

# **Novedades de Oracle® Solaris 11.4**

Agosto de 2018

En este documento, se resumen las funciones que son nuevas o se mejoraron en la versión Oracle Solaris 11.4.

## Funciones clave de Oracle Solaris 11.4

Oracle Solaris es una plataforma segura y rápida diseñada para despliegues empresariales a gran escala. Oracle Solaris ofrece actualizaciones simples, supervisión de conformidad, supervisión de rendimiento y virtualización sin sobrecarga para aislar cargas de trabajo críticas.

Conformidad y seguridad demostradas y automatizadas:

- Protocolo de interoperabilidad de gestión de claves (KMIP): los clientes de criptografía de KMIP de Oracle Solaris se pueden comunicar con los servidores KMIP remotos, donde se crean y gestionan las claves en sistemas de datos en reposo protegidos.
- Silicon Secured Memory (SSM): proteja automáticamente la aplicación y el sistema operativo con SSM.
- Modernice las auditorías de seguridad con generación de informes de conformidad integrados y automatizados.
- Proteja el despliegue de la plataforma de aplicaciones con una nueva herramienta de gestión de sandbox de aplicaciones.

Optimizado:

- Plataforma más rápida y segura para ejecutar Oracle Database y Java.
- Maximice la seguridad y el aislamiento multi-arrendamiento de Oracle Database.

Simplicidad:

- Migre sin inconvenientes las cargas de trabajo tradicionales a máquinas virtuales.
- Use `cloudbase-init` para definir la configuración inicial de despliegues de sistemas operativos invitados.
- Use el panel de control de la interfaz web del sistema Oracle Solaris para ver el rendimiento, la conformidad y los datos del sistema.

Actualizaciones de software en paquetes. Consulte [“Actualizaciones de software integrado de Oracle Solaris 11.4” de Software gratis disponible en Oracle Solaris 11.4](#) para obtener más información:

- Nuevas versiones de numerosos paquetes de software, incluidos GNOME 3.24, ISC BIND 9.10, MySQL 5.7, Open Fabric Enterprise Distribution 3.18, Oracle Instant Client 12.2, Perl 5.26, Puppet 5.5, Python 3.5 y Xorg 1.19.
- Nuevas aplicaciones de software en paquete, incluidas Augeas, Cython, el módulo de Python `cx_oracle`, el compilador Google Go, LLVM/Clang, MCollective, Oracle Database Programming Interface-C (ODPI-C) y el filtro de impresión `paps`.

Oracle Solaris 11.4 admite las siguientes actualizaciones de aplicaciones de Oracle:

- Oracle VM Server for SPARC 3.6. Consulte [Oracle VM Server for SPARC](#) y la [Biblioteca de documentación de Oracle VM Server for SPARC 3.6](#).
- Oracle Solaris Cluster 4.4. Consulte [Oracle Solaris Cluster](#) y la [Biblioteca de información de Oracle Solaris Cluster 4.4](#).

## Funciones de seguridad y conformidad

En esta sección, se describen las características de seguridad y conformidad nuevas de esta versión. Estas nuevas funciones ayudan a evitar nuevas amenazas a través de la protección contra malware y permiten cumplir con las obligaciones de conformidad más estrictas.

## Sandboxes seguros

Los sandboxes son juegos de atributos de procesos con nombres únicos que se pueden usar para especificar requisitos de aislamiento de recursos y seguridad. En Oracle Solaris 11.4, puede ejecutar procesos que no sean de confianza en sandboxes temporales. Se pueden crear sandboxes persistentes y jerárquicos mediante el comando `sandboxadm`. Para ingresar tanto a los sandboxes persistentes como a los temporales, se puede usar el comando `sandbox`.

Los sandboxes son adecuados para restringir aplicaciones con privilegios o sin ellos. Los controles de mitigación de vulnerabilidades de seguridad mejorados que aprovechan la memoria de silicio protegida de SPARC protegen automáticamente las aplicaciones clave y el núcleo del sistema.

Para obtener más información, consulte “[Configuring Sandboxes for Project Isolation](#)” de *Securing Users and Processes in Oracle Solaris 11.4* y las páginas del comando `man sandboxing(7)`, `man sandbox(1)` y `man sandboxadm(8)`.

## Evaluación de conformidad de seguridad

Esta versión de Oracle Solaris admite la ejecución y el almacenamiento de informes de conformidad de manera remota y permite filtrar los informes según los metadatos.

- Puede ejecutar y administrar informes de conformidad desde un sistema central y almacenarlos en un servidor común. Consulte el [Capítulo 2, “Centrally Managing Compliance Assessments”](#) de *Oracle Solaris 11.4 Compliance Guide* y la página del comando `man compliance-roster(8)`.
- Puede etiquetar evaluaciones de conformidad para identificación y filtrado. Consulte “[Using Metadata to Manage Assessments](#)” de *Oracle Solaris 11.4 Compliance Guide* y la sección *Parámetros de coincidencia* de la página del comando `man compliance(8)`.

## Comprobaciones de conformidad de Oracle Solaris Cluster

La referencia estándar para el comando `compliance` de Oracle Solaris incluye comprobaciones de Oracle Solaris Cluster. Las comprobaciones de Oracle Solaris Cluster se ejecutan solo cuando Oracle Solaris Cluster está instalado y configurado en el sistema.

Consulte la siguiente documentación para obtener información sobre referencias, perfiles, el comando `compliance` y las comprobaciones de conformidad de Oracle Solaris Cluster:

- Página del comando `man compliance(8)`
- “[What’s New in Compliance in Oracle Solaris 11.4](#)” de *Oracle Solaris 11.4 Compliance Guide*
- Directrices de seguridad de *Oracle Solaris Cluster 4.4*

## Auditoría por archivo

La auditoría por archivo en Oracle Solaris 11.4 proporciona auditoría detallada y en el acceso de archivos y directorios específicos. Con esta característica, los administradores del sistema y la seguridad pueden escoger archivos específicos para auditar. Se puede acceder de una manera determinada a los archivos especificados, lo cual simplifica mucho la recopilación y el análisis de los datos de auditoría.

Por ejemplo:

```
# chmod A+everyone@:write_data/read_data:successful_access/failed_access:audit /data/db1
```

Esta ACE de auditoría garantiza que se genere un registro de auditoría de todas las operaciones de lectura o escritura, tanto las de acceso permitido como las de acceso denegado, realizadas por cualquier usuario del sistema en el archivo `/data/db1`. También se pueden agregar ACE de auditoría para cambios de metadatos.

Para obtener más información, consulte [“What’s New in the Audit Service in Oracle Solaris 11.4” de \*Managing Auditing in Oracle Solaris 11.4\*](#).

## Auditoría de inicio verificado

En Oracle Solaris 11.4, esta nueva característica le permite generar registros de auditoría para indicar los resultados de la verificación de la firma de los módulos del núcleo. La característica comprueba el valor `boot_policy` del inicio verificado cuando se inicia Oracle Solaris 11.4 y muestra el valor en un registro de auditoría del evento `AUE_SYSTEMBOOT`. Si el inicio verificado está activado con la propiedad `boot_policy` configurada como `warning` o `enforce`, la auditoría de Oracle Solaris produce eventos de auditoría `AUE_MODLOAD` si se produce un error de verificación de firma `elfsign` cuando se debe cargar un módulo. Con el inicio verificado activado, puede realizar un seguimiento de eventos de módulos del núcleo que tienen firmas no válidas o firmas que no se cargaron en el sistema.

Para obtener más información, consulte [“New Feature – Auditing Verified Boot” de \*Managing Auditing in Oracle Solaris 11.4\*](#).

## Generación de informes de historial de ejecución de comandos con privilegios

Oracle Solaris 11.4 introduce la utilidad `admhist`, que se usa para proporcionar, en un formato útil y fácil de entender, un resumen de eventos relacionados con la administración del sistema que se ejecutaron en el sistema. La utilidad `admhist` usa los datos de auditoría que permiten a las utilidades `praudit` y `auditreduce` proporcionar análisis de log más detallados.

Hay disponible una variedad de opciones que permiten limitar los resultados por usuario, fecha, hora o tipo de evento, como se indica a continuación. Por ejemplo, puede identificar ejecuciones de comandos con privilegios por un ID de usuario en particular en las últimas 24 horas:

```
# admhist -v -a "last 24 hours"
2017-05-09 10:58:55 user1@example.com cwd=/export/home/user1 /usr/sbin/zfs get quota rpool/export/home/
user1
2017-05-09 10:59:16 user1@example.com cwd=/export/home/user1 /usr/sbin/zfs set quota 40g
2017-05-09 10:59:27 user1@example.com cwd=/export/home/user1 /usr/sbin/zfs get quota rpool/export/home/
user1
2017-05-09 10:59:31 user1@example.com cwd=/export/home/user1 /usr/bin/bash
2017-05-09 10:59:31 user1@example.com cwd=/usr/bin/su
```

La salida muestra que el usuario `user1` cambió al usuario `root` y aumentó su cuota. Los privilegios que se usan durante toda la vida del proceso se examinan cuando se cierra el comando, y es por este motivo que la operación `su` se incluye al final de la salida.

Para obtener más información, consulte la página del comando `man admhist(8)`, [“New Feature – Per-Privilege Logging of Audit Events” de \*Managing Auditing in Oracle Solaris 11.4\* y \*Uso del análisis de Oracle Solaris 12\*](#).

## Soporte al cliente para KMIP

Oracle Solaris 11.4 proporciona soporte al cliente para el uso del protocolo de interoperabilidad de gestión de claves (KMIP), versión 1.1. En la estructura criptográfica de Oracle Solaris se incluye un nuevo proveedor `PKCS#11, pkcs11_kmip`, que permite a las aplicaciones `PKCS#11` funcionar como clientes KMIP y comunicarse con servidores compatibles con KMIP.

Oracle Solaris 11.4 también incluye un nuevo comando, `kmipcfg`, que inicializa y gestiona los estados del proveedor `pkcs11_kmip`.

Para obtener más información, consulte [Capítulo 5, “KMIP and PKCS #11 Client Applications” de \*Managing Encryption and Certificates in Oracle Solaris 11.4\*](#) y las páginas del comando `man pkcs11_kmip(7)` y `kmipcfg(8)`.

## Etiquetado de procesos y archivos

El etiquetado de procesos y archivos en Oracle Solaris 11.4 proporciona una estructura para restringir el acceso a información confidencial. Ahora se pueden etiquetar archivos y directorios para proporcionar acceso a usuarios o roles con suficiente `clearance`. La política de `clearance` también se aplica a procesos con todos los privilegios. Oracle Solaris 11.4 puede generar logs de cada acceso a los archivos etiquetados, lo que se puede usar para cumplir con los estándares de conformidad, como PCI-DSS y HIPAA.

Para obtener más información, consulte [“Etiquetas y acreditaciones” de \*Protección de archivos y verificación de la integridad de archivos en Oracle Solaris 12\*](#) y la página del comando `man clearance(7)`.

## Mitigaciones de vulnerabilidades de seguridad de Silicon Secured Memory

Silicon Secured Memory (SSM) agrega la comprobación en tiempo real del acceso a los datos de la memoria como una protección contra las intrusiones malintencionadas y el código de programa con errores en producción, para mayor seguridad y confiabilidad.

SSM está disponible a través de la funcionalidad de asignación de memoria del sistema por defecto y se encuentra dentro de una zona del núcleo. Consulte [“Compatibilidad con Silicon Secured Memory en zonas del núcleo de Oracle Solaris” \[19\]](#).

La funcionalidad de asignación por defecto del sistema (`libc malloc`) ahora incluye la integridad de datos de aplicaciones (ADI). Los archivos binarios etiquetados con el comando `sxadm` reciben la protección automáticamente. Consulte las protecciones `ADIHEAP` y `ADISTACK` en la sección Extensiones de seguridad de la página del comando `man sxadm(8)`.

Hay interfaces de programación de aplicaciones de SSM disponibles para personalización avanzada. Consulte [“Protecting Against Malware With Security Extensions” de \*Securing Systems and Attached Devices in Oracle Solaris 11.4\*](#) y la página del comando `man adi(2)`.

## Filtro de paquetes

Oracle Solaris 11.4 incluye el firewall de filtro de paquetes (PF) OpenBSD para filtrar tráfico TCP/IP. El firewall de PF sustituye al filtro IP (IPF) en Oracle Solaris 11.4, lo que permite tanto la gestión del ancho de banda como la asignación de prioridades de paquetes. Para usar el firewall de PF, instale el paquete `pkg:/network/firewall` y active la instancia de servicio `svc:/network/firewall:default`.

---

**Nota** - Asegúrese de configurar el firewall antes de activar el servicio. La configuración por defecto pasa el servicio a un estado degradado. El firewall degradado bloquea todas las sesiones entrantes con la excepción de `ssh`. Las sesiones salientes están permitidas.

