StorageTek Tape Analytics

Guía de instalación y configuración

Versión 2.1.0

E60937-02

Febrero de 2015

ORACLE

StorageTek Tape Analytics

Guía de instalación y configuración

E60937-02

Tabla de contenidos

Lista de figuras

Lista de tablas

Lista de ejemplos

Prefacio

En este documento, se proporcionan conceptos y procedimientos para instalar y configurar StorageTek Tape Analytics (STA) de Oracle.

Destinatarios

Este documento está destinado a los siguientes destinatarios:

- Administrador de Linux: instala, configura y administra Linux en el servidor de STA.
- Administrador de STA: instala, configura y administra la aplicación de STA.
- Administrador de bibliotecas: configura y administra las bibliotecas de StorageTek.
- Programador del sistema MVS: configura y administra el acceso a STA por parte de los usuarios del mainframe de IBM.

Accesibilidad a la documentación

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

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

Documentos relacionados

El conjunto de documentación de STA consta de los siguientes documentos.

Para los usuarios de la aplicación de STA

- *Guía de inicio rápido de STA*: utilice esta guía para conocer la aplicación de STA y algunas de las características de la interfaz de usuario.
- *Guía del usuario de STA*: utilice esta guía para obtener instrucciones sobre el uso de todas las características de la aplicación de STA, lo que incluye el panel de control, las plantillas, los filtros, las alertas, los informes ejecutivos, los grupos lógicos y la validación de medios de STA. En esta guía también se proporcionan instrucciones para administrar y gestionar nombres de usuario, direcciones de correo electrónico, logs de servicio y conexiones SNMP de STA con las bibliotecas supervisadas.

- *Guía de principios básicos de pantalla de STA*: utilice esta guía para obtener detalles completos acerca de la interfaz de usuario de STA. Describe la navegación y la distribución de la pantalla y utiliza los gráficos y las tablas.
- *Guía de referencia de datos de STA*: utilice esta guía para buscar definiciones para todas las pantallas del sistema de biblioteca de cintas STA y los atributos de datos.

Para los instaladores y administradores del servidor y la aplicación STA

- *Notas de la versión de STA*: lea este documento antes de instalar y usar STA. Contiene información importante de la versión, incluidos los problemas conocidos. Este documento está incluido en la descarga del paquete de medios de STA.
- *Guía de requisitos de STA*: utilice esta guía para obtener información sobre los requisitos mínimos y los recomendados para el uso de STA. En esta guía, se incluyen los siguientes requisitos: biblioteca, unidad, servidor, interfaz de usuario, validación de medios de STA y control de acceso de RACF de IBM.
- *Guía de instalación y configuración de STA*: utilice esta guía para planificar la instalación de STA, instalar el sistema operativo Linux, instalar la aplicación de STA y configurarla para comenzar a supervisar las bibliotecas. En esta guía también se proporcionan instrucciones para actualizar a una versión más reciente de STA.
- *Guía de administración de STA*: utilice esta guía para obtener información acerca de las tareas administrativas del servidor de STA, por ejemplo, la configuración de servicios, la copia de seguridad y la restauración de bases de datos y la administración de contraseñas para cuentas de bases de datos de STA.
- *Guía de seguridad de STA*: lea este documento para obtener información importante de seguridad acerca de STA, incluidos los requisitos, las recomendaciones y los principios generales de seguridad.
- *Manual de usuario de información sobre licencias de STA*: lea este documento para obtener información acerca del uso de tecnología de terceros distribuida con el producto STA.

Convenciones

En este documento, se utilizan las siguientes convenciones de texto:

Convención	Significado
negrita	El tipo de fuente en negrita indica elementos de la interfaz gráfica de usuario asociados a una acción o términos definidos en el texto o el glosario.
cursiva	El formato de cursiva indica títulos de libros, énfasis o variables de pendientes de asignación para los que se proporcionan valores concretos.
`monoespacio`	El tipo de fuente monoespaciada indica comandos dentro de un párrafo, direcciones URL, código en ejemplos, texto que aparece en la pantalla o texto que el usuario escribe.

Novedades

En esta sección, se resumen las funciones nuevas y mejoradas de StorageTek Tape Analytics 2.1.0.

STA 2.1.0, enero de 2015

Consulte los manuales indicados para obtener información detallada acerca de las funciones nuevas y mejoradas.

Temas que se describen en la *Guía de requisitos de STA*

- Nuevos niveles recomendados de firmware de biblioteca y unidad para compatibilidad con STA 2.1.0.
- Compatibilidad con el protocolo TTI 5.50 para unidades StorageTek T10000C y T10000D de Oracle.
- Actualización de requisitos recomendados para bibliotecas y unidades para compatibilidad con STA 2.1.0.
- Actualización de configuración recomendada para el servidor de STA.

Temas que se describen en la *Guía de instalación y configuración de STA*

- Nuevo instalador y desinstalador de STA 2.1.0, que proporcionan las siguientes funciones:
  - Usuario y grupo de instalación de Oracle: usuario y grupo de Linux usado exclusivamente para instalar y actualizar productos de Oracle en el servidor de STA.
  - Ubicación de directorio raíz de almacenamiento de Oracle definida por el usuario: la aplicación de STA y el software asociado de Oracle se pueden instalar en cualquier sistema de archivos que tenga espacio suficiente.
  - Ubicaciones de base de datos y copia de seguridad local definidas por el usuario.
  - Ubicación de inventario central de Oracle: directorio para llevar un control de la información sobre los productos de Oracle instalados en el servidor de STA.
  - Modo silencioso de instalador y desinstalador de STA: permite no usar la interfaz gráfica de usuario y proporcionar las opciones de instalación en un archivo de propiedades XML.
  - Nuevos logs detallados de instalador y desinstalador de STA.
  - Ayuda contextual para todas las pantallas de instalador y desinstalador gráficos de STA.
- Requisito de paquete RPM de Linux adicional: se debe instalar el paquete *`xorg-x11-utils`* para ejecutar el instalador gráfico de STA.
- Los puertos predeterminados para la consola de administración de WebLogic ahora son 7019 (HTTP) y 7020 (HTTPS). Si utilizaba las asignaciones predeterminadas previas, sería conveniente que las cambie por las nuevas.

- Nuevos requisitos de contraseña para nombres de usuario de STA y MySQL.
- Nuevo proceso para actualizar bases de datos de STA 1.0.x y STA 2.0.x a STA 2.1.0.

Temas que se describen en la *Guía de inicio rápido de STA*

- Sin cambios importantes.

Temas que se describen en la *Guía del usuario de STA*

- Actualizaciones menores de las siguientes plantillas para proporcionar información adicional y mejorar la facilidad de uso:
  - STA-Complex-Configuration
  - STA-Complex-Utilization
  - STA-Lib-Configuration
  - STA-Drive-MV
  - STA-Media-All
  - STA-Media-MV-Calibration
  - Pantalla Media Validation Overview (Descripción general de validación de medios), plantilla STA-Default
- Cambios de documentación: los siguientes capítulos se reubicaron de la *Guía de administración de STA*. En la *Guía del usuario de STA*, ahora se describen todas las funciones y las actividades que se pueden realizar desde la interfaz de usuario de STA.
  - Nombre de usuario y correo electrónico de STA
  - Logs de servicio de STA
  - Gestión de conexiones SNMP en STA

Temas que se describen en la *Guía de principios básicos de pantalla de STA*

- Sin cambios importantes.

Temas que se describen en la *Guía de referencia de datos de STA*

- Los atributos que se presentan en algunas pantallas se reorganizaron para mejorar la facilidad de uso.
- Los atributos "Last Messages" (Últimos mensajes) están disponibles en las pantallas respectivas para CAP, unidades, elevadores, bibliotecas, PTP y robots.

Temas que se describen en la *Guía de administración de STA*

- Cambios de documentación: los siguientes capítulos se movieron a la *Guía del usuario de STA*:
  - Usuarios y correo electrónico
  - Registro
  - Gestión de SNMP

1

Planificación previa a la instalación

En este capítulo, se incluyen las siguientes secciones:

1.1. Descripción general de la implementación de STA

Para la instalación y la configuración iniciales de STA, realice las siguientes actividades en el orden indicado. Puede realizar el proceso por su cuenta o adquirir los servicios de instalación de Oracle.

Para actualizar STA a partir de una versión previa, consulte el Capítulo 8, *Actualización a STA 2.1.0*.

Orden	Actividad	Detalles e instrucciones
1	Revise y verifique los requisitos de STA en la organización.	*Guía de requisitos de STA*
2	Prepare las solicitudes de servicio para las unidades y las bibliotecas, según sea necesario.	Sección 1.2, “Preparación de solicitudes de servicio para preparar las bibliotecas ”
3	Instale Linux en el servidor de STA.	Capítulo 2, *Instalación de Linux*
4	Instale STA en el servidor de STA.	Capítulo 3, *Instalación de STA*
5	Configure las bibliotecas para enviar datos a STA.	Capítulo 5, *Configuración de SNMP en las bibliotecas*
6	Configure STA para recibir datos de las bibliotecas y comenzar la supervisión.	Capítulo 6, *Configuración de conexiones de bibliotecas en STA*
7	Configure nombres de usuario y direcciones de correo electrónico adicionales de STA.	*Guía del usuario de STA*
8	Configure los servicios de copia de seguridad de bases de datos y supervisión de STA	Capítulo 7, *Configuración de los servicios de STA*
9	Configure un certificado de seguridad aprobado (opcional).	Apéndice D, *Configuración de certificados de seguridad*
10	Configure un proveedor externo para el control de acceso a STA (opcional).	Apéndice E, *Configuración de un proveedor de servicios de seguridad para STA*

1.2. Preparación de solicitudes de servicio para preparar las bibliotecas

Use este procedimiento y las secciones a las que se hace referencia para proporcionar al servicio de soporte de Oracle la información necesaria para preparar la biblioteca para la supervisión con STA.

Nota:

Si STA supervisará un complejo de bibliotecas, prepare una solicitud de servicio para cada biblioteca del complejo. Asimismo, abra una solicitud de servicio para instalar el firmware de unidad más reciente admitido por STA.

1. Verifique la versión de firmware de la biblioteca. Consulte Sección 4.3.2, “Verificación de la versión de firmware de la biblioteca”.
2. Verifique que haya instalada una tarjeta HBT con gran capacidad de memoria (solo SL3000 y SL8500). Consulte Sección 4.3.3, “Verificación de la versión de la tarjeta del controlador de unidad (solo SL3000 y SL8500)”.
3. Active ADI en la biblioteca y las unidades LTO: para bibliotecas con unidades LTO solamente. Consulte Sección 4.3.4, “Activación de ADI en la biblioteca (todas las bibliotecas, excepto SL150)”.
4. Configure el ID del complejo de bibliotecas (solo SL8500). Consulte Sección 4.3.5, “Uso del ID de complejo de bibliotecas correcto (solo SL8500)”.
5. Configure la fecha y la hora de la biblioteca. Para asegurarse de que las marcas de fecha y hora de la biblioteca se correlacionan con las marcas de fecha y hora del servidor de STA, el reloj de la biblioteca debe ser configurado por el servicio de soporte de Oracle.
6. Envíe las solicitudes de servicio necesarias.

2

Instalación de Linux

En este capítulo, se incluyen los siguientes temas:

Antes de instalar Linux en el servidor de STA, consulte los requisitos del sistema en *Guía de requisitos de STA*.

Nota:

No se puede realizar una actualización en el lugar de Linux 5.x a Linux 6.x. Si está instalando Linux 6.x como parte de una actualización a STA 2.0.x; consulte el Capítulo 8, *Actualización a STA 2.1.0*

Para instalar y configurar Linux para STA, realice las tareas de la Tabla 2.1, “Tareas de instalación de Linux” en el orden indicado.

Tabla 2.1. Tareas de instalación de Linux

Categoría	Tarea
Preparación	1. Sección 2.1.1, “Revisión de documentación relacionada” [26] 2. Sección 2.1.3, “Descarga del paquete de medios del instalador de Linux” [28]
Instalación	1. Sección 2.2.1, “Recopilación de la información necesaria” [29] 2. Sección 2.2.2, “Instalación de Linux ” [29] 3. Sección 2.2.3, “Ejecución del agente de configuración de Linux” [31]
Tareas posteriores a la instalación	1. Sección 2.3.1, “Desactivación de SELinux” [32] 2. Sección 2.3.2, “Desactivación del firewall de Linux” [33] 3. Sección 2.3.3, “Desactivación del control de acceso” [34] 4. Sección 2.3.4, “Configuración del proxy de red” [34] 5. Sección 2.3.5, “Configuración correcta de Yum (opcional)” [35] 6. Sección 2.3.6, “Instalación de los paquetes de Linux requeridos” [36] 7. Sección 2.3.7, “Configuración correcta de SSH” [37] 8. Sección 2.3.8, “Configuración correcta de DNS” [37] 9. Sección 2.3.9, “Desactivación de servicios de nombres” [38] 10. Sección 2.3.10, “Funcionalidad de explorador local (opcional)” [38]

2.1. Tareas de preparación

Realice estos procedimientos antes de instalar Linux en el servidor de STA.

2.1.1. Revisión de documentación relacionada

Debido a la amplia variedad de requisitos y opciones de configuración de red, consulte los siguientes documentos para obtener ayuda con la instalación y la configuración del hardware, el software y la red. En estos documentos, se analiza en detalle la configuración de las redes IPv4 e IPv6.

- Guías para la instalación de Linux de Oracle:

  `http://docs.oracle.com/en/operating-systems/`
- Documentación de RedHat Linux:

  `https://access.redhat.com/home`

2.1.2. Revisión de la disposición del sistema de archivos de STA

En la Tabla 2.2, “Disposición recomendada para el sistema de archivos”, se describe la disposición del sistema de archivos recomendada para el servidor de STA. La disposición se configura durante la instalación de Linux.

Las siguientes ubicaciones están definidas por el usuario, lo que significa que puede configurar la disposición para adecuarse a las necesidades de la organización.

- Directorio raíz de almacenamiento de Oracle: el instalador de STA le solicitará que defina esta ubicación. No hay ningún valor por defecto. Consulte Ubicación de directorio raíz de almacenamiento de Oracle para obtener detalles.
- Base de datos de STA: el instalador de STA le solicitará que defina esta ubicación. El valor predeterminado es */dbdata*.
- Copia de seguridad local de la base de datos de STA: el instalador de STA le solicitará que defina esta ubicación. El valor predeterminado es */dbbackup*.
- Logs de STA y MySQL: el valor predeterminado es */var/log/tbi*. Si desea usar otra ubicación, después de completar la instalación de Linux y antes de instalar STA, debe crear un enlace simbólico que vaya desde la ubicación deseada a */var/log/tbi* después de haber instalado STA. Consulte Sección 3.6.6, “Reubicación del directorio de logs de STA (opcional)” para obtener instrucciones.

Oracle recomienda crear todos estos sistemas de archivos antes de instalar STA, ya que de lo contrario, STA se instala en el directorio raíz "*/*" y el directorio */var*, y se necesitaría asignación de espacio adicional para esos directorios. Si bien el instalador de STA crea directorios según sea necesario, usted tiene un mayor control de las propiedades del sistema de archivos si crea los sistemas de archivos con antelación.

Tabla 2.2. Disposición recomendada para el sistema de archivos

Sistema de archivos	Punto de montaje predeterminado	Tamaño	Descripción y recomendaciones
root	`/`	32 GB como mínimo	Si `/tmp` está incluido en este sistema de archivos, se debe mantener un mínimo de 4 GB de espacio libre; este espacio se necesita durante las instalaciones y las actualizaciones de STA.
swap	Ninguno. Definido como memoria.	Del 50 al 100 % del tamaño de la RAM	Usado para espacio de intercambio.

Directorio raíz de almacenamiento de Oracle	`/Oracle`	30 GB como mínimo
		
		50 GB recomendado
			Ubicación de los archivos de las aplicaciones del middleware de STA y Oracle (WebLogic, MySQL, RDA).
			
			Esta ubicación es definida por el usuario. Debe ser un sistema de archivos independiente en un volumen independiente. Mantenga un mínimo de 4 GB de espacio libre para las instalaciones y las actualizaciones de STA. Mantenga 5 GB de espacio libre adicional para la rotación de registros de WebLogic.
			
			STA crea automáticamente los siguientes subdirectorios de middleware de Oracle:
			
			• Registros de WebLogic rotados:
			
			`/Oracle_storage_home/Middleware/user_projects/domains/TBI/servers`
			• Instantánea de CLI más reciente de RDA:
			
			`/Oracle_storage_home/Middleware/rda/output`
			• Paquetes de logs de instantánea de GUI de STA:
			
			`/Oracle_storage_home/Middleware/rda/snapshots`

Ubicación de la base de datos de STA	`/dbdata`	De 250 GB a 2 TB	Ubicación de la base de datos de STA. Esta ubicación es definida por el usuario. Oracle recomienda colocar este directorio en su propio volumen, separado de las ubicaciones root, de intercambio, de directorio raíz de almacenamiento de Oracle y de los logs de STA. Para optimizar el rendimiento, las copias de seguridad y las tareas de mantenimiento, lo ideal es usar un conjunto de unidades duplicadas o segmentadas independiente. El tamaño requerido depende de la cantidad de bibliotecas, unidades, medios, intercambios por día y años de datos históricos. Oracle recomienda configurar los servicios de STA para que envíen alertas si la utilización del espacio excede un porcentaje especificado.
Ubicación de copia de seguridad de base de datos local de STA	`/dbbackup`	Del 70 al 80 % del tamaño de `/dbdata`	Ubicación de la copia de seguridad local más reciente de la base de datos. Esta ubicación es definida por el usuario. Oracle recomienda que se encuentre en un volumen diferente del de la base de datos de STA y en unidades duplicadas o segmentadas en caso de daño o error de la base de datos.
Ubicación de los logs de STA	`/var/log/tbi`	30 GB como mínimo Se recomienda de 50 GB a 100 GB	Ubicación de los logs de STA y MySQL. Esta ubicación debe ser un volumen independiente en un punto de montaje independiente. El contenido tiende a crecer y se administra mediante la rotación de logs. La ubicación predeterminada es `/var/log/tbi`, pero puede cambiarla en cualquier momento después de la instalación de STA. Consulte Sección 3.6.6, “Reubicación del directorio de logs de STA (opcional)” para obtener instrucciones.

Sistema de archivos	Punto de montaje predeterminado	Tamaño	Descripción y recomendaciones
			Nota: Con la excepción de la rotación de registros, STA no gestiona el espacio. **Precaución**: Debe configurar la utilidad de copia de seguridad de STA para gestionar los archivos log que se encuentran en `/STA_logs/db/stadb_bin.*`. De lo contrario, estos archivos pueden requerir que se los gestione de manera manual (consulte información detallada en *Guía de administración de STA*).

2.1.3. Descarga del paquete de medios del instalador de Linux

Utilice este procedimiento para descargar el paquete de medios del instalador de Linux desde el sitio web de Oracle Software Delivery Cloud. El paquete de medios se entrega como un archivo de imagen ISO comprimido, el cual puede extraer y escribir en el medio portátil que desee (unidad flash, DVD, etc.).

Antes de realizar esta tarea, debe solicitar a su representante de soporte de Oracle un ID de usuario y una contraseña para Oracle Software Delivery Cloud.

1. Abra un explorador web y navegue al sitio web de Oracle Software Delivery Cloud:

   `http://edelivery.oracle.com/linux`
2. Haga clic en **Sign In/Register** (Conexión/Registro).
3. Escriba el ID de usuario y la contraseña proporcionados por el servicio de soporte de Oracle.
4. En la pantalla Terms & Restrictions (Condiciones y restricciones), seleccione las casillas para indicar que acepta el acuerdo de licencia y las restricciones de exportación y, a continuación, haga clic en **Continue** (Continuar).
5. En la pantalla Media Pack Search (Búsqueda de paquetes de medios):
   a. En el menú Select a Product Pack (Seleccionar un paquete de productos), seleccione **Oracle Linux**.
   b. En el menú Platform (Plataforma), seleccione **x86 64** bits (STA requiere Linux de 64 bits).
   c. Haga clic en **Go** (Ir).
6. Seleccione una versión de Linux y, a continuación, haga clic en **Continue** (Continuar).

   Consulte los requisitos de la versión de Linux en *Guía de requisitos de STA*.
7. Haga clic en **Download** (Descargar) para la opción de 64 bits.
8. Guarde el archivo ISO y escríbalo en un medio físico.

2.2. Tareas de instalación

Para los siguientes procedimientos, se supone que se realiza la instalación de Oracle Enterprise Linux (OEL) 6u4 desde un DVD con instalador gráfico y agente de configuración.

Si instala una versión diferente de Linux, usa otro tipo de medio o usa el modo de consola, los pasos y los paquetes pueden variar.

2.2.1. Recopilación de la información necesaria

Póngase en contacto con el administrador del sistema para obtener la siguiente información:

- Nombre de host y dirección IP del servidor de STA
- Dirección IP de la puerta de enlace y la máscara de red de la red
- Direcciones IP del servidor de DNS y dominios de búsqueda de la red
- Dirección IP de los servidores NTP (protocolo de tiempo de red) que utilizará
- Información del proxy de la red, si corresponde

2.2.2. Instalación de Linux

Use este procedimiento para realizar la instalación de Linux.

1. Conecte el medio físico de instalación al servidor de STA.
2. Siga las instrucciones del archivo README (LÉAME) del medio para iniciar el instalador de Linux.
3. Seleccione **Install or upgrade an existing system** (Instalar o actualizar un sistema existente).
4. Si está realizando la instalación desde un DVD, aparecerá la pantalla del CD encontrado. De manera opcional, puede realizar una prueba del medio. Para omitir la prueba, presione la **tecla de tabulación** para resaltar la opción **Skip** (Omitir) y, a continuación, presione la **barra espaciadora**.
5. En la pantalla Welcome (Bienvenido), haga clic en **Next** (Siguiente).
6. Seleccione un idioma y haga clic en **Next** (Siguiente).
7. Seleccione una distribución de teclado y haga clic en **Next** (Siguiente).
8. Seleccione **Basic Storage Devices** (Dispositivos de almacenamiento básicos) y, a continuación, haga clic en **Next** (Siguiente).
9. Introduzca un nombre de host para el servidor de STA y haga clic en **Configure Network** (Configurar red).
10. Seleccione el nombre del adaptador de red y haga clic en **Edit** (Editar).
11. Asegúrese de que las opciones **Connect automatically** (Conectar automáticamente) y **Available to all users** (Disponible para todos los usuarios) estén seleccionadas.
12. En los separadores restantes, configure el adaptador con las especificaciones de IPv4 o IPv6 que le indicó el administrador de la red. Debe especificar una dirección IP estática para el servidor de STA y, al menos, un servidor de DNS. Al finalizar, haga clic en **Apply** (Aplicar), **Close** (Cerrar) y **Next** (Siguiente).
13. Seleccione la zona horaria del servidor de STA, seleccione la casilla de control **System clock uses UTC** (El reloj del sistema usa UTC) y, a continuación, haga clic en **Next** (Siguiente).

14. Introduzca una nueva contraseña de root Linux para el servidor, confírmela y, a continuación, haga clic en **Next** (Siguiente).
15. Identifique la disposición de partición que se usará en el servidor:
    a. Como STA requiere un servidor dedicado, Oracle recomienda seleccionar **Use All Space** (Usar todo el espacio).
    b. Seleccione la casilla de verificación **Review and modify partitioning layout** (Revisar y modificar disposición de partición) y, a continuación, haga clic en **Next** (Siguiente).
16. Use la Tabla 2.2, “Disposición recomendada para el sistema de archivos” para modificar la disposición del sistema de archivos, ya que el utilizado de manera predeterminada no cumple con los requisitos mínimos para STA. De manera alternativa, puede usar la utilidad *`system-config-lvm`* para modificar el sistema de archivos después de la instalación de Linux.

    Al finalizar, haga clic en **Next** (Siguiente).
17. Cuando esté listo, seleccione **Write changes to disk** (Escribir cambios en el disco).
18. En la pantalla del cargador de inicio, deje todas las opciones como están y, a continuación, haga clic en **Next** (Siguiente).
19. En la pantalla de selección de software, seleccione **Basic Server** (Servidor básico) y no cambie las opciones del repositorio. Después, seleccione **Customize now** (Personalizar ahora) y haga clic en **Next** (Siguiente).
20. En la pantalla de selección de paquetes, use la Tabla 2.3, “Selección de paquetes de Linux” para configurar los paquetes de cada categoría de paquetes:
    a. Seleccione una categoría de paquetes.
    b. Seleccione la casilla de cada paquete en la columna Select (Seleccionar).
    c. Si un paquete requiere una opción (indicado con un signo +), resalte el paquete principal, haga clic en el botón **Optional packages** (Paquetes opcionales), seleccione el paquete secundario en la lista y, a continuación, haga clic en **Close** (Cerrar).
    d. Quite la selección de la casilla de cada paquete en la columna Deselect (Cancelar la selección).
    e. Deje las demás casillas de verificación como están.

Tabla 2.3. Selección de paquetes de Linux

Categoría de paquetes	Seleccionar	Anular selección
Sistema base	• Base • Bibliotecas de compatibilidad • Herramientas de Internet de la consola • Plataforma Java • Compatibilidad con UNIX heredado + *`ksh-xxxxxxxx-xx.el6.x86_64`*	• Herramientas de depuración • Compatibilidad con redes telefónicas • Cliente de directorio • Utilidades de supervisión de hardware • Rendimiento de sistemas grandes • Cliente de sistema de archivos de red • Herramientas de rendimiento
Servidores (opcional)	• Herramientas de administración del sistema	N/D
Servicios web	N/D	Todos los paquetes

Categoría de paquetes	Seleccionar	Anular selección
Bases de datos	N/D	Todos los paquetes
System Management	N/D	N/D
Virtualización	N/D	N/D
Escritorios (recomendado): se usa para realizar ciertos pasos posteriores a la instalación en un entorno gráfico; consulte información detallada en Sección 2.3, “Tareas posteriores a la instalación”.	• Escritorio • Plataforma de escritorio • Escritorio para uso general • Herramientas de administración gráficas + *system-config-lvm-x.x.xx-xx.el6.noarch*[1] • Compatibilidad con sistemas X Window heredados • X11 (sistema X Window, versión 11)	N/D
Aplicaciones (opcional): se puede usar para configurar y gestionar localmente el servidor de STA con la interfaz de la GUI.	• Explorador de Internet	N/D
Desarrollo	• Herramientas de desarrollo + *expect-x.xx.x.xx-x.el6.x86_64*	N/D
Lenguajes	N/D	N/D

[1]Opcional. Se puede usar para configurar o volver a configurar el sistema de archivos después de haber completado la instalación de Linux.

21. Cuando finalice con la selección de paquetes, haga clic en **Next** (Siguiente). Comienza la instalación.

    Si hace clic en **Next** (Siguiente) accidentalmente antes de haber configurado todos los paquetes, haga clic en **Back** (Atrás) después de que el software finalice la comprobación de dependencias.
22. Cuando aparezca la pantalla de felicitaciones, elimine los medios de instalación y haga clic en **Reboot** (Reiniciar).

    En */root/install.log*, puede encontrar un registro completo de la instalación.

2.2.3. Ejecución del agente de configuración de Linux

El agente de configuración de Linux se inicia automáticamente cuando reinicia el servidor Linux. Use este procedimiento para configurar el entorno del sistema.

1. En la pantalla Welcome (Bienvenido), haga clic en **Forward** (Adelante).
2. Lea el acuerdo de licencia, seleccione **Yes, I agree to the License Agreement** (Sí, acepto el acuerdo de licencia) y haga clic en **Forward** (Adelante).
3. En la pantalla Software Updates (Actualizaciones de software), si desea registrar el sistema para recibir actualizaciones, seleccione **Yes, I'd like to register now** (Sí, deseo registrarme ahora). De lo contrario, seleccione **No, I prefer to register at a later time** (No, prefiero registrarme en otro momento) y haga clic en **Forward** (Adelante).

4. En la pantalla Finish Updates Setup (Finalizar configuración de actualizaciones), haga clic en **Forward** (Adelante).
5. En la pantalla Create User (Crear usuario), deje los campos en blanco, haga clic en **Forward** (Adelante) y, a continuación, haga clic en **Yes** (Sí) para continuar. El servidor de STA no necesita un usuario que no sea administrador.
6. En la pantalla Date and Time (Fecha y hora):
   a. Configure la fecha y la hora actuales.
   b. Seleccione la casilla de control **Synchronize date and time over the network** (Sincronizar fecha y hora a través de la red).
   c. Agregue o quite los servidores NTP deseados (con la información que le dio el administrador de sistemas) y haga clic en **Forward** (Adelante).

   Nota:

   Para asegurarse de que los datos de STA y los archivos de registro sean correctos, la fecha y la hora del servidor de STA deben ser correctas. Además, las bibliotecas conectadas a STA también deben tener la hora correcta.
7. En la pantalla Kdump, *no* seleccione **Enable kdump?** (¿Activar kdump?). A continuación, haga clic en **Finish** (Finalizar).

   El sistema se reinicia.
8. Una vez reiniciado el sistema, inicie sesión como usuario root:
   a. Haga clic en **Other...** (Otro...).
   b. Introduzca el nombre de usuario **root** y, a continuación, haga clic en **Log In** (Iniciar sesión).
   c. Introduzca la contraseña del usuario root y vuelva a hacer clic en **Log In** (Iniciar sesión).

   Si aparece un mensaje que dice que inició sesión como superusuario root, puede omitirlo.
9. Confirme la versión y el nivel de actualización de Linux. Este paso es opcional.

```
# cat /etc/*-release
Oracle Linux Server release 6.4
Red Hat Enterprise Linux Server release 6.4 (Santiago)
Oracle Linux Server release 6.4
```

2.3. Tareas posteriores a la instalación

Realice las siguientes tareas para asegurarse de que el servidor de STA esté bien configurado para la instalación de STA.

2.3.1. Desactivación de SELinux

Oracle recomienda desactivar SELinux en el servidor de STA.

1. Abra una sesión de terminal en el servidor de STA.
2. Abra el archivo de configuración de SELinux con un editor de texto.

```
# vi /etc/sysconfig/selinux
```

3. En el archivo, configure *SELINUX* con el valor *disabled* (desactivado):

```
SELINUX=disabled
```

4. Guarde el archivo y ciérrelo.

2.3.2. Desactivación del firewall de Linux

Oracle recomienda desactivar el firewall en el servidor de STA. Sin embargo, puede elegir activar y configurar el firewall en función de los requisitos del sitio.

Utilice este procedimiento para desactivar el firewall.

1. Abra una sesión de terminal en el servidor de STA.
2. Compruebe la configuración del firewall de Linux (para el siguiente inicio).

```
# chkconfig --list |grep "ip"
```

Si el firewall está configurado para desactivarse en el siguiente inicio, todas las salidas de iptables e ip6tables aparecerán con el valor *off*. Si no fuera así, desactive el firewall.

```
# chkconfig iptables off
# chkconfig ip6tables off
```

3. Compruebe el estado actual del firewall de Linux.

```
# service iptables status
# service ip6tables status
```

La salida del comando indicará si el firewall se está ejecutando. Si el firewall se está ejecutando, deténgalo.

```
# service iptables stop
# service ip6tables stop
```

4. Si alguna de las siguientes opciones está configurada como true, deberá reiniciar el servidor.
   - Desactivó SELinux en Sección 2.3.1, “Desactivación de SELinux” [32].

- Desactivó el firewall de Linux (con *chkconfig*) en esta sección.

2.3.3. Desactivación del control de acceso

El control de acceso debe estar desactivado para ciertos directorios.

1. Muestre los permisos del directorio raíz de almacenamiento, la base de datos de STA, la copia de seguridad local de la base de datos de STA y los logs de STA. Por ejemplo:

   ```
   # ls –ld /Oracle /dbdata /dbbackup /var/log/tbi

   drwxr-xr-x 2 oracle oinstall  4096 Jul 30 14:48 /Oracle
   drwxr-xr-x 3 root   root  4096 Jul 30 14:46 /dbdata
   drwxr-xr-x 3 root   root  4096 Jul 29 14:13 /dbbackup
   drwxrwxrwx 4 root  root 4096 Jul 30 14:46 /var/log/tbi
   ```

2. En la salida de cada comando, busque un punto al final de los permisos. En el ejemplo siguiente, observe el "*.*" después de *drxwr-xr-x*.

   ```
   # ls -ld /Oracle

   drxwr-xr-x.  5  oracle oinstall  4096  Jul  30  18:27  /Oracle
   ```

3. Si ninguno de los directorios contiene un punto después de la declaración de los permisos, el control de acceso ya está desactivado y puede pasar a la siguiente tarea.

   Si el control de acceso está activado en un directorio, como usuario root del sistema, ejecute el siguiente comando para ese directorio:

   ```
   # setfattr -h -x security.selinux directory_name
   ```

   Por ejemplo:

   ```
   # setfattr -h -x security.selinux /Oracle
   ```

2.3.4. Configuración del proxy de red

Puede configurar el servidor de STA para que se conecte con la red directamente o a través de un servidor proxy.

1. En el menú **System** (Sistema) del escritorio de Linux, seleccione **Preferences** (Preferencias) y, a continuación, seleccione **Network Proxy** (Proxy de red).
2. En el cuadro de diálogo Network Proxy Preferences (Preferencias de proxy de red), especifique la configuración del proxy según los requisitos del sitio.
3. Haga clic en **Close** (Cerrar).

2.3.5. Configuración correcta de Yum (opcional)

Use este procedimiento solo si usará Yum (Yellowdog Updater, Modified) para instalar los paquetes de software de RPM (Red Hat Package Manager) Linux requeridos. (Consulte cuáles son los paquetes requeridos en Sección 2.3.6, “Instalación de los paquetes de Linux requeridos”).

Hay una variedad de métodos para instalar los paquetes de RPM, entre ellos Yum. El uso de Yum es opcional pero recomendado, ya que simplifica mucho el proceso de instalación de los paquetes. Yum busca automáticamente en los repositorios de paquetes de RPM las versiones más recientes de los paquetes y sus dependencias. Este procedimiento garantiza que Yum esté bien configurado en el servidor de STA.

Nota:

Los siguientes ejemplos de comandos usan el repositorio de Yum para Oracle Linux. En los comandos, la ”l” de ”ol6” es una "L" minúscula.

