
# cluster status -t interconnect
```

Índice

A

- ajuste
 - configuración de pingpong_interval, 60
 - política de failover para comunicaciones de la biblioteca, 59
 - redundant electronics, 60
 - registro de notificación por correo electrónico, 61

C

- componentes de software
 - actualización de Solaris Cluster, 73
 - eliminación de paquete ACSLS, 70
 - eliminación de Solaris Cluster, 73
 - instalación de actualizaciones de ACSLS, 71
 - instalación de parches para ACSLS, 69
 - reinstalación de ACSLS HA o instalación de actualizaciones, 71
- configuración de Solaris Cluster y ACSLS HA
 - configuración de acceso de root, 19
 - disco de rutas múltiples, 26
 - interfaz de biblioteca, 25
 - interfaz pública e IPMP, 22
 - red de rutas múltiples, 20
- configuración del sistema de archivos ZFS
 - creación de raíz reflejada, 29
 - creación de un sistema de archivos reflejado para ACSLS, 31
- control del cluster de ACSLS
 - apagado de ACSLS HA, 66
 - creación de un único cluster de nodo, 67
 - encendido de un sistema de cluster de ACSLS suspendido, 67
 - inicio, 64
 - operación y mantenimiento, 65
 - suspensión, 65

D

- diagnóstico y pruebas
 - recuperación y failover, 77
 - utilidades de supervisión del cluster, 76

I

- instalación de ACSLS 8.3

- primer nodo, 39
- instalación de ACSLS 8.4
 - nodo adyacente, 40

P

- paquetes de software
 - ACSLs 8.4, 35
 - ACSLs HA, 37
 - Oracle Cluster 4.1, 36

R

- requisitos del sistema
 - opciones de matriz de almacenamiento, 13
 - opciones del servidor, 12
 - red, 13
 - software, 13

S

- Solaris Cluster 4.1
 - ejecución de scinstall, 46
 - instalación de paquete de cluster, 43
 - rutina scinstall, 45
 - verificación de configuración de cluster, 47