---

PF incluye la característica `pflogd`, que es un daemon de registro de paquetes que guarda de manera segura los paquetes registrados por el firewall de PF. Estos paquetes están disponibles mediante un enlace de datos

de captura. El daemon lee paquetes de este enlace de datos y los almacena en un archivo. Para obtener más información, consulte la página del comando `man pflogd(8)`.

PF es compatible con `ftp-proxy`, un proxy semitransparente para FTP, que admite NAT de IPv4. Los sistemas que ejecutan el firewall de PF para NAT pueden usar `ftp-proxy` para permitir que las conexiones FTP atraviesen el firewall. Para obtener más información, consulte la página del comando `man ftp-proxy(8)`.

Para obtener más información, consulte [Capítulo 4, “Oracle Solaris Firewall” de \*Securing the Network in Oracle Solaris 11.4\*](#) y las páginas del comando `man pfctl(8)`, `pf.conf(7)` y `pf.os(7)`.

## Kerberos

Oracle Solaris 11.4 proporciona una versión actualizada de Kerberos, que incluye mejoras con respecto a la versión más reciente de Kerberos de MIT, y mejoras hechas para Oracle Solaris. Kerberos proporciona autenticación de red y, de manera opcional, proporciona privacidad e integridad de mensajes, según cómo lo use la aplicación.

Para obtener más información, consulte [Capítulo 1, “Kerberos on Oracle Solaris” de \*Managing Kerberos in Oracle Solaris 11.4\*](#) y la página del comando `man kerberos.7`.

## libsasl2

La estructura de autenticación sencilla y capa de seguridad (SASL) proporciona autenticación y servicios de seguridad opcionales para los protocolos de red. Oracle Solaris 11.4 basa la implementación de SASL en Cyrus SASL versión 2.1.26 (código abierto) con algunos cambios.

Los plugins de SASL están en el directorio `/usr/lib/sasl2`, y la ubicación por defecto de los archivos de configuración de SASL es el directorio `/etc/sasl2`. Al basar la versión de SASL en código abierto, Oracle Solaris 11.4 puede proporcionar las características más recientes de SASL, incluidas las actualizaciones de seguridad.

Para obtener más información, consulte el [Capítulo 2, “Using Simple Authentication and Security Layer” de \*Managing Authentication in Oracle Solaris 11.4\*](#).

## Servicio `account-policy`

Esta versión de Oracle Solaris ofrece una alternativa para la edición de archivos individuales del directorio `/etc` para establecer la política del sistema. El servicio `account-policy` de la utilidad de gestión de servicios (SMF) almacena la configuración de `login`, `su`, variables de shell, registro, política de seguridad (`policy.conf`) y RBAC como propiedades en SMF. Cuando el servicio está activado, la política del sistema se define y se obtiene por medio del servicio. Tenga en cuenta que los archivos de `/etc` tal vez no indiquen cuáles son las políticas vigentes. Para obtener más información, consulte la página del comando `man account-policy(8S)` y [“Modifying Rights System-Wide As SMF Properties” de \*Securing Users and Processes in Oracle Solaris 11.4\*](#).

## Compatibilidad con PKCS #11 v2.40 para la estructura criptográfica de Oracle Solaris

La estructura criptográfica de Oracle Solaris se actualizó de PKCS #11 v2.20 a PKCS #11 v2.40. Entre las actualizaciones, se incluyen algunos de los mecanismos más recientes de PKCS #11 v2.40, incluidos los de

PKCS #11 v2.30. En PKCS #11 v2.40 también se introdujeron un nuevo código de error y un nuevo valor. Se agregaron los siguientes mecanismos nuevos:

- Firma y verificación de AES

- CKM\_AES\_XCBC\_MAC
  - CKM\_AES\_XCBC\_MAC\_96
  - CKM\_AES\_CMAC
  - CKM\_AES\_GMAC

- Cifrado y descifrado de AES

- CKM\_AES\_GCM
  - CKM\_AES\_CCM
  - CKM\_AES\_CFB128

- Generación de resúmenes de mensajes SHA-512/t

- CKM\_SHA512\_224
  - CKM\_SHA512\_256
  - CKM\_SHA512\_T

- Longitud general de SHA-512/t con HMAC

- CKM\_SHA512\_224\_HMAC\_GENERAL
  - CKM\_SHA512\_256\_HMAC\_GENERAL
  - CKM\_SHA512\_T\_HMAC\_GENERAL
  - CKM\_SHA512\_224\_HMAC
  - CKM\_SHA512\_256\_HMAC
  - CKM\_SHA512\_T\_HMAC

- Derivación de claves SHA-512/t

- CKM\_SHA512\_224\_KEY\_DERIVATION
  - CKM\_SHA512\_256\_KEY\_DERIVATION
  - CKM\_SHA512\_T\_KEY\_DERIVATION

- TLS 1.2

- CKM\_TLS12\_MASTER\_KEY\_DERIVE
  - CKM\_TLS12\_MASTER\_KEY\_DERIVE\_DH
  - CKM\_TLS12\_KEY\_AND\_MAC\_DERIVE
  - CKM\_TLS12\_KEY\_SAFE\_DERIVE
  - CKM\_TLS\_KDF - replacing CKM\_TLS\_PRK
  - CKM\_TLS\_MAC - replacing CKM\_TLS\_PRK

- Código de error CKR\_CURVE\_NOT\_SUPPORTED para curva elíptica

- Si no se puede admitir una curva elíptica específica, se devuelve el código de error CKR\_CURVE\_NOT\_SUPPORTED. En la versión anterior, se devolvía el código de error CKR\_TEMPLATE\_INCONSISTENT si no se admitía la curva.

- CK\_UNAVAILABLE\_INFORMATION

- Cuando se llama a la función `C_GetAttributeValue()`, si no se puede devolver un atributo por no ser válido o no estar disponible, `ulValueLen` se define con el valor `CK_UNAVAILABLE_INFORMATION`. El emisor de la llamada debe comprobar si el valor del atributo devuelto no es válido o no está disponible, para lo cual debe comparar `ulValueLen` con `CK_UNAVAILABLE_INFORMATION`. Además, el emisor la llamada debe considerar `ulValueLen = 0` como un valor válido.

- Atributos CKA\_DESTROYABLE y CKR\_ACTION\_PROHIBITED

- Si un objeto tiene `CKA_DESTROYABLE = CK_FALSE`, una solicitud a `C_DestroyObject` para este objeto en particular debería generar la devolución del código de error `CKR_ACTION_PROHIBITED`.

- Eliminación de restricciones con `cku_so`

- Este cambio elimina las restricciones de tener una sesión de solo lectura abierta con sesión iniciada de `cku_so`. Si bien las sesiones de solo lectura ahora pueden coexistir con `cku_so`, esas sesiones se

comportan como `CKS_RO_PUBLIC_SESSION`. No se puede usar una sesión de solo lectura para `c_Login` con `CKU_SO`.

`CKR_SESSION_READ_ONLY_EXISTS` y `CKR_SESSION_READ_WRITE_SO_EXISTS` están en desuso.

Para obtener más información, consulte las páginas del comando `man SUNW_C_GetMechSession(3EXT)`, `SUNW_C_KeyToObject(3EXT)`, `libpkcs11(3LIB)`, `pkcs11_softtoken(7)`, `pkcs11_kms(7)` y `pkcs11_tpm(7)`.

## Funciones de gestión de datos

En esta sección, se describen las características de gestión de datos nuevas de esta versión. Estas funciones permiten escalar horizontalmente el diseño con capacidad ilimitada para el futuro crecimiento y también proporcionan integridad de datos mejorada.

Consulte también [“Configuración de zonas invariables mediante ejecución en la ruta de confianza” \[19\]](#).

## Extracción de dispositivos de nivel superior de ZFS

El comando `zpool remove` le permite extraer dispositivos de datos de nivel superior. Al extraer un dispositivo de datos de nivel superior se migran los datos desde el dispositivo que se extrae hasta los dispositivos de datos restantes de la agrupación. El comando `zpool status` informa el avance de la operación de extracción hasta la finalización de la reconstrucción.

Consulte [Extracción de dispositivos ZFS de Oracle Solaris, “Removing Devices From a Storage Pool” de \*Managing ZFS File Systems in Oracle Solaris 11.4\*](#) y la página del comando `man zpool(8)` para obtener información acerca de la extracción de dispositivos de datos de nivel superior.

## Limpieza programada de ZFS

De manera predeterminada, la limpieza de agrupaciones de ZFS se ejecuta en segundo plano cada 30 días con una prioridad ajustada automáticamente. La prioridad de la limpieza por defecto es baja, pero aumenta automáticamente si el sistema está inactivo. La prioridad de la limpieza se ajusta en función del intervalo de limpieza especificado, el avance de la operación y la carga del sistema. El comando `zpool status` informa la hora de inicio de la última limpieza realizada correctamente.

Puede personalizar la programación de la limpieza de la agrupación, incluida su desactivación, mediante la configuración de la propiedad `scrubinterval`. Consulte [“Scheduled Data Scrubbing” de \*Managing ZFS File Systems in Oracle Solaris 11.4\*](#) y la página del comando `man zpool(8)` para obtener información acerca de las propiedades `scrubinterval` y `lastscrub`.

## Copiado rápido de archivos basado en ZFS

Las funciones `reflink()` y `reflinkat()` le permiten aprovechar la tecnología ZFS subyacente para copiar archivos con mucha rapidez. La función `reflink()` crea un archivo nuevo con el contenido de uno existente sin leer ni escribir los bloques de datos subyacentes. El archivo existente y el archivo que se crea deben estar en la misma agrupación ZFS.

Para obtener más información, consulte la página del comando `man reflink(3C)`.

La opción `-z` (copiado rápido) del comando `cp` usa `reflink`. Consulte la página del comando `man cp(1)`.

## Flujos de envío raw de ZFS

En Oracle Solaris 11.4, puede optimizar las transmisiones de flujos `send` de ZFS de sistemas de archivos comprimidos y reducir el tráfico de transmisión de la red mediante el uso de flujos `send raw` de ZFS.

En versiones previas, un flujo `send` de un sistema de archivos ZFS comprimido primero se descomprimía para la transmisión y, a continuación, los bloques se volvían a comprimir si en el extremo de destino estaba habilitada la compresión. En Oracle Solaris 11.4, estos dos pasos se evitan porque los bloques comprimidos del sistema de archivos incluidos en el flujo permanecen comprimidos. El uso de esta optimización también reduce el tráfico de transmisión de red. Para optimizar un flujo `send` de ZFS, puede enviarlo en el modo raw con la nueva opción `zfs send -w`. La activación de esta nueva opción permite al flujo `send` codificar la presencia de bloques raw de modo que el sistema que los recibe sepa que debe procesarlos sin comprimirlos.

Por ejemplo, para crear un sistema de archivos ZFS con compresión activada y enviar el flujo de instantáneas con la opción `-w` y sin ella y revisar los tamaños de los flujos resultantes:

```
# zfs create compression=on pond/cdata
# cp -r somefiles /pond/data
# zfs snapshot pond/cdata@snap1
# zfs get compressratio pond/cdata@snap1
NAME                PROPERTY           VALUE  SOURCE
pond/cdata@snap1    compressratio      1.79x  -

# zfs send pond/cdata@snap1 > /tmp/stream
# zfs send -w compress pond/cdata@snap1 > /tmp/cstream
# ls -lh /tmp/*stream*
-rw-r--r--  1 root    root      126M Feb 15 14:35 /tmp/cstream
-rw-r--r--  1 root    root      219M Feb 15 14:35 /tmp/stream
```

Los sistemas que ejecutan versiones anteriores de Oracle Solaris no pueden recibir estos flujos, por lo que se generará un mensaje de error.

Para obtener más información, consulte [Gestión de sistemas de archivos ZFS en Oracle Solaris 12](#).

## Flujos de envío de ZFS reanudables

En Oracle Solaris 11.4, si una transmisión de red se interrumpe o se produce un error, los flujos `send` de ZFS se pueden reiniciar desde el punto de interrupción.

El uso de `send` y `receive` de ZFS para transferir instantáneas de ZFS entre sistemas es una manera cómoda de replicar los datos de un sistema de archivos ZFS que antes sufrían los siguientes problemas:

- Una operación `send` de `zfs` podía tardar varias horas o días hasta finalizar. Durante ese tiempo, la operación `send` podía verse interrumpida por una interrupción de la red o un fallo del sistema.
- Si la operación `send` no logra finalizar, incluso aunque esté casi completa, se la debe reiniciar desde el principio.
- Podía suceder que la operación `send` de ZFS no pudiera transferir grandes flujos en el período comprendido entre las interrupciones.
- Podía suceder que una operación `recv` de ZFS no pudiera detectar e informar errores de transmisión hasta después de que se procesara todo el flujo.

Oracle Solaris 11.4, con las siguientes opciones nuevas, proporciona una manera de reanudar los flujos `send` de ZFS desde el punto de la interrupción:

- `zfs receive -c`: escribe un punto de control de recepción en `stdout`.
- `zfs send -c`: lee un punto de control de recepción de `stdin`.
- `zfs send -s (nocheck)`: desactiva el nuevo formato de transferencia.
- `zfs list -I (state)`: muestra de manera recursiva los juegos de datos incompletos, ya que por defecto los juegos de datos incompletos no se muestran.