1. Haga ping con el servidor de Yum público de Oracle para asegurarse de que la conexión de red esté funcionando.

```
# ping public-yum.oracle.com
```

2. Cambie al directorio del repositorio de Yum y determine el nombre de archivo del repositorio de Yum.

```
# cd /etc/yum.repos.d
# ls
public-yum-ol6.repo
```

3. Quite el archivo existente del repositorio de Yum.

```
# rm public-yum-ol6.repo
```

4. Descargue el archivo más reciente del repositorio de Yum desde el sitio web de Yum.

```
# wget http://public-yum.oracle.com/public-yum-ol6.repo
```

Nota:

Las ejecuciones subsiguientes de este comando copiarán un nuevo archivo de repositorio en la carpeta *`yum.repos.d`* con una nueva extensión (por ejemplo, *`public-yum-ol6.repo.1`*). Sin embargo, Yum siempre usa el archivo de repositorio que no tiene extensión.

5. Abra el archivo de repositorio con un editor de texto.

```
# vi public-yum-ol6.repo
```

6. En el archivo, localice la entrada que coincida con la versión de Linux que utiliza y actívela mediante la configuración *enabled=1*. Desactive todas las demás entradas; para ello, defina *enabled=0*.

   Por ejemplo:

   ```
   [Linux_Version]
   name=Oracle Linux $releasever Update x installation media copy ($basearch)
   baseurl=http://public-yum.oracle.com/repo/OracleLinux/OL6/x/base/$basearch/
   gpgkey=http://public-yum.oracle.com/RPM-GPG-KEY-oracle-ol6
   gpgcheck=1
   enabled=1
   ```

7. Guarde el archivo y ciérrelo.

2.3.6. Instalación de los paquetes de Linux requeridos

Para la instalación y el funcionamiento de STA se necesitan paquetes de RPM adicionales. El instalador de STA comprueba la presencia de los siguientes paquetes y, si no los encuentra, se genera un error en la instalación de STA.

Nota:

Los nombres de los paquetes de RPM diferencian mayúsculas de minúsculas.

• *binutils*	• *gcc-c++*	• *libstdc++*
• *compat-libcap1*	• *glibc*	• *libstdc++-devel*
• *compat-libstdc++-33.i686*	• *glibc-devel*	• *net-snmp-utils*
• *cronie*	• *libaio*	• *rpm-build*
• *expect*	• *libaio-devel*	• *sysstat*
• *gcc*	• *libgcc*	• *xorg-x11-utils*

Puede usar una variedad de métodos para instalar los paquetes de RPM requeridos. Este procedimiento describe cómo usar Yum.

El comando de instalación de paquetes de Yum busca la versión más actual del paquete para la versión de Linux que se está usando y, a continuación, instala el paquete y sus dependencias. En función de la instalación de Linux, tal vez algunos de estos paquetes ya estén instalados. Si alguno de los paquetes ya está instalado y la versión instalada es la más reciente, el sistema se lo notifica.

1. Abra una sesión de terminal en el servidor de STA.
2. Siga estos pasos:
   - Si puede conectarse con el servidor de Yum público de Oracle (consulte Sección 2.3.5, “Configuración correcta de Yum (opcional)”), use uno de los siguientes métodos para instalar paquetes:
     - Instale los paquetes de a uno. El paquete especificado se descarga y se comprueba; se debe responder a todos los pedidos de información o acción que aparezcan.

```
# yum install package_name
```

- Instale todos los paquetes simultáneamente sin que se le solicite información ni realizar ninguna acción. La opción *–y* responde "yes" (sí) automáticamente a todas las solicitudes de la instalación.

```
# yum –y install binutils compat-libcap1 compat-libstdc++-33.i686 cronie
 expect gcc gcc-c++ glibc glibc-devel libaio libaio-devel libgcc libstdc++
 libstdc++-devel net-snmp-utils rpm-build sysstat xorg-x11-utils
```

- Si el firewall de la red prohíbe el acceso a redes externas, puede usar Yum para instalar desde los medios físicos de Linux paquetes que estén disponibles localmente. Por ejemplo:

```
# cd /mnt/install_media_mount_location/packages
# yum install ./package_name
```

2.3.7. Configuración correcta de SSH

Use este procedimiento para asegurarse de que SSH (shell seguro) esté bien configurado en el servidor de STA. Esto acelerará las transferencias de las copias de seguridad de la base de datos de STA a un host remoto.

1. Abra el archivo de configuración de SSH con un editor de texto.

```
# vi /etc/ssh/sshd_config
```

2. Busque las entradas *AddressFamily* y *UseDNS*. Modifíquelas para que *no* estén precedidas por el carácter de comentario y sus valores sean los siguientes:

```
AddressFamily inet
UseDNS no
```

3. Guarde el archivo y ciérrelo.
4. Reinicie el daemon de sshd.

```
# service sshd restart
```

2.3.8. Configuración correcta de DNS

Use este procedimiento para asegurarse de que la dirección IP del servidor de STA esté asignada al nombre de host correcto.

1. Abra el archivo de hosts con un editor de texto.

```
# vi /etc/hosts
```

2. Al final del archivo, agregue la dirección IP del servidor de STA, seguida por una tabulación y el nombre de host del servidor de STA. Por ejemplo:

```
127.0.0.1    localhost localhost.localdomain localhost4...
::1          localhost localhost.localdomain localhost6...
192.0.2.20    sta_server
```

3. Guarde el archivo y ciérrelo. No es necesario reiniciar el servidor de STA para que la nueva configuración entre en efecto.

2.3.9. Desactivación de servicios de nombres

Los servicios de nombres, por ejemplo LDAP, pueden entrar en conflicto con la instalación de STA. Use este procedimiento para desactivar estos servicios transitoriamente.

1. Abra el archivo de configuración Name Service Switch (Cambio de servicio de nombres) con un editor de texto.

```
# vi /etc/nsswitch.conf
```

2. Desactive las entradas de servicios de nombres que haya en el archivo. Por ejemplo, para desactivar LDAP, convierta en comentario "ldap" en las siguientes líneas como se muestra:

```
passwd:     files #ldap nis nisplus
shadow:     files #ldap nis nisplus
group:      files #ldap nis nisplus
```

3. Guarde el archivo y ciérrelo. No es necesario reiniciar el servidor de STA para que la nueva configuración entre en efecto. Después de instalar STA, puede modificar el archivo nsswitch.conf para volver a activar los servicios de nombres.

2.3.10. Funcionalidad de explorador local (opcional)

Para configurar y administrar STA de manera local en el servidor de STA, asegúrese de tener instaladas las versiones y los complementos de explorador mínimos admitidos (consulte la *Guía de requisitos de STA*).

Nota:

Oracle no recomienda el acceso local a la aplicación de STA porque esto ocasiona una degradación del rendimiento del servidor.

3

Instalación de STA

En este capítulo, se asume que está realizando una nueva instalación de STA en este servidor.

- Si está actualizando STA desde una versión previa, consulte el Capítulo 8, *Actualización a STA 2.1.0*. Oracle recomienda instalar o actualizar con la versión más reciente de STA.
- Si necesita reinstalar STA o reparar una instalación actual, consulte el Capítulo 9, *Desinstalación y restauración de STA*

Nota:

Oracle proporciona soporte solo si STA está instalado en un servidor dedicado (llamado *servidor de STA* en toda esta guía).

En este capítulo, se incluyen los siguientes temas:

- Usuarios, grupos y ubicaciones usados por el instalador de STA
- Cuentas y puertos configurados durante la instalación de STA
- Logs de instalación y desinstalación de STA
- Modos del instalador de STA
- Tareas de instalación de STA

El Apéndice C, *Hojas de trabajo de instalación y actualización* incluye hojas de trabajo que se pueden usar para organizar las actividades de la instalación y registrar los valores de configuración.

3.1. Usuarios, grupos y ubicaciones usados por el instalador de STA

En esta sección, se describen los conceptos y los términos clave utilizados en el proceso de instalación de STA.

Grupo de instalación de Oracle
Grupo de Linux utilizado para instalar y actualizar los productos de Oracle en el servidor de STA. Oracle recomienda crear un grupo dedicado independiente con este fin.

Para realizar la instalación de STA, debe iniciar sesión como un usuario que sea miembro de este grupo. No puede instalar STA como usuario `root` de Linux ni ningún otro usuario que tenga privilegios de superusuario.

Para las instrucciones y los ejemplos de esta guía, se usa el nombre *oinstall* para este grupo. Reemplace este nombre por el que haya elegido si es diferente.

Usuario de instalación de Oracle
Usuario de Linux para instalar y actualizar productos de Oracle en el servidor de STA. Puede ser cualquier usuario que pertenezca al grupo de instalación de Oracle.

Para las instrucciones y los ejemplos de esta guía, se usa el nombre *oracle* para este usuario. Reemplace este nombre por el que haya elegido si es diferente.

Ubicación de inventario central de Oracle
Directorio usado para llevar un control de la información sobre los productos de Oracle instalados en el servidor de STA. Los logs del instalador y del desinstalador de STA se guardan en el subdirectorio *logs* dentro de esta ubicación.

El usuario de instalación de Oracle debe ser el propietario de este directorio y tener permisos completos para él. Para asegurarse de que los demás usuarios del grupo de instalación de Oracle tengan el acceso adecuado para poder instalar productos de Oracle, no se debe usar el directorio raíz del usuario de instalación de Oracle.

Esta ubicación debe ser independiente de los demás directorios que se describen en esta sección. Para las instrucciones y los ejemplos de esta guía, se usa */opt/oracle/oraInventory* para esta ubicación. Reemplace el directorio por el que haya elegido si es diferente.

Nota:

Oracle recomienda registrar esta ubicación después de que haya finalizado la instalación de STA para que todos los instaladores de Oracle usen la misma ubicación de inventario central en este servidor. Consulte Sección 3.6.7, “Registro de la ubicación del inventario central de Oracle” para obtener detalles.

Ubicación de directorio raíz de almacenamiento de Oracle
Directorio en el que se instalan STA y el software asociado de Oracle. STA se instala automáticamente en el subdirectorio *StorageTek_Tape_Analytics* dentro de esta ubicación. Consulte Directorio raíz de STA.

Si este directorio ya existe, el usuario de instalación de Oracle debe tener permisos completos para él. Si el directorio no existe, el instalador de STA lo crea automáticamente en el caso de que el usuario de instalación de Oracle tenga permisos completos para el directorio principal.

Nota:

Si había una versión anterior de STA instalada en este servidor, el directorio tal vez ya exista. De ser así, debe verificar que el propietario sea el grupo de instalación de Oracle, no *root*.

Esta ubicación debe ser independiente de los demás directorios que se describen en esta sección. Para las instrucciones y los ejemplos de esta guía, se usa */Oracle* para esta ubicación. Reemplace el directorio por el que haya elegido si es diferente.

Directorio raíz de STA
Directorio en el que se instala todo el software de STA. El directorio recibe el nombre *StorageTek_Tape_Analytics*, y el instalador de STA lo crea automáticamente dentro de Ubicación de directorio raíz de almacenamiento de Oracle.

En las instrucciones y los ejemplos de esta guía, se usa */Oracle/StorageTek_Tape_Analytics* para esta ubicación.

Ubicación de instalador de STA
Directorio en el que se descarga el instalador de STA.

Esta ubicación debe ser independiente de los demás directorios que se describen en esta sección. Para las instrucciones y los ejemplos de esta guía, se usa */Installers* para esta ubicación. Reemplace el directorio por el que haya elegido si es diferente.

Ubicación de trabajo de instalador de STA
De forma predeterminada, el instalador de STA se descomprime en el directorio */tmp* y consume aproximadamente 4 GB de espacio. Puede especificar otra ubicación de trabajo; para ello, ejecute el instalador de STA con la siguiente opción: *–J–Djava.io.tmpdir=working_directory*.

working_directory debe ser una ruta de acceso absoluta. Por ejemplo:

```
$ ./sta_installer_linux64.bin –J–Djava.io.tmpdir=/Oracle/tmp
```

Consulte Apéndice B, *Instalador y desinstalador en modo silencioso de STA* para obtener detalles sobre el uso de esta opción.

Ubicación de logs de STA
Ubicación de los logs de STA y MySQL. El contenido tiende a crecer y se administra mediante la rotación de logs. La ubicación predeterminada es */var/log/tbi*, pero puede cambiarla en cualquier momento después de la instalación de STA. Consulte Sección 3.6.6, “Reubicación del directorio de logs de STA (opcional)” para obtener instrucciones.

Consulte Sección 2.1.2, “Revisión de la disposición del sistema de archivos de STA” para conocer los requisitos de espacio.

3.2. Requisitos del nombre de usuario y la contraseña

Los requisitos para los nombres de usuario son los siguientes:

- Debe tener de 1 a 16 caracteres.
- Todos los nombres de usuario deben ser únicos.

Los requisitos para las contraseñas son los siguientes:

- Debe tener de 8 a 31 caracteres.
- Debe incluir al menos un número y una letra mayúscula.
- No debe tener espacios.

- No debe incluir ninguno de los siguientes caracteres especiales:

  ```
  & ' ( ) < > ? { } *  / ' "
  ```

3.3. Cuentas y puertos configurados durante la instalación de STA

El instalador de STA configura las cuentas de usuario y los números de puerto en función de las especificaciones que usted proporcione.

3.3.1. Cuentas de usuario para administrar STA

Las siguientes cuentas requeridas se crean durante la instalación de STA. Estas cuentas son específicas para STA y *no* son nombres de usuario de Linux.

- Cuentas de WebLogic
- Cuentas de base de datos de STA

3.3.1.1. Cuentas de WebLogic

Las siguientes cuentas de WebLogic se usan para iniciar sesión en la consola de administración de WebLogic o la aplicación de STA.

Administración de WebLogic
Se usa para iniciar sesión en la consola de administración de WebLogic para hacer cambios en el entorno de WebLogic (por ejemplo, para conectar WebLogic con un servidor de LDAP o RACF).

> **Precaución:**
>
> El nombre de usuario y la contraseña de esta cuenta no se pueden recuperar. Si se pierden estas credenciales, se debe reinstalar STA.

Administrador de STA
Se usa para iniciar sesión en la aplicación de STA con privilegios de acceso completo.

Una vez que haya finalizado la instalación de STA, puede usar la aplicación de STA para crear cuentas de usuario adicionales con roles asignables. Consulte la *Guía del usuario de STA* para obtener detalles.

3.3.1.2. Cuentas de base de datos de STA

Las siguientes cuentas de la base de datos de STA son cuentas de MySQL que STA utiliza para acceder a la base de datos de STA y administrarla.

Usuario root de la base de datos de STA
Es propietario de la base de datos de MySQL y se usa para crear la instalación de la base de datos root. El nombre de usuario predefinido es `root` y no se puede cambiar.

Precaución:

La contraseña de esta cuenta no se puede recuperar.

Usuario de aplicaciones de la base de datos de STA
Nombre de usuario de MySQL definido por el usuario (por ejemplo, *stadb*) que STA usa para conectarse a la base de datos. Se necesita para los privilegios de creación, actualización, supresión y lectura en las tablas de datos.

Usuario de informes de la base de datos de STA
Nombre de usuario de MySQL definido por el usuario (por ejemplo, *starpt*) que pueden usar las aplicaciones que no son de STA y las aplicaciones de terceros para conectarse a la base de datos. Tiene acceso de solo lectura a ciertas tablas de la base de datos.

Usuario administrador de la base de datos de STA
Nombre de usuario de MySQL definido por el usuario (por ejemplo, *stadba*) que usan las utilidades de administración y supervisión de STA para conectarse a la base de datos, principalmente para configurar y ejecutar copias de seguridad programadas. Tiene todos los privilegios del DBA, excepto por la "opción de otorgar" para todas las tablas de la base de datos.

3.3.2. Puertos utilizados por STA

STA usa los siguientes puertos para recuperar y recibir datos. Son puertos dedicados y deben estar siempre disponibles para STA. El instalador de STA verifica que los puertos no estén siendo utilizados para otro fin en la red.

Precaución:

Después de haber configurado estos puertos durante la instalación de STA, no se pueden cambiar sin desinstalar y volver a instalar STA.

3.3.2.1. Puertos externos no configurables

Los puertos que se describen en la Tabla 3.1, “Puertos externos no configurables” son puertos externos que se usan para la comunicación entre el servidor de STA y las demás entidades de la red. Los valores de los puertos son fijos y no se pueden cambiar durante la instalación de STA.

Configuración del firewall o el enrutador: debe ser accesible entre el servidor de STA y el servidor de copia de seguridad (para SSH) y entre el servidor de STA y las bibliotecas supervisadas (para SNMP y SNMPTRAP).

Tabla 3.1. Puertos externos no configurables

Puerto	Protocolo	Descripción/Finalidad
22	SSH	Shell seguro. Copia de seguridad de la base de datos de STA; inicio de sesión en biblioteca.
161	SNMP	Protocolo simple de administración de redes (SNMP). Para transmisión de solicitudes de SNMP.

Puerto	Protocolo	Descripción/Finalidad
162	SNMPTRAP	Para recepción de notificaciones (capturas) de SNMP.

3.3.2.2. Puertos externos configurables

Los puertos que se describen en la Tabla 3.2, “Puertos externos configurables” son puertos externos que se usan para la comunicación entre el servidor de STA y las demás entidades de la red. Estos puertos son el equivalente configurable de los puertos estándares 80 y 8080 (HTTP) y 443 (HTTPS), y deben ser únicos con respecto a otros puertos HTTP y HTTPS de la red. Póngase en contacto con el administrador de la red para que lo ayude a elegir los valores.

Configuración del firewall o el enrutador: debe ser accesible entre el servidor de STA y el cliente que ejecuta la GUI de STA.

Tabla 3.2. Puertos externos configurables

Puerto predeterminado	Protocolo	Descripción/Finalidad
7019	HTTP	Acceso a la consola de administración de WebLogic, no seguro
7020	HTTPS	Acceso a la consola de administración de WebLogic, seguro
7021	HTTP	Servidor gestionado staUi. Acceso a la GUI de STA, no seguro.
7022	HTTPS	Servidor gestionado staUi. Acceso a la GUI de STA, seguro.

3.3.2.3. Puertos internos configurables

Los puertos que se describen en la Tabla 3.3, “Puertos internos configurables” se usan para las comunicaciones internas de STA. Estos valores de puerto deben ser únicos.

Configuración del firewall o el enrutador: no aplicable

Tabla 3.3. Puertos internos configurables

Puerto predeterminado	Protocolo	Descripción/Finalidad
7023	HTTP	Servidor gestionado staEngine. Aspectos internos básicos de STA, no seguro.
7024	HTTPS	Servidor gestionado staEngine. Aspectos internos básicos de STA, seguro.
7025	HTTP	Servidor gestionado staAdapter. Comunicación de SNMP, no seguro.
7026	HTTPS	Servidor gestionado staAdapter. Comunicación de SNMP, seguro.

3.4. Logs de instalación y desinstalación de STA

Puede usar los logs de instalación y desinstalación de STA para ayudar a resolver problemas. La mayoría de los nombres de los archivos log incluye un registro de hora para identificar la

instancia de instalación o desinstalación. El registro de hora corresponde a la fecha y la hora de inicio de la instalación o la desinstalación.

En particular, los siguientes logs proporcionan información valiosa si se produce algún error durante la instalación o la desinstalación. Consulte */STA_logs*/install para obtener detalles sobre su ubicación.

- *installtimestamp.log*
- *sta_installtimestamp.log*
- *deinstalltimestamp.log*
- *sta_deinstalltimestamp.log*

3.4.1. Ubicaciones de archivos log

La ubicación de los logs de instalación y desinstalación de STA varía en función del estado de la instalación o la desinstalación. Los logs se encuentran en los siguientes directorios. Consulte Sección 2.1.2, “Revisión de la disposición del sistema de archivos de STA” para obtener detalles sobre estos directorios.

/tmp/OraInstall*timestamp*
Este directorio incluye logs de instalaciones o desinstalaciones en curso. A continuación, se presenta un ejemplo de lista de logs que puede haber en este directorio.

```
install2014-09-24_04-14-04PM.log
installProfile2014-09-24_04-14-04PM.log
launcher2014-09-24_04-14-04PM.log
```

/*Oracle_storage_home*/oraInventory/logs
Donde *Oracle_storage_home* es la ubicación del directorio raíz de almacenamiento de Oracle definida durante la instalación de STA.

Este directorio incluye logs de instalaciones y desinstalaciones que finalizaron correctamente. Algunos logs, por ejemplo, logs de parches o errores, se incluyen solo si corresponde.

A continuación, se presenta un ejemplo de lista de logs que puede haber en este directorio.

```
2014-09-24_02-57-41PM.log
install2014-09-24_02-57-41PM.log
install2014-09-24_02-57-41PM.out
installActions2014-09-24_02-57-41PM.log
installProfile2014-09-24_02-57-41PM.log
installSummary2014-09-24_02-57-41PM.txt
launcher2014-09-24_02-57-41PM.log1
OPatch2014-09-24_02-58-47-PM.log
oraInstall2014-09-24_02-57-41PM.err
```

```
oraInstall2014-09-24_02-57-41PM.out
```

/*STA_logs*/install
De forma predeterminada, *`STA_logs`* se encuentra en */var/log/tbi*. De forma opcional, puede reubicar este directorio en la ubicación que desee en cualquier momento después de la instalación de STA. Consulte Sección 3.6.6, “Reubicación del directorio de logs de STA (opcional)” para obtener instrucciones.

Este directorio incluye logs de instalaciones y desinstalaciones que finalizaron correctamente o presentaron errores. Incluye logs relacionados con la instalación del servidor de WebLogic y la base de datos de MySQL, así como logs de la instalación y la configuración de la aplicación de STA.

A continuación, se presenta un ejemplo de lista de logs que puede haber en este directorio.

```
dbinstall.log
dbinstall.mysqld.err
dbinstall.stadb-slow.log
install2014-09-24_02-52-09PM.log
install_weblogic.log
sta_install2014-09-24_02-53-22PM.log
```

3.5. Modos del instalador de STA

Puede usar cualquiera de los siguientes modos para instalar STA:

Modo gráfico
Es el modo de instalación recomendado. Este modo proporciona una interfaz gráfica de usuario para instalar STA y requiere una visualización X11. Consulte Apéndice A, *Referencia de la pantalla del instalador y del desinstalador gráficos de STA* para obtener detalles.

Modo silencioso
Este modo le permite omitir la interfaz gráfica de usuario y proporcionar las opciones de instalación en un archivo de propiedades XML llamado *archivo de respuesta*. Consulte Apéndice B, *Instalador y desinstalador en modo silencioso de STA* para obtener detalles.

Este modo es útil para instalaciones desatendidas y para instalar STA en varios equipos. Al usar un archivo de respuesta, puede proporcionar un único conjunto de parámetros y automatizar la instalación. Puede ejecutar el instalador en el modo silencioso desde un script o desde la línea de comandos de Linux.

3.6. Tareas de instalación de STA

Para instalar STA, realice todas las tareas enumeradas a continuación en el orden indicado.

- Sección 3.6.1, “Identificación o creación de la información requerida para la instalación”
- Sección 3.6.2, “Verificación de los requisitos de la instalación”

- Sección 3.6.3, “Descarga de STA”
- Sección 3.6.4, “Instalación de STA”
- Sección 3.6.5, “Verificación de la instalación”
- Sección 3.6.6, “Reubicación del directorio de logs de STA (opcional)”
- Sección 3.6.7, “Registro de la ubicación del inventario central de Oracle”

3.6.1. Identificación o creación de la información requerida para la instalación

Use este procedimiento para identificar y, si es necesario, crear usuarios y ubicaciones para ejecutar el instalador de STA. Puede usar la Tabla C.2, “Hoja de trabajo de ubicaciones y usuarios de instalación” para registrar esta información. Consulte Sección 3.1, “Usuarios, grupos y ubicaciones usados por el instalador de STA” para obtener detalles sobre estos elementos.

1. Inicie sesión como usuario root de Linux.
2. Determine si hay un archivo indicador del inventario central de Oracle, */etc/oraInst.loc*, en el servidor de STA. El archivo existe si el inventario central de Oracle se registró previamente. Consulte Ubicación de inventario central de Oracle para obtener detalles.
   - Si el archivo existe, registre el contenido. Por ejemplo:

     ```
     # cat /etc/oraInst.loc
     inventory_loc=/opt/oracle/oraInventory
     inst_group=oinstall
     ```

     La entrada *inventory_loc* identifica la ubicación del inventario central de Oracle, mientras que la entrada *inst_group* identifica el grupo de instalación de Oracle.
   - Si el archivo no existe, continúe con el paso 3 para crear los usuarios y las ubicaciones necesarios. Por ejemplo:

     ```
     # cat /etc/oraInst.loc
     cat: /etc/oraInst.loc: No such file or directory
     ```

3. Si en el paso 2 no encontró un archivo indicador del inventario central de Oracle, cree el grupo de instalación de Oracle. Consulte Grupo de instalación de Oracle para obtener detalles. Por ejemplo:

   ```
   # groupadd oinstall
   ```

4. Obtenga el nombre de usuario y la contraseña de un usuario de instalación de Oracle, o cree uno nuevo en caso de ser necesario. Este usuario debe pertenecer al grupo de instalación de Oracle. Consulte Usuario de instalación de Oracle para obtener detalles. Por ejemplo:

```
# useradd -g oinstall -d /home/oracle oracle
# passwd oracle
Changing password for user oracle.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

5. Si en el paso 2 no encontró un archivo indicador del inventario central de Oracle, cree la ubicación del inventario central de Oracle. El usuario de instalación de Oracle debe ser el propietario de este directorio. Consulte Ubicación de inventario central de Oracle para obtener detalles. Por ejemplo:

```
# mkdir /opt/oracle/oraInventory
# chown oracle /opt/oracle/oraInventory
# ls -la /opt/oracle/oraInventory
total 8
drwxr-xr-x 2 oracle oinstall 4096 Feb 11 10:49 .
drwxr-xr-x 3 root   root     4096 Feb 11 10:49 ..
```

6. Localice la ubicación del directorio raíz de almacenamiento de Oracle o cree el directorio si todavía no existe. El usuario de instalación de Oracle debe ser el propietario de este directorio. Consulte Ubicación de directorio raíz de almacenamiento de Oracle para obtener detalles. Por ejemplo:

```
# mkdir /Oracle
# chown oracle /Oracle
# ls -la /Oracle
total 8
drwxr-xr-x 2 oracle oinstall 4096 Feb 11 10:49 .
drwxr-xr-x 3 root   root     4096 Feb 11 10:49 ..
```

7. Localice la ubicación del instalador de STA o cree el directorio si todavía no existe. Consulte Ubicación de instalador de STA para obtener detalles. Por ejemplo:

```
# mkdir /Installers
```

8. Obtenga la contraseña del usuario root de Linux. El instalador de STA requiere acceso root para realizar ciertas tareas y le solicitará la contraseña.
9. Elija los nombres de usuario para las cuentas de administrador de WebLogic, de administrador de STA y de MySQL que se crean durante la instalación. Consulte Sección 3.3.1, “Cuentas de usuario para administrar STA” para obtener detalles.
10. Elija los números de puerto para los puertos configurables internos y externos requeridos para las operaciones de STA. Asegúrese de que los puertos externos estén abiertos en las redes requeridas. Consulte Sección 3.3.2, “Puertos utilizados por STA” para obtener detalles.

11. Obtenga el nombre de dominio del sitio para configurar el agente de diagnóstico remoto (RDA) de Oracle. Consulte la *Guía del usuario de STA* para obtener detalles.

3.6.2. Verificación de los requisitos de la instalación

Use este procedimiento para verificar los requisitos antes de ejecutar el instalador de STA. Este procedimiento es opcional, pero si no se cumple alguno de los requisitos, la instalación de STA fallará. Consulte la *Guía de requisitos de STA* para obtener una lista completa de requisitos de instalación.

Todos estos pasos se realizan en el servidor de STA. Si necesita ayuda, póngase en contacto con el administrador de Linux.

Nota:

Para la instalación de STA, se asume que se instaló Linux de 64 bits con los paquetes RPM de Linux especificados en el Capítulo 2, *Instalación de Linux*. Si no se instaló alguno de los paquetes requeridos, la instalación de STA fallará. Consulte los siguientes documentos para obtener detalles:

- Consulte la *Guía de requisitos de STA* para conocer las versiones compatibles de Linux.
- Consulte Sección 2.3.6, “Instalación de los paquetes de Linux requeridos” [36] para obtener una lista de los paquetes requeridos.

Precaución:

Antes de elegir eliminar o reemplazar de manera permanente el software existente, haga una copia de seguridad de los archivos según sea necesario.

1. Verifique que STA no esté instalado en el servidor. El instalador de STA se usa solo para instalaciones nuevas. Consulte otras instrucciones en las siguientes secciones, según corresponda:
   - Si desea actualizar STA a partir de una versión previa, consulte el Capítulo 8, *Actualización a STA 2.1.0*.
   - Si necesita reinstalar STA o reparar una instalación actual, consulte Capítulo 9, *Desinstalación y restauración de STA*.

   En el siguiente ejemplo, se muestra que STA no está instalado.

```
$ ls /etc/init.d/sta*
ls: cannot access /etc/init.d/sta*: No such file or directory$ ls /usr/bin/STA
ls: cannot access /usr/bin/STA: No such file or directory
$
```

2. Verifique que MySQL no esté instalado en el servidor de STA. Si MySQL está instalado, el instalador lo elimina y lo vuelve a instalar, y todas las bases de datos existentes de MySQL se suprimen.
3. Verifique que el directorio */tmp* tenga por lo menos 4 GB de espacio libre. Es la ubicación de trabajo predeterminada del instalador de STA.

```
$ df /tmp
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/mapper/vg_sta_server-lv_root
                      51606140  42896756   6087944  88% /
```

Nota:

De forma opcional, puede especificar otro directorio de trabajo al iniciar el instalador de STA. Consulte Ubicación de trabajo de instalador de STA para obtener detalles.

4. Verifique que SELinux esté desactivado. Si siguió las instrucciones que se detallan en "Tareas posteriores a la instalación", SELinux ya debería estar desactivado. Consulte Sección 2.3.1, “Desactivación de SELinux” [32] para obtener detalles.

```
$ sestatus
SELinux status:         disabled
```

5. Verifique que el firewall de Linux (IPTables) esté detenido. Si siguió las instrucciones que se detallan en "Tareas posteriores a la instalación", IPTables ya debería estar detenido. Consulte Sección 2.3.2, “Desactivación del firewall de Linux” [33] para obtener detalles.

```
$ service iptables status
iptables: Firewall is not running.
```

Nota:

Si el sitio requiere que el servicio IPTables se esté ejecutando, puede iniciar el servicio después de haber instalado STA, configurado las bibliotecas y confirmado que STA esté supervisando las bibliotecas. Después de iniciar IPTables, debe reconfirmar que STA esté supervisando las bibliotecas.

6. Detenga los servicios de SNMP y desconfigúrelos.

   Para evitar colisiones en los puertos de la red y otros problemas, el servidor de STA no debe estar ejecutando los servicios de SNMP. El instalador de STA se cierra si se produce alguna de las siguientes situaciones:

   - Los servicios de daemon snmpd y snmptrapd se están ejecutando.
   - Los puertos 161 (SNMP) y 162 (SNMPTRAP) de UDP no están disponibles.

   Realice los siguientes pasos según sea necesario.

   a. Muestre el estado actual de los servicios *snmpd* y *snmptrapd* de SNMP.

```
# service snmpd status
snmpd is stopped
# service snmptrapd status
snmptrapd is stopped
```

b. Si es necesario, detenga los servicios de SNMP de inmediato.