Para obtener más información, consulte [Gestión de sistemas de archivos ZFS en Oracle Solaris 12](#).

## Límites de rendimiento configurables de lectura y escritura de ZFS

Oracle Solaris 11.4 permite limitar las operaciones de lectura y escritura en disco de un sistema de archivos ZFS. Para activar un límite `read` o `write` en un sistema de archivos ZFS, debe configurar las propiedades `readlimit` y `writelimit`, expresadas en unidades de bytes por segundo. El uso de estas características le permite optimizar los recursos de E/S de ZFS en entornos de multi-arrendamiento.

Las propiedades `defaultwritelimit` y `defaultreadlimit` se agregan para facilitar la gestión de un gran número de sistemas de archivos ZFS. Si se configuran las propiedades `defaultwritelimit` y `defaultreadlimit`, todos los descendientes del sistema de archivos heredan el valor asignado. Si aplica el límite por defecto de `read` o `write` al sistema de archivos ZFS, este solo se aplica a los sistemas de archivos descendientes, no al sistema de archivos en sí. Las propiedades de solo lectura `effectivereadlimit` y `effectivewritelimit` se agregan para proporcionar una vista del límite vigente en un sistema de archivos. El límite vigente informado es el límite de datos más bajo en cualquier punto entre el sistema de archivos principal y el sistema de archivos indicado.

Por ejemplo, se configurarían los límites `read` y `write` de la siguiente manera:

```
# zfs set writelimit=500mb pond/apps/web
# zfs set readlimit=200mb pond/apps/logdata
```

En el siguiente ejemplo se muestra cómo presentar los límites `read` y `write`:

```
# zfs get -r writelimit,readlimit pond/apps
NAME                PROPERTY  VALUE  SOURCE
pond/apps           writelimit default default
pond/apps           readlimit default default
pond/apps/logdata   writelimit default default
pond/apps/logdata   readlimit 200M   local
pond/apps/web       writelimit 500M   local
pond/apps/web       readlimit default default
pond/apps/web/tier1 writelimit default default
pond/apps/web/tier1 readlimit default default
```

Puede mostrar el límite de escritura vigente de la siguiente manera:

```
# zfs get effectivewritelimit pond/apps/web
NAME                PROPERTY  VALUE  SOURCE
pond/apps/web       effectivewritelimit 500M   local
```

Para obtener más información, consulte [Gestión de sistemas de archivos ZFS en Oracle Solaris 12](#).

## Supervisión y gestión de migración shadow ZFS

Oracle Solaris 11.4 proporciona un mejor funcionamiento de la migración shadow ZFS y mejoras en la visibilidad de la supervisión de los errores de migración y del control de las migraciones en curso. Se introducen las siguientes opciones nuevas:

- `shadowstat -E` y `-e`: se proporciona para la supervisión de errores en todas las migraciones o en una única migración.
- `shadowadm`: permite controlar las migraciones en curso.

Por ejemplo, puede identificar errores de migración shadow de múltiples operaciones de migración:

```
# shadowstat
DATASET                BYTES  EST  BYTES  ELAPSED
XFRD                   LEFT   ERRORS  TIME
tank/logarchive        16.4M  195M  1      00:01:20
```

pond/dbarchive	4.49M	248M	-	00:00:51
tank/logarchive	16.6M	194M	1	00:01:21
pond/dbarchive	4.66M	248M	-	00:00:52
tank/logarchive	16.7M	194M	1	00:01:22
pond/dbarchive	4.80M	248M	-	00:00:53
tank/logarchive	17.1M	194M	1	00:01:23
pond/dbarchive	5.00M	248M	-	00:00:54
tank/logarchive	17.3M	194M	1	00:01:24
pond/dbarchive	5.16M	247M	-	00:00:55

Puede identificar el error de migración específico de la siguiente manera:

```
# shadowstat -E
tank/logarchive:
PATH                                ERROR
e-dir/socket                        Operation not supported
pond/dbarchive:
No errors encountered.
```

Por ejemplo, para cancelar la migración porque el socket abierto no se puede migrar:

```
# shadowadm cancel tank/logarchive
```

Para obtener más información, consulte [Gestión de sistemas de archivos ZFS en Oracle Solaris 12](#).

## Conservación de la herencia de ACL en ZFS

En Oracle Solaris 11.4, una nueva característica de ACL para ZFS permite proporcionar una mejor experiencia al compartir un sistema de archivos ZFS tanto por medio del protocolo NFS como por medio del protocolo de bloque de mensajes del servidor (SMB). Se introduce un nuevo valor de herencia para la propiedad `aclinherit` que permite el uso de semántica de `passthrough` pero sustituye los permisos configurados en las ACE heredadas `owner@`, `group@` y `everyone@` por los valores solicitados en la llamada de sistema `open`, `create` o `mkdir`. Cuando están configuradas, las ACE heredables conservan los bits de herencia. Este comportamiento es importante para permitir que el uso compartido de SMB y NFS herede las listas de control de acceso de una manera natural. El nuevo valor se denomina `passthrough-mode-preserve`. No se realizaron cambios en la propiedad `aclmode`, pero la operación `chmod` tiene en cuenta cuál es el comportamiento de herencia con respecto a la propiedad `aclinherit`. En particular, conserva los bits de herencia durante una operación `chmod`.

Para obtener más información, consulte [Gestión de sistemas de archivos ZFS en Oracle Solaris 12](#).

## Compatibilidad del servidor con la versión 4.1 de NFS

Oracle Solaris 11.4 incluye compatibilidad del servidor para la versión 4.1 de NFS. El protocolo proporciona las siguientes novedades y consideraciones:

- Semántica de una sola vez (EOS): proporciona una caché de solicitud duplicada confiable para el protocolo NFS versión 4.1. Esta caché de solicitud duplicada garantiza que las solicitudes no idempotentes, como la solicitud de extracción, se ejecuten solo una vez, aun en casos de fallos transitorios de la red y retransmisiones. Esta característica elimina los problemas persistentes de las versiones 3 y 4 de NFS.
- `reclaim_complete`: es una nueva característica de protocolo que permite al servidor reanudar el servicio NFS con rapidez después de un reinicio del servidor. A diferencia de versión 4 de NFS, el usuario no necesita esperar un tiempo específico, conocido como período de gracia, antes de reanudar el servicio. Con `reclaim_complete`, el servidor puede finalizar el período de gracia después de que todos los clientes se hayan recuperado. Esta característica es especialmente importante para entornos de alta disponibilidad.
- Recuperación sin período de gracia planificada (PGR): permite a un servidor de Oracle Solaris que usa la versión 4 o 4.1 de NFS conservar el estado de versión 4 de NFS a lo largo de los reinicios del servicio

NFS o de un reinicio controlado del sistema, de modo que el servidor con la versión 4 de NFS no entre en el período de gracia para recuperar el estado de versión 4 de NFS. La ventaja es que las aplicaciones de clientes NFS pueden evitar un tiempo de inactividad de datos de potencialmente 90 segundos entre reinicios del servicio NFS y reinicios controlados del sistema.

- Tenga en cuenta las siguientes consideraciones de interoperabilidad:
  - Un servidor Oracle Solaris con la versión 4.1 de NFS admite tanto clientes Linux como VMware. Sin embargo, se debe desactivar la delegación en el servidor para clientes Linux.
  - Hay problemas conocidos relacionados con el bloqueo y la recuperación en estado cuando se usa la delegación con clientes Linux.

```
# sharectl set -p server_delegation=off nfs
```

Puede desactivar la compatibilidad con la versión 4.1 de NFS en el servidor de la siguiente manera:

```
# sharectl set -p server_versmax=4.0 nfs
```

Para obtener más información, consulte [Gestión de sistemas de archivos de red en Oracle Solaris 12](#).

## Montaje de NFSv3 con TCP

Cuando se usa la versión 3 de NFS para montar un sistema de archivos y TCP es el transporte seleccionado, la configuración de montaje inicial también usará TCP como transporte. En versiones anteriores de Oracle Solaris, se usaba UDP para la configuración del montaje y TCP solo después de haber establecido el montaje.

Si permite montajes NFS a través de un firewall, esta característica podría permitirle simplificar la configuración del firewall.

Esta característica también le permite usar la versión 3 de NFS en sitios donde el tráfico UDP está bloqueado.

Para obtener más información, consulte [Gestión de sistemas de archivos de red en Oracle Solaris 12](#) y la página del comando `man mount_nfs(8)`.

## Atributos extendidos de sistemas de archivos en `tmpfs`

Los sistemas de archivos `tmpfs` admiten atributos de sistema extendidos. Consulte las páginas del comando `man tmpfs(4FS)` y `fgetattr(3C)`.

## Compatibilidad con SMB 3.1.1

Oracle Solaris 11.4 proporciona compatibilidad con el protocolo SMB 3.1.1 en el servidor SMB de Oracle Solaris, lo que incluye las siguientes características de SMB:

- Recursos compartidos con disponibilidad continua: esta característica permite a un servidor SMB de Oracle Solaris hacer que los recursos compartidos tengan disponibilidad continua en caso de bloqueo o reinicio del servidor.
- Multicanal: esta característica permite a un servidor de archivos SMB de Oracle Solaris usar múltiples conexiones de red por sesión de SMB para proporcionar mayor rendimiento y mayor tolerancia a fallos.
- Cifrado: esta característica permite a un servidor SMB de Oracle Solaris cifrar el tráfico de red de SMB entre los clientes y el servidor. El cifrado SMB hace que las sesiones de SMB sean seguras y protege contra ataques de intrusión y alteraciones.

Para obtener más información, consulte [Managing SMB File Sharing and Windows Interoperability in Oracle Solaris 11.4](#) y la página del comando `man smbstat(8)`.

## Funciones de red

En esta sección, se describen las características de red nuevas de esta versión. Estas funciones mejoran la tecnología de red existente y las redes definidas por software para generar servicios que cumplan con los requisitos de rendimiento organizativos y proporcionar una mayor agilidad de las aplicaciones y la flexibilidad que usted necesita.

## Migración de configuración de red persistente a SMF

En Oracle Solaris 11.4, la configuración de red persistente se migró al repositorio de la utilidad de gestión de servicios (SMF). Este movimiento le permite personalizar los parámetros de red y crear configuraciones de red más complejas durante una instalación automatizada. Este cambio también aliena la configuración de la red con otros componentes del sistema que usan SMF como repositorio de almacenamiento principal. Para adaptar la migración de los parámetro de configuración de red a SMF, también se cambiaron ciertos nombres de la propiedad `d1adm`.

Para obtener más información sobre los cambios de nombres de la propiedad `d1adm`, consulte el [Capítulo 2, “Administering Datalink Configuration in Oracle Solaris”](#) de [Configuración y gestión de componentes de red en Oracle Solaris 12](#) y la página del comando `man d1adm(8)`. Para obtener más información, consulte [Instalación automática de los sistemas Oracle Solaris 12](#).

## Compatibilidad de clientes Oracle Solaris con IEEE 802.1X

En Oracle Solaris 11.4, puede usar el estándar IEEE802.1X para autenticar los clientes Oracle Solaris. Antes, si una LAN segura que se desplegaba necesitaba que se autenticaran los sistemas cliente antes de proporcionar servicios, la autenticación no se admitía en un sistema Oracle Solaris.

Esta nueva característica permite a los administradores de la red configurar un sistema cliente Oracle Solaris y usar un servidor que se encuentre detrás de una LAN segura para autenticarlo. El sistema Oracle Solaris ejecuta el daemon `nacd`. El sistema cliente está conectado a una LAN segura por medio de un puerto de un conmutador de la LAN. Para poder obtener un servicio como DHCP de la LAN, primero, el daemon se comunica con un servidor de la LAN segura para obtener la autenticación. El administrador de la red también puede usar el comando `nacadm` para configurar las credenciales de seguridad y el comando `d1adm` para activar o desactivar la autenticación en un enlace determinado.

Para obtener más información, consulte las páginas del comando `man nacd(8)`, `nacadm(8)` y `d1adm(8)`. También puede consultar .

## TCP de centro de datos

Oracle Solaris 11.4 incluye TCP de centro de datos (DCTCP), que es una mejora del control de congestión de TCP para el tráfico de centro de datos. DCTCP usa un mejor procesamiento de notificación explícita de congestión (ECN) para estimar la fracción de bytes que presentan congestión, en lugar de simplemente detectar que se ha producido una congestión. DCTCP después escala el período de congestión de TCP en función de esta estimación. Este método logra una alta tolerancia a ráfagas, baja latencia y alto rendimiento con conmutadores con buffer superficial.

Para obtener más información, consulte [“Implementing Traffic Congestion Control” de Administración de redes TCP/IP, IPMP y túneles IP en Oracle Solaris 12.](#)

## Migración en vivo y conmutación por error de alta disponibilidad para `anets` con SR-IOV activada

Oracle Solaris 11.4 brinda la siguiente funcionalidad nueva de DLMP y la compatibilidad correspondiente para las zonas del núcleo de Oracle Solaris:

- Una arquitectura DLMP novedosa que permite la creación de VNIC con SR-IOV y particiones IPoIB en la zona global
- Compatibilidad con migración en vivo para `anets` con SR-IOV activada en zonas del núcleo de Oracle Solaris
- Conmutación por error de alta disponibilidad para `anets` con SR-IOV activada en zonas del núcleo de Oracle Solaris

Para obtener más información sobre, consulte [Capítulo 2, “Configuring High Availability by Using Link Aggregations” de Gestión de enlaces de datos de red en Oracle Solaris 12.](#)

## Especificación de un nombre para una ruta estática persistente

En Oracle Solaris 11.4, el comando `route` agrega una opción `-name` para poder asignar nombres a rutas estáticas persistentes. Este nombre de ruta se puede usar para cambiar, obtener o suprimir la ruta estática. El nombre también se puede usar para distinguir entre distintas rutas estáticas persistentes.

Para obtener más información, consulte la página del comando `man route(8)`. También puede consultar [“How to Specify a Name for a Persistent Route” in Configuring and Managing Network Components in Oracle Solaris 11.4.](#)

## Open Fabric Enterprise Distribution 3.18

Los siguientes componentes de la estructura de omisión de sistema operativo de InfiniBand (IB) de Open Fabrics Enterprise Distribution (OFED) se actualizaron a la versión 3.18:

- Biblioteca de verbos (transporte) de InfiniBand
- Controlador de espacio de usuario para HCA de InfiniBand de Mellanox ConnectX
- Biblioteca de gestor de comunicaciones (CM) de RDMA de espacio de usuario
- Biblioteca de datagramas de gestión (MAD) de InfiniBand
- Biblioteca de datagramas de gestión de espacio de usuario (uMAD) de InfiniBand
- Utilidades de gestión de InfiniBand de nivel de usuario
- Herramientas de diagnóstico de InfiniBand
- Comando `qperf`

Para obtener más información, consulte las páginas del comando `man` incluidas en los paquetes de `network/open-fabrics`.

## ISC BIND 9.10.3

Oracle Solaris 11.4 incluye una versión actualizada de ISC BIND que incluye muchas características nuevas, como regeneración de firma automática de zonas DNSSEC, nuevos informes de estadísticas

y limitación de demora de respuesta. Los usuarios ahora pueden desplegar DNSSEC con facilidad. La supervisión se simplificó y el servicio es más resistente a ataques de DOS.

## Rendimiento y observación

En esta sección, se describen las mejoras de plataforma y rendimiento nuevas de esta versión. Estas funciones ayudan a optimizar sistemas basados en Oracle Solaris para SPARC y x86, por lo que aumentan el rendimiento y proporcionan un mejor diagnóstico para sus sistemas.

### Proveedor de DTrace SCSI

Oracle Solaris 11.4 introduce un nuevo proveedor de DTrace SCSI diseñado para rastrear comandos SCSI y funciones de gestión de tareas emitidas por un sistema Oracle Solaris. El proveedor SCSI tiene las siguientes ventajas:

- Le permite rastrear comandos SCSI en un sistema Oracle Solaris sin conocer la estructura interna.
- Incluye sondeos y estructuras que siguen lo más posible los estándares SCSI T10.
- Proporciona una contraparte para el proveedor de E/S de DTrace que rastrea el tráfico de E/S en una capa distinta.
- Brinda una secuencia de comandos `scsitrace` que consume los nuevos sondeos.

En el siguiente ejemplo, se muestra un rastreo de una línea que identifica restablecimientos de destinos SCSI:

```
# dtrace -n 'scsi:::tmf-request
          /(args[1] == SCSI_TMF_TARGET_RESET) &&
          (args[0]->addr_path != "NULL")/ {
    printf("Target Reset sent to %s", args[0]->addr_path);}'
```

Para obtener más información, consulte [“iscsi Provider” de Guía de Oracle Solaris 12 DTrace \(Dynamic Tracing\)](#).

### Proveedor de fileops de DTrace

El proveedor de `fileops` expone un juego completo de sondeos de operación de archivos UNIX estándar destinados más a un administrador de Oracle Solaris que a un desarrollador. Por ejemplo, el proveedor puede mostrar información de latencia de `read` o `write` para todos los sistemas de archivos, incluidos los pseudosistemas de archivos.

Los sondeos de `fileops` corresponden a las operaciones de archivo `open`, `close`, `read`, `write`, etc. Estos sondeos no son específicos de ningún tipo de sistema de archivos ni dependen de la E/S a dispositivos de almacenamiento externo. Por ejemplo, el sondeo de `fileops:::read` se activa con cualquier operación de lectura desde un archivo, independientemente de si los datos provienen de un disco o están almacenados en la memoria caché.

Puede usar el sondeo de `read` para observar las latencias de lectura en distintos tipos de sistemas de archivos. Por ejemplo:

```
fileops:::read
{
    @[args[0]->fi_fs] =
    quantize(args[1]);
}
```

La salida resultante proporciona un gráfico de recuentos de lecturas y latencias para todos los tipos de sistemas de archivos presentes en el sistema.

Para obtener más información, consulte [“fileops Provider” de Guía de Oracle Solaris 12 DTrace \(Dynamic Tracing\)](#).

## Proveedor de DTrace MIB para TCP, UDP y IP

Oracle Solaris 11.4 extiende el proveedor de DTrace MIB existente para observar eventos de la pila de red con información de protocolo, de modo de poder identificar conexiones TCP, UDP e IP.

Para obtener más información, consulte [“mib Provider” de Guía de Oracle Solaris 12 DTrace \(Dynamic Tracing\)](#).

## Acción `pcap()` de DTrace

Se agregó una nueva acción, `pcap()`, a DTrace. La acción `pcap()` ejecutará una de las siguientes opciones:

- Mostrar datos de paquetes como lo hace `tracemem()`, pero fusionados en un buffer contiguo.
- Si `freopen()` especificó un archivo de captura, la acción `pcap()` capturará los datos de paquete en un archivo de captura de paquete mediante la función `pcap_dump()` de `libpcap`. DTrace hace lo siguiente con los datos del paquete:
  1. Recopila los datos del paquete en un contexto de sondeo.
  2. Fusiona los datos del paquete en un buffer contiguo si todavía no están en uno.
  3. Vuelca los datos en el archivo especificado mediante la función `pcap_dump()`, que se llamó al recopilar los datos.

La siguiente acción de `pcap()` vuelca memoria en `stdout` como lo hace `tracemem()`:

```
pcap(mblk, protocol);
```

Las llamadas siguientes vuelcan los datos del paquete en el archivo de captura con un sufijo que especifica el valor de `pid` actual:

```
freopen("/tmp/cap.%d", pid);  
pcap(mblk, protocol);
```

Esto le permite organizar seguimientos de paquetes por proceso o servicio, por ejemplo. Como `freopen()` está clasificada como una acción destructiva, la secuencia de comandos anterior debe especificar la opción `-w` (“destructive”) `dtrace`. La acción `pcap()` no es destructiva.

## Acción `print()` de DTrace

DTrace tiene una nueva acción `print()` para mostrar tipos arbitrarios, como se muestra en el siguiente ejemplo:

```
# dtrace -q -n 'fop_close:entry {print(*args[0]);exit(0)}'  
  
vnode_t {  
  v_lock = {  
    _opaque = [ NULL ]  
  }  
  v_flag = 0x0  
  v_count = 0x1  
  v_data = 0xfffffc10054425378  
  v_vfsp = specfs`spec_vfs  
  v_stream = 0xfffffc100623354e8  
  v_type = VCHR  
  v_rdev = 0xee00000026  
  v_vfsmountedhere = NULL  
  v_op = 0xfffffc10029d98040  
  v_pages = NULL  
  v_filocks = NULL
```

```

v_shrlocks = NULL
v_nblock = {
  _opaque = [ NULL ]
}
v_cv = {
  _opaque = 0x0
}
v_pad = 0xbadd
v_count_dnlc = 0x0
v_locality = NULL
v_femhead = NULL
v_path = "/devices/pseudo/udp@0:udp"
v_rdcnt = 0x0
v_wrcnt = 0x0
v_mmap_read = 0x0
v_mmap_write = 0x0
v_mpssdata = NULL
v_fopdata = NULL
v_vsd_lock = {
  _opaque = [ NULL ]
}
v_vsd = NULL
v_xattrdir = NULL
v_fw = 0xbaddcafebaddcafe
}
#

```

Para obtener más información, consulte “[print Action](#)” de *Guía de Oracle Solaris 12 DTrace (Dynamic Tracing)*.

## Estructura de kstats v2

La estructura de estadísticas de núcleo (kstats) v2 proporciona mejor rendimiento y una serie de optimizaciones con respecto a la estructura de kstats anterior. Estos son algunos de los componentes nuevos más destacados:

- API de núcleo, que proporciona la funcionalidad para crear y manipular kstats v2. Las estadísticas de núcleo se identifican mediante un URI único e incluyen metadatos tanto para la estadística de núcleo como para los pares de nombre y valor que contiene la estadística de núcleo. Esta API permite a la estadística de núcleo describir los valores que informa.
- Biblioteca `libkstat2`, que proporciona acceso a kstats v2 creadas en el núcleo. Las kstats se buscan por medio del URI único que las identifica y se presentan como hashmaps. Los desarrolladores pueden suscribirse a eventos en un nivel de URI de kstats en particular y recibirán notificaciones cuando se agregue o elimine alguna estadística de núcleo debajo de ese nivel del árbol de URI.
- Utilidad `/usr/bin/kstat2` que proporciona acceso de CLI a las kstats. Esta nueva utilidad examina las kstats disponibles en el sistema e informa las estadísticas que coinciden con los criterios especificados en la línea de comandos. A continuación, cada estadística coincidente se imprime con su URI y el valor real. Se admiten diversos formatos de salida, incluidos el formato legible por el usuario, el formato analizable y el formato de notación de objetos JavaScript (JSON).

Para obtener información sobre la API del núcleo, consulte las páginas del comando `man kstat2_create(9F)`, `kstat2_create_with_template(9F)` y `kstat2_create_histogram(9F)`. Para obtener más información sobre la biblioteca `libkstat2`, consulte las páginas del comando `man libkstat2(3LIB)` y `kstat2(3KSTAT2)`. Para obtener información sobre la utilidad `kstat2`, consulte la página del comando `man kstat2(8)`.

## Diagnóstico de archivos de núcleo de FMA

Oracle Solaris 11.4 incluye la característica de diagnóstico de archivos de núcleo, que proporciona un resumen de telemetría básica para archivos de núcleo de espacio de usuario, genera alertas de FMA para notificar al usuario y proporciona una política de retención de núcleo de diagnóstico y asociación de casos de SMF.

Los archivos de núcleo de diagnóstico incluyen solo el contenido necesario, por lo que el tamaño del contenido es pequeño. Los archivos de núcleo se suprimirán una vez que se hayan generado los archivos de resumen de texto a partir de ellos, lo que reduce el uso de espacio en disco. Con otras características nuevas, como el diagnóstico de pilas, FMA podrá buscar en las pilas del archivo de resumen de la base de datos de Oracle para detectar problemas conocidos. La política de retención permite al usuario establecer la política de núcleo de diagnóstico mediante el comando `coreadm`. El comando `coreadm` también proporciona funcionalidades como la supresión de núcleos de inmediato o la conservación de un cierto número de núcleos durante un tiempo determinado. La característica de asociación de casos es para el motor de diagnóstico `sw-diag-response`. Se pueden ver todas las alertas de diagnóstico de núcleo que llevan a un fallo del servicio de software, junto con el juego de datos de entorno y pila de cada evento.

El usuario ahora tiene más control sobre los núcleos de diagnóstico. Cuando un servicio de software no se ejecuta correctamente y se retira de servicio, el administrador puede ver con rapidez y facilidad todos los eventos que originaron el fallo del servicio y estar mejor informado acerca de los procesos que tuvieron errores y en qué lugar de la ejecución de código se produjeron los errores.

Para obtener más información, consulte la página del comando `man coreadm(8)`.

## Mejoras de `pfiles`

En Oracle Solaris 11.4, el comando `pfiles` acepta un nombre de archivo de núcleo como argumento y puede mostrar información acerca de los descriptores de archivo abiertos por un proceso que hace volcados de núcleo. Esta funcionalidad proporciona ayuda adicional en la depuración del volcado de núcleo del proceso para determinar la causa raíz del volcado.

A diferencia de versiones anteriores de Oracle Solaris, en Oracle Solaris 11.4 el comando `pfiles` ya no detiene un proceso objetivo en ejecución mientras recupera datos sobre archivos abiertos en ese proceso.

Para obtener más información, consulte la página del comando `man proc(1)`.