```
# service snmpd stop
# service snmptrapd stop
```

> **Nota:**
>
> Si aparece un error que indica "FAILED" (Error) con alguno de estos comandos, significa que los servicios tal vez ya estén detenidos.

c. Escriba lo siguiente para desactivar los servicios de SNMP en el archivo de configuración de servicios de Linux para que no se inicien automáticamente al reiniciar Linux:

```
# chkconfig snmpd off
# chkconfig --list snmpd
snmpd           0:off   1:off   2:off   3:off   4:off   5:off   6:off
# chkconfig snmptrapd off
# chkconfig --list snmptrapd
snmptrapd       0:off   1:off   2:off   3:off   4:off   5:off   6:off
```

7. Revise y verifique los requisitos aplicables específicos del modo, de la siguiente manera:
   - Para el instalador gráfico de STA, consulte Sección A.1, “Requisitos de visualización para el modo gráfico”.
   - Para el instalador de STA en modo silencioso, consulte Sección B.1.1, “Requisitos del modo silencioso ”.

3.6.3. Descarga de STA

La descarga del instalador de STA incluye los siguientes archivos. *`version`* es el número de versión de la instalación de STA.

- *`sta_install_version_linux64.bin`*: requerido para todas las instalaciones.
- *`sta_install_version_linux64-2.zip`*: requerido para todas las instalaciones.
- *`silentInstallUtility_version.jar`*: utilidad de generación de archivo de respuesta. Requerido solo si se usarán el instalador o el desinstalador de STA en modo silencioso. Consulte el Apéndice B, *Instalador y desinstalador en modo silencioso de STA* para obtener detalles.

1. En una ventana del explorador, acceda al sitio web de Oracle Software Delivery Cloud en la siguiente dirección URL:

   `http://edelivery.oracle.com/`

2. Haga clic en **Sign In/Register** (Conexión/Registro).
3. Escriba el ID de usuario y la contraseña proporcionados por el soporte de Oracle o cree una nueva cuenta.

4. En la pantalla Terms & Restrictions (Condiciones y restricciones), seleccione las casillas de verificación para indicar que acepta el acuerdo de licencia y las restricciones de exportación y, a continuación, haga clic en **Continue** (Continuar).
5. Realice los siguientes pasos en la pantalla Media Pack Search (Búsqueda de paquetes de medios):
   a. En el menú **Select a Product Pack** (Seleccionar un paquete de productos), seleccione Oracle StorageTek Products (Productos StorageTek de Oracle).
   b. En el menú **Platform** (Plataforma), seleccione Linux x86-64.
   c. Haga clic en **Go** (Ir).
6. En la tabla Results (Resultados), seleccione **Oracle StorageTek Tape Analytics 2.1.0** y haga clic en **Continue** (Continuar).
7. Haga clic en **Download** (Descargar) para cada uno de los archivos zip del paquete de medios y guárdelos en una ubicación que tenga al menos 4 GB de espacio libre.
8. Use una herramienta de descompresión para extraer el contenido de los archivos zip en la ubicación del instalador de STA que seleccionó en Sección 3.6.1, “Identificación o creación de la información requerida para la instalación” (por ejemplo, */Installers*).
9. Asegúrese de que el usuario de instalación de Oracle tenga permisos de ejecución para el archivo *sta_install_version_linux64.bin* y acceso de lectura para el archivo *sta_install_version_linux64-2.zip*. Por ejemplo:

```
# cd /Installers
# ls -la
-rw-r--r--   1 oracle oinstall       5964 Oct 23 16:14 silentInstallUtility.jar
-rw-r--r--   1 oracle oinstall 1275158996 Oct 23 13:35 sta_install_2.1.0.64.124_linux64-2.zip
-rw-r--r--   1 oracle oinstall 1599220560 Oct 23 13:01 sta_install_2.1.0.64.124_linux64.bin

# chmod u+x  sta_install*.bin
# chmod u+r sta_install*.zip
# ls -la
-rw-r--r--   1 oracle oinstall       5964 Oct 23 16:14 silentInstallUtility.jar
-rw-r--r--   1 oracle oinstall 1275158996 Oct 23 13:35 sta_install_2.1.0.64.124_linux64-2.zip
-rwxr--r--   1 oracle oinstall 1599220560 Oct 23 13:01 sta_install_2.1.0.64.124_linux64.bin
```

10. Lea *Notas de la versión de STA*, que se incluye en el paquete de descarga del instalador.

3.6.4. Instalación de STA

Use este procedimiento para ejecutar el instalador de STA. Para instalar STA, puede usar el modo gráfico o el modo silencioso. Consulte Sección 3.5, “Modos del instalador de STA” para obtener detalles.

1. En una ventana de terminal, establezca conexión con el servidor de STA e inicie sesión como usuario de instalación de Oracle. Consulte Usuario de instalación de Oracle para obtener detalles.

2. Cambie a la ubicación del instalador de STA. Consulte Ubicación de instalador de STA para obtener detalles. Por ejemplo:

```
$ cd /Installers
```

3. Inicie el instalador de STA con uno de los siguientes comandos:
   - Para usar el instalador gráfico de STA:

     ```
     $ ./sta_install_version_linux64.bin
     ```

     Donde *version* es la versión del instalador de STA que descargó. Por ejemplo:

     ```
     $ ./sta_install_2.1.0.64.124_linux64.bin
     ```

     Para este modo, se requiere una visualización X11. Consulte el Apéndice A, *Referencia de la pantalla del instalador y del desinstalador gráficos de STA* para obtener instrucciones.
   - Para usar el instalador silencioso de STA:

     ```
     $ ../sta_install_version_linux64.bin –silent  –responseFile response_file
     ```

     Donde:
     - *version* es la versión del instalador de STA que descargó.
     - *response_file* es la ruta de acceso absoluta del archivo de respuesta creado previamente.

     Por ejemplo:

     ```
     $ ./sta_install_2.1.0.64.124_linux64.bin –silent –responseFile /Installers/
     SilentInstall.rsp
     ```

     Antes de usar este modo, debe descargar también el archivo *silentInstallUtility.jar* y crear un archivo de respuesta en el que se especifiquen las opciones de instalación. Consulte el Apéndice B, *Instalador y desinstalador en modo silencioso de STA* para obtener instrucciones.

3.6.5. Verificación de la instalación

Use este procedimiento para verificar que STA se esté ejecutando.

1. Use los siguientes pasos para asegurarse de que el directorio bin de STA esté incluido en la variable *PATH* para el usuario root del sistema.

a. Abra una sesión de terminal en el servidor actual de STA e inicie sesión como usuario root del sistema.
b. Use un editor de texto para abrir el perfil del usuario. Por ejemplo:

```
# vi /root/.bash_profile
```

c. Agregue el directorio bin de STA a la definición de *PATH*. Por ejemplo, agregue la siguiente línea al archivo:

```
PATH=$PATH:Oracle_storage_home/StorageTek_Tape_Analytics/common/bin
```

Donde *Oracle_storage_home* es la ubicación del directorio raíz de almacenamiento de Oracle especificada durante la instalación de STA.
d. Guarde el archivo y ciérrelo.
e. Cierre sesión y vuelva a iniciar sesión como usuario root del sistema.
f. Confirme que la variable *PATH* se haya actualizado correctamente.

```
# echo $PATH
/usr/lib64/qt-3.3/bin:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/
usr/bin:/root/bin:/Oracle/StorageTek_Tape_Analytics/common/bin
```

2. Use el comando *STA* para verificar que todos los servicios de STA se estén ejecutando y estén activos. En el Ejemplo 3.1, “Pantalla de estado correcto de STA”, se muestra cómo se ve el estado correcto. Consulte la *Guía de administración de STA* para obtener detalles.

Ejemplo 3.1. Pantalla de estado correcto de STA

```
$ STA status all
mysql is running
staservd service is running
weblogic service is runningstaengine service is running
 .... and the deployed application for staengine is in an ACTIVE state
staadapter service is running
 .... and the deployed application for staadapter is in an ACTIVE state
staui service is running
 .... and the deployed application for staui is in an ACTIVE state
```

3. Siga estos pasos:
   - Si los servicios de STA se están ejecutando y están activos, puede comenzar a configurar las bibliotecas y STA. Consulte el Capítulo 5, *Configuración de SNMP en las bibliotecas*y el Capítulo 6, *Configuración de conexiones de bibliotecas en STA* para obtener instrucciones.

- Si hay algún problema con los servicios de STA, puede revisar los logs de la instalación y STA para obtener más información. Consulte Sección 3.4, “Logs de instalación y desinstalación de STA” para conocer las ubicaciones de estos logs.

3.6.6. Reubicación del directorio de logs de STA (opcional)

Use este procedimiento solamente si desea reubicar los logs de STA y MySQL en una ubicación que no sea la predeterminada, que es */var/log/tbi*. Después de finalizar este procedimiento, los nuevos logs se escribirán en la ubicación que indique. Puede realizar este procedimiento en cualquier momento después de haber instalado STA. Consulte Sección 2.1.2, “Revisión de la disposición del sistema de archivos de STA” para conocer los requisitos de ubicación.

1. Inicie sesión como usuario root del sistema.
2. Detenga todos los servicios de STA.

```
# STA stop all
Stopping the staui service......
Successfully stopped the staui service
Stopping the staadapter service......
Successfully stopped the staadapter service
Stopping the staengine service......
Successfully stopped the staengine service
Stopping the weblogic service......
Successfully stopped the weblogic service
Stopping the staservd Service...
Successfully stopped staservd service
Stopping the mysql service.....
Successfully stopped mysql service
#
```

3. Cree el nuevo directorio de logs de STA que desea usar para los logs de STA y MySQL. Por ejemplo:

```
# mkdir -p /LOGS_DIR/log/
# ls -ld /LOGS_DIR/log
drwxr-xr-x 2 root root 4096 Jan 20 14:17 /LOGS_DIR/log
```

4. Cambie los permisos de acceso al directorio para que STA y MySQL puedan escribir en él. Por ejemplo:

```
# chmod 777 /LOGS_DIR/log
# ls -ld /LOGS_DIR/log
drwxrwxrwx 2 root root 4096 Jan 20 14:17 /LOGS_DIR/log
```

5. Mueva el directorio actual */var/log/tbi* al directorio de logs de STA que acaba de crear.

```
# mv /var/log/tbi /LOGS_DIR/log/
# ls -l /LOGS_DIR/log/tbi
total 20
drwxrwxrwx 2 mysql mysql 4096 Jan  7 10:45 backups
drwxrwxrwx 3 mysql mysql 4096 Jan  7 10:45 db
drwxrwxrwx 2 mysql mysql 4096 Jan  7 11:30 install
-rwxrwxrwx 1 root  root  1191 Jan 20 13:04 monitor_staserver.log
drwxrwxrwx 2 root  root  4096 Jan  7 11:03 uidumps
```

6. Cree un enlace simbólico desde el nuevo directorio de logs de STA hasta la ubicación predeterminada. Por ejemplo:

```
# ln -s /LOGS_DIR/log/tbi /var/log/tbi
# ls -l /var/log/tbi
lrwxrwxrwx 1 root   root          15 Jan 20 14:22 /var/log/tbi -> /LOGS_DIR/log/
tbi
#
```

7. Reinicie STA.

```
# STA start all
Starting mysql Service..
mysql service was successfully started
Starting staservd Service.
staservd service was successfully started
Starting weblogic Service......
weblogic service was successfully started
Starting staengine Service.........
staengine service was successfully started
Starting staadapter Service..........
staadapter service was successfully started
Starting staui Service.........
staui service was successfully started
#
```

3.6.7. Registro de la ubicación del inventario central de Oracle

Use este procedimiento después de que haya finalizado la instalación de STA para registrar la ubicación del inventario central de Oracle en el servidor de STA. Solo hace falta usar una vez este procedimiento en este servidor.

Con este procedimiento, se crea un archivo indicador del inventario central de Oracle, */etc/oraInst.loc*, lo que permite a todos los instaladores de Oracle usados en este servidor conocer el grupo de instalación de Oracle y la ubicación del inventario central de Oracle.

1. Inicie sesión como usuario *root* de Linux.
2. Cambie al directorio del inventario central de Oracle. Por ejemplo:

   ```
   # cd /opt/oracle/oraInventory
   ```

3. Ejecute el script de registro, que se encuentra en ese directorio.

   ```
   # ./createCentralInventory.sh
   Setting the inventory to /opt/oracle/oraInventory
   Setting the group name to oinstall
   Creating the Oracle inventory pointer file (/etc/oraInst.loc)
   Changing permissions of /opt/oracle/oraInventory to 770.
   Changing groupname of /opt/oracle/oraInventory to oinstall.
   The execution of the script is complete
   #
   ```

   La ubicación del inventario central de Oracle y el grupo de instalación de Oracle ahora se identifican en el archivo indicador del inventario central de Oracle, */etc/oraInst.loc*.

4

Configuración de funciones de biblioteca para STA

Para que las bibliotecas envíen datos SNMP de alta calidad a STA, hay ciertas funciones que se deben configurar correctamente. Estas funciones varían según el modelo de biblioteca. Debe completar las actividades de este capítulo antes de continuar con el Capítulo 5, *Configuración de SNMP en las bibliotecas*.

En este capítulo, se incluyen las siguientes secciones:

- Funciones de biblioteca que afectan los datos de STA
- Interfaces de usuario de las bibliotecas
- Tareas de configuración de funciones de bibliotecas

4.1. Funciones de biblioteca que afectan los datos de STA

4.1.1. Interfaz ADI para unidades LTO

Las bibliotecas modulares StorageTek son compatibles con las unidades LTO (cinta lineal abierta) de HP e IBM. Las unidades LTO que admiten la interfaz de unidad de automatización (ADI) pueden proporcionar datos enriquecidos (por ejemplo, rendimiento y utilización de la unidad) a la biblioteca, en función de la configuración de la unidad y el nivel de firmware.

Para que una biblioteca envíe datos de unidad LTO enriquecidos a STA, se debe activar la ADI tanto en la biblioteca como en las unidades LTO. Si la ADI no se activa en ambos lugares, la biblioteca envía solo datos básicos sobre las unidades LTO.

Consulte la *Guía de requisitos de STA* para obtener detalles sobre los niveles de firmware requeridos para las unidades.

4.1.1.1. Activación de ADI en unidades LTO

El método para activar ADI depende del fabricante y el modelo de la unidad.

- **LTO-3, LTO-4, LTO-5 y LTO-6 de HP**: estas unidades cambian automáticamente al modo ADI una vez que ADI se activa en la biblioteca y la biblioteca y las unidades se reinician. (Las unidades pueden reiniciarse con la consola SL).
- **LTO-3, LTO-4, LTO-5 y LTO-6 de IBM**: estas unidades deben configurarse explícitamente para el modo ADI y no serán reconocidas hasta que se active la ADI en la biblioteca y ésta se reinicie. En la Tabla 4.1, “Cómo se activa ADI en unidades LTO de IBM”, se proporcionan más detalles.

Nota:

La tarjeta de adaptador Belisarius proporciona la interfaz para la solución de cifrado de cintas Oracle Key Manager (OKM). Tanto la unidad como el firmware de la tarjeta Belisarius deben cumplir los requisitos mínimos para STA.

Tabla 4.1. Cómo se activa ADI en unidades LTO de IBM

Unidad LTO de IBM	LTO-3	LTO-4	LTO-5, LTO-6
IBM sin tarjeta de adaptador Belisarius	El soporte de Oracle configura el hardware de la unidad para el modo ADI.	El soporte de Oracle configura el hardware de la unidad para el modo ADI.	N/D
IBM con tarjeta de adaptador Belisarius	N/D	El soporte de Oracle configura el hardware de la unidad para el modo ADI.	El firmware de la unidad debe estar configurado para el modo ADI con Virtual Operator Panel (VOP). Póngase en contacto con el soporte de Oracle para obtener ayuda.

4.1.1.2. Activación de ADI en la biblioteca

De forma predeterminada, la ADI no está activada en las bibliotecas SL500, SL3000 y SL8500, por lo que el soporte de Oracle debe activarla manualmente. Como para activar la ADI hay que reiniciar la biblioteca, debe activarla de antemano si tiene pensado instalar unidades LTO.

Para bibliotecas SL3000 y SL8500, la ADI se puede activar solo si la biblioteca tiene una tarjeta de controlador de unidad con gran capacidad de memoria (HBT). Consulte la *Guía de requisitos de STA* para obtener detalles sobre la tarjeta HBT.

4.1.2. TCP/IP dual y Redundant Electronics (SL3000 y SL8500 solamente)

Redundant Electronics y TCP/IP dual son funciones opcionales para las bibliotecas SL3000 y SL8500.

TCP/IP dual protege las operaciones de la biblioteca y el host contra errores de la red al proporcionar dos puertos TCP/IP en la biblioteca, normalmente configurados en subredes independientes. En caso de interrupciones o errores de red en una de las subredes, la conexión de la biblioteca y el host realiza un failover automáticamente al otro puerto.

Redundant Electronics protege contra errores de hardware en el controlador de la biblioteca mediante dos tarjetas de controlador de biblioteca independientes y completamente funcionales, una como tarjeta activa y la otra en espera. Si se producen errores importantes en el controlador activo, el control de la biblioteca se puede transferir a la tarjeta en espera, con una interrupción mínima de las operaciones de host y biblioteca.

Consulte la *Guía del usuario* de la biblioteca para obtener detalles sobre estas funciones.

4.1.2.1. Configuración de la conexión de STA para admitir estas funciones

En función de cuál de estas funciones se active (TCP/IP dual, Redundant Electronics o ambas), una biblioteca SL3000 o SL8500 puede tener una, dos o cuatro direcciones IP. Sin embargo, STA puede mantener conexiones ininterrumpidas solo con hasta dos direcciones IP de bibliotecas de manera simultánea. Por lo tanto, en una biblioteca dada, se puede configurar STA para que admita TCP/IP dual o Redundant Electronics, pero no ambas funciones.

Al configurar la conexión de STA con la biblioteca, siempre se debe especificar una dirección IP principal de la biblioteca. De forma opcional, se puede especificar una dirección IP secundaria, según la configuración de funciones de la biblioteca y cuál es la función que desea que admita STA.

Nota:

Para las bibliotecas que tienen ambas funciones, Oracle recomienda configurar STA para que admita Redundant Electronics, ya que esta función es más importante para mantener el funcionamiento continuo de la biblioteca.

Si STA está configurado para admitir TCP/IP dual, mantiene una conexión con la biblioteca si se produce un failover de puerto.

Si STA está configurado para admitir Redundant Electronics y se produce una conmutación de la tarjeta de controlador, STA mantiene una conexión con la biblioteca a través del puerto especificado como dirección IP secundaria de la biblioteca.

Consulte la *Guía del usuario* de la biblioteca para obtener más información sobre estas funciones.

En la Tabla 4.2, “Direcciones IP de biblioteca recomendadas para la conexión de STA”, se resumen las direcciones IP de biblioteca que se recomiendan usar al configurar la conexión de STA con la biblioteca.

Tabla 4.2. Direcciones IP de biblioteca recomendadas para la conexión de STA

Funciones activadas	IP principal de biblioteca	IP secundaria de biblioteca
Ninguna	Puerto 2B	N/D
Solo TCP/IP dual	Puerto 2B	Puerto 2A en la tarjeta activa
Solo Redundant Electronics	Puerto 2B en la tarjeta activa	Puerto 2B en la tarjeta en espera
Ambas	Puerto 2B en la tarjeta activa	Puerto 2B en la tarjeta en espera

4.1.2.2. Consideraciones adicionales para estas funciones

- Para configurar STA para que admita TCP/IP dual en una biblioteca SL3000 o SL8500, tal vez tenga que usar enrutamiento de políticas. Para obtener más información, consulte la *Guía de conectividad de hosts* de SL3000 o SL8500. Si necesita asistencia con la configuración de TCP/IP dual, póngase en contacto con el soporte de Oracle.
- Si una biblioteca tiene Redundant Electronics y TCP/IP dual, la subred del servidor de STA debe ser diferente de la subred del puerto de la biblioteca que no se configuró para STA. Consulte Sección 6.1.4, “Configuración de la conexión SNMP con una biblioteca”. De no ser así, la biblioteca puede intentar enviar datos a través de estos puertos (desconocidos para STA), y los datos serán rechazados por STA.
- Asegúrese de que la puerta de enlace predeterminada sea la interfaz 2B.

4.1.3. ID de complejo de bibliotecas (solo SL8500)

Para que STA acumule datos de complejos de bibliotecas correctamente, cada complejo de bibliotecas del sitio debe tener un ID de complejo único. En bibliotecas SL8500, los ID de complejos se configuran de manera manual. En todos los demás modelos de biblioteca, los ID de complejos se configuran automáticamente, y, por lo tanto, no es necesaria la intervención manual ni la verificación.

Cada SL8500 independiente es considerada un complejo separado y, por lo tanto, debe tener un ID de complejo único. Asimismo, cada complejo de varias bibliotecas debe tener un ID de complejo único, y todas las bibliotecas dentro del complejo deben compartir el mismo ID. Los valores válidos de ID de complejo son del 1 al 127.

En la Tabla 4.3, “Ejemplos de asignaciones de ID de complejo”, se muestran algunos ejemplos de asignaciones de ID de complejo de SL8500 válidas.

Tabla 4.3. Ejemplos de asignaciones de ID de complejo

Tipo de complejo	Bibliotecas	ID de complejo asignado
Complejo de varias bibliotecas	SL8500-1	1
	SL8500-2	1
	SL8500-3	1
Bibliotecas independientes	SL8500‑4	2
	SL8500-5	3

Precaución:

Service Delivery Platform (SDP) de Oracle también utiliza ID de complejo únicos para realizar un seguimiento de los datos de la biblioteca. Si su sitio utiliza SDP, póngase en contacto con el soporte de Oracle antes de cambiar un ID de complejo. El cambio de un ID de complejo podría hacer que SDP falle. En la mayoría de los casos, los ID de complejo se definen correctamente cuando SDP está conectado.

Consulte Sección 4.3.5, “Uso del ID de complejo de bibliotecas correcto (solo SL8500)” para obtener instrucciones.

4.1.4. Advertencia de limpieza de unidad (solo SL3000 y SL8500)

El indicador de advertencia de limpieza de unidad indica si se debe emitir una advertencia de unidad cuando una unidad necesita limpieza. Este indicador se configura en el nivel de la biblioteca, de manera que se aplica la misma configuración a todas las unidades de la biblioteca.

- Cuando el indicador está configurado con el valor "on", cada unidad muestra un estado de advertencia cuando necesita limpieza. Como resultado, el estado de mantenimiento de nivel superior de la biblioteca se degradará en el monitor de STA.
- Cuando el indicador está configurado con el valor "off", el estado de cada una de las unidades no se ve afectado por la necesidad de limpieza; por lo tanto, el estado de nivel superior de la biblioteca en STA no se degrada.

Si tiene una gran cantidad de unidades en la biblioteca, tal vez sea conveniente configurar este indicador con el valor "off" para que la condición de nivel superior de la biblioteca no se degrade cada vez que alguna de las unidades necesita limpieza.

Consulte Sección 4.3.6, “Configuración de advertencia de limpieza de unidad (opcional, solo SL3000 y SL8500)” para obtener instrucciones.

4.1.5. Formato de etiqueta de volumen (solo SL500 y SL150)

Los números de serie de volumen (volsers) en los datos SNMP deben tener el formato correcto para que STA procese correctamente los datos de intercambio de bibliotecas. El volser de medios incluye un sufijo de dos caracteres que indica el tipo de medio. Por ejemplo, si el volser de un cartucho es ABC123L4, "L4" indica que el tipo de medio es LTO4. Para que STA realice informes correctamente, el sufijo de volser debe excluirse.

Para asegurarse de que el formato sea correcto, se deben configurar los siguientes parámetros:

- Para todas las bibliotecas SL500 supervisadas por STA, la orientación de la etiqueta para el host debe configurarse con el valor *`left6`* y el modo de STA (controlado por el indicador *`staConfig`*) debe configurarse con el valor *`on`*. El modo de STA afecta solo el formato del volser enviado al servidor de STA a través de SNMP, no el formato que se usa en la biblioteca SL500 en sí.
- Para todas las bibliotecas SL150 supervisadas por STA, el formato de etiqueta de volumen debe configurarse con el valor *`Trim last two characters`* (Recortar los dos últimos caracteres).

Precaución:

Si estos parámetros no se definen correctamente, los volsers recibirán un formato incorrecto, lo que hará que se bloquee el procesamiento de intercambios, que se produzcan intentos superfluos para obtener los datos de medios más recientes y que aparezcan registros de volsers de ocho caracteres irreversibles en la pantalla de descripción general de medios, siempre que la preferencia para mostrar medios eliminados esté configurada.

Consulte Sección 4.3.7, “Configuración del formato de etiqueta de volumen de SL500 (solo SL500)” y Sección 4.3.8, “Configuración del formato de etiqueta de volumen de SL150 y modo de direcciones de elementos de unidad (solo SL150)” para obtener instrucciones.

4.1.6. Opción SCSI FastLoad (solo SL500)

La opción SCSI FastLoad debe estar desactivada en las bibliotecas SL500, ya que las capturas de montaje de cartuchos no se envían correctamente a STA cuando la opción está activada. FastLoad está desactivada de forma predeterminada. Póngase en contacto con el soporte de Oracle si no sabe con certeza cuál es el estado de esta opción.

4.1.7. Números de serie de volumen duplicados

En el almacén de datos de STA, el historial de medios se conserva por número de serie de volumen (volser). Como todo el historial de cada medio en particular está vinculado a su volser, Oracle recomienda evitar el uso de volsers duplicados. Los volsers deben ser únicos en todas las bibliotecas supervisadas. Los volsers duplicados generarán mezclas de datos para los diferentes medios.

Consulte *Guía del usuario de STA* para obtener más detalles sobre volsers duplicados.

4.2. Interfaces de usuario de las bibliotecas

Las bibliotecas SL500, SL3000 y SL8500 tienen una interfaz de línea de comandos (CLI) y una interfaz gráfica de usuario, StorageTek Library Console (SL Console). La biblioteca SL150 usa exclusivamente una interfaz de usuario basada en explorador. Estas interfaces se usan para llevar a cabo los procedimientos de este capítulo.

4.2.1. Consejos de uso para la CLI de la biblioteca

Para la mayoría de los comandos de la CLI, la sintaxis es la misma en los modelos de biblioteca SL500, SL3000 y SL8500. Para los pocos comandos en los que la sintaxis varía por modelo de biblioteca, se proporcionan ejemplos. En la mayoría de los ejemplos de la CLI, se usa una biblioteca SL500. Si está configurando una biblioteca SL3000 o SL8500, los detalles devueltos por cada comando pueden variar levemente con respecto a lo que se muestra. A continuación, se presentan algunos consejos para usar la CLI de la biblioteca.

- Use un emulador de terminal, por ejemplo, PuTTY, para establecer una conexión SSH (shell seguro) con la CLI de la biblioteca.
- Active la generación de registros para poder revisar la actividad en caso de que necesite resolver errores.
- Con algunas versiones de firmware, la CLI agota el tiempo de espera después de seis horas.
- Para ver la ayuda de los comandos de la CLI, escriba `help` y el nombre del comando (por ejemplo, `help snmp`).
- Los comandos de las bibliotecas SL500 distinguen mayúsculas de minúsculas; los de las bibliotecas SL3000 y SL85000, no.

- Para evitar errores de entradas, puede escribir primero el comando en un archivo de texto y, a continuación, copiarlo y pegarlo en la CLI. Si necesita ayuda con los comandos de la CLI, escriba *`help snmp`*.
- Puede usar las siguientes funciones de la CLI para reducir las pulsaciones de teclas:
  - Presione la tecla de **tabulación** para que el comando se complete automáticamente.
  - Presione las teclas de **flecha hacia arriba** y **flecha hacia abajo** para desplazarse por el historial de comandos. Puede modificar los comandos introducidos previamente y después presionar **Intro** para ejecutarlos.
  - Para corregir un comando antes de presionar **Intro** para ejecutarlo, use las teclas de **flecha izquierda** y **flecha derecha** para mover el cursor hasta la ubicación del error y, a continuación, escriba la corrección. Los nuevos caracteres se insertan en la posición del cursor; para suprimir caracteres, use la tecla de **retroceso**.

4.2.2. Script de configuración de biblioteca (opcional)

STA proporciona un script de configuración de biblioteca para ayudarlo a completar el proceso de configuración de las bibliotecas. El script solicita los valores de configuración de la biblioteca y, en función de los valores que introduce, muestra comandos completos para que los copie y los pegue en la CLI de la biblioteca.

Nota:

Se recomienda analizar y comprender los pasos de configuración de la biblioteca que se describen en este capítulo antes de iniciar el script.

Para iniciar el script, abra una sesión de terminal en el servidor de STA y ejecute el siguiente comando:

```
# sh /Oracle_storage_home/StorageTek_Tape_Analytics/common/bin/STA-lib-config-steps.sh
```

donde *`Oracle_storage_home`* es el directorio en el que se instaló STA y el software asociado de Oracle. Consulte Sección 3.1, “Usuarios, grupos y ubicaciones usados por el instalador de STA” para obtener detalles.

Para obtener información adicional sobre el script y un ejemplo de uso, ejecute el siguiente comando:

```
# sh /Oracle_storage_home/StorageTek_Tape_Analytics/common/bin/STA-lib-config-steps.sh
 -? | more
```

4.3. Tareas de configuración de funciones de bibliotecas

Use la Tabla 4.4, “Tareas para configurar bibliotecas para STA” para determinar cuáles son las tareas aplicables a los modelos de biblioteca que se usan en su sitio. Debe realizar las tareas aplicables en cada una de las bibliotecas que desee supervisar con STA.

Tabla 4.4. Tareas para configurar bibliotecas para STA

Tarea	SL150	SL500	SL3000	SL8500
Sección 4.3.1, “Inicio de sesión en la biblioteca”	Sí	Sí	Sí	Sí
Sección 4.3.2, “Verificación de la versión de firmware de la biblioteca”	Sí	Sí	Sí	Sí
Sección 4.3.3, “Verificación de la versión de la tarjeta del controlador de unidad (solo SL3000 y SL8500)”	–	–	Sí	Sí
Sección 4.3.4, “Activación de ADI en la biblioteca (todas las bibliotecas, excepto SL150)”	–	Sí	Sí	Sí
Sección 4.3.5, “Uso del ID de complejo de bibliotecas correcto (solo SL8500)”	–	–	–	Sí
Sección 4.3.6, “Configuración de advertencia de limpieza de unidad (opcional, solo SL3000 y SL8500)”	–	–	Sí	Sí
Sección 4.3.7, “Configuración del formato de etiqueta de volumen de SL500 (solo SL500)”	–	Sí	–	–
Sección 4.3.8, “Configuración del formato de etiqueta de volumen de SL150 y modo de direcciones de elementos de unidad (solo SL150)”	Sí	–	–	–

Nota:

Para las bibliotecas SL500, SL3000 y SL8500, muchas de las tareas le permiten elegir la interfaz que desee usar: CLI o SL Console. Para las bibliotecas SL150, se usa exclusivamente la interfaz de usuario basada en explorador.

4.3.1. Inicio de sesión en la biblioteca

Con la CLI de la biblioteca (todas las bibliotecas, excepto SL150)

1. Establezca una conexión SSH con la biblioteca mediante la dirección IP o un alias de DNS.
2. Inicie sesión en la CLI con el nombre de usuario y la contraseña del usuario *admin*.

Con SL Console (todas las bibliotecas, excepto SL150)

1. Inicie la aplicación SL Console.
2. Haga clic en el botón **About** (Acerca de) para ver la versión actual de SL Console y verificar que cumpla con los requisitos mínimos del firmware de la biblioteca.
3. Haga clic en **Close** (Cerrar) para regresar a la pantalla de inicio de sesión.
4. Inicie sesión con el nombre de usuario y la contraseña del usuario *admin* y la dirección IP o el alias de DNS de la biblioteca.

   Para las bibliotecas SL3000 y SL8500 que tengan la función Redundant Electronics, puede iniciar sesión en el controlador activo solamente.

Con la interfaz de usuario de SL150

1. Navegue hasta el nombre de host o la dirección IP de la biblioteca SL150.
2. Inicie sesión con su ID de usuario y contraseña. El ID de usuario debe tener el rol de administrador.

4.3.2. Verificación de la versión de firmware de la biblioteca

Use este procedimiento para verificar que el firmware de la biblioteca satisfaga o supere los requisitos mínimos indicados en la *Guía de requisitos de STA*. De no ser así, envíe una solicitud de servicio al soporte de Oracle para actualizar el firmware.

Para las bibliotecas SL8500, el soporte de Oracle debe registrar la configuración de la conexión de red antes de realizar una actualización de firmware, ya que puede ser necesario volver a introducir o actualizar la configuración después de la actualización.

Con la CLI de la biblioteca (todas las bibliotecas, excepto SL150; no aplicable a bibliotecas SL3000 anteriores a FRS 4.x)

1. Ejecute el comando siguiente:

```
SL500> version print
Library Hardware Information
 Library Vendor: STK
...
 Firmware Version: xxxx (x.xx.xx)
```

Nota:

Si en la pantalla aparece el mensaje *SYNTAX ERROR!!* (Error de sintaxis), significa que el nivel de firmware de la biblioteca es menor que el requerido. Póngase en contacto con el soporte de Oracle para actualizar el firmware.

Con SL Console (todas las bibliotecas, excepto SL150)

1. En el menú **Tools** (Herramientas), seleccione **System Detail** (Detalle del sistema).
2. En el árbol de navegación, seleccione **Library** (Biblioteca).
3. Seleccione el separador **Properties** (Propiedades) y, a continuación, el separador **Library Controller** (Controlador de biblioteca).

   La versión del firmware aparece debajo de la sección Code Version (Versión de código).

Con la interfaz de usuario de SL150

1. En el árbol de navegación, seleccione **Firmware**.

   La versión del firmware aparece debajo de la sección Library Firmware (Firmware de la biblioteca). De forma alternativa, puede hacer clic en el botón **About** (Acerca de) en la barra de estado para obtener la versión de firmware.

4.3.3. Verificación de la versión de la tarjeta del controlador de unidad (solo SL3000 y SL8500)

Para que las bibliotecas SL3000 y SL8500 envíen datos de unidad más completos a STA, la biblioteca debe tener una tarjeta de controlador de unidad con gran capacidad de memoria

(HBT). Esto normalmente es algo que se debe tener en cuenta en las bibliotecas más antiguas (adquiridas antes de mediados de 2006), debido a que las unidades más recientes ya incluyen una tarjeta con gran capacidad de memoria. Consulte la *Guía de requisitos de STA* para conocer detalles sobre los requisitos de nivel de firmware.

Use este procedimiento para verificar que haya instalada una tarjeta HBT con gran capacidad de memoria en la biblioteca. Si la biblioteca no tiene una tarjeta HBT con gran capacidad de memoria, envíe una solicitud de servicio al soporte de Oracle para que le instalen una.

Este procedimiento se realiza con SL Console. Para los modelos SL8500 FRS 8.x y SL3000 FRS 4.x, también puede usar el comando `config print` de la CLI para mostrar la información de la tarjeta HBT.

Este procedimiento se realiza con SL Console.

1. En el menú **Tools** (Herramientas), seleccione **System Detail** (Detalle del sistema).
2. En el árbol de navegación, seleccione **Library** (Biblioteca).
3. Seleccione el separador **Properties** (Propiedades) y, a continuación, el separador **Drive Controller** (Controlador de unidad).

   En la pantalla, se muestran los detalles de la tarjeta de controlador de unidad (HBT) activa.
4. Verifique que la tarjeta HBT con gran capacidad de memoria indique `true`.
5. Si tiene una biblioteca SL3000 (FRS 4.x) o SL8500 (FRS 8.x) con Redundant Electronics, expanda la carpeta Redundant Electronics y, a continuación, seleccione cada una de las tarjetas HBT (hbta, hbtb). Ambas deben indicar `True` para la tarjeta HBT con gran capacidad de memoria.

Nota:

Tanto la tarjeta HBT activa como la que está en espera deben estar instaladas y en comunicación, y ambas deben tener gran capacidad de memoria.

4.3.4. Activación de ADI en la biblioteca (todas las bibliotecas, excepto SL150)

Si la biblioteca incluye unidades LTO, se debe activar la ADI tanto en las unidades como en la biblioteca para que STA pueda recibir datos de unidades más completos. Use este procedimiento para asegurarse de que la interfaz de unidad ADI esté activada en la biblioteca. Consulte Sección 4.1.1, “Interfaz ADI para unidades LTO” para obtener detalles.

Este procedimiento se realiza con la CLI de la biblioteca.

Para bibliotecas SL3000 o SL8500

1. Muestre el estado de la interfaz ADI.

```
drive adiEnable print
```

2. Si el valor de "Attributes Adi Status" (Estado de ADI de atributos) es *true*, puede salir de la tarea. Si es *false*, continúe con el siguiente paso.
3. Active la interfaz ADI.

```
drive adiEnable on
```

4. Reinicie la biblioteca para activar el cambio.

Para bibliotecas SL500

1. Muestre el estado de la interfaz ADI.

```
enableADI print
```

2. Si el valor de "enableADI set to" (Activar ADI en) es *on*, puede salir de la tarea. Si es *off*, continúe con el siguiente paso.
3. Active la interfaz ADI.