## Supervisión de latencia de E/S mediante `fsstat`

El comando `fsstat` tiene una nueva opción `-l` que devuelve la información de latencia correspondiente a las operaciones de `read`, `write` y `readdir`. La información de latencia es independiente de las operaciones de E/S físicas, de modo que representa el rendimiento del sistema de archivos tal como lo ven las aplicaciones. Esta característica permite a los usuarios observar la latencia del sistema de archivos para tipos de sistemas de archivos o sistemas de archivos individuales. Esta característica es útil para la resolución de problemas de rendimiento de sistemas de archivos.

Para obtener más información, consulte la página del comando `man fsstat(8)`.

## Estadísticas de distribución de tiempo de respuesta de E/S de SCSI

Oracle Solaris 11.4 ahora proporciona información de distribución de latencia de E/S o de tiempo de respuesta de E/S de SCSI para mejorar la capacidad de observación. La distribución de tiempo de respuesta de E/S se puede usar para identificar valores atípicos de tiempo de respuesta. La distribución se almacena en un histograma con tres opciones distintas de escala para `x`: `linear`, `log2-based` y `log10-based`. La distribución se puede mostrar mediante el comando `iostat`. La opción `-l` se agrega en combinación con las opciones `-x` e `-y` para mostrar el histograma. La información de distribución se puede usar para investigar problemas de rendimiento.

Para obtener más información, consulte las páginas del comando `man sd(4D)` y `iostat(8)`.

## Funciones de virtualización

En esta sección, se describen las características de virtualización nuevas de esta versión. Estas funciones proporcionan virtualización eficaz en la nube sin pérdida del rendimiento y le permiten ejecutar aplicaciones a gran escala en la nube con el uso optimizado de recursos.

## Configuración de zonas invariables mediante ejecución en la ruta de confianza

La característica de sistema de archivos invariable introducida originalmente en Oracle Solaris 11.11 (raíz de solo lectura para zonas no globales) se amplió considerablemente, por lo que ahora es mucho más sencillo adoptar y usar zonas invariables.

Antes, para hacer ciertos cambios de configuración en zonas invariables, había que hacer que la zona fuera temporalmente variable. En Oracle Solaris 11.4, puede ejecutar en el dominio de ruta de confianza (TPD) mientras la zona sigue siendo invariable para otros usuarios.

Para ejecutar en el TPD, realice una de las siguientes acciones:

- Agregue el usuario al archivo `/etc/security/tpdusers` y configure `start/trusted_path` con el valor `true` en el servicio `console-login`.
- Para acceso remoto RAD a la ruta de confianza, configure `method_context/trusted_path` con el valor `true` en el servicio `rad:remote` y agregue `tpd=yes` en la entrada `user_attr` para cada uno de los usuarios para los que se autoriza el acceso remoto al TPD.

Estos procedimientos se describen en detalle en [“Administering an Immutable Zone by Using the Trusted Path Domain”](#) de *Creating and Using Oracle Solaris Zones*.

Además de los administradores que se ejecutan en el TPD, puede configurar que algunos servicios se ejecuten en el TPD como se describe en [“SMF Services in Immutable Zones”](#) de *Creating and Using Oracle Solaris Zones*.

## Compatibilidad con Silicon Secured Memory en zonas del núcleo de Oracle Solaris

La compatibilidad de Software in Silicon en las zonas del núcleo de Oracle Solaris se mejoró para incluir Silicon Secured Memory (SSM). SSM agrega comprobación en tiempo real del acceso a los datos de la memoria como protección contra intrusiones malintencionadas y código de programa con errores en producción para mayor seguridad y confiabilidad.

La protección de SSM se utiliza en Oracle Database 12c por defecto, y su activación es sencilla para otras aplicaciones. Consulte [“Software in Silicon Features on Kernel Zones”](#) de *Creating and Using Oracle Solaris Kernel Zones*.

Consulte también [“Mitigaciones de vulnerabilidades de seguridad de Silicon Secured Memory”](#) [5].

## Compatibilidad de zona de núcleo de Oracle Solaris para coprocesadores SPARC M7 y M8 DAX

Esta característica permite que el software de Oracle Solaris utilice la funcionalidad de consulta del acelerador de análisis de datos (DAX) de SPARC M7 y M8 mediante la biblioteca de núcleos de alto

rendimiento (HPK) del producto de base de datos en memoria de Oracle al ejecutarse en una zona de núcleo de Oracle Solaris.

La biblioteca de HPK del producto RDBMS proporciona operaciones optimizadas por hardware sobre datos de vectores o columnas para bases de datos de columna en memoria (IMC). La biblioteca usa capacidades específicas de hardware para ejecutar operaciones con eficiencia, y puede hacer uso de las capacidades de consulta de DAX si están disponibles en una zona de núcleo de Oracle Solaris.

Para obtener más información, consulte [Recursos de configuración de zonas de Oracle Solaris](#), “[Software in Silicon Features on Kernel Zones](#)” de [Creación y uso de zonas del núcleo de Oracle Solaris](#) y la página del comando `man zonecfg(8)`.

## Zonas de núcleo de Oracle Solaris con VLAN

Una VLAN divide una red de capa 2 (L2) en varias redes lógicas, de modo que cada red lógica es su propio dominio de difusión. Esta característica significa que todos los dispositivos conectados a una VLAN pueden ver la trama de difusión de cada uno de los demás dispositivos independientemente de su ubicación física.

En versiones anteriores, las zonas de núcleo de Oracle Solaris podían afirmar solo un ID de VLAN. En Oracle Solaris 11.4, se puede especificar el nuevo tipo de recurso `vlan` en la configuración de una zona para afirmar ID de VLAN adicionales por `anet`.

Para obtener más información, consulte “[Configuring Virtual LANs in Kernel Zones](#)” de [Creating and Using Oracle Solaris Kernel Zones](#).

## Reiniciador delegado de zonas de Oracle Solaris

El reiniciador delegado de zonas (`system/zones:default`) permite controlar el orden de inicio mediante dependencias y prioridades. En versiones anteriores de Oracle Solaris, este servicio no permitía asignar prioridades ni gestionar el orden de inicio de las zonas. Si hay aplicaciones que se encuentran en zonas distintas del mismo sistema que dependen unas de otras, por ejemplo, puede ser conveniente iniciar todas esas zonas en paralelo.

Además de proporcionar hitos para el inicio de zonas, el reiniciador delegado de zonas también permite agregar dependencias para otras zonas u otros servicios. Por ejemplo, se puede configurar la zona `zone-c` para que se inicie después de que haya finalizado el inicio de las zonas `zone-A` y `zone-B`, o después de que se haya iniciado un servicio de firewall.

Consulte las páginas del comando `man svc.zones(8)` y `man zonecfg(8)` para obtener información acerca de las nuevas propiedades `boot-priority` y `smf-dependency`.

## Reconfiguración de zonas activas para juegos de datos en zonas nativas de Oracle Solaris

La capacidad de cambiar la configuración de una zona de Oracle Solaris sin causar una interrupción para el usuario final o el servicio es fundamental para cumplir con los acuerdos de nivel de servicio (SLA) actuales. Con la reconfiguración de zonas activas (LZR), los usuarios pueden hacer cambios en la configuración de zonas de Oracle Solaris y enviarlos a una zona de ejecución como cambios permanentes o temporales sin necesidad de reiniciar la zona.

En Oracle Solaris 11.4, puede agregar juegos de datos de ZFS a una zona nativa de Oracle Solaris, o eliminarlos de ella, con la metodología de LZR.

Para obtener más información, consulte el [Capítulo 4, “Live Zone Reconfiguration of Kernel Zones” de Creación y uso de zonas del núcleo de Oracle Solaris](#).

## Movimiento de zonas de Oracle Solaris

Oracle Solaris 11.4 le permite usar el comando `zoneadm` con el subcomando `move` para mover una zona instalada de Oracle Solaris de un URI de almacenamiento a otro. Puede realizar las siguientes acciones:

- Mueva una zona de Oracle Solaris desde un sistema de archivos local (por defecto) hasta un almacenamiento compartido.
- Mueva una zona de Oracle Solaris desde un almacenamiento compartido hasta un sistema de archivos local.
- Mueva una zona de Oracle Solaris desde una ubicación de almacenamiento compartido a otra, y simultáneamente cambie el valor de `zonepath`.
- Cambie el valor de `zonepath` sin mover la instalación de la zona de Oracle Solaris.

Para obtener más información, consulte las páginas del comando `man solaris(7)`, `zones(7)` y `zoneadm(8)`. También puede consultar [Creación y uso de zonas de Oracle Solaris](#).

## Migración en frío de zonas

En Oracle Solaris 11.4, las zonas de Oracle Solaris que se encuentran en un estado de instaladas usan almacenamiento compartido que se puede migrar a otro sistema mediante el comando `zoneadm`. Las zonas de núcleo de Oracle Solaris que se encuentran en un estado de instaladas o suspendidas y usan almacenamiento compartido también se pueden migrar. Las zonas de núcleo de Oracle Solaris y las zonas de Oracle Solaris que no están en ejecución se pueden evacuar mediante el comando `sysadm`, lo que permite lograr una mejor disponibilidad de zonas durante tiempos de inactividad programados de la zona global.

Para obtener más información, consulte las páginas del comando `man zoneadm(8)`, `solaris(7)`, `solaris-kz(7)` y `sysadm(8)`.

## Múltiples rutas para HBA SCSI virtuales de Oracle VM Server for SPARC

En Oracle Solaris 11.4, el subsistema de HBA virtuales admite controladores de HBA físicos que tengan activadas múltiples rutas en sus respectivos archivos `driver.conf`. Esta característica permite admitir la función de múltiples rutas de E/S de Oracle Solaris en un dominio de servicio `sun4v` por puerto de HBA, como se describe en [Gestión de rutas múltiples y dispositivos SAN en Oracle Solaris 12](#).

El módulo `vhba` admite múltiples rutas en el dominio invitado desde la versión inicial de Oracle Solaris 11.3. La posibilidad de usar múltiples rutas en ambos dominios de un sistema `sun4v` mejora la tolerancia a fallos y el rendimiento de E/S para dispositivos SCSI.

## Enmascaramiento de dispositivos para HBA SCSI virtuales de Oracle VM Server for SPARC

Oracle Solaris 11.4 permite al usuario configurar un dispositivo SAN (red de área de almacenamiento) virtual para que represente un juego explícito de dispositivos SCSI físicos. El comportamiento original y por

defecto de un dispositivo vSAN es representar a *todos* los dispositivos SCSI físicos a los que se puede llegar desde el puerto iniciador del HBA SCSI especificado por el usuario.

En Oracle Solaris 11.4, el usuario puede introducir comandos para agregar dinámicamente dispositivos SCSI físicos explícitos a un dispositivo vSAN especificado, o eliminarlos de él. Al asociar un dispositivo vSAN específico con un dominio invitado específico, el usuario tiene control total sobre cuáles son los dispositivos SCSI físicos a los que puede acceder un dominio invitado específico.

## Funciones de gestión del sistema

En esta sección, se describen las características de gestión de sistema nuevas de esta versión. Estas características permiten configurar servicios con gestión ininterrumpida de configuración, automatizar aplicaciones de configuración en sistemas y brindar acceso administrativo seguro y remoto.

Consulte también [“Configuración de zonas invariables mediante ejecución en la ruta de confianza”](#) [19].

## Visualización de datos del sistema y análisis de rendimiento con el panel de control de la interfaz web del sistema Oracle Solaris

Oracle Solaris proporciona numerosas herramientas para la observación del sistema, incluidas herramientas de estadísticas (como `mpstat`), DTrace y registros de auditoría. El panel de control de la interfaz web del sistema Oracle Solaris le permite ver con mayor facilidad distintas clases de datos de rendimiento de aplicaciones y del sistema agrupados gráficamente para una observación y un análisis más eficaces. Identifique el estado actual del sistema y visualice estadísticas, fallos y cambios administrativos con el transcurso del tiempo y en comparación con otros períodos. Abra una hoja de datos para ver más detalles y datos adicionales relacionados. Compare gráficos de datos actuales e históricos para visualizar anomalías y tendencias, visualice los datos relacionados de los gráficos en otros gráficos de la misma página y visualice eventos, como eventos de auditoría, en el mismo gráfico con otros datos.

El panel de control de la interfaz web del sistema Oracle Solaris muestra visualmente el rendimiento actual y reciente, los fallos recientes del sistema y otros eventos. Esta combinación de información es útil para determinar cuáles son los recursos del sistema que se deben examinar para diagnosticar problemas.

Puede ver la utilización media de todos los recursos de un tipo seleccionado o ver la utilización de un único recurso. Por ejemplo, puede determinar cuáles son las aplicaciones responsables de la mayor parte del tráfico de red en un sistema. De manera similar, además de los datos de uso de CPU en general, puede seleccionar la partición de zonas de los datos de uso de CPU para determinar cuáles son las zonas que más usan la CPU. Puede determinar si un recurso está asignado a una zona o carga de trabajo en particular.

Para obtener más información, consulte [Uso del análisis de Oracle Solaris 12](#). Para obtener información sobre cómo almacenar sus propios datos en el almacén de estadísticas subyacente, consulte [Agregación de datos personalizados al análisis de Oracle Solaris 12](#).

## Visualización de rendimiento y utilización de DAX

En sistemas SPARC M7, M8, T7 y T8, puede usar el comando `daxstat` para mostrar las estadísticas de DAX (por DAX, por CPU o por cola) en formato tabular.

El comando `daxinfo` permite a los usuarios determinar la configuración estática del hardware de DAX disponible en un sistema. Esta información se puede usar para la generación de informes de rendimiento y diagnóstico.

Para obtener más información, consulte [“Displaying DAX Information”](#) de *Managing System Information, Processes, and Performance in Oracle Solaris 11.4* y las páginas del comando `man daxstat(8)` y `daxinfo(8)`.

## Grupos de propiedades anidados de SMF

La utilidad de gestión de servicios (SMF) de Oracle Solaris proporciona una infraestructura para almacenar datos de configuración del sistema en una ubicación centralizada, en lugar de hacerlo en los archivos de configuración específicos de las aplicaciones. La capacidad de modelado de SMF anterior se limitaba al modelado de afiliaciones entre datos de configuración.

Oracle Solaris 11.4 modifica la relación de los grupos de propiedades de SMF de modo que el nodo principal de un grupo de propiedades, además de ser un servicio o una instancia, pueda ser también otro grupo de propiedades. Con la introducción de esta relación, ahora es posible modelar una mayor variedad de datos de configuración del sistema. Una consecuencia de agregar esta relación es que, al identificar de manera única un grupo de propiedades, no solo debe considerar el nombre, sino también el linaje.

Los grupos de propiedades anidados están sujetos al mismo modelo de privilegios y a la misma verificación de plantillas que los grupos de propiedades. Para obtener más información, consulte la página del comando `man smf_template(7)`.

## Nuevas capas de perfil de SMF

Oracle Solaris 11.4 introduce tres nuevas capas de perfiles de SMF: `enterprise-profile`, `node-profile` y `sysconfig-profile`. En versiones anteriores, la configuración de SMF solo se podía aplicar a las capas `site-profile` y `admin`. En esta versión, al usar múltiples capas, puede aplicar la configuración útil en general a la capa `enterprise-profile`, la configuración específica de la ubicación a la capa `site-profile` y la configuración específica del host a la capa `node-profile`. Esta característica permite utilizar de manera eficaz los perfiles de SMF en entornos donde hay subjuegos de sistemas o sistemas individuales que necesitan sustituir una configuración más general.

Para obtener más información, consulte [“Repository Layers”](#) de *Managing System Services in Oracle Solaris 11.4* y el [Capítulo 5, “Configuring Multiple Systems”](#) de *Managing System Services in Oracle Solaris 11.4*. Consulte también las páginas del comando `man smf(7)`, `svccfg(8)` y `svcprop(1)` y las páginas del comando `man sysconfig(8)`, `solaris(7)`, `solaris-kz(7)` y `smf_bootstrap(7)`.

## Servicios de objetivos

Oracle Solaris 11.4 incluye un nuevo tipo de servicios, los servicios de objetivos, que proporciona un único punto de supervisión para juegos de servicios configurables, de los que dependen los servicios de objetivos. Si no se puede satisfacer la dependencia de un servicio de objetivos, el servicio de objetivos pasa al estado de mantenimiento y genera una alerta de FMA de software.

Para obtener más información, consulte el [Capítulo 7, “Creating a Service that Notifies if Conditions are not Satisfied”](#) de *Desarrollo de los servicios del sistema en Oracle Solaris 12* y las páginas del comando `man smf(7)` y `svcadm(8)`.

## Diagnóstico de fallos de conexión en caliente de dispositivos

En Oracle Solaris 11.4, la nueva característica de información de uso de dispositivo ayuda a diagnosticar fallos de `hotplug`. En versiones anteriores, cuando el comando `hotplug` no lograba extraer un dispositivo

ocupado, aparecía el mensaje de error “Devices or resources are busy” (Los dispositivos o recursos están ocupados) sin ninguna otra explicación, lo que dificultaba el diagnóstico del problema. Ahora con esta característica, se muestra información adicional que explica qué es lo que abrió o retuvo al dispositivo, lo que ayuda a diagnosticar el problema.

Por ejemplo, para comprobar si el dispositivo está ocupado, use el siguiente comando:

```
# hotplug offline /pci@0,0 pci.1,0
ERROR: devices or resources are busy.
/pci@0,0/pci8086,3408@1/pci1000,1000@0/sd@0,0:
  { Hold: module devfs (modid=6). }
  { Hold: module specfs (modid=3): spec_open() }
  { Open: process format[123501]. }
  { Open: module zfs (modid=49). }
```

Para obtener más información, consulte [Gestión de dispositivos en Oracle Solaris 12](#).

## Utilidad `sysadm`

Oracle Solaris 11.4 introduce la nueva utilidad `sysadm`, que se puede usar para controlar el modo de mantenimiento de un sistema y ejecutar la evacuación de zonas alojadas en el sistema. Al iniciarse el modo de mantenimiento, se genera un log de un registro de auditoría y se impide la ejecución de operaciones subsiguientes de conexión, inicio o migración entrante de cualquiera de las zonas hacia el sistema. Para evacuar el host, se pueden migrar todas las zonas con marca `solaris-kz` desde el sistema hacia destinos especificados en una instancia de servicio de SMF de zonas.

El modo de mantenimiento y la evacuación se pueden usar para realizar tareas de administración en el host de una zona o para retirarlo de servicio. Puede evitar que se conecten o inicien zonas nuevas, migrar zonas de núcleo que estén en ejecución hacia otros destinos, realizar un mantenimiento que requiera un reinicio, como la actualización de Oracle Solaris, y, finalmente, volver a migrar esas zonas de núcleo, tan solo con algunos comandos y sin interrupciones para las zonas de núcleo que estén en ejecución.

Para obtener más información, consulte la página del comando `man sysadm(8)`.

## Automatización de la configuración de servidores OUD y OpenLDAP

La utilidad `ldapservcfg` automatiza la configuración de servidores OpenLDAP y servidores Oracle Unified Directory (OUD) para admitir gestión de cuentas y servicios de nombres LDAP de Oracle Solaris. La utilidad está integrada con el servicio `svc:/network/ldap/server:openldap` de SMF y configura automáticamente el servidor cuando se la activa por primera vez. También se la puede ejecutar de manera interactiva para personalizar la configuración del servidor OpenLDAP o para configurar el servidor OUD. La utilidad `ldapservcfg` ayuda a los usuarios a desplegar con facilidad servidores OpenLDAP y OUD en sistemas Oracle Solaris. También activa la funcionalidad para la gestión de cuentas remota mediante RAD.

Para obtener más información, consulte la página del comando `man ldapservcfg(8)`.

## Software de gestión de configuración de Puppet

Puppet es un software multiplataforma que se puede utilizar para automatizar la gestión de la configuración de múltiples plataformas, incluidos los servidores Oracle Solaris y sus subsistemas.

Puede usar Puppet para estandarizar y aplicar las configuraciones de recursos en toda la infraestructura de TI. Oracle Solaris 11.4 incluye tipos de recursos de núcleo de Puppet, incluidos archivos, paquetes, usuarios

y servicios. Asimismo, se incluyen numerosos módulos para gestionar otras aplicaciones de software de terceros en Oracle Solaris. Finalmente, se proporcionan varios tipos de recursos específicos de Oracle Solaris para usar en la versión de Oracle Solaris, como las zonas de Oracle Solaris.

La nueva opción de configuración de Puppet de Oracle Solaris `config/ degrade_smf_on_error degrade_smf_on_error` hace que el servicio `puppet:agent` cambie a un estado de degradado cuando se produce un error de algún recurso durante la aplicación de un manifiesto de Puppet. Puppet se sigue ejecutando después de haberse marcado como degradado. Esta opción hace que los errores de recursos en las aplicaciones de manifiestos de Puppet sean más visibles para el usuario.

Tenga en cuenta que Oracle Solaris 11.4 admite Puppet 5.5. Este paquete de software no está instalado por defecto en el sistema.

Si un sistema tiene instalada una versión anterior de Puppet, esa versión se actualizará automáticamente a Puppet 5.5. Consulte [“What’s New in Puppet in Oracle Solaris 11.4” de \*Uso de Puppet para la gestión de configuración en Oracle Solaris 12\*](#) para obtener información importante sobre este cambio de versión.

Para obtener información general sobre Puppet, consulte [Puppet Documentation](#).

## MCollective

Marionette Collective, conocida como MCollective, es una estructura que le permite generar y gestionar un número grande de servidores con mayor facilidad. Cuando se trabaja con un gran número de servidores, es difícil contar con una lista estática de herramientas para la gestión del sistema. MCollective usa un método de detección que se basa en metadatos y filtrado para buscar hosts.

MCollective también usa un patrón de publicación-suscripción para la difusión de solicitudes a todos los servidores que están conectados al componente de middleware. Estas solicitudes tienen filtros conectados de modo que solo los servidores que coincidan con un filtro actúen en relación con las solicitudes.

Para obtener más información, consulte [Uso de Puppet para la gestión de configuración en Oracle Solaris 12](#) y [Using MCollective Command Line Applications](#).

## Augeas

Augeas es una biblioteca y herramienta de línea de comandos que proporciona una manera unificada de editar archivos de configuración de UNIX de distintos formatos. Cuando se la llama, Augeas proporciona una interfaz de línea de comandos donde se pueden leer los archivos de configuración, que se presentan organizados en forma de árbol. Estos datos se pueden manipular en la interfaz de Augeas. Posteriormente, los datos se vuelven a convertir al formato de los archivos de configuración originales para guardarlos.

Augeas proporciona una única API pública para manipular diversos archivos de configuración de UNIX. Otras aplicaciones pueden aprovechar esta API, en lugar de que cada una cuente con su propia solución para modificar archivos de configuración.

## Atributos de usuario por defecto para cuentas LDAP

En Oracle Solaris 11.4, la funcionalidad de atributos de usuario cualificados se amplía para proporcionar ajustes por defecto para hosts o grupos de red específicos. Las cuentas de usuario basadas en LDAP que no tengan atributos asignados explícitamente pueden heredar los atributos por defecto correspondientes al host en el que se ejecutan. Si no se especifican atributos por defecto basados en el host, y si el usuario pertenece a un grupo de red, se heredan los atributos asociados con el grupo de red. Esta funcionalidad simplifica

la administración de cuentas basadas en LDAP al permitirles compartir atributos de usuario comunes en función de la pertenencia a un grupo de red.

Para obtener más información, consulte las páginas de los códigos man [user\\_attr\(5\)](#), [useradd\(8\)](#), [userdel\(8\)](#) y [usermod\(8\)](#).

## Herramienta `useradm`

La herramienta `useradm` es un herramienta interactiva basada en menús para la administración de cuentas de usuarios y roles. Esta herramienta sustituye a User Manager de Visual Panels. La herramienta se implementa como cliente RAD mediante los enlaces Python que se describen en `usermgr(3rad)`, y se puede ejecutar en cualquier ventana de terminal. La interfaz de usuario consiste en menús jerárquicos que incluyen listas de selecciones disponibles.

La interfaz basada en menús de `useradm` simplifica la gestión de usuarios y roles, y es compatible con todos los aspectos de la gestión de cuentas, como la gestión de derechos de acceso, auditorías y contraseñas. Todas las opciones válidas se presentan en listas que se desplazan que le permiten interactuar con el teclado y hacer selecciones mediante las teclas apropiadas.

Para obtener más información, consulte la página del comando man [useradm\(8\)](#).

## Identificación de bugs en salida de fallos

Una nueva característica `stackdiag` incorpora el comando `fmadm faulty` para mostrar una lista de bugs que podrían haber ocasionado el fallo. Con esta lista de bugs conocidos, puede buscar soluciones en My Oracle Support.

Para obtener más información, consulte [Gestión de fallos, defectos y alertas en Oracle Solaris 12](#) y la página del comando man [stackdiag\(1\)](#).

## Utilidad `fcinfo`

En Oracle Solaris 11.4, se mejoró la utilidad `fcinfo` para proporcionar la siguiente funcionalidad:

- Establecer si un puerto HBA tiene acceso a un puerto remoto o no. El comando `fcinfo remote-port` puede mostrar el número y los detalles de todos los puertos remotos para cada puerto HBA cuando no se especifica ninguna opción.
- Establecer la clase de ruta y el estado de la ruta para todos los LUN presentados por una matriz de almacenamiento individual. El comando `fcinfo lu -v` puede especificar el world wide name (WWN) del nodo y el puerto remoto con las opciones `-P` y `-N` respectivamente.

Para obtener más información, consulte la página del comando man [fcinfo\(8\)](#).