```
enableADI on
```

4. Reinicie la biblioteca para activar el cambio.

4.3.5. Uso del ID de complejo de bibliotecas correcto (solo SL8500)

Para que STA acumule datos de complejos de bibliotecas correctamente, cada complejo de bibliotecas del sitio debe tener un ID de complejo único. Use este procedimiento para asegurarse de utilizar el ID de complejo de bibliotecas correcto para cada biblioteca SL8500. Consulte Sección 4.1.3, “ID de complejo de bibliotecas (solo SL8500)” para obtener detalles.

Este procedimiento se realiza con la CLI de la biblioteca.

1. Para cada biblioteca SL8500 que se supervise con STA, muestre el ID de complejo actualmente asignado:

```
SL8500> config complexId print
 ...
 Complex Id 3
 ...
```

2. Verifique que cada biblioteca independiente y cada complejo de bibliotecas tengan un ID de complejo único y que todas las bibliotecas de cada complejo de bibliotecas tengan el mismo ID de complejo.

Si necesita cambiar el ID de complejo de una biblioteca independiente, continúe con este procedimiento.

Precaución:

Si necesita cambiar el ID de complejo de una biblioteca perteneciente a un complejo de bibliotecas, póngase en contacto con el soporte de Oracle. No continúe con este procedimiento.

3. Desconecte la biblioteca y espere a que se completen todas las transacciones.
4. Cambie el ID de complejo de una biblioteca independiente. *complex_ID* es un número entre 1 y 127.

```
config complexId set complex_ID
```

Ejemplo 4.1. Cambio de ID de complejo de SL8500 independiente

```
SL8500> config complexId set 5
 ...
 Complex Id 5
 Success true
 Done
 ...
 Note: TCP/IP stack reset may take a few seconds after command completion.
```

Nota:

Cuando se ejecuta este comando, todas las conexiones de TCP/IP se interrumpen. Tal vez deba volver a iniciar sesión en la biblioteca.

4.3.6. Configuración de advertencia de limpieza de unidad (opcional, solo SL3000 y SL8500)

Use este procedimiento opcional para comprobar la configuración actual del indicador de advertencia de limpieza de unidad en la biblioteca y modificarlo de ser necesario. Consulte Sección 4.1.4, “Advertencia de limpieza de unidad (solo SL3000 y SL8500)” para obtener detalles.

Este procedimiento se realiza con la CLI de la biblioteca.

1. Muestre la configuración actual del indicador de advertencia de limpieza de unidad.

```
SL3000> cleaning driveWarning get
 ...
 Object Drive Cleaning Warning true
 ...
```

2. Si desea configurar el indicador con el valor *false* (desactivado), use el siguiente comando:

```
cleaning driveWarning set off
```

4.3.7. Configuración del formato de etiqueta de volumen de SL500 (solo SL500)

Use este procedimiento para asegurarse de que los números de serie de volumen (volsers) estén correctamente formateados en los datos de SNMP enviados a STA. Consulte Sección 4.1.5, “Formato de etiqueta de volumen (solo SL500 y SL150)” para obtener detalles.

Este procedimiento se realiza con la CLI de SL500.

> **Nota:**
>
> Oracle recomienda suspender todas las actividades de la biblioteca antes de cambiar estos parámetros. Puede ser necesario hacer cambios de configuración en las aplicaciones de cinta o los hosts después de modificar estos parámetros.

1. Muestre la configuración actual del indicador *`orientlabel`*.

```
SL500> orientlabel print
Host: (left8) Window left-justified with 6 character label
Op Panel: (left8) Window left-justified with 8 character label
```

2. El indicador *`host`* debe estar configurado con el valor *`left6`*. Para hacerlo, use el siguiente comando:

```
SL500> orientlabel host left6
New settings were accepted...Setting are now in effect.
```

3. Muestre la configuración nuevamente para verificar que se haya actualizado correctamente.

```
SL500> orientlabel print
Host: (left6) Window left-justified with 6 character label
Op Panel: (left8) Window left-justified with 8 character label
```

4. Muestre la configuración actual del indicador *`staConfig`*.

```
SL500> staConfig print
STA mode is disabled
```

5. El indicador *`staConfig`* debe estar configurado con el valor *`on`*. Para hacerlo, use el siguiente comando:

```
SL500> staConfig on
```

6. Muestre la configuración nuevamente para verificar que se haya actualizado correctamente.

```
SL500> staConfig print
STA mode is enabled
```

4.3.8. Configuración del formato de etiqueta de volumen de SL150 y modo de direcciones de elementos de unidad (solo SL150)

Use este procedimiento para asegurarse de que los números de serie de volumen (volsers) estén correctamente formateados en los datos de SNMP enviados a STA.

Asimismo, para firmware 2.xx y versiones posteriores de SL150, use este procedimiento para configurar el modo de direcciones de elementos de unidad para que se incluyan los alojamientos de unidades vacíos en los datos enviados a STA.

Consulte Sección 4.1.5, “Formato de etiqueta de volumen (solo SL500 y SL150)” para obtener detalles.

Nota:

Oracle recomienda suspender todas las actividades de la biblioteca antes de cambiar estos parámetros. Puede ser necesario hacer cambios de configuración en las aplicaciones de cinta y los hosts después de modificar estos parámetros.

Este procedimiento se realiza con la interfaz basada en explorador de SL150.

1. En el árbol de navegación, seleccione **Configuration** (Configuración).
2. Seleccione el botón **Configure** (Configurar).
3. En la ventana Configuration Wizard (Asistente de configuración), seleccione la casilla de verificación **Configure Library Settings** (Configurar parámetros de biblioteca) y, a continuación, haga clic en **Next** (Siguiente).
4. Defina los siguientes parámetros según corresponda:
   - Drive Element Addressing Mode (Modo de direcciones de elementos de unidad): **Address All Drive Slots (Recommended)** (Incluir todas las ranuras de unidades [recomendado])
   - Library Volume Label Format (Formato de etiqueta de volumen de biblioteca): **Trim last two characters (Default)** (Recortar los dos últimos caracteres [predeterminado])

   Nota:

   Después de cambiar el modo de direcciones de elementos de unidad, debe esperar por lo menos 10 minutos para configurar SNMP en STA.
5. Haga clic en **Next** (Siguiente).
6. En la pantalla Summary of Configuration Changes (Resumen de cambios de configuración), seleccione la casilla de verificación **Accept all changes** (Aceptar todos los cambios) y, a continuación, haga clic en **Apply** (Aplicar).

7. En la pantalla Apply Configuration Changes (Aplicar cambios de configuración), seleccione la casilla de verificación **Set the Library back Online after applying the changes** (Establecer la biblioteca en línea después de aplicar los cambios) y, a continuación, haga clic en **OK** (Aceptar).
8. Cuando aparezca el mensaje **All configuration changes have been applied successfully** (Todos los cambios de configuración se aplicaron correctamente), haga clic en **Close** (Cerrar).

5

Configuración de SNMP en las bibliotecas

Para que STA supervise las bibliotecas del sitio, debe realizar algunas actividades de configuración en las bibliotecas y algunas en el servidor de STA. En este capítulo, se describen las actividades que se realizan en las bibliotecas. Debe completar las actividades de este capítulo antes de continuar con el Capítulo 6, *Configuración de conexiones de bibliotecas en STA*.

En este capítulo, se incluyen las siguientes secciones:

Para obtener información general sobre la implementación de SNMP en las bibliotecas StorageTek, consulte la *Guía de referencia de SNMP de bibliotecas modulares StorageTek*.

5.1. Descripción de la configuración de SNMP de bibliotecas para STA

La comunicación entre STA y las bibliotecas que supervisa se realiza a través del protocolo simple de administración de redes (SNMP). Las bibliotecas envían datos a STA mediante informes y capturas SNMP, y STA recupera los datos de configuración de las bibliotecas mediante funciones get de SNMP. En términos de SNMP, STA es un agente *cliente* y cada biblioteca es un agente *servidor*.

SNMP v3 es el protocolo recomendado para la comunicación de SNMP entre STA y las bibliotecas. Las funciones de autenticación, cifrado e integridad de los mensajes de SNMP v3 proporcionan un mecanismo seguro para enviar datos de la biblioteca. SNMP v3 también se requiere para la función de validación de medios de STA. La validación de medios de STA está disponible para las bibliotecas compatibles solamente. Consulte la *Guía de requisitos de STA* para obtener detalles.

En este capítulo, se describe la configuración recomendada para SNMP v3. Sin embargo, en función de los requisitos del sitio, puede elegir usar SNMP v2c para una o varias bibliotecas. Consulte el Apéndice F, *Configuración del modo SNMP v2c* para obtener instrucciones para la configuración de SNMP v2c.

Nota:

Si bien el protocolo SNMP v3 se usa para las capturas SNMP y las funciones get, el intercambio inicial de la comunicación entre una biblioteca y STA siempre se hace mediante el protocolo SNMP v2c.

5.1.1. Configuración del protocolo SNMP v3 en las bibliotecas

En cada biblioteca, para configurar la comunicación SNMP v3 entre STA y la biblioteca, se define la biblioteca como usuario de SNMP v3 y el servidor de STA como destinatario de capturas SNMP v3. Además, debe especificar mecanismos y contraseñas de autorización y privacidad. Para STA, el método de autorización siempre es SHA (algoritmo de comprobación aleatoria protegido) y el método de privacidad siempre es DES (estándar de cifrado de datos).

5.1.1.1. Usuario único de SNMP v3

STA admite solo un usuario de SNMP v3. Se debe definir el mismo usuario en todas las bibliotecas supervisadas por una única instancia de STA. En el Apéndice C, *Hojas de trabajo de instalación y actualización*, se proporciona una hoja de trabajo que se puede usar para registrar los valores que se utilizarán.

Nota:

Tal vez las bibliotecas ya tengan uno o varios usuarios de SNMP v3. De ser así, puede usar uno de ellos para la comunicación de STA. Sin embargo, Oracle recomienda que se configure un nuevo usuario único de SNMP v3 con este fin.

A continuación, se indican los valores que se deben proporcionar para definir el usuario de SNMP v3.

SNMP v3 username (Nombre de usuario de SNMP v3)
El servidor de STA recibe capturas enviadas por este usuario. También es el nombre del destinatario de SNMP v3 que se usa al crear destinatarios de capturas. Debe ser el mismo en todas las bibliotecas.

SNMP v3 authorization password (Contraseña de autorización de SNMP v3)
Contraseña de autorización que se asigna al usuario de SNMP v3.

Debe tener, por lo menos, ocho caracteres y no puede incluir coma, punto y coma ni el signo igual.

SNMP v3 privacy encryption password (Contraseña de cifrado de privacidad de SNMP v3)
Contraseña de privacidad que se asigna al usuario de SNMP v3.

Debe tener, por lo menos, ocho caracteres y no puede incluir coma, punto y coma ni el signo igual.

SNMP v2c user community (Comunidad de usuarios de SNMP v2c)
Cadena de la comunidad de usuarios de SNMP v2c, normalmente configurada como `public`. Esta cadena es necesaria para el intercambio inicial entre la biblioteca y el servidor de STA, aunque se use el protocolo SNMP v3.

Puede contener solo caracteres alfanuméricos (a-z, A-Z, 0-9). No se permiten caracteres especiales.

SNMP v2c trap community (Comunidad de capturas de SNMP v2c)
Nombre de la comunidad de capturas de SNMP v2c. Se usa solo si se usa SNMP v2c para la comunicación con la biblioteca. Si está usando SNMP v3, deje el valor predeterminado, `public`.

Puede contener solo caracteres alfanuméricos (a-z, A-Z, 0-9). No se permiten caracteres especiales.

5.1.1.2. ID de motores de SNMP

Como el protocolo SNMP v3 requiere que cada dispositivo SNMP tenga un ID de motor globalmente único, el servidor de STA y las bibliotecas deben tener sus propios ID de motor. En el caso de los complejos de bibliotecas SL8500, cada biblioteca del complejo también tiene su propio agente de SNMP, por lo tanto, tiene su propio ID de motor único. El ID de motor tiene un máximo de 31 caracteres hexadecimales.

Las capturas SNMP usan el ID de motor del *remitente*. Por lo tanto, debe especificar el ID de motor de la *biblioteca* al definir STA como destinatario de capturas de SNMP v3.

5.2. Tareas de configuración de SNMP de la biblioteca

En la Tabla 5.1, “Tareas para configurar bibliotecas para STA”, se resume el proceso de configuración de bibliotecas para enviar datos de SNMP correctos a STA. Debe realizar las tareas en el orden indicado en cada una de las bibliotecas que desee supervisar con STA.

Tabla 5.1. Tareas para configurar bibliotecas para STA

Tarea	SL150	SL500	SL3000	SL8500
Sección 5.2.1, “Recuperación de la dirección IP de la biblioteca”	Sí	Sí	Sí	Sí
Sección 5.2.2, “Activación de SNMP en la biblioteca”	Sí	Sí	Sí	Sí
Sección 5.2.3, “Uso de un usuario SNMP v2c”	Sí	Sí	Sí	Sí
Sección 5.2.4, “Creación de un usuario de SNMP v3”	Sí	Sí	Sí	Sí
Sección 5.2.5, “Recuperación del ID del motor de SNMP de la biblioteca (todas las bibliotecas, excepto SL150)”	–	Sí	Sí	Sí
Sección 5.2.6, “Creación del destinatario de capturas de SNMP v3 de STA”	Sí	Sí	Sí	Sí

Nota:

En estos procedimientos, se supone que está usando el protocolo SNMP v3 recomendado para las comunicaciones entre STA y las bibliotecas. Consulte Sección 5.1, “Descripción de la configuración de SNMP de bibliotecas para STA” para obtener detalles.

Nota:

Para las bibliotecas SL500, SL3000 y SL8500, algunas de las tareas le permiten elegir la interfaz que desea usar: CLI o SL Console. Para las bibliotecas SL150, se debe usar siempre la interfaz de usuario basada en explorador.

5.2.1. Recuperación de la dirección IP de la biblioteca

Use este procedimiento para recuperar y registrar la dirección IP de la biblioteca. Utilizará este valor para configurar la conexión con la biblioteca.

Para las bibliotecas SL3000 y SL8500, elija el método para admitir Redundant Electronics, TCP/IP dual o ninguna función. Consulte Sección 4.1.2, “TCP/IP dual y Redundant Electronics (SL3000 y SL8500 solamente)” para obtener detalles.

Este procedimiento se realiza con SL Console o la interfaz basada en explorador de SL150.

Dirección IP de SL500

1. En el menú **Tools** (Herramientas), seleccione **System Detail** (Detalle del sistema).
2. En el árbol de navegación, seleccione **Library** (Biblioteca).
3. Seleccione el separador **Properties** (Propiedades) y, a continuación, el separador **General**.

   La dirección IP de la biblioteca se indica debajo de la sección Library Interface TCP/IP (TCP/IP de interfaz de la biblioteca).
4. Registre la dirección IP de la biblioteca como dirección IP principal de la biblioteca. (Esta dirección corresponde al puerto 1B).

Dirección IP de SL3000 o SL8500: compatibilidad con Redundant Electronics

a. En el menú **Tools** (Herramientas), seleccione **System Detail** (Detalle del sistema).
b. En el árbol de navegación, seleccione la carpeta **Redundant Electronics**.

   Si la carpeta no aparece, significa que la función Redundant Electronics no está disponible en la biblioteca.
c. En el campo Device State (Estado del dispositivo), verifique que uno de los controladores de la biblioteca indique *`Duplex: software ready, switch possible`* (Dúplex: software listo, conmutación posible) (esta es la tarjeta activa) y que el otro indique *`Standby: software ready`* (En espera: software listo) (esta es la tarjeta en modo de espera).

   Estos estados indican que las tarjetas de los controladores están funcionando normalmente. Si no ve estos estados, póngase en contacto con el soporte de Oracle.
d. Expanda la carpeta **Redundant Electronics** y seleccione la tarjeta de controlador activa.
e. Registre la dirección IP del puerto 2B.
f. Repita el paso d y el paso e para la tarjeta de controlador alternativa (en espera).

Direcciones IP de SL3000 o SL8500: compatibilidad con TCP/IP dual

a. En el menú **Tools** (Herramientas), seleccione **System Detail** (Detalle del sistema).
b. En el árbol de navegación, seleccione **Library** (Biblioteca).

c. Seleccione el separador **Properties** (Propiedades) y, a continuación, el separador **General**.

   La información de dirección IP se muestra en las secciones Host Interface TCP/IP 2B (Interfaz de host TCP/IP 2B) y Host Interface TCP/IP 2A (Interfaz de host TCP/IP 2A).

   Nota:

   Si la biblioteca también incluye la función Redundant Electronics, las direcciones IP que se muestran son las correspondientes a la tarjeta de controlador activa solamente.

d. Registre la dirección IP principal (sección 2B) y la dirección IP secundaria (sección 2A).

Direcciones IP de SL3000 o SL8500: sin TCP/IP dual ni Redundant Electronics

a. En el menú **Tools** (Herramientas), seleccione **System Detail** (Detalle del sistema).
b. En el árbol de navegación, seleccione **Library** (Biblioteca).
c. Seleccione el separador **Properties** (Propiedades) y, a continuación, el separador **General**.

   La información de dirección IP aparece en la sección Host Interface TCP/IP 2B (Interfaz de host TCP/IP 2B). No hay información de dirección IP en la sección 2A.

d. Registre la dirección IP como dirección IP principal de la biblioteca.

Dirección IP de SL150

1. En el árbol de navegación, seleccione **Configuration** (Configuración).

   Seleccione **Settings** (Configuración) y, a continuación, seleccione **Network** (Red). La dirección IP de la biblioteca se muestra en la sección **Network Port 1 Settings** (Configuración de puerto de red 1). (La sección Network Port 2 Settings [Configuración de puerto de red 2] está reservada para uso por parte del servicio).

   Nota:

   El valor del campo Configure IP *xx* (Configurar IP xx) debe ser *Static* (Estática). Si no lo es, haga clic en el botón **Configure** (Configurar) y, a continuación, seleccione **Configure Network Settings** (Configurar valores de red) para especificar una dirección IP estática.

5.2.2. Activación de SNMP en la biblioteca

Use este procedimiento para activar SNMP en el puerto público de la biblioteca.

Con la CLI de la biblioteca

1. En función del modelo de biblioteca, use uno de los siguientes comandos:
   - Para las bibliotecas SL3000 y SL8500, active SNMP en el puerto 2B. Si la biblioteca incluye la función TCP/IP dual, este comando también activa SNMP en el puerto 2A.

     ```
     snmp enable port2b
     ```

- Para las bibliotecas SL500, active SNMP en el puerto 1B.

  ```
  snmp enable port1B
  ```

Con SL Console (solo SL500)

1. En el menú **Tools** (Herramientas), seleccione **System Detail** (Detalle del sistema).
2. En el árbol de navegación, seleccione **Library** (Biblioteca).
3. Seleccione el separador **SNMP** y, a continuación, seleccione el separador **Port Control** (Control de puertos).
4. Complete la sección Port Control (Control de puertos) de la siguiente manera:

   Port (Puerto): seleccione *Public (1B)* (Público [1B]).

   Command (Comando): seleccione *Enable* (Activar).
5. Haga clic en **Apply** (Aplicar).

Con la interfaz de usuario de SL150

1. En el árbol de navegación, seleccione **SNMP**.
2. Si SNMP aparece desactivado, seleccione **Enable SNMP** (Activar SNMP).
3. En la ventana de confirmación, haga clic en **OK** (Aceptar).

5.2.3. Uso de un usuario SNMP v2c

Para el intercambio inicial entre la biblioteca y el servidor de STA, se necesita un usuario de SNMP v2c. También se lo necesita si se desea usar SNMP v2c para la comunicación de STA. Consulte Sección 5.1, “Descripción de la configuración de SNMP de bibliotecas para STA” para obtener detalles.

Tenga en cuenta los siguientes requisitos de configuración:

- Debe haber solo un usuario de SNMP v2c en la biblioteca.
- La cadena de la comunidad de SNMP v2c puede contener solo caracteres alfanuméricos (a-z, A-Z, 0-9). No se permiten caracteres especiales.
- Los usuarios de SNMP v2c existentes normalmente están configurados en la comunidad *public* (pública), pero pueden estar definidos en otro nombre de comunidad.
- No debe eliminar los usuarios de SNMP v2c *public* (públicos) existentes sin consultar antes con el soporte de Oracle. En algunos casos, se necesita un usuario de SNMP v2c *public* (público) para la plataforma de prestación de servicios (SDP) de Oracle.

Con la CLI de la biblioteca (todas las bibliotecas, excepto SL150)

1. Determine si ya existe un usuario de SNMP v2c.

   ```
   snmp listUsers
   ```

2. Si ya hay definido un usuario de SNMP v2c, como en el siguiente ejemplo, puede salir de la tarea. De lo contrario, continúe con el siguiente paso.

```
SL500> snmp listUsers
 ...
 Attributes Community public
 Index 1
 Version v2c
 Object Snmp snmp
 ...
```

3. Agregue el usuario de SNMP v2c.

```
snmp addUser version v2c community community_name
```

Donde *community_name* es *public* u otro nombre. Por ejemplo:

```
SL3000> snmp addUser version v2c community public
```

4. Genere la lista de usuarios de SNMP nuevamente para verificar que el usuario de SNMP v2c se haya agregado correctamente.

```
snmp listUsers
```

Con SL Console (solo SL500)

1. En el menú **Tools** (Herramientas), seleccione **System Detail** (Detalle del sistema).
2. En el árbol de navegación, seleccione **Library** (Biblioteca).
3. Seleccione el separador **SNMP** y, a continuación, seleccione el separador **Add Users** (Agregar usuarios).
4. Si ya hay un usuario de SNMP v2c en la sección Users (Usuarios), puede salir de esta tarea. De lo contrario, continúe con el siguiente paso.
5. Para agregar el usuario de SNMP v2c, complete el separador **Add Users** (Agregar usuarios) de la siguiente manera:
   - *Version* (Versión): seleccione *v2c*.
   - *Community* (Comunidad): especifique una cadena de comunidad (por ejemplo, *public*).
6. Haga clic en **Apply** (Aplicar).

De forma predeterminada, el modelo SL150 no viene con un usuario de SNMP v2c definido. Si planea usar SNMP v2c para las comunicaciones de STA, cree un usuario de SNMP v2c como se indica a continuación.

Con la interfaz de usuario de SL150

1. En el árbol de navegación, seleccione **SNMP**.
2. En la sección (o el separador) SNMP Users (Usuarios de SNMP), seleccione **Add SNMP User** (Agregar usuario de SNMP).
3. En la pantalla Add SNMP User (Agregar usuario de SNMP), complete la información de la siguiente manera:

   Version (Versión): seleccione *v2c*.

   Community Name (Nombre de comunidad): especifique una cadena de comunidad (por ejemplo, *public*).
4. Haga clic en **OK** (Aceptar).

5.2.4. Creación de un usuario de SNMP v3

Todos los datos de las capturas SNMP y la base de información de gestión (MIB) se envían al servidor de STA por medio del usuario de SNMP v3. Tome nota del nombre de usuario y las contraseñas que especifique, ya que debe usar esta información al definir el destinatario de capturas de SNMP v3.

Tenga en cuenta los siguientes requisitos de configuración:

- El método de autorización debe ser *SHA* (algoritmo de comprobación aleatoria protegido) y el método de privacidad debe ser *DES* (cifrado de datos estándar).
- Todas las bibliotecas supervisadas por una sola instancia de STA deben tener el mismo nombre de usuario de SNMP v3. Debe crear un nuevo usuario que sea único para utilizarse con esta finalidad.
- Las contraseñas de autorización y privacidad deben tener, por lo menos, ocho caracteres y no puede incluir coma, punto y coma ni el signo igual.

Con la CLI de la biblioteca (todas las bibliotecas, excepto SL150)

1. Cree un usuario de SNMP v3:

   ```
   snmp addUser version v3 name name auth SHA authPass auth_password priv DES
    privPass priv_password
   ```

   Donde:
   - *name* es el nombre de usuario de SNMP v3.
   - *auth_password* y *priv_password* son la contraseña de autorización y la contraseña de privacidad, respectivamente.

   Nota:

   Para las bibliotecas SL3000 y SL8500, escriba todas las variables entre comillas simples (Ejemplo 5.1, “Creación de usuario de SNMP v3 en SL3000 o SL8500”).

Ejemplo 5.1. Creación de usuario de SNMP v3 en SL3000 o SL8500

```
SL3000> snmp addUser version v3 name 'STAsnmp' auth SHA authPass 'authpwd1' priv
 DES privPass 'privpwd1'
```

Ejemplo 5.2. Creación de usuario de SNMP v3 en SL500

```
SL500> snmp addUser version v3 name STAsnmp auth SHA authPass authpwd1 priv DES
 privPass privpwd1
```

2. Genere la lista de usuarios de SNMP para verificar que el usuario de SNMP v3 se haya agregado correctamente.

   ```
   snmp listUsers
   ```

Con SL Console (solo bibliotecas SL500)

1. En el menú **Tools** (Herramientas), seleccione **System Detail** (Detalle del sistema).
2. En el árbol de navegación, seleccione **Library** (Biblioteca).
3. Seleccione el separador **SNMP** y, a continuación, seleccione el separador **Add Users** (Agregar usuarios).
4. Complete el separador **Add Users** (Agregar usuarios) de la siguiente manera:
   - *`Version`* (Versión): seleccione *`v3`*.
   - *`UserName`* (Nombre de usuario): nombre del usuario de SNMP v3.
   - *`Auth`* (Autorización): seleccione *`SHA`*.
   - *`AuthPass`* (Contraseña de autorización): especifique una contraseña de autorización.
   - *`Priv`* (Privacidad): seleccione *`DES`*.
   - *`PrivPass`* (Contraseña de privacidad): especifique una contraseña de privacidad.
5. Haga clic en **Apply** (Aplicar).

Con la interfaz de usuario de SL150

1. En el árbol de navegación, seleccione **SNMP**.
2. En la sección SNMP Users (Usuarios de SNMP), seleccione **Add SNMP User** (Agregar usuario de SNMP).
3. Para la versión, seleccione *`v3`* y, a continuación, complete la información de la siguiente manera:
   - *`User Name`* (Nombre de usuario): nombre del usuario de SNMP v3.
   - *`Authentication Protocol`* (Protocolo de autenticación): seleccione *`SHA`*.
   - *`Authentication Passphrase`* (Frase de contraseña de autenticación): especifique una contraseña de autorización.
   - *`Privacy Protocol`* (Protocolo de privacidad): seleccione *`DES`*.

- *Privacy Passphrase* (Frase de contraseña de privacidad): especifique una contraseña de privacidad.

4. Haga clic en **OK** (Aceptar).

5.2.5. Recuperación del ID del motor de SNMP de la biblioteca (todas las bibliotecas, excepto SL150)

Use este procedimiento para mostrar el ID del motor de SNMP de la biblioteca (por ejemplo, 0x81031f88804b7e542f49701753).

Este procedimiento se realiza con la CLI de la biblioteca.

1. En función del modelo de biblioteca, use uno de los siguientes comandos:
   - Para bibliotecas SL3000 y SL8500:

     ```
     snmp engineId print
     ```

   - Para bibliotecas SL500:

     ```
     snmp engineId
     ```

2. Guarde el ID del motor en un archivo de texto para utilizarlo en las tareas de configuración de SNMP restantes.

5.2.6. Creación del destinatario de capturas de SNMP v3 de STA

Use este procedimiento para definir el servidor de STA como destinatario autorizado de capturas SNMP y para definir las capturas que envía la biblioteca.

Tenga en cuenta los siguientes requisitos de configuración:

- Para evitar registros duplicados, no defina el servidor de STA como destinatario de capturas en varias instancias. Por ejemplo, no cree una definición de destinatario de capturas de SNMP v3 y SNMP v2c para el servidor de STA.
- Los niveles de captura 13 (captura de prueba) y 14 (captura de estado) son nuevos en STA 2.0.x. Es posible que el nivel de captura 4 no sea compatible con versiones de firmware de biblioteca antiguas. Sin embargo, siempre se lo puede especificar al crear destinatarios de capturas.

Con la CLI de la biblioteca (todas las bibliotecas, excepto SL150)

1. Cree un destinatario de capturas de SNMP v3. Use comas para separar los niveles de captura.

```
snmp addTrapRecipient trapLevel 1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100
 host STA_server_IP version v3 name recipient_name auth SHA authPass auth_password
 priv DES privPass priv_password engineId library_engineID
```

Donde:

- *STA_server_IP* es la dirección IP del servidor de STA.
- *recipient_name* es el nombre de usuario de SNMP que creó en Sección 5.2.4, “Creación de un usuario de SNMP v3” [82].
- *auth_password* y *priv_password* son las contraseñas de autorización y privacidad que creó en Sección 5.2.4, “Creación de un usuario de SNMP v3” [82].
- *library_engineID* es el ID del motor de la biblioteca que visualizó en Sección 5.2.5, “Recuperación del ID del motor de SNMP de la biblioteca (todas las bibliotecas, excepto SL150)” [84], incluido el prefijo 0x.

Nota:

Para bibliotecas SL3000 y SL8500, escriba los valores de *recipient_name*, *auth_password* y *priv_password* entre comillas simples (Ejemplo 5.3, “Creación de destinatario de capturas de SNMP v3 en SL3000 o SL8500”).

Ejemplo 5.3. Creación de destinatario de capturas de SNMP v3 en SL3000 o SL8500

```
SL3000> snmp addTrapRecipient trapLevel
 1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100 host 192.0.2.20 version v3
 name 'STAsnmp' auth SHA authPass 'authpwd1' priv DES privPass 'privpwd1' engineId
 0x00abcdef000000000000000000
```

Ejemplo 5.4. Creación de destinatario de capturas de SNMP v3 en SL500

```
SL500> snmp addTrapRecipient trapLevel
 1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100 host 192.0.2.20 version v3
 name STAsnmp auth SHA authPass authpwd1 priv DES privPass privpwd1 engineId
 0x00abcdef000000000000000000
```

2. Genere una lista de los destinatarios de capturas y verifique que el destinatario se haya agregado correctamente.

```
snmp listTrapRecipients
```

Con SL Console (solo bibliotecas SL500)

1. En el menú **Tools** (Herramientas), seleccione **System Detail** (Detalle del sistema).
2. En el árbol de navegación, seleccione **Library** (Biblioteca).

3. Seleccione el separador **SNMP** y, a continuación, seleccione el separador **Add Trap Recipients** (Agregar destinatarios de capturas).
4. Complete los campos de la pantalla de destinatarios de capturas de la siguiente manera:
   - *Host*: dirección IP del servidor de STA.
   - *TrapLevel* (Nivel de captura): lista de los niveles de captura que la biblioteca debe enviar a STA, separados por coma: 1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100.
   - *Version* (Versión): seleccione *v3*.
   - *TrapUserName* (Nombre de usuario de captura): nombre de usuario de SNMP que creó en Sección 5.2.4, “Creación de un usuario de SNMP v3” [82].
   - *Auth* (Autorización): seleccione *SHA*.
   - *AuthPass* (Contraseña de autorización): contraseña de autorización que creó en Sección 5.2.4, “Creación de un usuario de SNMP v3” [82].
   - *Priv* (Privacidad): seleccione *DES*.
   - *PrivPass* (Contraseña de privacidad): contraseña de privacidad que creó en Sección 5.2.4, “Creación de un usuario de SNMP v3” [82].
   - *EngineID* (ID de motor): ID de motor de biblioteca que visualizó en Sección 5.2.5, “Recuperación del ID del motor de SNMP de la biblioteca (todas las bibliotecas, excepto SL150)” [84]. No introduzca el prefijo 0x.
5. Haga clic en **Apply** (Aplicar).

Con la interfaz de usuario de SL150

1. En el árbol de navegación, seleccione **SNMP**.
2. En la sección SNMP Trap Recipients (Destinatarios de capturas de SNMP), seleccione **Add Trap Recipient** (Agregar destinatario de capturas).
3. Complete los campos la siguiente manera:
   - *Host Address* (Dirección de host): dirección IP del servidor de STA.
   - *Trap Level* (Nivel de captura): lista de los niveles de captura que la biblioteca debe enviar a STA, separados por coma: 1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100.
   - *Version* (Versión): seleccione *v3*.
   - *Trap User Name* (Nombre de usuario de captura): nombre de usuario de SNMP que creó en Sección 5.2.4, “Creación de un usuario de SNMP v3” [82].
   - *Authentication Protocol* (Protocolo de autenticación): seleccione *SHA*.
   - *Authentication Passphrase* (Frase de contraseña de autenticación): contraseña de autorización que creó en Sección 5.2.4, “Creación de un usuario de SNMP v3” [82].
   - *Privacy Protocol* (Protocolo de privacidad): seleccione *DES*.
   - *Privacy Passphrase* (Frase de contraseña de privacidad): contraseña de privacidad que creó en Sección 5.2.4, “Creación de un usuario de SNMP v3” [82].

- *Engine ID* (ID de motor): este campo se proporciona automáticamente. No modifique el valor.

4. Haga clic en **OK** (Aceptar).

6

Configuración de conexiones de bibliotecas en STA

Para que STA supervise las bibliotecas de la organización, debe realizar algunas actividades de configuración en las bibliotecas y algunas en el servidor de STA. En este capítulo, se describen las actividades que se realizan en el servidor de STA.

En este capítulo, se incluye la siguiente sección:

6.1. Tareas de configuración de STA

Debe completar los procedimientos en el orden indicado. Después de haber completado este proceso, STA puede comenzar a supervisar las bibliotecas y realizar análisis.

6.1.1. Inicio de sesión en STA

Use este procedimiento para iniciar sesión en STA a fin de realizar los demás procedimientos de esta sección. Consulte las instrucciones completas en *Guía del usuario de STA*.

1. Abra un explorador web compatible en el equipo e introduzca la dirección URL de la aplicación de STA.

   http(s)://*STA_host_name*:*port_number*/**STA/**

   Donde:

   - *host_name* es el nombre de host del servidor de STA.
   - *port_number* es el número de puerto de STA que especificó durante la instalación. El puerto HTTP predeterminado es el 7021; el puerto HTTPS predeterminado es el 7022.

- *STA* debe estar en mayúsculas.

Por ejemplo:

```
https://staserver.example.com:7022/STA/
```

2. En la pantalla de inicio de sesión, introduzca el nombre de usuario y la contraseña de STA.

6.1.2. Verificación de la comunicación de SNMP con una biblioteca

Use este procedimiento para confirmar que la conexión SNMP entre el servidor de STA y una biblioteca sea correcta.

Este procedimiento verifica que los puertos UDP 161 y 162 estén activados en todos los nodos de la red entre el servidor de STA y la biblioteca. No puede validar que se haya especificado correctamente un destinatario de captura SNMP v3.

Realice este procedimiento para cada biblioteca supervisada. Para bibliotecas SL3000 o SL8500 con Redundant Electronics o TCP/IP dual, realice este procedimiento dos veces para la biblioteca: una vez para la dirección IP principal de la biblioteca y una vez para la dirección IP secundaria.

Nota:

Este procedimiento se realiza desde la línea de comandos del sistema en el servidor de STA.

1. Abra una ventana de terminal en el servidor de STA e inicie sesión como usuario root del sistema.
2. Pruebe la conexión de SNMP v3. Los valores que especifique deben coincidir con los correspondientes en la biblioteca.