## Nuevas opciones de gestión del repositorio de IPS

Image Packaging System (IPS) de Oracle Solaris tiene nuevas opciones para facilitar la gestión de acceso al repositorio de paquetes y la resolución de algunos problemas de instalación y actualización:

- Ignore la caché de red. Se agregó una nueva opción global llamada `--no-network-cache` para ignorar los datos almacenados en la caché de red.

Los problemas relacionados con el acceso a los datos de los paquetes pueden deberse al almacenamiento en caché de los proxies que se encuentran entre los repositorios de paquetes basados en la red y el cliente de paquetes. Para resolver estos problemas, use la opción `--no-network-cache` para obtener los datos de los paquetes siempre desde un repositorio y no desde las memorias caché que pueda tener un proxy HTTP.

Para obtener más información, consulte [“Initial Troubleshooting Steps” de Agregación de software y actualización de sistemas en Oracle Solaris 12](#) y la página del comando `man pkg(1)`.

- Active o desactive un origen específico. La combinación de `-d`, `-e` y `-g` del subcomando `pkg set-publisher` se puede usar para activar o desactivar un origen específico de un editor.

Para obtener más información, consulte [“Enabling and Disabling Publisher Origins” de Agregación de software y actualización de sistemas en Oracle Solaris 12](#) y la página del comando `man pkg(1)`.

Los mensajes de errores de IPS también son mejores. Por ejemplo, un mensaje de error que informa que falta una entrada de archivo también incluye el paquete que entrega el archivo.

## Instalación y funciones de gestión de software

En esta sección, se describen las características de gestión de software e instalación nuevas de esta versión. Estas funciones permiten realizar actualizaciones y despliegues rápidos a través de herramientas de gestión e instalación de software.

### Inicio de servicios de sistema en el primer inicio

La herramienta `svc-create-first-boot` proporciona una única interfaz para crear, personalizar y publicar un paquete de servicios para el primer inicio. Proporcione la ruta del repositorio de paquetes y la secuencia de comandos del primer inicio como argumentos en la línea de comando; la herramienta publicará el paquete de servicios del primer inicio en el repositorio especificado. El uso de esta herramienta simplifica la ejecución automática de secuencias de comandos durante el primer inicio.

Para obtener más información, consulte la página del comando `man svc-create-first-boot(1)`.

### API de RAD para Automated Installer

Oracle Solaris 11.4 introduce la API de RAD para Automated Installer. Esta API proporciona funcionalidad para la administración remota de un servidor de Automated Installer (AI). Puede escribir programas para gestionar el servidor AI con cualquiera de los lenguajes de cliente admitidos de RAD.

Para obtener más información, consulte la página del comando `man autoinstall(3rad)`.

### Compatibilidad con Automated Installer para HMAC-SHA256

Las instalaciones de AI de Oracle Solaris ahora se pueden proteger con HMAC-SHA256. Los administradores pueden elegir HMAC-SHA256 como política para el algoritmo HMAC, para proteger los nuevos clientes y servicios de AI. Los administradores también pueden cambiar la versión del tipo de HMAC para que los servicios y los clientes se apliquen de inmediato, o generar claves de HMAC-SHA256 para que las instale el usuario, después de lo cual el administrador puede aplicar HMAC-SHA256. Los sistemas existentes protegidos con HMAC-SHA1 continuarán con esa protección hasta que se cambie la versión.

HMAC-SHA256 proporciona autenticación e integridad para las primeras fases de inicio de la instalación de AI de Oracle Solaris mediante el protocolo de inicio WAN. Esta compatibilidad en AI, sumada a la compatibilidad con el firmware de OBP de SPARC, garantiza el uso de estándares de seguridad modernos para instalaciones de red de área extensa.

Para obtener más información, consulte la página del comando `man installadm(8)`.

## Deshidratación y rehidratación para archivos unificados de Oracle Solaris

La deshidratación y la rehidratación para archivos unificados (UAR) de Oracle Solaris mejoran la tecnología de archivo actual para utilizar la tecnología de deshidratación/rehidratación de IPS y minimizar el espacio utilizado de los UAR creados.

En este contexto, deshidratar un archivo significa eliminar todos los archivos no editables y los enlaces físicos presentes en el paquete de la raíz alternativa de una imagen de archivo. Un archivo no editable del paquete es un archivo entregado por la versión actualmente instalada de un paquete que no tiene atributo de conservación o superposición, o que tiene un valor no etiquetado de `dehydrate=False`. Por otro lado, la rehidratación reinstala todos los archivos y los enlaces físicos eliminados por la deshidratación, para restaurar el estado original de la imagen de archivo.

Esta característica permite a los proveedores de software independientes (ISV) entregar pilas de aplicación dentro de un UAR, donde se deshidrataría el sistema operativo base y se alivianaría así la carga relacionada con el copyright y los derechos de distribución relacionados con el sistema operativo. En la práctica, el ISV crearía una pila de aplicación y una imagen del sistema operativo completamente desplegable y, a continuación, mediante una operación de deshidratación, se eliminaría la imagen del sistema operativo del archivo y quedaría solo la aplicación del ISV. El cliente podría posteriormente desplegar este archivo deshidratado y rehidratar el sistema operativo a partir de una copia propia legítima del repositorio del sistema operativo.

Los archivos a veces pueden ser de gran tamaño y la deshidratación ofrece una buena solución porque los archivos usan menos espacio en el sistema, lo que permite una mejor gestión del almacenamiento para múltiples archivos.

Si los clientes tienen algunos archivos deshidratados que desean desplegar en varios sistemas, sería útil un subcomando `rehydrate`. Al rehidratar un archivo deshidratado y regresarlo a su estado hidratado normal, puede minimizar el tiempo de despliegue, ya que lleva menos tiempo desplegar un archivo hidratado que uno deshidratado.

Para obtener más información, consulte la página del comando `man archiveadm(8)`.

## Compatibilidad con `cloudbase-init`

El servicio `cloudbase-init` realiza la configuración inicial de sistemas operativos invitados en la nube. Estas tareas incluyen la creación de usuarios, la generación de contraseñas, la configuración de red estática, el nombre de host, las claves públicas SSH y las secuencias de comandos de datos de usuario.

La versión de `cloudbase-init` de Oracle Solaris 11.4 es un servicio de utilidad de gestión de servicios (SMF) (`application/cloudbase-init`) que entrega el paquete IPS `cloudbase-init`.

- El paquete `cloudbase-init` no está instalado por defecto. Instale el paquete solo en imágenes que se vayan a desplegar en entornos de nube.

- El servicio está activado por defecto.
- El archivo de configuración, `/etc/cloudbase-init.conf`, solo activa el plugin `UserData`.

Las secuencias de comandos que se exportan por medio de datos de usuario, por lo general, realizan tareas de configuración del sistema y de aplicaciones que requieren acceso con privilegios. Por lo tanto, el servicio `cloudbase-init` se ejecuta como usuario `root`, de modo que las secuencias de comandos de datos de usuario también se deben ejecutar como `root`.

## Inicio de Oracle Solaris mediante agrupaciones de inicio sobre iSCSI-iSER

Con esta característica, las agrupaciones de inicio pueden usar iSCSI-iSER como protocolo de transporte por defecto en lugar de iSCSI-IPoIB para iniciar Oracle Solaris. El servidor puede usar agrupaciones de inicio para iniciar dispositivos de almacenamiento a los que no tiene acceso el firmware sobre destinos iSCSI. El uso del protocolo iSCSI-iSER brinda las siguientes ventajas:

- Inicia Oracle Solaris más rápido que con iSCSI-IPoIB.
- Accede a `rpool` a través de iSCSI-iSER con:
  - Mayor rendimiento
  - Menor latencia de transporte
  - Baja utilización de CPU
- No requiere configuración

## Inicio seguro de UEFI

El inicio seguro de UEFI en Oracle Solaris x86 le permite instalar e iniciar Oracle Solaris en plataformas donde está activado el inicio seguro de UEFI. Esta característica proporciona mayor seguridad porque mantiene una cadena de confianza durante el inicio: las firmas digitales del firmware y el software se verifican antes de ejecutar la siguiente etapa. No se producen interrupciones de la cadena debido a firmware o software sin firma, dañado o no autorizado durante el proceso de inicio. Esta característica permite garantizar que el firmware y el software que se usan para iniciar Oracle Solaris en una plataforma de hardware sean correctos y que no se los haya modificado ni estén dañados.

Para obtener más información, consulte [Protección de sistemas y dispositivos conectados en Oracle Solaris 12](#).

## Mejoras para desarrolladores

En esta sección, se describen las nuevas mejoras para desarrolladores de esta versión que hacen que el desarrollo de aplicaciones en la plataforma de Oracle Solaris sea más sencillo gracias a bibliotecas de última generación y estructuras confiables.

## Compatibilidad con estándar de lenguaje de programación C11

Oracle Solaris 11.4 incluye compatibilidad con el estándar de lenguaje de programación C11: "ISO/IEC 9899:2011 Tecnología de la información - Lenguajes de programación - C". El estándar C11 es una revisión compatible del estándar C99. Históricamente, el estándar del lenguaje de programación C ha sido parte de

la especificación única de UNIX. Sin embargo, el nuevo estándar del lenguaje de programación C, C11, está disponible de manera independiente de la próxima especificación de UNIX y fue publicado antes que esta.

Oracle Solaris 11.4 es compatible con C11 y C99 para que los clientes puedan usar C11 antes de su inclusión en una especificación futura de UNIX. El nuevo estándar se puede usar con los compiladores Oracle Developer Studio 12.5 o 12.6, GCC 5 o 7 y LLVM/Clang 6.0 C. Los desarrolladores también pueden escribir programas en C con el estándar del lenguaje de programación C más reciente.

## Entorno de compilación estándar

En Oracle Solaris 11.4, el modo de compilación por defecto (cuando no se usa ninguna macro de prueba de características para solicitar conformidad con un estándar POSIX en particular) hace visible lo siguiente:

- El espacio de nombres que corresponde a la especificación más reciente de POSIX
- Todas las demás funciones y nombres que normalmente proporciona el sistema operativo de Oracle Solaris

Para Oracle Solaris 11.4, la especificación más reciente de POSIX es Especificaciones básicas del estándar IEEE 1003.1-2008, Edición 7 (también conocida como XPG7, UNIX V7, SUSv4).

Se conserva la compatibilidad binaria. Sin embargo, la compatibilidad de origen podría verse afectada de las siguientes maneras:

Threads de POSIX	La macro de prueba de características <code>_POSIX_PTHREAD_SEMANTICS</code> es obsoleta y ya no se necesita. No la probará ningún archivo de cabecera. Las versiones de interfaces que antes solo eran visibles mediante <code>-D_POSIX_PTHREAD_SEMANTICS</code> o macros de prueba de características de estándares apropiados ahora son visibles por defecto. Se incluyen <code>asctime_r()</code> , <code>ctime_r()</code> , <code>getgrgid_r()</code> , <code>getgrnam_r()</code> , <code>getlogin_r()</code> , <code>getpwnam_r()</code> , <code>getpwuid_r()</code> , <code>readdir_r()</code> , <code>sigwait()</code> y <code>ttynam_r()</code> . Las interfaces por defecto anteriores, que se basaban en un estándar de threads de POSIX provisional, siguen estando disponibles en el momento de la compilación si se usa <code>-D__USE_DRAFT6_PROTOTYPES__</code> . Consulte la página del comando <code>man intro(3)</code> para obtener más información.
Sockets X/Open (XNS, edición 4)	Antes, se requería <code>-D_XOPEN_SOURCE=500</code> para usar las interfaces de sockets definidas por el estándar X/Open. Estas interfaces ahora son visibles también en el entorno de compilación por defecto. La compilación de aplicaciones que utilizan los sockets de estilo SunOS4.x antiguos ahora requiere el uso de <code>-D__USE_SUNOS_SOCKETS__</code> . Consulte <code>socket.h(3HEAD)</code> para obtener más información.

## Biblioteca de control de procesos

Oracle Solaris 11.4 incluye una nueva biblioteca de control de procesos, `libproc`, que proporciona una interfaz de nivel superior para características de la interfaz `/proc`. La biblioteca también proporciona acceso a información como tablas de símbolos, que son necesarias para examinar y controlar procesos y threads.

Un proceso de control que usa `libproc` normalmente puede:

- Capturar un proceso víctima y suspender su ejecución
- Examinar el estado del proceso víctima
- Examinar y modificar el espacio de dirección del proceso víctima
- Hacer que el proceso víctima ejecute llamadas de sistema en nombre del proceso de control
- Liberar el proceso víctima para que se pueda volver a ejecutar sin interrupciones

La biblioteca `libproc` proporciona todos los mecanismos que necesita un depurador de punto de ruptura para hacer su trabajo. También facilita la creación de aplicaciones de control simples de un uso para hacer cosas simples a procesos víctima sin que los procesos noten la intrusión.

Para obtener más información, consulte la página del comando `man libproc(3LIB)`.