```
# snmpget –v3 –u SNMP_user –a SHA –A auth_pwd –x DES –X priv_pwd –l
 authPriv library_IP_addr 1.3.6.1.4.1.1211.1.15.3.1.0
```

Donde:

- *v3* indica SNMP v3.
- *SNMP_user* es el nombre de usuario de SNMP v3.
- *SHA* indica el protocolo de autenticación.
- *auth_pwd* es la contraseña de autorización.
- *DES* indica el protocolo de privacidad.
- *priv_pwd* es la contraseña de privacidad.
- *authPriv* indica que se aplica privacidad en el comando.

- *library_IP_addr* es la dirección IP del puerto público en la biblioteca.
  - Para bibliotecas SL150, es el puerto de red 1.
  - Para bibliotecas SL500, es el puerto 1B.
  - Para bibliotecas SL3000 y SL8500, puede ser necesario probar varios puertos, en función de la activación de TCP/IP dual o Redundant Electronics en la biblioteca. Si hay varios puertos, ejecute este comando para cada dirección IP.
- *1.3.6.1.4.1.1211.1.15.3.1.0*: es el identificador de objeto (OID) de SNMP de la biblioteca, que es el mismo para todos los modelos de bibliotecas.

  Si la salida del comando muestra el modelo de biblioteca, la prueba se realizó correctamente. Algunos ejemplos de comandos:

  Ejemplo 6.1. Comando snmpget correcto

  ```
  # snmpget –v3 –u STAsnmp –a SHA –A authpwd1 –x DES –X privpwd1 –l authPriv 192.0.2.20 1
  .3.6.1.4.1.1211.1.15.3.1.0
  SNMPv2–SMI::enterprises.1211.1.15.3.1.0 =STRING: "SL8500"
  ```

  Ejemplo 6.2. Comando snmpget con errores: se agotó el timeout de la red

  ```
  # snmpget –v3 –u STAsnmp –a SHA –A authpwd1 –x DES –X privpwd1 –l authPriv 192.0.2.20 1
  .3.6.1.4.1.1211.1.15.3.1.0
  Timeout: No Response from 192.0.2.20.
  ```

  Ejemplo 6.3. Comando snmpget con errores: contraseña no válida

  ```
  # snmpget –v3 –u WrongUsr –a SHA –A authpwd1 –x DES -X WrongPwd -l authPriv 192.0.2.20
   1.3.6.1.4.1.1211.1.15.3.1.0
  snmpget: Authentication failure (incorrect password, community or key)
  ```

3. Pruebe la conexión de SNMP v2c.

   ```
   # snmpget –v2c –c public –l authPriv library_IP_addr
   ```

   Donde:
   - *v2c* indica SNMP v2c.
   - *public* indica la cadena de comunidad.
   - *authPriv* indica que se aplica privacidad en el comando.
   - *library_IP_addr* es la dirección IP del puerto público en la biblioteca.
4. Si ambas pruebas de la conexión SNMP son correctas, puede salir de este procedimiento. Si alguna de las pruebas tiene errores, continúe con el paso siguiente para resolver posibles problemas de red, según sea necesario.
5. Confirme la ruta de los paquetes desde el servidor de STA a la biblioteca.

   ```
   # traceroute –I library_IP_addr
   ```

Donde:

- *-I* ("I" mayúscula) indica que se deben usar paquetes de solicitudes de eco de ICMP (protocolo de mensajes de control de Internet) en lugar de datagramas de UDP (protocolo de datagramas de usuario).
- *library_IP_addr* es la dirección IP del puerto público en la biblioteca.

La salida muestra el número de saltos y el tiempo de ida y vuelta para llegar a cada uno. El tiempo de ida y vuelta (la última línea de la salida del comando) debe ser menos de un segundo. Si no lo es, confirme el rendimiento de la red con el administrador de la red.

6. Supervise los paquetes TCP/IP enviados entre el servidor STA y la biblioteca.

```
# tcpdump –v host library_IP_addr > /var/tmp/file_name &
```

Donde:

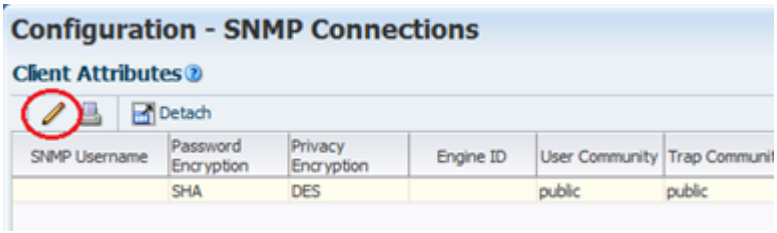
- *-v* indica salida detallada.
- *host* indica que solo se deben recopilar los paquetes provenientes del host indicado o enviados al host indicado (en este caso, la biblioteca).
- *library_IP_addr* es la dirección IP del puerto público en la biblioteca.
- *file_name* es el nombre del archivo en el que se guarda la salida.

6.1.3. Configuración de los parámetros del cliente de SNMP para STA

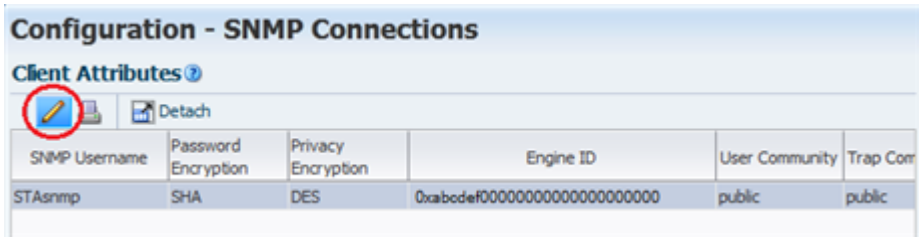
Use este procedimiento para agregar o modificar valores de configuración del cliente de SNMP para STA. Estos valores de configuración permiten a STA recibir datos de SNMP de una o varias bibliotecas.

Hay solo una entrada de cliente de SNMP por cada instancia de STA en su sitio.

1. En el separador **Setup & Administration** (Configuración y administración), seleccione **Configuration** (Configuración) y, a continuación, seleccione **SNMP Connections** (Conexiones SNMP).
2. Siga estos pasos:
   - Para la configuración inicial del cliente, seleccione la fila vacía de la tabla Client Attributes (Atributos de cliente) y, a continuación, haga clic en **Edit** (Editar).



- Para modificar la configuración existente del cliente, seleccione la entrada deseada en la tabla Client Attributes (Atributos de cliente) y, a continuación, haga clic en **Edit** (Editar).



Aparece el cuadro de diálogo Define SNMP Client Settings (Definir configuración de cliente SNMP). Si se trata de una nueva configuración, los campos están vacíos.

3. Complete el cuadro de diálogo del siguiente modo. Los valores que especifique deben coincidir con los correspondientes en las bibliotecas.

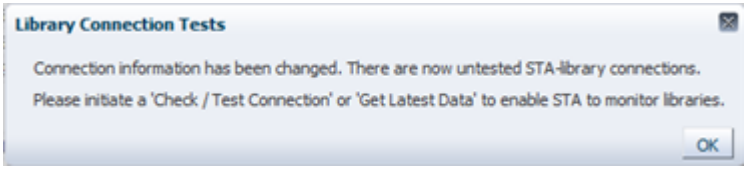
Nota:

Aunque STA supervisará solamente las bibliotecas configuradas para comunicaciones SNMP v2c, debe completar todos los campos, incluidos los correspondientes a SNMP v3. No puede dejar ningún campo en blanco.

- *`STA SNMP Connection Username (Auth)`* (Nombre de usuario de conexión SNMP de STA [autenticación]): escriba el nombre de usuario de SNMP v3.
- *`Enter STA SNMP Connection Password (Auth)`* (Introducir contraseña de conexión SNMP de STA [autenticación]): escriba la contraseña de autorización de conexión.
- *`Enter Privacy Encryption Password (Privacy)`* (Introducir contraseña de cifrado de privacidad [privacidad]): escriba la contraseña de cifrado de privacidad.
- *`User Community`* (Comunidad de usuarios): este campo es necesario para el establecimiento de comunicación de SNMP con la biblioteca o, si está usando SNMP v2c, para la comunicación de STA con la biblioteca. Escriba el nombre de comunidad especificado en la biblioteca. El valor predeterminado es *`public`* (público).
- *`Trap Community`* (Comunidad de captura): se utiliza solamente si se usa SNMP v2c para la comunicación con la biblioteca. Si está usando SNMP v3, deje el valor predeterminado, *`public`* (público). Si está usando SNMP v2c, escriba el nombre de comunidad de captura especificado en la biblioteca.

4. Haga clic en **Save** (Guardar).

   El registro de configuración se actualiza y aparece un mensaje que indica que debe realizar una prueba de la conexión de la biblioteca para establecer o restablecer la comunicación de SNMP con las bibliotecas.



5. Haga clic en **OK** (Aceptar) para descartar el mensaje.

6.1.4. Configuración de la conexión SNMP con una biblioteca

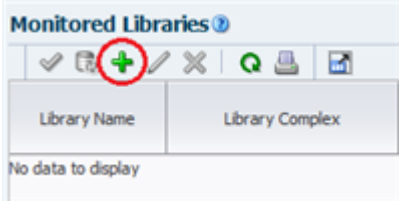
Use este procedimiento para configurar una conexión SNMP con cada biblioteca que desea que STA supervise o para modificar una conexión existente. Para conexiones existentes, *debe* realizar este procedimiento si hay cambios en alguno de los valores de configuración de SNMP en una biblioteca supervisada, por ejemplo, un cambio de la dirección IP de la biblioteca.

Nota:

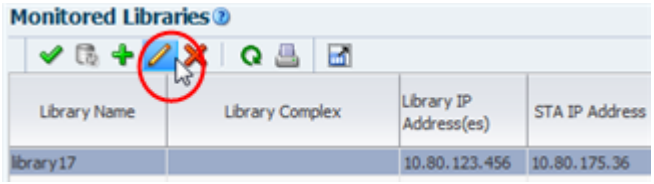
Si está configurando varias conexiones de biblioteca simultáneamente, para minimizar las interrupciones a la biblioteca, complete este procedimiento para todas las bibliotecas antes de probar las conexiones SNMP.

1. En el separador **Setup & Administration** (Configuración y administración), seleccione **Configuration** (Configuración) y, a continuación, seleccione **SNMP Connections** (Conexiones SNMP).
2. Siga estos pasos:

- Para la configuración inicial de una conexión con una biblioteca, haga clic en **Add** (Agregar) en la barra de herramientas Monitored Libraries (Bibliotecas supervisadas).



- Para modificar una conexión de biblioteca existente, seleccione la biblioteca en la tabla Monitored Libraries (Bibliotecas supervisadas) y, a continuación, haga clic en **Edit** (Editar).



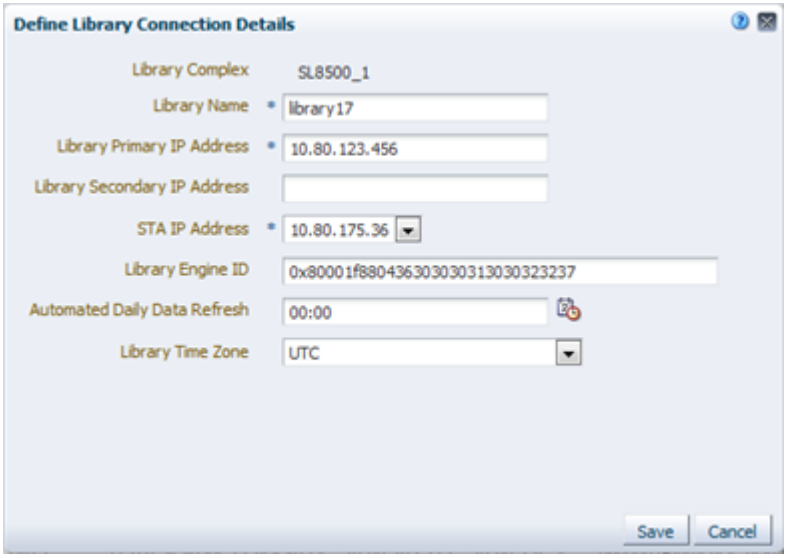
Aparece el cuadro de diálogo Define Library Connection Details (Definir detalles de conexión de biblioteca). Si se trata de una nueva conexión de biblioteca, los campos están vacíos.

3. Complete el cuadro de diálogo del siguiente modo. Los valores que especifique deben coincidir con los correspondientes en la biblioteca.
   - *`Library Name`* (Nombre de biblioteca): escriba un nombre para identificar la biblioteca en todas las pantallas de la interfaz de usuario de STA (por ejemplo, el nombre de host de la biblioteca).
   - *`Library Primary IP Address`* (Dirección IP principal de la biblioteca): escriba la dirección IP del puerto público principal de la biblioteca. No se puede especificar la dirección IP de otra biblioteca supervisada.
   - *`Library Secondary IP Address`* (Dirección IP secundaria de la biblioteca): se usa solo con bibliotecas SL3000 y SL8500 que usan TCP/IP dual o Redundant Electronics. Especifique la dirección IP del puerto público secundario de la biblioteca. No se puede especificar la dirección IP de otra biblioteca supervisada. Para todas las demás bibliotecas, incluidos todos los modelos SL500 y SL150, deje el campo en blanco.
   - *`STA IP Address`* (Dirección IP de STA): seleccione la dirección IP del servidor de STA.
   - *`Library Engine ID`* (ID de motor de biblioteca): no modifique este campo. Es el ID de motor de SNMP único de la biblioteca y se proporciona automáticamente cuando se establece la conexión inicial entre STA y la biblioteca. En el caso de conexiones nuevas, está en blanco.
   - *`Automated Daily Data Refresh`* (Refrescamiento de datos diario automatizado): especifica la hora del día a la que desea que STA recopile los datos de configuración más recientes de la biblioteca. Los datos se recopilan automáticamente cada 24 horas a esta hora. Debe elegir una hora a la que normalmente no se use mucho la biblioteca. La hora predeterminada es 00.00 (12.00 a. m.). Use el formato de 24 horas.

Precaución:

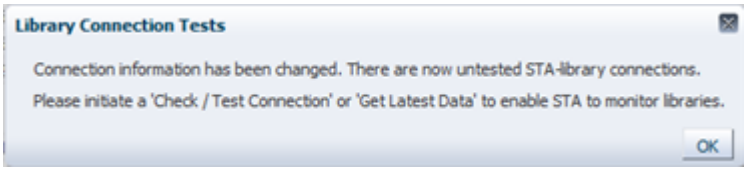
Si deja este campo en blanco, se desactiva la recopilación automática programada de los datos de la biblioteca. En este caso, los datos de configuración de la biblioteca de STA no estarán sincronizados con la biblioteca.

- *Library Time Zone* (Zona horaria de la biblioteca): seleccione la zona horaria local de la biblioteca.



4. Haga clic en **Save** (Guardar).

   El registro de configuración se actualiza y aparece un mensaje que indica que debe realizar una prueba de la conexión de la biblioteca para establecer o restablecer la comunicación de SNMP con las bibliotecas.



5. Haga clic en **OK** (Aceptar) para descartar el mensaje.

   Si modificó una conexión de la biblioteca existente, el campo Library Engine ID (ID de motor de biblioteca) de la tabla Monitored Libraries (Bibliotecas supervisadas) aparecerá vacío, lo que indica que se perdió la conexión SNMP.

6.1.5. Prueba de la conexión SNMP de una biblioteca

Use este procedimiento para probar la conexión SNMP entre STA y una biblioteca y establecer o restablecer la comunicación. Para evitar que se pierda la conexión y la pérdida de capturas de SNMP, debe realizar este procedimiento para cada biblioteca supervisada cada vez que agregue o modifique la configuración de SNMP para la biblioteca o el cliente STA.

Puede probar solo una conexión de biblioteca a la vez.

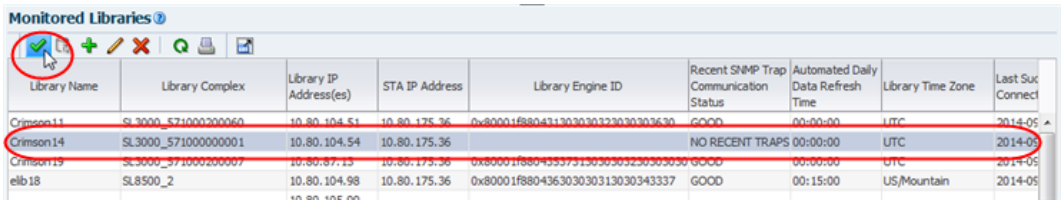
Nota:

Como la ejecución de una prueba de conexión puede ocasionar una pérdida momentánea de paquetes de SNMP entrantes, debe realizar este procedimiento solo si es absolutamente necesario.

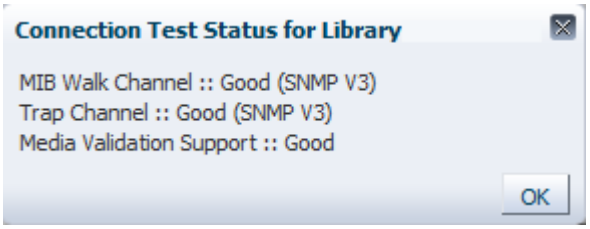
Nota:

Antes de realizar este procedimiento, tal vez sea conveniente verificar que la biblioteca esté funcionando.

1. En el separador **Setup & Administration** (Configuración y administración), seleccione **Configuration** (Configuración) y, a continuación, seleccione **SNMP Connections** (Conexiones SNMP).
2. En la tabla de bibliotecas supervisadas, seleccione una biblioteca y, a continuación, haga clic en **Check / Test Connection** (Comprobar/probar conexión).

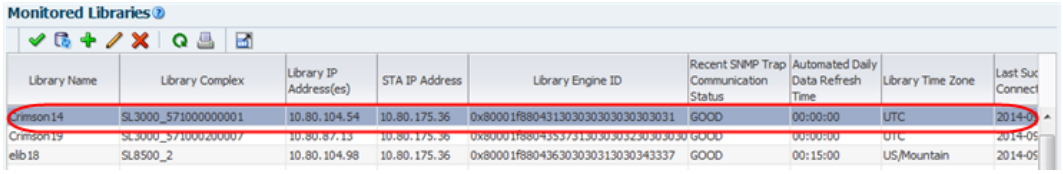


Aparece el cuadro de mensaje de estado de prueba de conexión, en el que se muestran los resultados correspondientes a las pruebas de canal de conexión de MIB, canal de captura y compatibilidad de validación de medios.



3. Haga clic en **OK** (Aceptar) para descartar el cuadro de mensaje.

La tabla Monitored Libraries (Bibliotecas supervisadas) se actualiza con los resultados de la prueba.



- Si el campo *`Library Complex`* (Complejo de bibliotecas) está en blanco, se lo proporcionará después de que se realice una recopilación de datos manual.
- *`Library Engine ID`* (ID de motor de biblioteca) indica el ID de motor SNMP único para la biblioteca.
- *`Last Connection Attempt`* (Último intento de conexión) indica la fecha y la hora en las que se inició la prueba de conexión.

- *Last Successful Connection* (Última conexión correcta) indica la fecha y la hora en las que se finalizó la prueba de conexión, si la prueba fue correcta.
- *Last Connection Status* (Estado de última conexión) indica el resultado de la prueba. Si la prueba tiene errores, STA proporciona información en el campo *Last Connection Failure Detail* (Detalle de error de última conexión). (Tal vez tenga que ampliar el ancho de la columna para ver el valor completo).

Nota:

Si el error de la prueba se debe a que se alcanzó el timeout, repita este procedimiento durante un período en el que haya menos actividad en la biblioteca. Cuando finalice la prueba, puede comparar los registros de fecha y hora para verificar que la biblioteca esté proporcionando información actual.

6.1.6. Realización de una recopilación de datos manual

Use este procedimiento para iniciar una recopilación de datos manual para una biblioteca y recibir los datos de configuración más recientes de la biblioteca. Si este procedimiento se completa correctamente, STA comienza a supervisar la biblioteca y a realizar análisis de los datos.

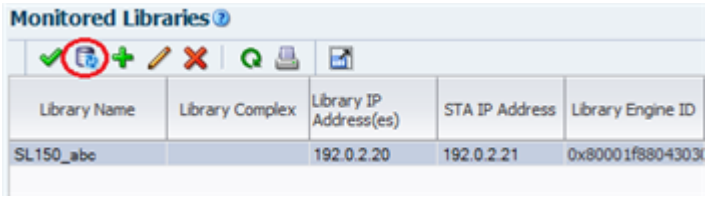
Si bien STA realiza una recopilación de datos automáticamente cada 24 horas a la hora programada, se debe realizar una recopilación de datos manual para cada biblioteca supervisada cada vez que se agregue o se cambie un valor de configuración de SNMP de la biblioteca o el cliente de STA.

Las recopilaciones de datos pueden tardar desde varios minutos hasta una hora, según el tamaño de la biblioteca.

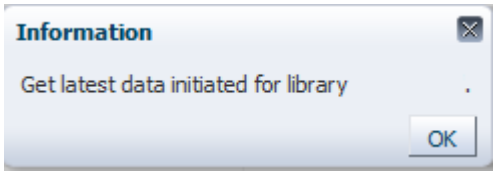
Nota:

Puede ejecutar varias recopilaciones de datos de manera simultánea, pero se las debe iniciar de a una. Repita este procedimiento tantas veces como sea necesario; seleccione una biblioteca diferente cada vez.

1. En el separador **Setup & Administration** (Configuración y administración), seleccione **Configuration** (Configuración) y, a continuación, seleccione **SNMP Connections** (Conexiones SNMP).
2. Seleccione una biblioteca en la tabla Monitored Libraries (Bibliotecas supervisadas) y, a continuación, haga clic en **Get latest data** (Obtener datos más recientes). Se puede seleccionar solo una biblioteca a la vez.



Aparece un cuadro mensaje de confirmación.



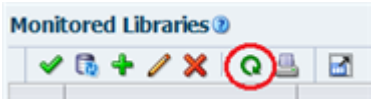
3. Haga clic en **OK** (Aceptar) para descartar el cuadro de mensaje.

   La recopilación de datos se realiza y la tabla Monitored Libraries (Bibliotecas supervisadas) se actualiza con los resultados.

   - *`Library Complex`* (Complejo de bibliotecas) indica el ID del complejo de bibliotecas.
   - *`Library Engine ID`* (ID de motor de biblioteca) indica el ID de motor SNMP único para la biblioteca.
   - *`Last Connection Attempt`* (Último intento de conexión) indica la fecha y la hora en las que se inició la recopilación de datos.
   - *`Last Successful Connection`* (Última conexión correcta) indica la fecha y la hora en las que se finalizó la recopilación de datos, si fue correcta.
   - *`Last Connection Status`* (Estado de última conexión) se actualiza de la siguiente manera:
     - *`IN PROGRESS`* (En curso): el proceso de recopilación de datos se está ejecutando.
     - *`SUCCESS`* (Correcto): la recopilación de datos se realizó correctamente. STA comienza a recibir datos de intercambio provenientes de la biblioteca.
     - *`FAILED`* (Error): el proceso de recopilación de datos no se realizó correctamente. Si es posible, STA proporciona información en el campo *`Last Connection Failure Detail`* (Detalle de error de última conexión). (Tal vez tenga que ampliar el ancho de la columna para ver el valor completo).

     Nota:

     El estado se actualiza cada cuatro minutos y el intervalo de refrescamiento predeterminado de la pantalla es 480 segundos. Sin embargo, puede hacer clic en el botón **Refresh Table** (Refrescar tabla) para forzar el refrescamiento de la tabla cuando lo desee.

   - El campo *`Recent SNMP Trap Communication Status`* (Estado de comunicación de captura SNMP reciente) puede indicar de manera intermitente *`MISSED HEARTBEAT`* (Latido perdido). Esto es normal.

7

Configuración de los servicios de STA

Use estos procedimientos para configurar el servicio de copia de seguridad de STA y las utilidades de servicio de supervisión de recursos de STA.

En este capítulo, se incluyen las siguientes secciones:

7.1. Descripción general de los servicios de STA

- Servicio de copia de seguridad de bases de datos de STA: para configurar el servicio de copia de seguridad de STA, se usa la utilidad de administración *staservadm*. Para mostrar una lista completa de las opciones de comandos para la utilidad, escriba *staservadm -h*. Consulte la *Guía de administración de STA* para obtener detalles.
- Servicio de supervisión de recursos de STA: para configurar el servicio de supervisión de recursos de STA, se usa la utilidad de administración *staresmonadm*. Para mostrar una lista completa de las opciones de comandos para la utilidad, escriba *staresmonadm -h* en la línea de comandos. Consulte *Guía de administración de STA* para obtener detalles.

Estas utilidades de servicio se encuentran en el directorio */Oracle_storage_home/StorageTek_Tape_Analytics/common/bin*. Consulte Sección 3.1, “Usuarios, grupos y ubicaciones usados por el instalador de STA” para obtener detalles sobre el directorio raíz de almacenamiento de Oracle.

7.2. Tareas de configuración de los servicios de STA

Tareas generales

Tareas de configuración de copia de seguridad de bases de datos de STA

- Sección 7.2.6, “Configuración del servicio de copia de seguridad de bases de datos de STA”

Tareas de configuración de supervisión de recursos de STA

- Sección 7.2.7, “Revisión de las preferencias de la utilidad de supervisión de recursos de STA”
- Sección 7.2.8, “Configuración del supervisor de recursos de STA”

7.2.1. Actualización de la ruta de acceso del sistema (opcional)

Use este procedimiento para asegurarse de que el directorio bin de STA esté incluido en la variable *PATH* para el usuario root del sistema. El directorio bin incluye las utilidades de servicio de STA, *staservadm* y *staresmonadm*.

a. Abra una sesión de terminal en el servidor actual de STA e inicie sesión como usuario root del sistema.
b. Use un editor de texto para abrir el perfil del usuario. Por ejemplo:

```
# vi /root/.bash_profile
```

c. Agregue el directorio bin de STA a la definición de *PATH*. Por ejemplo, agregue la siguiente línea al archivo:

```
PATH=$PATH:Oracle_storage_home/StorageTek_Tape_Analytics/common/bin
```

Donde *Oracle_storage_home* es la ubicación del directorio raíz de almacenamiento de Oracle especificada durante la instalación de STA.
d. Guarde el archivo y ciérrelo.
e. Cierre sesión y vuelva a iniciar sesión como usuario root del sistema.
f. Confirme que la variable *PATH* se haya actualizado correctamente.

```
# echo $PATH
/usr/lib64/qt-3.3/bin:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/
bin:/root/bin:/Oracle/StorageTek_Tape_Analytics/common/bin
```

7.2.2. Reinicio del daemon de servicios de STA (opcional)

Use este procedimiento para reiniciar el daemon de servicios de STA, *staservd*.

Este procedimiento es útil si modificó los valores de configuración de los servicios de copia de seguridad o supervisión de recursos de STA y desea que la nueva configuración entre en efecto de inmediato. Si no usa este procedimiento, la nueva configuración entrará en efecto cuando el servicio salga del intervalo de inactividad y procese los nuevos valores.

1. Detenga el daemon de servicios de STA.

```
# STA stop staservd
```

2. Inicie el daemon de servicios de STA.

```
# STA start staservd
```

3. Muestre el estado del daemon para confirmar que se esté ejecutando.

```
# STA status staservd
```

7.2.3. Verificación de la conectividad de la biblioteca

Cuando haya finalizado de configurar los servicios, confirme que todas las bibliotecas configuradas hayan completado las solicitudes de obtención de datos más recientes (el estado de la conexión más reciente debe indicar *SUCCESS*, y STA debería estar recibiendo datos de intercambio provenientes de las bibliotecas). Consulte la *Guía del usuario de STA* para obtener detalles.

7.2.4. Revisión de las preferencias de la utilidad de copia de seguridad de bases de datos de STA

Consulte la Tabla 7.1, “Atributos de la utilidad de administración del servicio de copia de seguridad de STA (staservadm)” para obtener las descripciones de los parámetros de configuración de preferencias disponibles y defina su configuración.

Tabla 7.1. Atributos de la utilidad de administración del servicio de copia de seguridad de STA (staservadm)

Opción	Atributo	Descripción	Valor predeterminado	Su valor
-S, --scp *-F, --ftp*	Tipo de transferencia de archivos	Método de transferencia de archivos usado para copiar los archivos de las copias de seguridad desde el servidor de STA hasta el host de copia de seguridad. Las opciones son SCP (recomendada) o FTP.	SCP	
-T, --time	Hora del volcado de la copia de seguridad completa	Hora del día a la que STA realiza un volcado de copia de seguridad de la base de datos completa. El volcado se realiza automáticamente cada 24 horas aproximadamente a esta hora. La hora real es unos segundos de "intervalo de inactividad" después de esta hora. El formato es *hh:mm*, con formato de 24 horas.	00:00	
-i, --int	Intervalo de inactividad	Cantidad de segundos que el daemon de servicios de STA espera para comprobar la existencia de nuevos archivos de copia de seguridad incremental.	300	
-s, --server	Nombre del host de copia de seguridad	Dirección IPv4 o IPv6 o nombre de host DNS completo del host del servidor en el que el servidor de STA copia los archivos de las copias de seguridad.	N/D	

Opción	Atributo	Descripción	Valor predeterminado	Su valor
-u, --usr	ID de usuario de copia de seguridad	ID del usuario del sistema autorizado a realizar transferencias de archivos SCP al host de copia de seguridad.	N/D	
-p, --pwd	Contraseña de copia de seguridad	Contraseña asignada al usuario de copia de seguridad.	N/D	
-d, --dir	Directorio de copia de seguridad	Directorio del host de copia de seguridad en el que se copian los archivos de las copias de seguridad.	N/D	
-U, --dbusr	Nombre de usuario de base de datos	Nombre de usuario de la base de datos autorizado para ejecutar el comando *mysqldump*. Se debe especificar el nombre de usuario de la cuenta del administrador de la base de datos de STA.	N/D	
-P, --dbpwd	Contraseña de base de datos	Contraseña del nombre de usuario de la base de datos.	N/D	

7.2.5. Configuración del servidor de copia de seguridad de bases de datos remoto

Use este procedimiento para configurar un servidor de copia de seguridad remoto (o equivalente) y recibir los archivos de copia de seguridad comprimidos generados por el servicio de copia de seguridad de bases de datos de STA. Oracle recomienda configurar un servidor de copia de seguridad remoto.

El espacio requerido es variable. El tamaño debe ser múltiplo del tamaño usado para la copia de seguridad local de la base de datos de STA, en función de la cantidad de copias que se deban conservar. El almacenamiento del servidor de copia de seguridad debe duplicarse o segmentarse.

1. En el servidor de copia de seguridad, inicie sesión como usuario root del sistema.
2. Cree un nuevo grupo para el usuario de copia de seguridad de STA. Por ejemplo:

   ```
   # groupadd -g 54321 stabckgr
   ```

   En este ejemplo, el ID del grupo es "stabckgr", y la opción *-g* se usa para especificar un GID numérico.
3. Cree el usuario de copia de seguridad de STA. Por ejemplo:

   ```
   # adduser stabck -c "STA database backup user" -m -d /home/stabck -g stabckgr -s /
   bin/bash -u 98765
   ```

   En este ejemplo, el ID del usuario es "stabck", y se usan las siguientes opciones:
   - *c*: comentario.
   - *m*: crea un directorio raíz para el usuario.
   - *d*: ruta de acceso absoluta del directorio raíz.

- -*g*: asigna el usuario al grupo especificado.
- -*s*: asigna el shell de inicio de sesión especificado al usuario.
- -*u*: asigna el UID numérico especificado al usuario.

4. Asigne una contraseña al usuario de copia de seguridad de STA. Por ejemplo:

```
# passwd stabck
Changing password for user stabck.
New UNIX password: bckpwd1
Retype new UNIX password: bckpwd1
passwd: all authentication tokens updated successfully.
```

5. Cree el directorio en el que se copiarán las copias de seguridad de STA. Por ejemplo:

```
# cd /home/stabck
# pwd
/home/stabck
# mkdir -p STAbackups
# ls
STAbackups
```

   En este ejemplo, se crea el directorio "STAbackups" en el directorio raíz del usuario de copia de seguridad de STA y se usa la opción *-p* para crear directorios principales según sea necesario.

6. Muestre los atributos del usuario para confirmar que la información se haya introducido correctamente. Por ejemplo:

```
# cat /etc/passwd |grep sta
stabck:x:98765:54321:STA database backup user:/home/stabck:/bin/bash
```

7. Asigne al usuario y al grupo de copia de seguridad de STA la propiedad exclusiva del directorio y los derechos de acceso. Por ejemplo:

```
# chown -R stabck:stabckgr STAbackups
# chmod -R 700 STAbackups
# chmod 755 /home/stabck
```

   En este ejemplo, se usa la opción *-R* para asignar de manera recursiva los atributos al directorio y sus archivos.

8. Genere una lista del directorio para confirmar que la información se haya introducido correctamente. Por ejemplo:

```
# ls -la |grep STA
drw------- 2 stabck stabckgr 4096 Oct 19 14:20 STAbackups
```

7.2.6. Configuración del servicio de copia de seguridad de bases de datos de STA

Use este procedimiento para configurar el servicio de copia de seguridad de bases de datos de STA. Puede designar un directorio en el que se copiarán los archivos de las copias de seguridad. Oracle recomienda que este directorio se encuentre en un servidor de copia de seguridad remoto.

Los valores de configuración entran en efecto cuando el servicio sale del intervalo de inactividad actual y procesa la nueva configuración o si se reinicia manualmente el daemon de servicios de STA (Sección 7.2.2, “Reinicio del daemon de servicios de STA (opcional)”).

1. En el servidor de STA, inicie sesión como usuario root del sistema.
2. Use el comando *staservadm -Q* para mostrar la configuración actual del servicio de copia de seguridad de STA.

   En este ejemplo, se muestra que el servicio todavía no está configurado y, por lo tanto, no realiza copias de seguridad.

   ```
   # ./staservadm -Q
   Contacting daemon...connected.
   Querying Preferences.
    Current STA Backup Service Settings:
      Configured            [no]
      File Transfer      -S [SCP]
      Full Backup        -T [00:00]
      Sleep Interval     -i [300 sec]
      Backup Hostname    -s []
      Backup Username    -u []
      Backup Password    -p []
      Backup Directory   -d []
      Database Username  -U []
      Database Password  -P []
   ```

3. Use la Tabla 7.1, “Atributos de la utilidad de administración del servicio de copia de seguridad de STA (staservadm)” como referencia para configurar los valores de los atributos con el comando *staservadm*.

   Puede configurar los atributos mediante comandos independientes o puede combinarlos en uno solo. Por ejemplo:

   ```
   # ./staservadm -S -T 11:00 -i 350 -s stabaksvr -u stabck -p bckpwd1 -d /home/
   stabck/STAbackups -U sta_dba -P password1
   ```

   La utilidad configura cada uno de los valores incluidos en el comando y, a continuación, muestra todos los valores de la configuración actual. Por ejemplo:

```
Contacting daemon...connected.
Setting File Transfer Type... SCP
Setting Sleep Interval..... 350
Setting Backup Hostname..... stabaksvr
Setting Backup Username..... stabck
Setting Backup Password..... *******
Setting Backup Directory..... /home/stabck/STAbackups
Setting Full Backup Time..... 11:00
Setting Database Username.... sta_dba
Setting Database Password.... *********
Done.
 Current STA Backup Service Settings:
   Configured            [yes]
   File Transfer      -S [SCP]
   Full Backup        -T [11:00]
   Sleep Interval     -i [350 sec]
   Backup Hostname    -s [stabaksvr]
   Backup Username    -u [stabck]
   Backup Password    -p [*******]
   Backup Directory   -d [/home/stabck/STAbackups]
   Database Username  -U [sta_dba]
   Database Password  -P [*********]
```

4. Revise la salida del comando para verificar que los valores se hayan configurado correctamente.

7.2.7. Revisión de las preferencias de la utilidad de supervisión de recursos de STA

Consulte las descripciones de las opciones en la Tabla 7.2, “Atributos del supervisor de recursos (staresmonadm) de STA” y defina su configuración. Un valor predeterminado de "-1" indica que el atributo no fue configurado.

Tabla 7.2. Atributos del supervisor de recursos (staresmonadm) de STA

Opción	Atributo	Descripción	Valor predeterminado	Su valor
-T, --time	Hora del informe diario	Hora del día a la que STA envía un informe diario estándar. El informe se envía automáticamente cada 24 horas aproximadamente a esta hora. La hora real es unos segundos de "intervalo de inactividad" después de esta hora. El formato es *hh:mm*, con formato de 24 horas.	00:00	
-i, interval	Intervalo de inactividad	Cantidad de segundos que el supervisor de recursos de STA espera entre un análisis y otro.	300	

Opción	Atributo	Descripción	Valor predeterminado	Su valor
-n, --nag	Modo de insistencia	Indica la frecuencia con la que STA genera alertas si se alcanzan los límites superiores. Si se configura con el valor "on", STA envía correos electrónicos de alerta cada vez que se analiza el sistema. Si se configura con el valor "off", las alertas simplemente se incluyen en el informe diario estándar.	Off (Desactivada)	
-U, --dbusr	Nombre de usuario de base de datos	Nombre de usuario de la base de datos que está autorizado a realizar consultas en las tablas "information_schema" y las variables globales del sistema interno del servidor de MySQL. Debe especificar el nombre de usuario de la cuenta del administrador de la base de datos de STA o el nombre de usuario de la cuenta root de la base de datos de STA (*root*).	N/D	
-P, --dbpwd	Contraseña de base de datos	Contraseña asignada al nombre de usuario de la base de datos.	N/D	
-t, --tblsphwm	HWM del espacio de tablas de la base de datos	Límite superior para el espacio de tablas de la base de datos, introducido como porcentaje del máximo disponible.	-1	
-b, --backvolhwm	HWM de copia de seguridad local	Límite superior para el volumen de copia de seguridad local de base de datos de STA (*/sta_db_backup*), introducido como porcentaje del máximo posible.	-1	
-d, --dbvolhwm	HWM de volumen de disco de base de datos	Límite superior para el volumen de base de datos de STA (*/sta_db/mysql*), introducido como porcentaje del máximo disponible.	*-1*	
-l, --logvolhwm	HWM de volumen de disco de registro	Límite superior para los registros de la base de datos de STA (*/STA_logs/db*), introducido como porcentaje del máximo disponible.	*-1*	
-z, --rootvolhwm	HWM del volumen root	Límite superior para el volumen root (*/*), introducido como porcentaje del máximo disponible.	*-1*	
-x, --tmpvolhwm	HWM de volumen temporario	Límite superior para el volumen del directorio temporario (*/tmp*), introducido como porcentaje del máximo disponible.	*-1*	
-m, --memhwm	HWM de memoria física (RAM)	Límite superior para la memoria total del sistema (excepto por la memoria virtual), introducido como porcentaje del máximo disponible.	*-1*	
-f, --from	Remitente de correo electrónico	Nombre o dirección de correo electrónico que aparece en el campo "From" (De) del correo electrónico del informe diario estándar.	*StaResMon@localhost*	
-r, --recips	Destinatarios de correo electrónico	Direcciones de correo electrónico de los destinatarios, introducidas como lista separada por dos puntos.	N/D	
-s, --subject	Asunto del correo electrónico	Entrada que aparece en el campo "Subject" (Asunto) del correo electrónico del informe diario estándar, hasta 128 caracteres. Use comillas si contiene espacios. Cuando el correo electrónico se envíe, se agrega a la	Informe del supervisor de recursos de STA	

Opción	Atributo	Descripción	Valor predeterminado	Su valor
		entrada un registro de hora en el formato *aaaa-mm-dd hh:mm:ss*.		
-o, --outfile	Archivo de datos de salida	Ruta absoluta del archivo de datos de salida, que es un archivo de valores separados por coma (CSV).	*/STA_logs/db/staresmon.csv* Por ejemplo: */var/log/tbi/db/staresmon.csv*	

7.2.8. Configuración del supervisor de recursos de STA

Use este procedimiento para configurar el servicio de supervisión de recursos de STA. Los valores de configuración entran en efecto cuando el servicio sale del intervalo de inactividad actual y procesa la nueva configuración o si se reinicia manualmente el daemon de servicios de STA (Sección 7.2.2, “Reinicio del daemon de servicios de STA (opcional)”).

1. En el servidor de STA, inicie sesión como usuario root del sistema.
2. Use el comando *staresmonadm -Q* para mostrar la configuración actual del servicio de supervisión de recursos de STA.

   En este ejemplo, se muestra que el servicio todavía no está configurado y por lo tanto no realiza análisis.

```
# ./staresmonadm -Q
Contacting daemon...connected.
Querying Preferences.
 Current STA Resource Monitor Service Settings:
   Configured                        [no]
   Send Reports                   -T [00:00]
   Sleep Interval                 -i [300 sec]
   Alert Nagging                  -n [off]
   DB Username                    -U []
   DB Password                    -P []
   DB Tablespace hwm              -t [-1%]
   DB Backup hwm   (/dbbackup)    -b [-1%]
   DB Data hwm     (/dbdata)      -d [-1%]
   Log Volume hwm  (/var/log/tbi) -l [-1%]
   Root Volume hwm (/)            -z [-1%]
   Tmp Volume hwm  (/tmp)         -x [-1%]
   System Memory hwm              -m [-1%]
   Email 'From:'                  -f [StaResMon@localhost]
   Email 'To:'                    -r []
   Email 'Subject:'               -s [STA Resource Monitor Report]
   Output File                    -o [/var/log/tbi/db/staresmon.csv]
```

3. Use la Tabla 7.2, “Atributos del supervisor de recursos (staresmonadm) de STA” como referencia para configurar los valores de los atributos con el comando *staresmonadm*.

   Puede configurar los atributos mediante comandos independientes o puede combinarlos en uno solo. Por ejemplo:

```
# ./staresmonadm -T 13:00 -i 600 -n on -U sta_dba -P password1 -t 65 -b 65 -d 65 -
l 65 -z 70 -x 80 -m 75 -r john.doe@company.com
```

   La utilidad configura cada uno de los valores incluidos en el comando y, a continuación, muestra todos los valores de la configuración actual. Por ejemplo:

```
Contacting daemon...connected.
Setting DB Tablespace HWM..... 65
Setting DB Disk Volume HWM.... 65
Setting Logging Volume HWM.... 65
Setting Backup Volume HWM..... 65
Setting Root Volume HWM....... 70
Setting Temp Volume HWM....... 80
Setting System Memory HWM..... 75
Setting 'To:' addresses....... john.doe@company.com
Setting Send Time............. 13:00
Setting Sleep Interval........ 600
Setting Alert Nag Mode........ ON
Setting DB Username........... sta_dba
Setting DB Password........... *********
Done.
 Current STA Resource Monitor Service Settings:
   Configured                      [yes]
   Send Reports                 -T [13:00]
   Sleep Interval               -i [600 sec]
   Alert Nagging                -n [on]
   DB Username                  -U [sta_dba]
   DB Password                  -P [*********]
   DB Tablespace hwm            -t [65%]
   DB Backup hwm   (/dbbackup)  -b [65%]
   DB Data hwm     (/dbdata)    -d [65%]
   Log Volume hwm  (/var/log/tbi) -l [65%]
   Root Volume hwm (/)          -z [70%]
   Tmp Volume hwm  (/tmp)       -x [80%]
   System Memory hwm            -m [75%]
   Email 'From:'                -f [StaResMon@localhost]
   Email 'To:'                  -r [john.doe@company.com]
   Email 'Subject:'             -s [STA Resource Monitor Report]
   Output File                  -o [/var/log/tbi/db/staresmon.csv]
```

4. Revise la salida del comando para verificar que los valores se hayan configurado correctamente.

8

Actualización a STA 2.1.0

En este capítulo, se proporcionan instrucciones para actualizar versiones previas de STA a STA 2.1.0. Incluye las siguientes secciones:

Si es la primera vez que instala STA, debe realizar una nueva instalación base. Consulte el Capítulo 3, *Instalación de STA* para obtener instrucciones.

El Apéndice C, *Hojas de trabajo de instalación y actualización* incluye hojas de trabajo que puede usar para organizar las actividades de la actualización y registrar los valores de configuración.

8.1. Descripción general del proceso de actualización

Durante una actualización, los datos existentes de STA se transforman de la versión actual de STA a la versión nueva. La base de datos de STA no será válida para la nueva versión de STA hasta que se hagan estas transformaciones. Después de la actualización, STA procesa los nuevos datos en función del nuevo esquema y las nuevas reglas de análisis de STA. Los datos históricos no se reprocesan.

Antes de comenzar la actualización, lea todas las instrucciones de este capítulo y asegúrese de asignar suficiente tiempo para todo el proceso. Algunas tareas de preparación de la actualización pueden requerir coordinación con otros grupos del sitio, por ejemplo, administración de red. Debe completar todas las tareas de preparación de antemano para poder hacer la actualización en sí en el menor tiempo posible.

Una vez que comienza el proceso de actualización propiamente dicho, no se puede ejecutar STA, y, por lo tanto, la aplicación no recibe la información de intercambio de las bibliotecas supervisadas. Asimismo, la nueva versión de STA no comienza a recibir información de las bibliotecas hasta que se completan todos los pasos de la actualización y se prueba la conexión SNMP con cada biblioteca supervisada.

Nota:

Algunos pasos de la actualización incluyen estimaciones de tiempo, que se proporcionan solo para facilitar la planificación. En función de la capacidad de servidor (cantidad de CPU, velocidad de CPU, velocidad de disco, memoria y espacio de intercambio disponible), el tiempo real puede variar.

8.2. Rutas válidas para la actualización de STA 2.1.0

Puede actualizar a STA 2.1.0 a partir de cualquiera de las siguientes versiones publicadas de STA:

- STA 2.0.x:
  - STA 2.0.0.83
  - STA 2.0.1.4
- STA 1.0.x:
  - STA 1.0.0.99
  - STA 1.0.1.133
  - STA 1.0.2.24

Nota:

Si está actualizando desde STA 1.0.x, debe instalar también una nueva versión de Linux antes de instalar STA 2.1.0. Consulte la *Guía de requisitos de STA* para obtener detalles.

8.3. Métodos de actualización

En función de sus objetivos y los recursos que tenga disponibles, puede realizar la actualización de STA con uno o dos servidores. Las tareas de actualización son en gran medida las mismas con los dos métodos, pero se realizan en diferente orden. Los dos métodos se presentan en las secciones siguientes:

- Sección 8.3.1, “Método de actualización de servidor único”
- Sección 8.3.2, “Método de actualización de dos servidores”

8.3.1. Método de actualización de servidor único

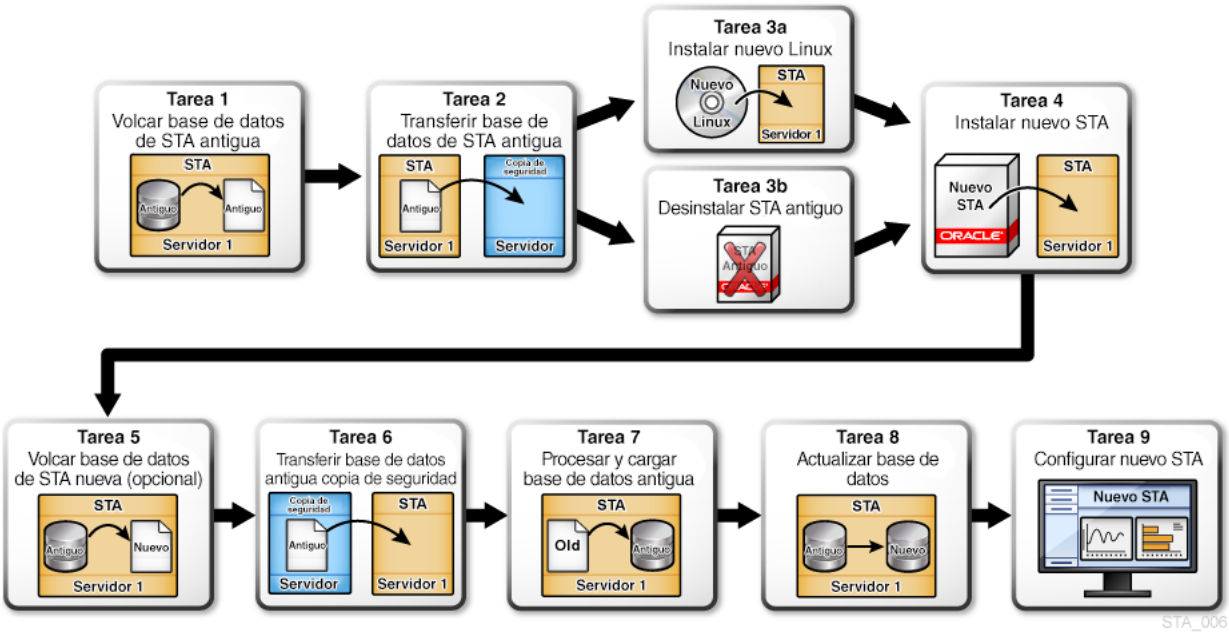
Al usar el método de servidor único, debe desinstalar STA antes de instalar la versión nueva y actualizar la base de datos en el mismo servidor. STA no supervisa las bibliotecas mientras se realiza este proceso.

La ventaja de este método es que no se necesita tener un servidor dedicado adicional para la actualización. Si está actualizando desde STA 2.0.x, no necesita instalar una nueva versión de Linux, por lo que este método puede ser suficiente para sus necesidades.

En la Figura 8.1, “Descripción general de la tarea de actualización de servidor único”, se ilustra el método de servidor único. Las tareas 1 a 9 se realizan en orden secuencial. En resumen:

- Vuelque la base de datos actual y transfiérala a un servidor de copia de seguridad como precaución (Tarea 1 y Tarea 2).
- En función de la versión que tenga actualmente de STA, instale Linux 6.x (Tarea 3a) o desinstale STA 2.0.x (Tarea 3b).
- Instale STA 2.1.0 y, como precaución, vuelque la nueva base de datos (Tarea 4 y Tarea 5).
- Transfiera el volcado de la base de datos antigua desde el servidor de copia de seguridad y, a continuación, cárguelo en la nueva versión de STA y actualícelo (Tarea 6 a Tarea 8).
- Restablezca las conexiones con las bibliotecas supervisadas y realice las tareas de configuración manuales necesarias (Tarea 9). Como se debe desinstalar la versión antigua de STA antes de instalar STA 2.1.0, debe volver a introducir manualmente algunos datos de configuración de usuario.

Figura 8.1. Descripción general de la tarea de actualización de servidor único



8.3.2. Método de actualización de dos servidores

Para el método de actualización de dos servidores, se necesita un segundo servidor dedicado de STA, pero tiene la ventaja de un menor tiempo de inactividad de la aplicación de STA. Este método es particularmente útil si se está actualizando desde STA 1.0.x, ya que la versión antigua de STA puede seguir supervisando las bibliotecas en el servidor antiguo mientras se instalan Linux y la nueva versión de STA en el nuevo servidor.

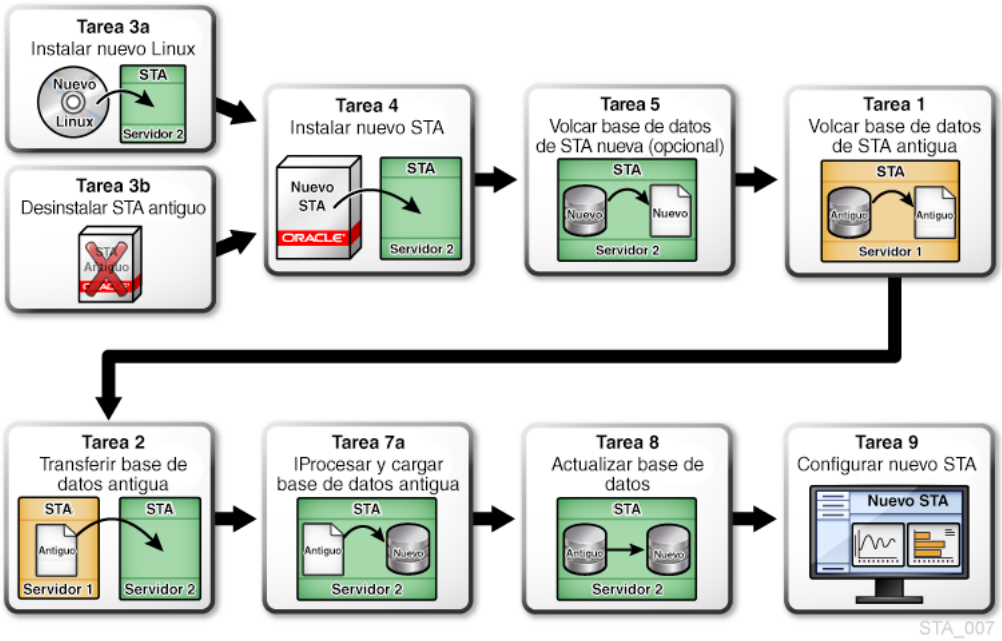
Sin embargo, aun con este método, STA no supervisa las bibliotecas mientras se actualiza la base de datos actual a la nueva versión de STA. La duración de la inactividad depende del tamaño de la base de datos actual.

En la Figura 8.2, “Descripción general de la tarea de actualización de dos servidores”, se ilustra el método de dos servidores. Debe completar las tareas en el orden que se muestra,

no en orden secuencial; la Tarea 6 se omite. Tenga en cuenta que no se hace un volcado de la base de datos actual de STA hasta que se instala la nueva versión de STA en el nuevo servidor. En resumen:

- En función de si el segundo servidor actualmente ejecuta una versión de STA, instale Linux 6.x (Tarea 3a) o desinstale STA 2.0.x (Tarea 3b).
- Instale STA 2.1.0 en el nuevo servidor y, como precaución, haga un volcado de la nueva base de datos (Tarea 4 y Tarea 5).
- Vuelque la base de datos actual en el servidor antiguo y transfiérala al nuevo servidor (Tarea 1 y Tarea 2).
- Cargue la base de datos actual en la nueva versión de STA y actualícela (Tarea 7 y Tarea 8).
- Restablezca las conexiones con las bibliotecas supervisadas y realice las tareas de configuración manuales necesarias (Tarea 9).

Figura 8.2. Descripción general de la tarea de actualización de dos servidores



8.4. Cambios de entorno para STA 2.1.0

A continuación, se presenta un resumen de los cambios del entorno que debe tener en cuenta al planificar la actualización a STA 2.1.0.

8.4.1. Versión de Linux

STA 2.1.0 requiere Linux 6.3 o posterior (consulte la *Guía de requisitos de STA* para obtener detalles). En función de la versión actual de STA, tal vez tenga que instalar una nueva versión de Linux como parte del proceso de actualización de STA.

- Si está actualizando desde STA 1.0.x, debe instalar Linux 6.3 o posterior antes de instalar STA 2.1.0. Linux no admite la actualización en el lugar de Linux 5.x a Linux 6.x; en cambio, usted debe realizar una nueva instalación de Linux 6.x en el servidor de STA.
- Si está actualizando desde STA 2.0.x, ya tiene Linux 6.3 o posterior; sin embargo, debe desinstalar la versión actual de STA antes de instalar STA 2.1.0. También puede tener que instalar o actualizar los paquetes RPM de Linux requeridos. Como parte de la preparación de la actualización, debe asegurarse de que estén instalados todos los niveles de paquetes RPM requeridos, y, como comprobación final, el instalador de STA también le notificará si falta alguno de los paquetes.

8.4.2. Números de puerto predeterminados de WebLogic

Los puertos predeterminados de la consola de administración de WebLogic se cambiaron en STA 2.1.0. Si actualmente está usando los números de puerto predeterminados antiguos, tal vez sea conveniente que cambie a los nuevos valores predeterminados. Los números de puerto predeterminados nuevos y antiguos son los siguientes:

- Valores predeterminados nuevos para STA 2.1.0: 7019 (HTTP) y 7020 (HTTPS)
- Valores predeterminados antiguos para STA 1.0.x y STA 2.0.x: 7001 (HTTP) y 7002 (HTTPS)

Nota:

Los puertos de la consola de administración de WebLogic son externos. El administrador de la red puede necesitar configurar firewalls y enrutadores para abrir la comunicación entre el servidor de STA y los clientes que acceden a la interfaz de administración de WebLogic.

8.4.3. Puertos requeridos para STA 2.0.x y posteriores

Nota:

Este cambio se incorporó en STA 2.0.x, de manera que es relevante solo si actualiza desde STA 1.0.x.

En STA 2.0.x, se agregaron puertos de STA para los servidores gestionados StaUi y StaEngine. Los números de puerto predeterminados del servidor gestionado de STA para STA2.0.x y STA 2.1.0 son los siguientes:

- StaUi: 7021 (HTTP) y 7022 (HTTPS)
- StaEngine: 7023 (HTTP) y 7024 (HTTPS)
- StaAdapter: 7025 (HTTP) y 7026 (HTTPS)

Nota:

Los puertos de StaUi son externos. El administrador de la red puede necesitar configurar firewalls y enrutadores para abrir la comunicación entre el servidor de STA y los clientes que acceden a la interfaz de usuario de STA.

8.4.4. Requisitos del nombre de usuario y la contraseña

Los requisitos del nombre de usuario y la contraseña en STA y MySQL cambiaron en STA 2 .1.0. Tal vez tenga que coordinar estos requisitos con los requisitos internos del sitio.

Los requisitos para los nombres de usuario son los siguientes:

- Debe tener de 1 a 16 caracteres.
- Todos los nombres de usuario deben ser únicos.

Los requisitos para las contraseñas son los siguientes:

- Debe tener de 8 a 31 caracteres.
- Debe incluir al menos un número y una letra mayúscula.
- No debe tener espacios.
- No debe incluir ninguno de los siguientes caracteres especiales:

```
& ' ( ) < > ? { } *  / ' "
```

8.5. Tareas de preparación de la actualización

Realice las siguientes tareas antes de comenzar la actualización de STA. La mayoría de estas tareas son opcionales. En la Tabla 8.1, “Directrices para cuándo realizar las tareas de preparación de actualización”, se proporcionan directrices para el uso de cada una de ellas.

Tabla 8.1. Directrices para cuándo realizar las tareas de preparación de actualización

Tarea	Cuándo realizarla
Sección 8.5.1, “Verificación del estado del sitio para la actualización”	Todas las actualizaciones
Sección 8.5.2, “Conservación de logs existentes (opcional)”	Desea conservar los logs de servicio de la versión actual de STA.
Sección 8.5.3, “Registro de los valores de configuración y usuarios actuales de STA (opcional)”	Desea conservar los nombres de usuario y los valores de configuración actuales de STA.
Sección 8.5.4, “Cambio de nombre de las plantillas personalizadas que comienzan con el prefijo STA– (opcional)”	Tiene plantillas personalizadas cuyos nombres comienzan con el prefijo "STA–".
Sección 8.5.5, “Registro de configuración actual de plantillas personalizadas (opcional)”	Desea conservar la configuración de propiedad y visibilidad de las plantillas personalizadas existentes.
Sección 8.5.6, “Registro de la configuración de las políticas de informes ejecutivos (opcional)”	Desea conservar la configuración de propiedad de las políticas de informes ejecutivos existentes.

8.5.1. Verificación del estado del sitio para la actualización

Use este procedimiento para analizar los requisitos de la actualización y verificar si el sitio está preparado.

8.5.1.1. Verificación de los requisitos de actualización

Use este procedimiento para asegurarse de que el entorno cumpla con todos los requisitos de STA 2.1.0.

1. Mire la versión actual de STA. Algunas tareas de actualización varían según se trate de una actualización desde STA 1.0.x o desde STA 2.0.x.
   a. Inicie sesión en STA con un nombre de usuario de administrador de STA.
   b. Haga clic en **About** (Acerca de) en la barra de estado.
   c. Verifique que esté ejecutando una versión actualmente publicada de STA. Consulte Sección 8.2, “Rutas válidas para la actualización de STA 2.1.0” para obtener detalles.
2. Decida si va a usar el método de actualización de servidor único o dos servidores. Consulte Sección 8.1, “Descripción general del proceso de actualización” para obtener detalles.
3. Verifique que el sitio y el servidor de destino cumplan con los requisitos de STA 2.1.0. Consulte la *Guía de requisitos de STA* para obtener detalles.
4. Determine si el sistema de archivos `/tmp` del servidor de STA de destino tiene suficiente espacio para la actualización. El tamaño de `/tmp` debe ser por lo menos igual al tamaño de la base de datos existente de STA sin comprimir. Se requiere un mínimo de 4 GB, y, para bases de datos más grandes, Oracle recomienda aumentar el tamaño de `/tmp` a 32 GB como mínimo.

   Si determina que debe aumentar el tamaño de `/tmp`, puede hacerlo justo antes de ejecutar el script de actualización. Consulte Sección 8.6.9, “Tarea 8: actualizar la base de datos antigua” para obtener instrucciones.
5. Analice los cambios de entorno relevantes para la ruta de actualización que haya elegido y haga los ajustes necesarios en el plan o el entorno. Consulte Sección 8.4, “Cambios de entorno para STA 2.1.0” para obtener detalles.
6. Si está actualizando desde STA 2.0.x, asegúrese de tener instalados todos los paquetes RPM requeridos en el servidor de STA. Consulte Sección 2.3.6, “Instalación de los paquetes de Linux requeridos” para obtener instrucciones. Como comprobación final, el instalador de STA también le notificará si falta algún paquete.

8.5.1.2. Verificación de la actividad actual de STA

Use este procedimiento para verificar que el entorno actual de STA esté funcionando normalmente.

1. Use los siguientes pasos para verificar que la versión actual de STA haya podido establecer recientemente la comunicación correcta con cada una de las bibliotecas supervisadas.
   a. Inicie sesión en STA como usuario administrador de STA.
   b. En el separador **Setup & Administration** (Configuración y administración), seleccione **SNMP Connections** (Conexiones SNMP).

c. Verifique los siguientes valores en la tabla Monitored Libraries (Bibliotecas supervisadas):
   - Recent SNMP Trap Communication Status (Estado de comunicación de captura SNMP reciente): GOOD (Bueno)
   - Last Connection Status (Estado de última conexión): SUCCESS (Correcto)

2. Use los siguientes pasos para verificar que STA esté procesando intercambios en todas las bibliotecas.
   a. En el separador **Tape System Activity** (Actividad del sistema de cintas), seleccione **Exchanges – Overview** (Descripción general de intercambios).
   b. Seleccione el **ícono para filtrar** y aplique el filtro Exchange End (No. Days) Less Than 1 (Fin de intercambio [cantidad de días] menos de 1).
   c. En la barra de herramientas de la tabla, seleccione **View** (Ver), **Sort** (Ordenar) y, a continuación, seleccione **Advanced** (Avanzado). Ordene por Drive Library Name (Nombre de biblioteca de unidades), Drive Serial Number (Número de serie de unidad).
   d. Verifique que todas las bibliotecas tengan actividad de intercambio.

8.5.2. Conservación de logs existentes (opcional)

Los logs de servicio y aplicación existentes no se conservan después de la actualización porque se debe desinstalar la versión actual de STA o instalar una versión nueva de Linux antes de instalar STA 2.1.0. Use este procedimiento para guardar los logs que desea conservar.

1. Localice los logs de instalación y de la base de datos que desea conservar, y muévalos a un lugar seguro. Los logs que pueden ser de interés se encuentran en la ubicación de STA que se definió para los logs durante la instalación. Consulte Sección 2.1.2, “Revisión de la disposición del sistema de archivos de STA” para obtener detalles.
2. Use los siguientes pasos para realizar una instantánea de los logs de servicio de la instalación actual de STA. Este paso es opcional, pero recomendado, ya que el soporte de Oracle puede usar los logs para resolver problemas que pueda haber habido antes de la actualización.
   a. Inicie sesión en STA como usuario administrador de STA.
   b. En el separador **Setup & Administration** (Configuración y administración), seleccione **Logs**.
   c. En la pantalla Service – Logs (Servicio – Logs), haga clic en el ícono **Create New Log Bundle** (Crear nuevo paquete de logs).
   d. En el cuadro de diálogo Create New Log Bundle (Crear nuevo paquete de logs), asigne un nombre para el paquete y haga clic en **Save** (Guardar). Este proceso puede tardar varios minutos para completarse.
3. Use los siguientes pasos para descargar el paquete de logs de servicio que acaba de crear, así como otros paquetes que desee conservar. Debe descargar un paquete por vez.
   a. En la pantalla Service – Logs (Servicio – Logs), seleccione el paquete que desea descargar.

b. Haga clic en el ícono **Download Selected Log Bundle** (Descargar paquete de logs seleccionado).
c. En el cuadro de diálogo, especifique la ubicación de destino y guarde el paquete de logs.

8.5.3. Registro de los valores de configuración y usuarios actuales de STA (opcional)

Esta sección es aplicable solo si desea conservar los nombres de usuario y los valores de configuración actuales de STA en STA 2.1.0. Use estos procedimientos para mostrar el registro de los valores actuales para poder volver a introducirlos en STA 2.1.0. La mayoría de estos valores se debe volver a introducir después de la actualización. Consulte Sección 8.6.10, “Tarea 9: configurar la nueva versión de STA” para obtener detalles.

8.5.3.1. Registro de nombres de usuario de MySQL

Use este procedimiento para mostrar y registrar los nombres de usuario existentes de MySQL utilizados para acceder a la base de datos de STA. El instalador de STA le solicitará estos valores. No se puede recuperar las contraseñas.

a. Abra una sesión de terminal en el servidor actual de STA e inicie sesión como usuario root del sistema.
b. Ejecute la siguiente consulta para mostrar todos los nombres de usuario de la base de datos de STA. Introduzca la contraseña del usuario root de la base de datos cuando se le solicite. Por ejemplo:

```
$ mysql -uroot -p -e "select distinct(user) from user order by user ;" mysql
Enter password: password
+--------+
| user   |
+--------+
| root   |
| staapp |
| stadba |
| starpt |
+--------+
```

c. Registre los nombres de usuario.

8.5.3.2. Registro de la configuración del cliente SNMP de STA

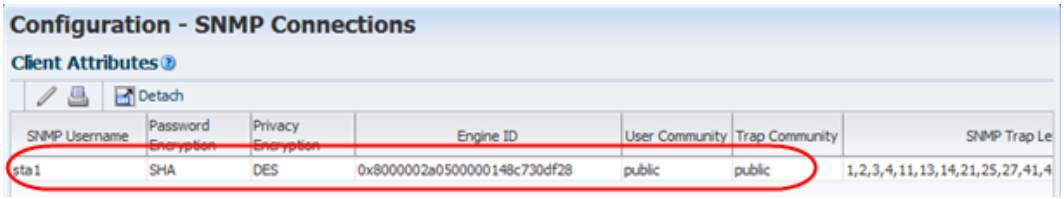
Use este procedimiento para mostrar y registrar la configuración del cliente SNMP para STA. Tendrá que volver a introducir estos valores después de la actualización.

Nota:

En la nueva versión de STA, los valores de SNMP deben coincidir con lo especificado en las bibliotecas supervisadas.

a. Inicie sesión en STA con un nombre de usuario de administrador de STA.
b. En el separador **Setup & Administration** (Configuración y administración), seleccione **SNMP Connections** (Conexiones SNMP).

   En la tabla Client Attributes (Atributos de cliente), se muestran los valores de configuración del cliente SNMP de STA.



c. Registre los valores de las siguientes columnas:
   - Nombre de usuario de SNMP
   - Comunidad de usuarios
   - Comunidad de capturas

8.5.3.3. Registro de nombres de usuario de WebLogic (solo actualizaciones desde STA 1.0.x)

Para actualizaciones desde STA 1.0.x, use este procedimiento para mostrar y registrar los nombres de usuario existentes de WebLogic para iniciar sesión en STA. Tendrá que volver a introducir estos valores después de la actualización. No se puede recuperar las contraseñas.

Nota:

A partir de STA 2.0.x, los nombres de usuario se crean y mantienen mediante la interfaz de usuario de STA. Consulte Sección 8.5.3.4, “Registro de nombres de usuario de STA (solo actualizaciones desde STA 2.0.x)” para obtener instrucciones.

a. Abra un explorador web compatible en el equipo e introduzca la dirección URL de la consola de administración de WebLogic.

   `http(s)://`*`STA_host_name`*`:`*`port_number`***`/console/`**

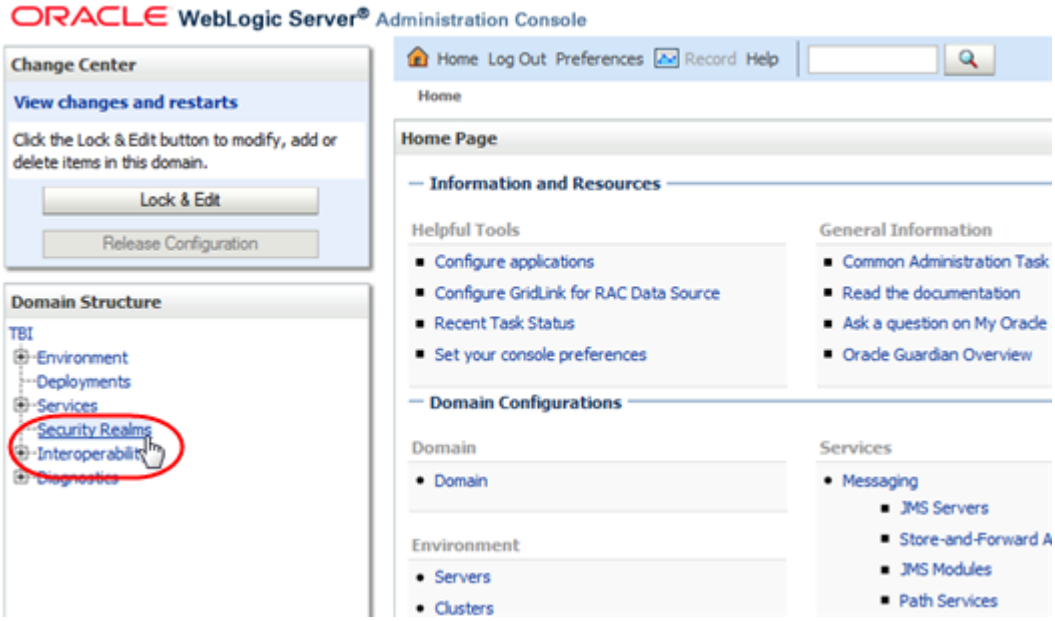
   Donde:
   - *`host_name`* es el nombre de host del servidor de STA.
   - *`port_number`* es el número de puerto de STA usado para la consola de administración de WebLogic en la versión actual de STA.
   - *`STA`* debe estar en mayúsculas.

   Por ejemplo:

```
https://staserver.example.com:7002/console/
```

b. Inicie sesión con el nombre de usuario y la contraseña de la consola de administración de WebLogic.

c. En el árbol de navegación de la estructura de dominio, haga clic en **Security Realms** (Dominios de seguridad).

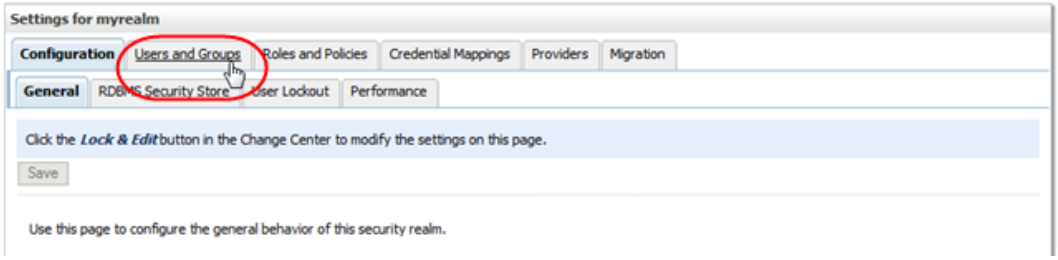


Aparece la pantalla Summary of Security Realms (Resumen de dominios de seguridad).

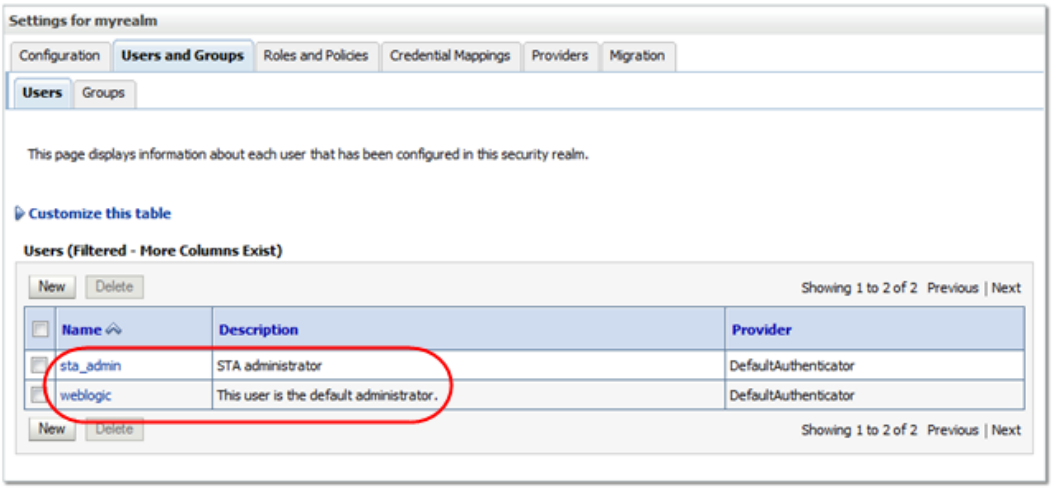
d. En la columna Name (Nombre), seleccione el enlace activo **myrealm** (no seleccione la casilla de verificación).

Aparece la pantalla Settings for myrealm (Configuración para myrealm).

e. Seleccione el separador **Users and Groups** (Usuarios y grupos).



En la tabla Users (Usuarios), se muestran los nombres de usuario disponibles.



f. Registre los nombres de usuario que desea conservar.

8.5.3.4. Registro de nombres de usuario de STA (solo actualizaciones desde STA 2.0.x)

Para actualizaciones desde STA 2,0.x, use este procedimiento para mostrar y registrar los nombres de usuario usados para iniciar sesión en STA. Tendrá que volver a introducir esta información después de la actualización. No se puede recuperar las contraseñas.

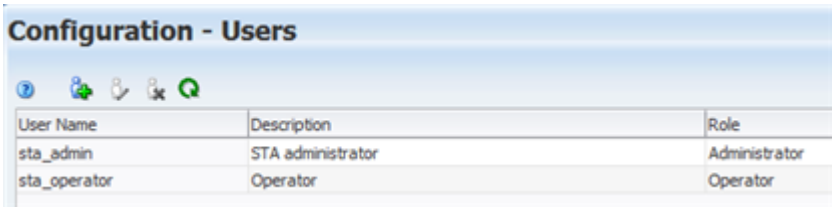
Nota:

Para STA 1.0.x, los nombres de usuario se crean y mantienen desde la consola de administración de WebLogic. Consulte Sección 8.5.3.3, “Registro de nombres de usuario de WebLogic (solo actualizaciones desde STA 1.0.x)” para obtener instrucciones.

a. Inicie sesión en STA con un nombre de usuario de administrador de STA.

b. En el separador **Setup & Administration** (Configuración y administración), seleccione **Users** (Usuarios).

La pantalla Configuration – Users (Configuración – Usuarios) muestra todos los nombres de usuario de STA y sus roles.



c. Registre los nombres de usuario y los roles que desea conservar.

8.5.3.5. Registro de la configuración del servidor de correo electrónico de STA

Use este procedimiento para mostrar y registrar el protocolo de correo electrónico de STA y, si el servidor de correo electrónico requiere autenticación, el nombre de usuario de la cuenta. Tendrá que volver a introducir estos valores después de la actualización. No se puede mostrar la contraseña.

a. Inicie sesión en STA con un nombre de usuario de administrador de STA.
b. En el separador **Setup & Administration** (Configuración y administración), seleccione **Email** (Correo electrónico).
c. En la tabla SMTP Server Settings (Configuración de servidor de SMTP), seleccione el registro StorageTek Tape Analytics Alerts (Alertas de StorageTek Tape Analytics) y, a continuación, haga clic en el ícono **Edit Selected SMTP Server** (Editar servidor de SMTP seleccionado).

   Aparece el cuadro de diálogo Define SMTP Server Details (Definir detalles de servidor de SMTP).

d. Registre los valores de los siguientes campos:

- Use Secure Connection Protocol (Usar protocolo de conexión segura)
- Username (Nombre de usuario)

8.5.4. Cambio de nombre de las plantillas personalizadas que comienzan con el prefijo STA– (opcional)

Este procedimiento es aplicable solo si tiene plantillas personalizadas cuyos nombres comienzan con el prefijo "STA–". Durante la instalación de STA 2.1.0, todas las plantillas que tengan el prefijo "STA–" se suprimen y se reemplazan por las nuevas plantillas predefinidas de STA.

Use este procedimiento para asignar nuevos nombres a las plantillas con el fin de que no se las suprima durante la actualización.

Nota:

Las plantillas predefinidas de STA comienzan con el prefijo "STA–". Por lo tanto, Oracle recomienda que *no* se use este prefijo al asignar nombres a plantillas personalizadas.

a. Inicie sesión en STA con un nombre de usuario de administrador.
b. En el separador **Setup & Administration** (Configuración y administración), seleccione **Templates Management** (Administración de plantillas).
c. Ordene la tabla por Created/Updated (Fecha de creación o actualización) para concentrarse en las plantillas que se hayan modificado desde la fecha de instalación de STA.
d. Seleccione el enlace de texto de una plantilla personalizada cuyo nombre comience con el prefijo "STA–".

   Lo llevará a la pantalla con la plantilla seleccionada aplicada.
e. Haga clic en **Save Template** (Guardar plantilla) en la barra de herramientas de plantillas.

   Se abrirá el cuadro de diálogo Save Template (Guardar plantilla).
f. En el campo **Template Name** (Nombre de plantilla), asigne un nuevo nombre que no comience con el prefijo "STA–". La entrada debe ser única.
g. Haga clic en **Save** (Guardar).

   La plantilla se guarda.

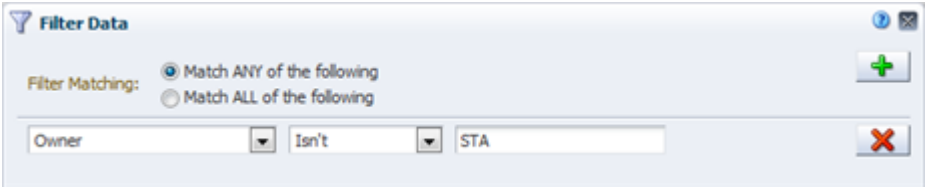
8.5.5. Registro de configuración actual de plantillas personalizadas (opcional)

Esta sección es aplicable solo si hay plantillas personalizadas. La actualización conserva las plantillas personalizadas, pero, después de la actualización, dichas plantillas pasan a ser propiedad de STA y tienen visibilidad pública.

Use este procedimiento para registrar la configuración actual de propiedad y visibilidad de todas las plantillas personalizadas, de manera de poder restaurarlas después de la

actualización en caso de ser necesario. Puede omitir este procedimiento si la propiedad y la visibilidad de las plantillas no son críticas para la implementación.

a. Inicie sesión en STA con un nombre de usuario de administrador.
b. En el separador **Setup & Administration** (Configuración y administración), seleccione **Templates Management** (Administración de plantillas).
c. Seleccione el **ícono para filtrar** y filtre la pantalla para mostrar solo las plantillas cuyo propietario no sea STA. De esta manera, se muestran solamente las planillas personalizadas.



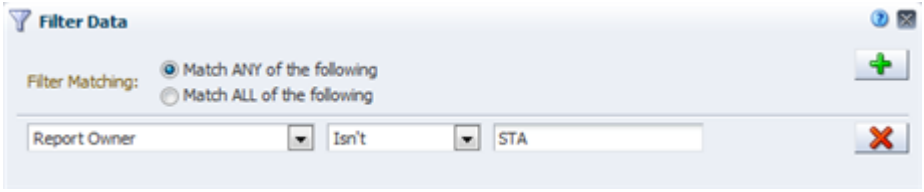
d. Registre la configuración actual de propietario y visibilidad pública de cada plantilla personalizada. Si tiene muchas plantillas, tal vez sea conveniente hacer una captura de pantalla.

8.5.6. Registro de la configuración de las políticas de informes ejecutivos (opcional)

Esta sección es aplicable solo si tiene políticas de informes ejecutivos que sean privadas. La actualización conserva todas las políticas de informes ejecutivos, pero, después de la actualización, todas las políticas privadas pasan a ser públicas.

Use este procedimiento para registrar la configuración actual de propiedad de todas las políticas privadas, de manera de poder restaurarlas después de la actualización en caso de ser necesario. Puede omitir este procedimiento si la propiedad de políticas de informes ejecutivos no es crítica para la implementación.

a. Inicie sesión en STA con un nombre de usuario de administrador de STA.
b. En el separador **Setup & Administration** (Configuración y administración), seleccione **Executive Reports Policies** (Políticas de informes ejecutivos).
c. Seleccione el **ícono para filtrar** y filtre la pantalla para mostrar solo las políticas cuyo propietario no sea STA. De esta manera, se muestran solamente las políticas privadas.



d. Registre el propietario de informe actual de cada política. Si tiene muchas políticas, tal vez sea conveniente hacer una captura de pantalla.

8.6. Tareas de actualización

Precaución:

Solo un administrador de Linux y un administrador de STA deben realizar la actualización. Todas las tareas son obligatorias y se deben realizar exactamente como se describe en el orden especificado; de no hacerlo, se podría producir la pérdida de datos.

Si está usando el método de actualización de servidor único, las tareas se deben realizar en orden secuencial. Consulte la Figura 8.1, “Descripción general de la tarea de actualización de servidor único” para obtener detalles.

Si está usando el método de actualización de dos servidores, las tareas *no* se realizan en orden secuencial y la Tarea 6 se omite. Consulte la Figura 8.2, “Descripción general de la tarea de actualización de dos servidores” para conocer el orden de las tareas.

8.6.1. Tarea 1: volcar la base de datos antigua de STA

Use este procedimiento para realizar un volcado completo de la base de datos antigua (actual) de STA.

1. Use los siguientes pasos para visualizar el tamaño de la base de datos actual de STA.
   a. Inicie sesión en STA con un nombre de usuario de administrador de STA.
   b. Haga clic en **About** (Acerca de) en la barra de estado.
   c. En el cuadro de diálogo About (Acerca de), desplácese hacia abajo hasta la sección en la que aparece el campo Database Current Size (Tamaño actual de la base de datos) y registre el valor.
2. Use los siguientes pasos para verificar que la ubicación en la que quiere hacer el volcado de la base de datos tenga suficiente espacio.
   1. Abra una sesión de terminal en el servidor de STA e inicie sesión como usuario root del sistema.

2. Muestre el espacio disponible en el destino del volcado de la base de datos y verifique que sea suficiente para el archivo del volcado. Por ejemplo:

```
# df -h /dbdumpfiles
Filesystem            Size  Used Avail Use% Mounted on
/dev/mapper/sta_server-STA_DbVol
                      200G   53G   243G  27% /dbdumpfiles
```

3. Detenga todos los servicios de STA.

```
# STA stop all
```

4. Inicie el servicio MySQL.

```
# service mysql start
```

5. Haga el volcado de la base de datos de STA en un único archivo. Introduzca la contraseña del usuario root de la base de datos cuando se le solicite.

```
# mysqldump -uroot -p --opt --add-drop-database --comments --complete-insert --
dump-date --events --flush-logs --routines --single-transaction --triggers --
databases stadb > /dumpfile_path/dumpfile_name.sql
Enter password: mysql_root_password
```

Nota:

No se recomienda usar el parámetro opcional *–v* (para obtener una salida detallada), ya que, cuando se lo usa, aparece una gran cantidad de mensajes en la ventana de terminal y se puede reducir marcadamente la velocidad de procesamiento del comando en el caso de bases de datos voluminosas.

En el Ejemplo 8.1, “Volcado de base de datos antigua”, se hace un volcado de la base de datos de STA 1.0.x en la carpeta */dbdumpfiles* del servidor de STA con el nombre de archivo *Dec14_dump.sql*.

Ejemplo 8.1. Volcado de base de datos antigua

```
# mysqldump -uroot -p --opt --add-drop-database --comments --complete-insert --
dump-date --events --flush-logs --routines --single-transaction --triggers --
databases stadb > /dbdumpfiles/Dec14_dump.sql

Enter password: mysql_root_password
...
-- Retrieving view structure for table v_library_complex_io...
...
-- Retrieving view structure for table v_library_summary_averages...
-- It's base table, skipped
...
```

```
-- Retrieving table structure for table v_mdv_status_codes...-- It's a view,
 create dummy table for view
...
-- Disconnecting from localhost...
```

6. Para reducir el tamaño del archivo de volcado en aproximadamente un 50 %, comprima el archivo con formato gzip.

```
# cd /path_to_dump_file/
# gzip dump_file_name.sql
```

8.6.2. Tarea 2: transferir el volcado de la base de datos antigua

Use este procedimiento para transferir el volcado comprimido de la base de datos antigua de STA a un servidor de copia de seguridad externo a la plataforma (método de servidor único) o al nuevo servidor de STA 2.1.0 (método de dos servidores).

Precaución:

Si está actualizando desde STA 1.0.x con el método de servidor único, debe hacer una copia de seguridad de la base de datos de STA en otro servidor. No haga la copia de seguridad de la base de datos en un sistema de archivos del servidor de STA actual, ya que la instalación de Linux 6.x en Sección 8.6.3, “Tarea 3a: instalar la nueva versión de Linux (actualizaciones desde STA 1.0.x)” [131] destruirá todos los datos del servidor.

1. Si todavía no lo hizo, detenga todos los servicios de STA.

```
# STA stop all
```

2. Realice una suma de comprobación antes de transferir el archivo al servidor de copia de seguridad.

```
# cksum dump_file_name.sql.gz
```

   La salida incluye un valor de suma de comprobación y una cantidad de bytes. Registre el valor de la suma de comprobación, ya que lo usará para verificar la integridad del archivo después de haberlo transferido al servidor de copia de seguridad.

3. Transfiera el archivo al servidor de destino mediante una utilidad de transferencia, por ejemplo, SCP. La opción *–p* preserva los valores de registro de hora.

```
# scp -p dump_file_name.sql.gz target_host:/path/
```

   En el Ejemplo 8.2, “Transferencia de la base de datos antigua al servidor de copia de seguridad (método de servidor único)”, se usa SCP para transferir el archivo del volcado de la base de datos comprimido, *Dec14_dump.sql.gz*, a la carpeta */dbdumpfiles* del

host de copia de seguridad *backup1*. La carpeta */dbdumpfiles* ya existe en el host de copia de seguridad.

Ejemplo 8.2. Transferencia de la base de datos antigua al servidor de copia de seguridad (método de servidor único)

```
# cd /dbdumpfiles
# scp -p Dec14_dump.sql.gz backup1:/dbdumpfiles
```

En el Ejemplo 8.3, "Transferencia de la base de datos antigua al nuevo servidor de STA (método de dos servidores)", se usa SCP para transferir el archivo del volcado de la base de datos comprimido, *Dec14_dump.sql.gz*, a la carpeta */dbdumpfiles* del host de STA 2.1.0 *sta_new*.

Ejemplo 8.3. Transferencia de la base de datos antigua al nuevo servidor de STA (método de dos servidores)

```
# cd /dbdumpfiles
# scp -p Dec14_dump.sql.gz sta_new:/dbdumpfiles
```

4. En el servidor de destino, realice una suma de comprobación del archivo transferido. Verifique que los valores de las sumas de comprobación sean iguales.

```
# cd /path_to_dump_file/
# cksum dump_file_name.sql.gz
```

8.6.3. Tarea 3a: instalar la nueva versión de Linux (actualizaciones desde STA 1.0.x)

Este procedimiento es aplicable solo para actualizaciones desde STA 1.0.x. Instale Linux 6.3 o posterior en el servidor de STA. Consulte el Capítulo 2, *Instalación de Linux* para obtener instrucciones.

Precaución:

Esta actividad destruye todos los datos del servidor. Si está usando el método de actualización de servidor único, use este procedimiento solamente después de haber realizado la Sección 8.6.1, "Tarea 1: volcar la base de datos antigua de STA" y la Sección 8.6.2, "Tarea 2: transferir el volcado de la base de datos antigua".

8.6.4. Tarea 3b: desinstalar la versión antigua de STA (actualizaciones desde STA 2.0.x)

Este procedimiento es aplicable solo para actualizaciones desde STA 2.0.x. Desinstale la versión actual de STA. Consulte Sección 9.2.1, "Desinstalación de STA" y Sección 9.2.2, "Verificación de la desinstalación" para obtener instrucciones.

Precaución:

Esta actividad destruye todos los datos de STA del servidor. Si está usando el método de actualización de servidor único, use este procedimiento solamente después de haber realizado la Sección 8.6.1, “Tarea 1: volcar la base de datos antigua de STA” y la Sección 8.6.2, “Tarea 2: transferir el volcado de la base de datos antigua”.

8.6.5. Tarea 4: instalar la nueva versión de STA

Use este procedimiento para instalar STA 2.1.0.

1. Instale STA 2.1.0. Consulte Capítulo 3, *Instalación de STA* para obtener instrucciones.
2. Para verificar que STA esté funcionando correctamente y completar la configuración del administrador de STA en WebLogic, inicie sesión en la aplicación de STA.

   Aparece el panel de control.

   Nota:

   Como el proceso de actualización todavía no finalizó, los portlets del panel de control muestran el mensaje "No data to display" (No hay datos para mostrar); esto es normal. Los datos de la biblioteca se mostrarán correctamente después de actualizar la base de datos y configurar la nueva versión de STA.
3. Cierre sesión de STA.
4. Abra una sesión de terminal en el servidor de STA e inicie sesión como usuario root del sistema.
5. Detenga todos los servicios de STA.

   ```
   # STA stop all
   ```

6. Este paso es aplicable solo si desea que STA supervise las bibliotecas con SNMP v2c (consulte el Apéndice F, *Configuración del modo SNMP v2c* para obtener detalles). A partir de STA 2.0.x, SNMP v2c está activado de forma predeterminada. Use los siguientes pasos para confirmar que esté activado.
   a. Cambie al directorio de archivos de configuración de STA.

      ```
      # cd /Oracle_storage_home/Middleware/user_projects/domains/TBI
      ```

   b. Abra el archivo de propiedades de la versión de SNMP y verifique que el parámetro *V2c* esté configurado con el valor *true*.

      ```
      # cat TbiSnmpVersionSupport.properties
      V2c=true
      Verbal=false
      ```

   c. Si el valor del parámetro no es true, consulte Sección F.1.3, “Activación del modo SNMP v2c para STA” a fin de obtener instrucciones para cambiarlo.

8.6.6. Tarea 5: volcar la base de datos nueva de STA (opcional)

Este procedimiento es opcional, pero recomendado. Use este procedimiento para volcar la base de datos vacía de STA 2.1.0 como protección. Si no se puede finalizar la actualización de la base de datos (Tarea 8: actualizar la base de datos antigua), puede restaurar la base de datos vacía para recuperar STA 2.1.0 en un estado que permita configurarlo para ejecutarse como si estuviera recién instalado y sin datos. Consulte Recuperación de una actualización de base de datos con error (opcional) para obtener detalles sobre el proceso de recuperación.

1. Abra una sesión de terminal en el servidor de STA e inicie sesión como usuario root del sistema.
2. Si todavía no lo hizo, detenga todos los servicios de STA.

   ```
   # STA stop all
   ```

3. Inicie el servicio MySQL.

   ```
   # STA start mysql
   ```

4. Cree el archivo de copia de seguridad de la base de datos. Introduzca la contraseña del usuario root de la base de datos cuando se le solicite.

   ```
   # mysqldump -uroot -p --opt --add-drop-database --comments --complete-insert --
   dump-date --events --flush-logs --routines --single-transaction --triggers --
   databases stadb > /dumpfile_path/dumpfile_name.sql
   ```

   Nota:

   No se recomienda usar el parámetro opcional *–v* (para obtener una salida detallada), ya que, cuando se lo usa, aparece una gran cantidad de mensajes en la ventana de terminal y se puede reducir marcadamente la velocidad de procesamiento del comando en el caso de bases de datos voluminosas.

   En el Ejemplo 8.4, “Volcado de nueva base de datos”, se hace un volcado de la base de datos de STA 2.1.0 en la carpeta */dbdumpfiles* del servidor de STA con el nombre de archivo *STA_FRESH_INSTALL_BACKUP.sql*.

Ejemplo 8.4. Volcado de nueva base de datos

```
# mysqldump -uroot -p --opt --add-drop-database --comments --complete-insert --
dump-date --events --flush-logs --routines --single-transaction --triggers --
databases stadb >  /dbdumpfiles/STA_FRESH_INSTALL_BACKUP.sql
Enter password: mysql_root_password
...
-- Retrieving view structure for table v_mdv_request_states...
-- Retrieving view structure for table version_info...
...
-- Disconnecting from localhost...
```

Nota:

Si aparece el mensaje "Can’t connect to local MySQL server" (No se puede establecer conexión con el servidor local de MySQL), significa que el servidor de MySQL no se está ejecutando. Asegúrese de haber iniciado MySQL (paso 3).

8.6.7. Tarea 6: transferir la base de datos antigua de STA al servidor de STA

Nota:

Este procedimiento es aplicable solo para el método de servidor único.

Use este procedimiento para transferir la copia de seguridad de la base de datos de STA 1.0.x o STA 2.0.x al servidor de STA 2.1.0.

1. Si todavía no lo hizo, detenga todos los servicios de STA.

```
# STA stop all
```

2. Transfiera la base de datos. La opción *–p* en SCP preserva los valores de registro de hora.

```
# scp -p backup_host:/path_to_dump_file/dump_file_name.sql.gz /local_path
```

En el Ejemplo 8.5, “Transferencia de la base de datos antigua al nuevo servidor de STA”, se usa SCP para transferir el archivo del volcado de la base de datos comprimido, *Dec14_dump.sql.gz*, de la carpeta */dbdumpfiles* del host *backup1* a la carpeta */dbdumpfiles* del servidor de STA 2.1.0.

Ejemplo 8.5. Transferencia de la base de datos antigua al nuevo servidor de STA

```
# scp -p backup1:/dbdumpfiles/Dec14_dump.sql.gz /dbdumpfiles
```

3. Realice una suma de comprobación del archivo transferido. Verifique que el valor de la suma de comprobación coincida con el que recibió en la Sección 8.6.1, “Tarea 1: volcar la base de datos antigua de STA” [128].

```
# cd /path_to_dump_file/
# cksum dump_file_name.sql.gz
```

8.6.8. Tarea 7: procesar y cargar la base de datos antigua de STA

Use este procedimiento para descomprimir la base de datos de STA 1.0.x o STA 2.0.x y restablecerla en el servidor de STA 2.1.0. La base de datos descomprimida puede requerir de 10 a 15 veces el espacio que ocupa la base de datos comprimida.

1. Si todavía no lo hizo, detenga todos los servicios de STA.

```
# STA stop all
```

2. Descomprima el archivo de copia de seguridad.

```
# gunzip dump_file_name.sql.gz
```

3. Use los siguientes pasos para depurar los datos obsoletos de la base de datos de STA, por ejemplo, registros de SNMP procesados y registros de análisis vacíos.

   Estimación de tiempo: para STA 1.0.x y STA 2.0.x, hasta un minuto por gigabyte de tamaño de instantánea de la base de datos descomprimida.

   Nota:

   En la base de datos de STA, se guarda un registro permanente de la actividad del comando *purgerecs*. A partir de STA 2.0.x, la depuración de la base de datos también se realiza automáticamente durante el tiempo de ejecución. De manera periódica, el programador de eventos de MySQL depura registros de las diversas tablas para atenuar el crecimiento de la base de datos.

   a. Cambie al directorio de actualizaciones de la base de datos de STA.

```
# cd /Oracle_storage_home/StorageTek_Tape_Analytics/db/updates
```

   b. Inicie la depuración.

```
# ./purgerecs /path_to_dump_file/dump_file_name.sql /path_to_dump_file/dump
_file_name_PURGED.sql
```

   Nota:

   Para obtener ayuda con el comando *purgerecs*, escriba el siguiente comando:

```
# ./purgerecs -h
```

En el Ejemplo 8.6, “Depuración de datos obsoletos de la copia de seguridad de la base de datos antigua ”, la utilidad *purgerecs* procesa el archivo de volcado de MySQL *Dec14_dump.sql* que se encuentra en */dbdumpfiles*. La salida se envía a un nuevo archivo llamado *Dec14_dump_PURGED.sql*, que se encuentra en */dbdumpfiles*. Aparece un punto de progreso por cada uno de los 200 registros procesados.

Ejemplo 8.6. Depuración de datos obsoletos de la copia de seguridad de la base de datos antigua

```
# cd /Oracle/StorageTek_Tape_Analytics/db/updates
# ./purgerecs /dbdumpfiles/Dec14_dump.sql /dbdumpfiles/Dec14_dump_PURGED.sql
.............................................
          STA v1.0.2, Schema 33.02
Processed 11,689 lines from '20130711_dump.sql':
---------------------------------------------
snmp_storage_cells........1,614,255
snmp_media................110,205
...
media_summaries...........254
transform_logs............0
=============================================
Records Processed:........13,143,283
Records Purged:...........2,857,623
Records Remaining:........10,285,660
Elapsed Time:.............00:00:11
```

4. Este paso es opcional. Determine el tamaño del archivo de la base de datos y estime el tiempo del proceso de carga.

   Estimación de tiempo: para STA 1.0.x y STA 2.0.x, de tres a diez minutos por gigabyte de tamaño de instantánea de la base de datos descomprimida.

   ```
   # ls -s -h dump_file_name_PURGED.sql
   ```

5. Inicie el servidor de MySQL.

   ```
   # STA start mysql
   ```

6. Cargue la base de datos de STA 1.0.x o STA 2.0.x. Introduzca la contraseña del usuario root de la base de datos cuando se le solicite. A menos que especifique la opción *–v* (detallado) (no recomendado), no se muestra la salida del comando a medida que se ejecuta el proceso.

   Nota:

   No se recomienda usar el parámetro opcional *–v* (para obtener una salida detallada), ya que, cuando se lo usa, aparece una gran cantidad de mensajes en la ventana de terminal y se puede reducir marcadamente la velocidad de procesamiento del comando en el caso de bases de datos voluminosas.

   ```
   # mysql -uroot -p -e "SET SESSION SQL_LOG_BIN=0; SOURCE /path_to_dump_file/dump
   _file_name_PURGED.sql;"
   Password: mysql_root_password
   ```

Donde:

- *–p*: solicita la contraseña del usuario root de la base de datos establecida durante la instalación de STA.
- *–e*: ejecuta las siguientes declaraciones entre comillas:
  - *SET SESSION SQL_LOG_BIN=0;*: desactiva la generación innecesaria de registros binarios, lo que acelera la carga.
  - *SOURCE* /*path_to_dump_file*/*dump_file_name_PURGED.sql*: carga el archivo de volcado en la base de datos.

Si el comando se ejecuta correctamente, aparece el símbolo del sistema al finalizar el proceso.

8.6.9. Tarea 8: actualizar la base de datos antigua

Use este procedimiento para actualizar la base de datos de STA 1.0.x o STA 2.0.x con el nuevo esquema de STA 2.1.0.

Estimación de tiempo: tiempo aproximado, por gigabyte del tamaño de la instantánea de la base de datos descomprimida.

- Desde STA 1.0.x: hasta 5 minutos por gigabyte
- Desde STA 2.0.x: hasta 30 minutos por gigabyte

1. Si todavía no lo hizo, detenga todos los servicios de STA.

   ```
   # STA stop all
   ```

2. Si en Sección 8.5.1.1, “Verificación de los requisitos de actualización” determinó que el tamaño de */tmp* no era suficiente para la actualización, aumente el tamaño de */tmp* según sea necesario.

   De no ser posible, use los siguientes pasos para definir una variable de entorno para que MySQL use una ubicación temp alternativa:

   a. Cree una ubicación temp alternativa y asígnele permisos de apertura. Por ejemplo:

      ```
      # mkdir /dbbackup/tmp
      # chmod 777 /dbbackup/tmp
      ```

   b. Detenga MySQL.

      ```
      # STA stop mysql
      ```

   c. Edite el archivo de configuración de MySQL. Por ejemplo:

      ```
      #  vi /etc/my.cnf
      ```

d. En la sección *mysqld* del archivo, agregue una línea para definir la ubicación temp alternativa, que se identifica mediante la variable *tmpdir*. A continuación, se presenta un ejemplo de un archivo después de haber agregado esta línea.

```
[mysqld]
#----- mysqld MySQL Server Options -------------------------

tmpdir                          = /dbbackup/tmp
server-id                       = 1
...
```

e. Reinicie MySQL.

```
# STA start mysql
```

3. Cambie al directorio de actualizaciones de la base de datos.

```
# cd /Oracle_storage_home/StorageTek_Tape_Analytics/db/updates
```

4. Inicie el script de actualización e introduzca la contraseña de usuario root de la base de datos cuando se le solicite. Por motivos de seguridad, la contraseña no se muestra en la pantalla.

```
# ./upgradedb.sh
```

Nota:

Puede realizar este paso como usuario root del sistema o como el usuario de instalación de Oracle.

A continuación, se muestra un ejemplo de la pantalla.