## Mayor compatibilidad con configuraciones regionales

Oracle Solaris 11.4 incluye mejoras en las API de compatibilidad con configuraciones regionales existentes proporcionadas por `libc`, y la adición de nuevas API definidas en el estándar UNIX V7. Se introdujeron `uselocale` y otras API definidas en el estándar UNIX V7 para admitir configuraciones regionales entre threads y permitir el cambio de configuración regional del thread. En combinación con las nuevas API, las API de compatibilidad de configuración regional existentes se actualizaron por completo para multithreading. El procesamiento subyacente de la configuración regional de `libc` se mejoró para obtener un mejor rendimiento y lograr un menor uso de recursos por parte de las aplicaciones que usan múltiples configuraciones regionales.

Para obtener más información, consulte las páginas del comando `man uselocale(3C)`, `newlocale(3C)`, `freelocale(3C)`, `wctype(3C)` y `localedef(1)`.

## Puntos de observación de modo de usuario

Oracle Solaris 11.4 ahora implementa puntos de observación de modo de usuario con Silicon Secured Memory (SSM) en lugar de asignaciones de memoria virtual. Un punto de observación es un evento que se dispara cuando se escribe en una ubicación de memoria, o cuando se lee una, y que se puede usar para depuración y análisis de rendimiento. Actualmente, para implementar los puntos de observación se hace que la página que incluye la dirección sea inaccesible. Esta acción ralentiza mucho la ejecución si el thread toca con frecuencia ubicaciones no relacionadas en la misma página. En comparación, SSM tiene una granularidad mucho más fina con la línea de caché de 64 bytes. Además, SSM usa multithread, mientras que todos los threads comparten las mismas páginas de memoria virtual.

Para obtener más información, consulte las páginas del comando `man dbx(1)` y `mdb(1)`.

## Biblioteca de DTrace

Oracle Solaris 11.4 incluye una nueva biblioteca de control de procesos, `libdtrace`, que permite a los desarrolladores escribir aplicaciones *bespoke* de DTrace.

Para obtener más información, consulte el [Apéndice A, “libdtrace API Reference,” de Guía de Oracle Solaris 12 DTrace \(Dynamic Tracing\)](#).

## Compatibilidad con DWARF en DTrace

En Oracle Solaris 11.4, DTrace puede usar DWARF para realizar traducción de metadatos de direcciones a código fuente para procesos de usuario. La nueva opción `uresolve` permite que las acciones `ustack`, `uaddr` y `printf` de DTrace traduzcan direcciones de usuario a números de línea y nombres de archivo de código fuente, dada la presencia de información de depuración de DWARF. Esta característica proporciona una interpretación más intuitiva de la salida común del diagnóstico sin dejar de ser compatible con estándares de compiladores comunes.

Para obtener más información, consulte las acciones `ustack`, `uaddr` y `printf` en [“Data Recording Actions” de Guía de Oracle Solaris 12 DTrace \(Dynamic Tracing\)](#).

## Compatibilidad con `pstack` para números de línea codificados en DWARF

En Oracle Solaris 11.4, el comando `pstack` hará anotaciones en marcos con metadatos de código fuente, dada la presencia de información de depuración de DWARF. Esta característica proporciona una interpretación más intuitiva de la salida común del diagnóstico sin dejar de ser compatible con estándares de compiladores comunes.

Para obtener más información, consulte `pstack` en la página del comando `man proc(1)`.

## Reversión de DWARF en `pstack` y `mdb`

En Oracle Solaris 11.4, tanto `pstack` como `mdb` admiten reversión de pila de DWARF y del estilo de DWARF para procesos de usuario. Además, `pstack` y `mdb` también permiten la recuperación de argumentos de funciones a partir de procesos compilados con la nueva opción `-preserve_argvalues=complete` de Oracle Developer Studio. Esta capacidad proporciona mejoras específicas para la observación y el diagnóstico de los procesos `amd64`, aunque la funcionalidad se aplica a procesos de 32 bits y de 64 bits tanto en `x64` como en `SPARC`.

El comando `mdb ::stackregs dcmd` ahora está activado para `amd64`, donde los registros de los marcos se recuperan mediante tablas de reversión de estilo DWARF.

## Cython

Cython es un compilador estático de optimización que se usa para el lenguaje de programación Python y el lenguaje de programación ampliado Cython, que se basa en Pyrex. Esta característica permite la generación de código de alto rendimiento con Python.

Para obtener más información, consulte [Extensiones C de Cython para Python](#).

## Oracle Database Programming Interface-C

Oracle Database Programming Interface-C (ODPI-C) es un envoltorio para Oracle Call Interface (OCI) que funciona de manera transparente con distintas versiones de las bibliotecas Oracle Instant Client.

ODPI-C elimina el requisito de que las aplicaciones definan `LD_LIBRARY_PATH` antes de la ejecución. Asimismo, ODPI-C funciona de manera transparente con múltiples versiones de las bibliotecas de Oracle Instant Client. El software que requiere el uso de las bibliotecas de Oracle Instant Client no requerirá la configuración de `ORACLE_HOME` antes de la ejecución.

Para usar ODPI-C, instale el paquete `developer/oracle/odpi`.

Para obtener más información sobre ODPI-C, consulte el proyecto [Interfaz de programación de Oracle Database para controladores y aplicaciones](#) en GitHub y la página del comando `man libodpic(3LIB)`. Oracle Instant Client está disponible en formato IPS, y no es necesario visitar OTN para descargar archivos `.zip`.

## Módulo de Python `cx_oracle`

`cx_oracle` es un módulo de Python que le permite acceder a Oracle Database 12c y 11i desde aplicaciones de Python. Si bien el módulo suele estar disponible mediante paquetes pregenerados para otros sistemas

operativos, hasta ahora no había estado disponible de manera similar para Oracle Solaris. El módulo está disponible para formatos de 32 bits y de 64 bits. Oracle Solaris versión 5.2 se puede usar con Python 2.7 y 3.4.

Para obtener más información, consulte [Documentación de cx\\_Oracle](#).

## Novedades adicionales

En esta sección, se describen las nuevas características adicionales de esta versión. Estas características y mejoras se suman a la completa recopilación actual de utilidades, servicios y herramientas que brindan mayor productividad.

## Entorno de escritorio GNOME

El entorno de escritorio de Oracle Solaris se actualizó de GNOME 2.30 a GNOME 3.24 en Oracle Solaris 11.4. Las aplicaciones centrales de escritorio también se actualizaron. Algunas aplicaciones opcionales ya no se incluyen en Oracle Solaris. Los usuarios pueden elegir entre el entorno de shell moderno GNOME o el entorno clásico GNOME en la pantalla de inicio de sesión. Para obtener información detallada, consulte [Oracle Solaris 11.4 Desktop](#).

Oracle Solaris 11.4 ya no admite el escritorio de Trusted Extensions con etiquetas de varios niveles ni configuraciones de Sun Ray. Para obtener información detallada, consulte [Fin de características \(EOF\) planificado para versiones futuras de Oracle Solaris](#).

## Mejoras de los comandos `man`

En Oracle Solaris 11.4, las páginas del comando `man` que usan las secciones de System V se renumeraron según las secciones estándar. Las secciones `1m`, `4`, `5`, `7` y sus subsecciones, que se usaban en las versiones anteriores, ahora son `8`, `5`, `7`, `4` y sus subsecciones, respectivamente. Los usuarios que están familiarizados con otras plataformas, como BSD, Linux o MacOS X, pueden usar los mismos números de sección con el comando `man`.

El comando `man` admite búsquedas del nombre jerárquico de la página del comando `man`, que incluye una o más barras diagonales. Por ejemplo, `man system/name-service/switch` puede mostrar la página del comando `man` desde `usr/share/man/man8s/system/name-service/switch.8s`.

El comando `man` también admite el estilo de abreviación para las subsecciones. Por ejemplo, la página del comando `man printf(3c)` se puede buscar mediante `man printf.3 0 man -s 3 printf`.

El comando `man` puede asignar los números de sección de System V antiguos a los números estándar cuando sea necesario, de modo de facilitar la búsqueda de referencias en la documentación antigua.

Para obtener más información, consulte la página del comando `man` [man\(1\)](#).

## Oracle Solaris Online Documents for RAD and Web Dashboard

La aplicación Oracle Solaris Online Documents for RAD and Web Dashboard muestra documentos para búsquedas en el panel de control de la interfaz web del sistema Oracle Solaris. Para acceder a la documentación proporcionada por esta aplicación, use el menú de aplicación de panel de control de interfaz web del sistema. Los documentos se instalan mediante paquetes IPS en la siguiente ubicación: `/usr/lib/webui/htdocs/solaris/apps/docs`.

El panel de control de la interfaz web del sistema Oracle Solaris es el único punto de acceso para la documentación de la API de RAD. Para documentos que podrían estar disponibles en varias ubicaciones, el acceso del panel de control de la interfaz web es muy cómodo.

Para obtener más información, consulte las páginas del comando `man odoc-bundle(5)` y `o doctool(1)`.

## Filtro de impresión `paps`

`paps` convierte texto en lenguaje PostScript mediante la biblioteca Pango. `paps` lee un archivo de entrada y escribe lenguaje PostScript o un formato especificado por el usuario que representa el archivo como salida estándar. `paps` acepta texto internacional en cualquier configuración regional y proporciona un diseño de texto internacionalizado que incluye la forma del texto y representación de texto bidireccional.

Para obtener más información, consulte la página del comando `man paps(1)`.

## Modernización de la estructura `iconv`

El comando `iconv` y la API `iconv()` de Oracle Solaris se modernizaron para usar la API `cconv` internamente para la conversión. `cconv` es un mecanismo de conversión unificado que usa Unicode como codificación intermedia. `cconv` admite una amplia variedad de juegos de códigos y proporciona el comando `geniconvtbl` para generar tablas de conversión con reglas de conversión personalizadas.

Para obtener más información, consulte las páginas del comando `man iconv(1)`, `iconv(3C)`, `cconv(3C)`, `cconv_open(3C)`, `cconv_close(3C)`, `cconvct1(3C)`, `geniconvtbl(1)` y `geniconvtbl-cconv(5)`.

## Mecanismo de reserva de nombre de configuración regional

Esta nueva característica de Oracle Solaris 11.4 amplía la capacidad de búsqueda del comando `gettext` a directorios adicionales. Al buscar un catálogo de mensajes, el comando `gettext` también busca directorios de reserva en función del idioma y el territorio, como `fr_FR` y `fr`, además de `fr_FR.UTF-8`. Esta característica permite que el comando `gettext` se comporte de manera similar a otros sistemas operativos similares a UNIX.

Para obtener más información, consulte la página del comando `man gettext(3C)`.

## Compatibilidad con estándar de productos de Open Group UNIX V7

Oracle Solaris 11.4 cuenta con certificación de conformidad con el estándar de productos de The Open Group UNIX V7. Esta certificación tiene muchas mejoras con respecto a la certificación anterior, UNIX 03. El cambio más importante es la alineación con la especificación única de UNIX, versión 4, que incluye las especificaciones básicas de The Open Group, edición 7, y las correcciones técnicas aprobadas. Esta versión también permite a los sistemas certificados admitir el control de acceso basado en roles como opción.

Al usar el compilador C Oracle Developer Studio 12.5 o 12.6, o las versiones más recientes de `gcc`, LLVM o `clang` que se encuentran en Oracle Solaris 11.4, Oracle Solaris 11.4 admite lo siguiente:

- Las interfaces (C) de lenguaje de programación C ANSI X3.159-1989 y lenguaje de programación C ISO/IEC 9899:1990
- ISO/IEC 9899:1990 enmienda 1:1995: Integridad de C

- Lenguajes de programación C ISO/IEC 9899:1999
- Lenguajes de programación C INCITS/ISO/IEC 9899:2011

Para obtener más información, consulte [Estándar IEEE 1003.1TM, 2008/Especificaciones básicas de estándar técnico de The Open Group, edición 7](#). También puede consultar la página del comando `man standards(7)`.

## Compatibilidad con Unicode 8.0

Las configuraciones regionales de UTF-8 de Oracle Solaris se actualizaron con la versión 8.0 del estándar de Unicode. Unicode es un estándar de la industria informática para la codificación, la representación y el procesamiento uniformes de texto expresado en la mayoría de los sistemas de escritura del mundo.

## Actualización de CLDR 28

Las configuraciones regionales de Oracle Solaris 11.4 se actualizaron con CLDR versión 28, que proporciona mejoras en la calidad de los datos de la configuración regional. Para obtener más información, consulte [Guía de entornos de idiomas internacionales para Oracle Solaris 12](#).



Novedades de Oracle Solaris 11.4

**Referencia: E74963-01**

Copyright © 2018, 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 subsidiarias declinan toda responsabilidad derivada de los daños causados por el uso de este software o hardware en aplicaciones de riesgo.

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

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

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

**Accesibilidad a la documentación**

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

**Acceso a Oracle Support**

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

**Part No: E74963-01**

Copyright © 2018, Oracle and/or its affiliates. All rights reserved.