```
# ./upgradedb.sh

DB Root Password:
+-------------------------------------------------------------+
| STA DATABASE UPGRADE                                        |
| Upgrading DB schema from 58.00r0 to 59.00r0                 |
| Started: 2014-12-12 15:14:45                                |
+-------------------------------------------------------------+
STA database is 5.15 GB and contains approximately 12,636,002 records.
Checking if current database v58.00 is a valid upgrade candidate...
...DB v58.00 is a valid upgrade candidate...
+-------------------------------------------------------------+
==> You may ABORT using CTRL-C within 7 seconds
==> .....6.....5.....4.....3.....2.....1
==> CTRL-C disabled!
+-------------------------------------------------------------+
```

```
Starting upgrade...
```

Cuando el proceso finaliza, aparece un cartel similar al siguiente.

Precaución:

Espere hasta ver el cartel antes de continuar.

```
+-------------------------------------------------------------+
| Started.................2014-12-12 15:14:45                 |
| Finished................2014-12-12 17:07:11                 |
| Elapsed Time............01:52:26                             |
| Starting Version........58.00r0                             |
| Final Schema Version....59.00r0                             |
| Schema Release Date.....2014-12-12 11:00:00                 |
| Records (approximate)...12,636,002                          |
+-------------------------------------------------------------+
```

5. Si en Sección 8.6.9, “Tarea 8: actualizar la base de datos antigua” aumentó el tamaño de */tmp* o creó una ubicación temp alternativa, restaure el tamaño y la ubicación normales.
6. Inicie todos los servicios de STA.

   ```
   # STA start all
   ```

7. Este paso es opcional. Suprima el archivo *STA_FRESH_INSTALL_BACKUP.sql* para liberar espacio de disco en el volumen de copias de seguridad de la base de datos de STA.

8.6.10. Tarea 9: configurar la nueva versión de STA

Use estos procedimientos para configurar las bibliotecas y STA 2.1.0 con el fin de que STA pueda comenzar a supervisar la actividad de las bibliotecas.

8.6.10.1. Actualización del destinatario de capturas de STA en las bibliotecas

En STA 2.0.x, se agregaron dos nuevos niveles de captura: 13 (captura de prueba) y 14 (captura de estado). Realice los siguientes pasos en cada biblioteca supervisada para asegurarse de que estos niveles de captura estén incluidos en la definición del destinatario de capturas de STA.

1. En función de la ruta de actualización que esté usando, haga lo siguiente:
   - Si está usando el método de servidor único para actualizar desde STA 2.0.x, siga con Sección 8.6.10.2, “Configuración de parámetros de SNMP en STA” [141].
   - Si está usando el método de servidor único para actualizar desde STA 1.0.x, vaya al paso 2 para agregar los nuevos niveles de captura al destinatario de capturas existente de STA en cada biblioteca supervisada.

- Si está usando el método de actualización de dos servidores, vaya al paso 3 para agregar un nuevo destinatario de capturas de STA a cada biblioteca supervisada.

2. Si está usando el método de servidor único para actualizar desde STA 1.0.x, use los pasos correspondientes al modelo de biblioteca para agregar los nuevos niveles de captura al destinatario de capturas de STA.

   Para todos los modelos de biblioteca, excepto SL150, para modificar un destinatario de capturas, primero debe suprimir la definición existente y después agregar una nueva.

   ### Todas las bibliotecas, excepto SL150

   a. Inicie sesión en la CLI de la biblioteca.
   b. Muestre todos los destinatarios de capturas existentes y tome nota del número de índice del destinatario de STA.

      ```
      snmp listTrapRecipients
      ```

   c. Suprima el destinatario de capturas de STA.

      ```
      snmp deleteTrapRecipient id index
      ```

      Donde:

      - *index* es el número de índice del destinatario de capturas de STA.

   d. Vuelva a agregar el destinatario de capturas de STA e incluya los nuevos niveles de captura en la lista de niveles de captura. Consulte Sección 5.2.6, “Creación del destinatario de capturas de SNMP v3 de STA” o Sección F.1.2, “Creación del destinatario de capturas SNMP v2c de STA en la biblioteca” para obtener instrucciones.

   ### Bibliotecas SL150

   a. Inicie sesión en la interfaz de usuario basada en explorador.
   b. En el menú **SNMP**, seleccione **SNMP Trap Recipients** (Destinatarios de capturas de SNMP).
   c. En la lista, seleccione el destinatario de capturas de STA.
   d. Seleccione **Modify Trap Recipient** (Modificar destinatario de capturas).
   e. Agregue los nuevos niveles de captura a la lista de niveles de captura y, a continuación, haga clic en **Save** (Guardar).

3. Si está usando el método de actualización de dos servidores, agregue el nuevo servidor de STA 2.1.0 como destinatario de capturas en cada biblioteca. Consulte Sección 5.2.6, “Creación del destinatario de capturas de SNMP v3 de STA” [84] o Sección F.1.2, “Creación del destinatario de capturas SNMP v2c de STA en la biblioteca”.

8.6.10.2. Configuración de parámetros de SNMP en STA

Realice estos pasos para todas las actualizaciones. Estos pasos se realizan en STA.

1. Inicie sesión en STA como usuario administrador de STA.
2. Vuelva a introducir los valores de configuración del cliente SNMP de STA usando los valores que registró antes de la actualización. Consulte Sección 8.5.3, “Registro de los valores de configuración y usuarios actuales de STA (opcional)”. Estos valores deben coincidir con lo que se haya configurado en las bibliotecas supervisadas. Consulte Sección 6.1.3, “Configuración de los parámetros del cliente de SNMP para STA” para obtener instrucciones.
3. Para restaurar la comunicación de SNMP entre STA y las bibliotecas, pruebe la conexión con cada biblioteca supervisada. Consulte Sección 6.1.5, “Prueba de la conexión SNMP de una biblioteca” para obtener instrucciones.

   Nota:

   Después de haber completado correctamente este paso, STA comienza a recibir y procesar datos de cada una de las bibliotecas supervisadas.

   Tal vez observe que hay intercambios incompletos en la pantalla Exchanges Overview (Descripción general de intercambios) correspondientes a intercambios que estaban en curso cuando se detuvo STA o cuando se restauraron las conexiones con las bibliotecas. Consulte la *Guía del usuario de STA* para obtener detalles sobre intercambios incompletos.

4. Obtenga los datos de configuración de la biblioteca de SNMP más recientes de cada biblioteca. Consulte Sección 6.1.6, “Realización de una recopilación de datos manual” para obtener instrucciones.

8.6.10.3. Configuración de servicios e información de usuarios de STA

Realice estos pasos para todas las actualizaciones. Estos pasos se realizan en el servidor de STA.

Si desea conservar la configuración de la versión previa de STA, use los valores que registró antes de la actualización. Consulte Sección 8.5.3, “Registro de los valores de configuración y usuarios actuales de STA (opcional)”.

Nota:

Después de la actualización, STA pasa a ser el propietario de todos los grupos lógicos. La propiedad de grupos lógicos no es crítica para el funcionamiento de STA, y cualquier usuario de STA que tenga privilegios de operador o administrador puede modificar los grupos lógicos.

1. Configure el servicio de copia de seguridad de STA y las utilidades de servicio de supervisión de recursos de STA. Consulte el Capítulo 7, *Configuración de los servicios de STA* para obtener detalles.
2. Cree los nombres de usuario y las contraseñas de STA. Consulte la *Guía del usuario de STA* para obtener instrucciones. Tal vez también desee hacer lo siguiente:

- Notifique a los usuarios acerca de los nuevos requisitos para contraseñas en STA 2.1.0.
- Indique a los usuarios que vuelvan a introducir sus preferencias de usuario personalizadas si corresponde.

3. Si el servidor de correo electrónico de STA requiere autenticación, debe introducir el nombre de usuario y la contraseña de la cuenta de correo electrónico. Consulte la *Guía del usuario de STA* para obtener instrucciones.
4. Restaure la propiedad original de las plantillas personalizadas, según corresponda. Consulte la *Guía del usuario de STA* para obtener instrucciones.
5. Restaure la propiedad original de las políticas privadas de informes ejecutivos, según corresponda. Consulte la *Guía del usuario de STA* para obtener instrucciones.

8.6.10.4. Desactivación del servidor antiguo de STA (opcional)

Este procedimiento es aplicable solo si usó el método de actualización de dos servidores. Puede usar este procedimiento después de verificar que el nuevo servidor de STA esté funcionando según lo esperado.

1. Elimine el servidor antiguo de STA 1.0.x o STA 2.0.x como destinatario de capturas de la configuración de SNMP de cada biblioteca. Consulte *Guía del usuario de STA* para obtener instrucciones.
2. Desactive el servidor antiguo de STA 1.0.x o STA 2.0.x.

8.6.11. Recuperación de una actualización de base de datos con error (opcional)

Precaución:

Realice este procedimiento solo si se lo indica su representante de soporte de Oracle.

Use este procedimiento solo si la actualización de la base de datos realizada en la Sección 8.6.9, “Tarea 8: actualizar la base de datos antigua” [137] no finaliza correctamente y se produjeron errores también al intentar repetir la actualización.

1. Repita desde la "Tarea 7: procesar y cargar la base de datos antigua de STA" [135], Paso 6, hasta la "Tarea 8: actualizar la base de datos antigua" [137].

   Si se vuelve a producir algún error en la actualización, significa que la base de datos se encuentra en un estado desconocido, posiblemente con daño, y se debe restaurar a su estado original como si estuviera recién instalada. Continúe con el siguiente paso.
2. Suprima la base de datos actualizada dañada.

   ```
   # mysql -uroot -p -e "drop database stadb;"
   ```

3. Cambie a la ubicación de la copia de seguridad de la base de datos de STA y cargue el archivo de volcado de la base de datos de la nueva instalación que creó en la Sección 8.6.6, “Tarea 5: volcar la base de datos nueva de STA (opcional) ” [133].

Por ejemplo:

```
# cd /dbbackup
# mysql -uroot -p -e < /home/oracle/STA_FRESH_INSTALL_BACKUP.sql
```

4. Realice la Sección 8.6.9, “Tarea 8: actualizar la base de datos antigua” [137].
5. Configure STA como una nueva instalación. Consulte las secciones siguientes para obtener detalles:
   - Capítulo 6, *Configuración de conexiones de bibliotecas en STA*
   - Capítulo 7, *Configuración de los servicios de STA*

9

Desinstalación y restauración de STA

En este capítulo, se incluyen las siguientes secciones:

Precaución:

Oracle no admite el cambio a una versión anterior de STA. Los datos de la base de datos creados con una versión más reciente de STA se pierden si se instala una versión anterior de STA.

9.1. Descripción general de la desinstalación de STA

El desinstalador de STA elimina la aplicación de STA y todos los datos asociados, así como el software de Oracle. Se hacen las siguientes actualizaciones:

- El subdirectorio *`StorageTek_Tape_Analytics`* del directorio raíz de almacenamiento de Oracle se elimina por completo. Los demás directorios del directorio raíz de almacenamiento de Oracle no se ven afectados.
- Se eliminan todos los logs de STA y MySQL de la ubicación de logs. Consulte Sección 2.1.2, “Revisión de la disposición del sistema de archivos de STA” para obtener información detallada acerca de esta ubicación.
- Se eliminan todos los logs de servicio de STA.
- Se elimina la base de datos de STA y todas las copias de seguridad locales. Si el directorio de la base de datos o el directorio de las copias de seguridad locales son puntos de montaje o incluyen archivos definidos por el usuario, los directorios se conservan; de lo contrario, se los elimina.

La ubicación del inventario central de Oracle *no* se elimina al desinstalar STA. Todos los datos de este directorio se conservan, incluidos todos los logs de instalación y desinstalación de STA y la información del inventario de software de Oracle. Consulte información detallada en Ubicación de inventario central de Oracle.

El desinstalador de STA está disponible en modo gráfico y modo silencioso. Consulte Sección 3.5, “Modos del instalador de STA” para obtener detalles.

Consulte Sección 3.4, “Logs de instalación y desinstalación de STA” para obtener información detallada acerca de los logs de desinstalación de STA.

9.2. Tareas de desinstalación de STA

En las siguientes secciones, se describe cómo usar el desinstalador de STA.

9.2.1. Desinstalación de STA

Use este procedimiento para desinstalar STA.

Precaución:

La desinstalación elimina todos los datos de la base de datos de STA. Antes de iniciar este procedimiento, debe realizar un volcado completo de la base de datos. Consulte las instrucciones en Sección 8.6.1, “Tarea 1: volcar la base de datos antigua de STA”.

Nota:

Para desinstalar STA, debe iniciar sesión como usuario que sea miembro del grupo de instalación de Oracle. No puede desinstalar STA como usuario *root* de Linux ni ningún otro usuario que tenga privilegios de superusuario. Consulte información detallada en Grupo de instalación de Oracle.

1. Inicie sesión como usuario de instalación de Oracle.
2. Cambie al directorio raíz de almacenamiento de Oracle. Por ejemplo:

   ```
   $ cd /Oracle
   ```

3. Cambie al directorio binario de instalador de STA.

   ```
   $ cd StorageTek_Tape_Analytics/oui/bin
   ```

4. Inicie el desinstalador de STA con uno de los siguientes comandos:
   - Para usar el desinstalador gráfico de STA:

     ```
     $ ./deinstall.sh
     ```

     Para este modo, se requiere una visualización X11. Consulte las instrucciones en Apéndice A, *Referencia de la pantalla del instalador y del desinstalador gráficos de STA*.
   - Para usar el desinstalador silencioso de STA:

     ```
     $ ./deinstall.sh –silent  –responseFile response_file
     ```

     Donde *response_file* es la ruta de acceso absoluta del archivo de respuesta creado previamente.

Antes de usar este modo, debe descargar también el archivo *silentInstallUtility.jar* y crear un archivo de respuesta en el que se especifiquen las opciones de instalación. Consulte el Apéndice B, *Instalador y desinstalador en modo silencioso de STA* para obtener instrucciones.

9.2.2. Verificación de la desinstalación

Use este procedimiento para verificar que se hayan eliminado todos los componentes de STA del servidor de STA después de la desinstalación.

1. Inicie sesión como usuario de instalación de Oracle.
2. Visualice el contenido del directorio raíz de almacenamiento de Oracle. Debería estar vacío. Por ejemplo:

```
$ ls -la /Oracle
total 8
drwxr-xr-x   2 oracle oinstall 4096 Sep 23 14:55 .
dr-xr-xr-x. 31 root   root     4096 Sep 23 16:41 ..
$
```

9.2.3. Restauración de STA

Use este procedimiento para desinstalar y reinstalar STA (por ejemplo, para reparar una instalación actual). No puede usar el instalador de STA para reinstalar o sobrescribir una instalación actual.

1. Genere una instantánea del log de servicio en la instalación actual de STA. El servicio de soporte de Oracle puede usar los logs de servicio generados para solucionar problemas que pueda haber habido antes de la actualización. Consulte la *Guía del usuario de STA* para obtener instrucciones detalladas.
2. Detenga todos los servicios de STA:

```
# STA stop all
```

3. Realice una instantánea de la base de datos.
   a. Inicie el servicio MySQL.

```
# STA start mysql
```

   b. Cree un archivo de copia de seguridad.

```
# /usr/bin/mysqldump -uroot -p --opt --routines --triggers --events --flush-
logs --single-transaction --complete-insert --comments --dump-date --add-drop-
database --databases stadb -v > /sta_db_backup/backup_filename.sql
Enter password: mysql_root_password
```

La salida será similar a la siguiente:

```
...
-- Retrieving view structure for table v_mdv_request_states...
-- Retrieving view structure for table version_info...
...
-- Disconnecting from localhost...
```

Nota:

Si aparece el mensaje "Can’t connect to local MySQL server" (No se puede establecer conexión con el servidor local de MySQL), significa que el servidor de MySQL no se está ejecutando. Regrese al paso a y verifique que MySQL se haya iniciado.

4. Mueva la instantánea del log de servicio y la instantánea de la base de datos a otro servidor, ya que todos los archivos de STA se eliminarán en el siguiente paso. Las instantáneas se encuentran en los siguientes directorios:
   - La instantánea del log de servicio se encuentra en */Oracle_storage_home/Middleware/rda/snapshots*. Por ejemplo, */Oracle/Middleware/rda/snapshots*
   - La instantánea de la base de datos se encuentra en la ubicación de la base de datos especificada durante la instalación de STA. Por ejemplo, */dbbackup*
5. Haga copias de seguridad de otros archivos según sea necesario.
6. Desinstale STA. Consulte Sección 9.2.1, “Desinstalación de STA” para obtener instrucciones.
7. Reinstale STA. Consulte Capítulo 3, *Instalación de STA* para obtener instrucciones.
8. Detenga todos los servicios de STA:

   ```
   # STA stop all
   ```

9. Restaure la base de datos. Consulte la *Guía de administración de STA* para obtener instrucciones.
10. Inicie todos los servicios de STA:

    ```
    # STA start all
    ```

11. Configure STA. Consulte Sección 8.6.10.2, “Configuración de parámetros de SNMP en STA” para obtener instrucciones.

Apéndice A

Referencia de la pantalla del instalador y del desinstalador gráficos de STA

En este capítulo, se incluyen las siguientes secciones:

A.1. Requisitos de visualización para el modo gráfico

El instalador y el desinstalador gráficos de STA requieren X Window System, versión 11 (X11). La configuración de X11 no se incluye en esta guía, pero se aplican las directrices generales que se indican a continuación. Para obtener más información, póngase en contacto con el administrador del sistema.

Para ejecutar el instalador y el desinstalador en el modo gráfico, el servicio X11 se debe estar ejecutando en el servidor de STA y debe estar configurado para permitir el reenvío de X11. Si Linux se instaló como se indicó en el Capítulo 2, *Instalación de Linux*, estas condiciones deberían estar cumplidas.

Asimismo, las autorizaciones y la visualización de X11 se deben configurar correctamente para el usuario de instalación de Oracle. Esto se hace de diferentes maneras según se inicie sesión a través de una conexión local o una remota.

Consulte la sección siguiente para obtener más detalles.

Nota:

El tiempo de respuesta para las conexiones remotas depende de las configuraciones y del rendimiento de la red y la VPN.

A.1.1. Conexiones locales

Para conexiones directas con el servidor de STA, debe iniciar sesión como usuario de instalación de Oracle y, a continuación, configurar la variable `DISPLAY` de manera manual. Por ejemplo:

```
# export DISPLAY=hostname:0.0
```

Es posible que también sea necesario verificar que el usuario de instalación de Oracle tenga la autorización adecuada para X11. Póngase en contacto con el administrador de Linux para obtener ayuda.

A.1.2. Conexiones remotas con shell seguro (SSH)

Si usa un shell seguro (SSH) con reenvío de X11 activado, la autorización y la visualización de X11 son procesadas automáticamente por el usuario de inicio de sesión. Por ejemplo, si usa este método e inicia sesión como usuario *oracle*, el servicio SSH del servidor de STA configura automáticamente la autorización y la visualización adecuadas de X11 para el usuario *oracle*. No debe configurar la variable *DISPLAY* de forma manual.

Sin embargo, si inicia sesión como otro usuario (*root*, por ejemplo) y después usa el comando *su* para cambiar al usuario *oracle*, las autorizaciones y la visualización de X11 no se configuran correctamente para el usuario *oracle*, por lo que se las debe configurar de forma manual. Las instrucciones para realizar esta acción no se incluyen en esta guía. Póngase en contacto con el administrador de Linux para solicitar ayuda.

A.1.2.1. Conexión desde un equipo Linux

Para activar el reenvío de X11 en un equipo Linux, use el comando *ssh* con las opciones *–X* o *–Y*. Por ejemplo:

```
$ ssh –X oracle@sta_server
```

A.1.2.2. Conexión desde un equipo Microsoft Windows

El equipo debe estar ejecutando un servidor X11, por ejemplo, Xming o Cygwin/X, y un cliente SSH, por ejemplo, PuTTY o WinSCP. A continuación, se muestra un ejemplo del procedimiento para conectarse mediante PuTTY.

1. Verifique que el servidor X11 se esté ejecutando en el equipo. De ser necesario, póngase en contacto con el administrador del sistema para solicitar ayuda.
2. Inicie PuTTY y haga lo siguiente:
   a. En la ventana principal de la sesión, introduzca lo siguiente:
      - En el campo **Host Name** (Nombre de host), escriba el nombre o la dirección IP del servidor de STA.
      - En el campo **SSH Connection type** (Tipo de conexión SSH), seleccione **SSH**.
   b. En el árbol del menú Category (Categoría), amplíe **Connection** (Conexión), amplíe **SSH** y, a continuación, seleccione **X11**. En esta ventana, seleccione lo siguiente:
      - En el campo **X11 forwarding** (Reenvío de X11), seleccione la casilla de verificación **Enable X11 forwarding** (Activar reenvío de X11).

- En el campo **Remote X11 authentication protocol** (Protocolo de autenticación de X11 remoto), seleccione **MIT-Magic-Cookie-1**.
- Deje los demás campos en blanco.

A.1.3. Conexiones remotas con uso compartido de escritorio

Para ejecutar el instalador de STA mediante el uso compartido de escritorio, tanto el servidor de STA como el equipo local deben estar ejecutando una aplicación de uso compartido de escritorio, por ejemplo, el servidor VNC en el servidor de STA y el visor de VNC en el equipo local. Además, el equipo local debe poder conectarse al servidor de STA a través de una red privada, por ejemplo, una red privada virtual (VPN).

A continuación, se muestra un ejemplo del proceso para conectarse mediante VNC.

1. Instale y configure el servidor VNC en el servidor de STA.
2. Instale y configure el visor de VNC en el equipo local.
3. Conéctese al servidor de STA a través de la red privada. Póngase en contacto con el administrador de sistemas para obtener instrucciones.

A.1.4. Resolución de problemas de visualización gráfica

El instalador y el desinstalador de STA verifican que X11 esté bien configurado para el usuario de instalación de Oracle. Si se produce algún error al verificar este requisito previo, póngase en contacto con el administrador de sistemas Linux para obtener ayuda. Puede usar los siguientes pasos para ayudar a resolver problemas.

1. Inicie sesión en el servidor de STA como usuario de instalación de Oracle y visualice los paquetes RPM actualmente instalados.

   ```
   # yum list installed
   ```

   En la lista, debería aparecer la entrada *xorg-x11-util*. Por ejemplo:

   ```
   xorg-x11-utils.x86_64                  7.5-6.el6
   ```

2. Muestre la configuración de visualización actual para el usuario de instalación de Oracle. Por ejemplo:

   ```
   $ echo $DISPLAY
   :0.0
   ```

3. Verifique que la visualización tenga la configuración adecuada de X11. Por ejemplo:

   ```
   $ xdpyinfo –display :0.0
   ```

En el Ejemplo A.1, “Ejemplo de visualización de X11 bien configurada”, se muestra la primera parte de la salida del comando, donde se indica la visualización bien configurada.

Ejemplo A.1. Ejemplo de visualización de X11 bien configurada

```
$ xdpyinfo
name of display:    :0.0
version number:    11.0
vendor string:    The X.Org Foundation
vendor release number:    11300000
X.Org version: 1.13.0
maximum request size:  16777212 bytes
motion buffer size:  256
...
```

En el Ejemplo A.2, “Ejemplo de visualizaciones de X11 mal configuradas”, se muestran algunas salidas de comandos de visualizaciones que no están bien configuradas.

Ejemplo A.2. Ejemplo de visualizaciones de X11 mal configuradas

```
$ xdpyinfo
xdpyinfo:  unable to open display ":0.0".

$ xdpyinfo
PuTTY X11 proxy: MIT-MAGIC-COOKIE-1 data did not matchxdpyinfo:  unable to open
 display ":0.0".
```

A.2. Pantallas del instalador gráfico de STA

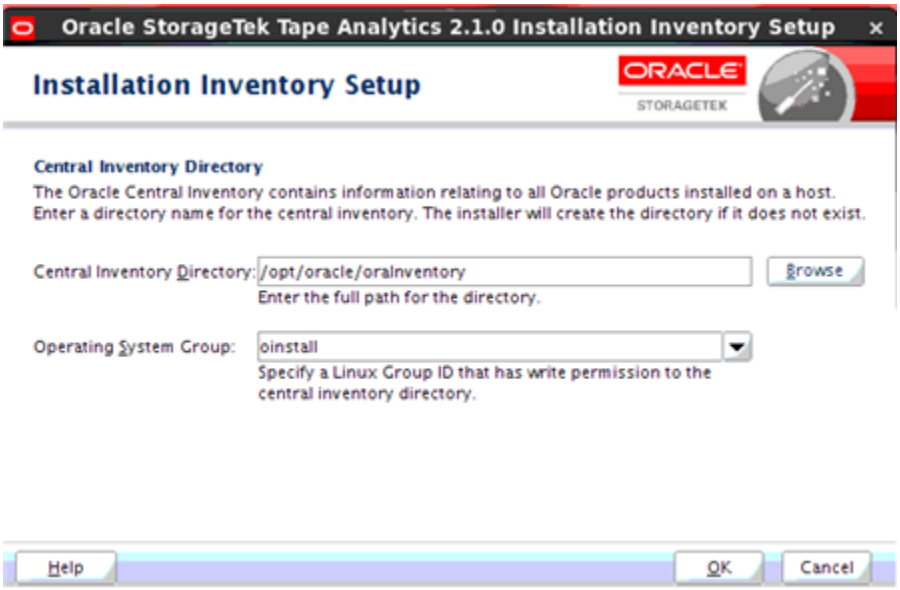
En esta sección, se proporciona referencia detallada para cada una de las pantallas del instalador gráfico de STA.

- Sección A.2.2, “Bienvenido”
- Sección A.2.3, “Ubicación de Instalación”
- Sección A.2.4, “Comprobaciones de requisitos”
- Sección A.2.5, “Introducción de la contraseña del usuario root”
- Sección A.2.6, “Configuración de directorios de la base de datos”
- Sección A.2.7, “Configuración de cuentas de administración”
  - Sección A.2.8, “Administrador de WebLogic”
  - Sección A.2.9, “Administrador de STA”
- Sección A.2.10, “Configuración de cuentas de base de datos”
  - Sección A.2.11, “Usuario root de la base de datos”
  - Sección A.2.12, “Usuario de aplicación de base de datos”
  - Sección A.2.13, “Usuario de informes de la base de datos”

Nota:

Al iniciar el instalador gráfico de STA, Oracle Universal Installer muestra mensajes en la ventana de terminal a medida que realiza algunas comprobaciones básicas del entorno. Los requisitos para ejecutar el instalador gráfico de STA pueden exceder estas comprobaciones mínimas.

A.2.1. Instalación y configuración del inventario



Se usa el directorio del inventario central de Oracle para llevar un control de los nombres y las ubicaciones de todo el software de Oracle instalado en este servidor. Todos los logs de instalación y desinstalación de STA se guardan automáticamente en esta ubicación.

Para asegurarse de que los demás usuarios del grupo de instalación de Oracle tengan acceso a este directorio, debe ser independiente del directorio raíz del usuario de instalación de Oracle. Es posible que los directorios raíz no tengan los permisos adecuados para el grupo de instalación de Oracle.

Esta pantalla es parte de Oracle Universal Installer. Si sigue las prácticas recomendadas para registrar la ubicación del inventario central de Oracle, esta pantalla solamente aparece la primera vez que se instala STA en este servidor. Las instalaciones subsiguientes encontrarán la ubicación automáticamente sin necesidad de solicitar la información. Consulte Sección 3.6.7, “Registro de la ubicación del inventario central de Oracle” para obtener detalles.

A.2.1.1. Campos de la pantalla

Inventory Directory (Directorio de inventario)
Introduzca el nombre del directorio que desea designar como directorio del inventario central de Oracle.

El valor predeterminado es *`$USER_HOME/oraInventory`*. Debe especificar una ruta de acceso absoluta o hacer clic en el botón **Browse** (Examinar) para navegar hasta un directorio existente.

- Si especifica un directorio existente, el usuario de instalación de Oracle debe tener permisos completos para él.
- Si especifica un directorio que no existe, el instalador lo crea automáticamente si el usuario de instalación de Oracle tiene permisos completos para el directorio principal.

Operating System Group (Grupo de sistema operativo)
Seleccione el grupo de Linux que desea designar como grupo de instalación de Oracle. Todos los miembros de este grupo podrán instalar software de Oracle en este servidor.

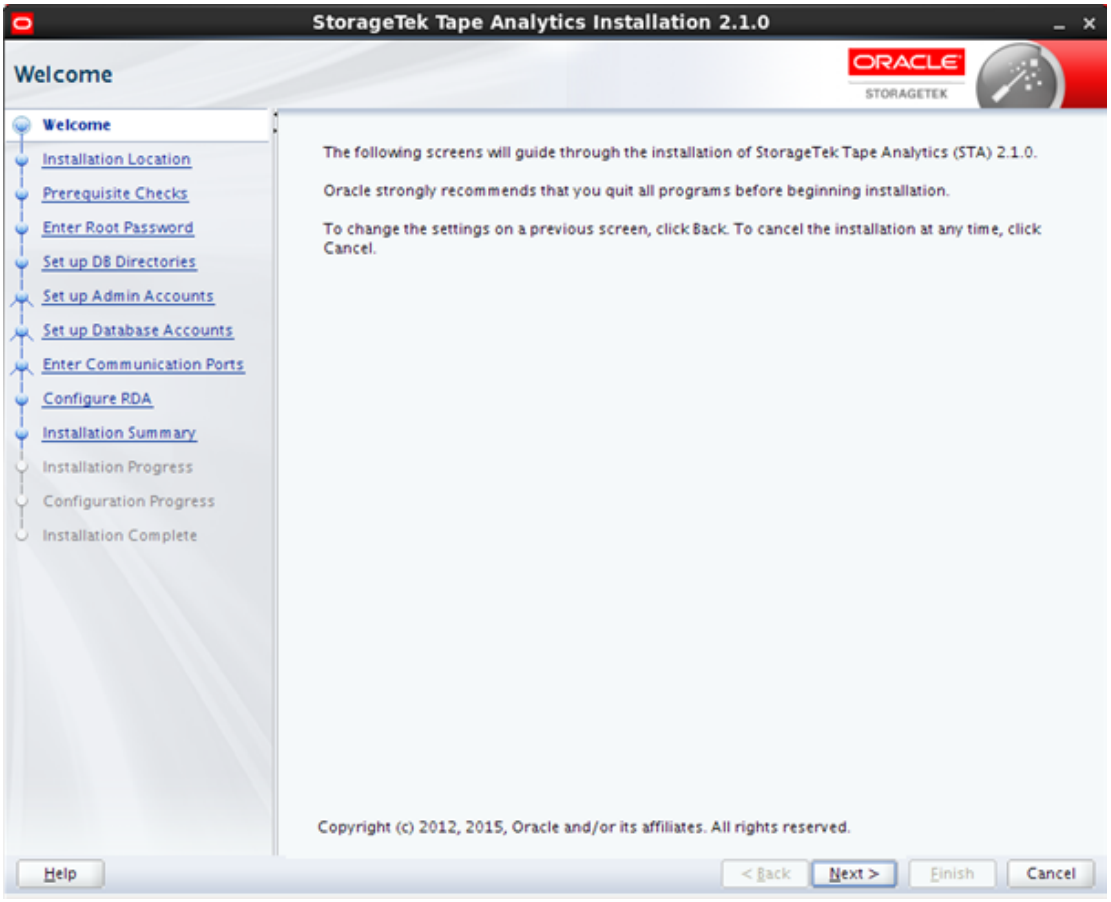
En el menú, se muestran todos los grupos a los que pertenece el usuario de instalación de Oracle. El valor predeterminado es el grupo principal del usuario de instalación de Oracle.

A.2.1.2. Botones específicos de la pantalla

Browse (Examinar)
Haga clic para navegar hasta el directorio que desea especificar.

OK (Aceptar)
Haga clic para iniciar el instalador de STA. La ventana Installation Inventory Setup (Configuración de inventario de instalación) desaparece y puede haber una leve demora hasta que aparezca la pantalla de presentación del instalador de STA.

A.2.2. Bienvenido



Esta pantalla proporciona información general para ejecutar el instalador de STA. Lea el texto y, a continuación, haga clic en **Next** (Siguiente) para comenzar la instalación.

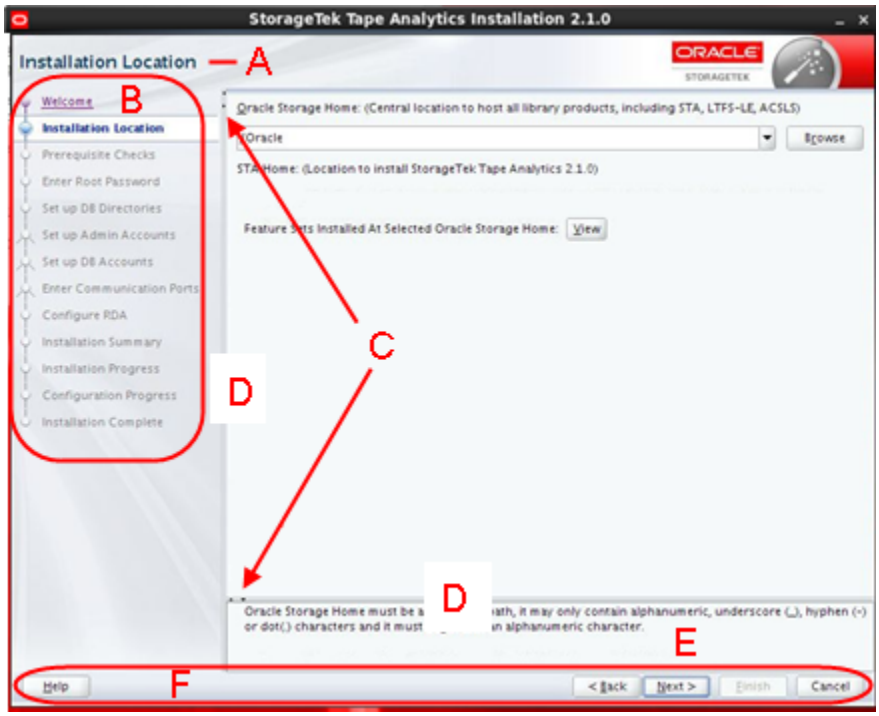
Nota:

Los cambios del sistema se implementan después de haber completado todas las pantallas de entrada de información del instalador de STA y haber hecho clic en **Install** (Instalar) en Sección A.2.21, “Resumen de instalación”. Antes de ese paso, puede regresar a una pantalla anterior cuando lo desee y modificar la información introducida.

Consulte Sección A.2.2.1, “Disposición general de la pantalla del instalador” para obtener información sobre las pantallas del instalador de STA.

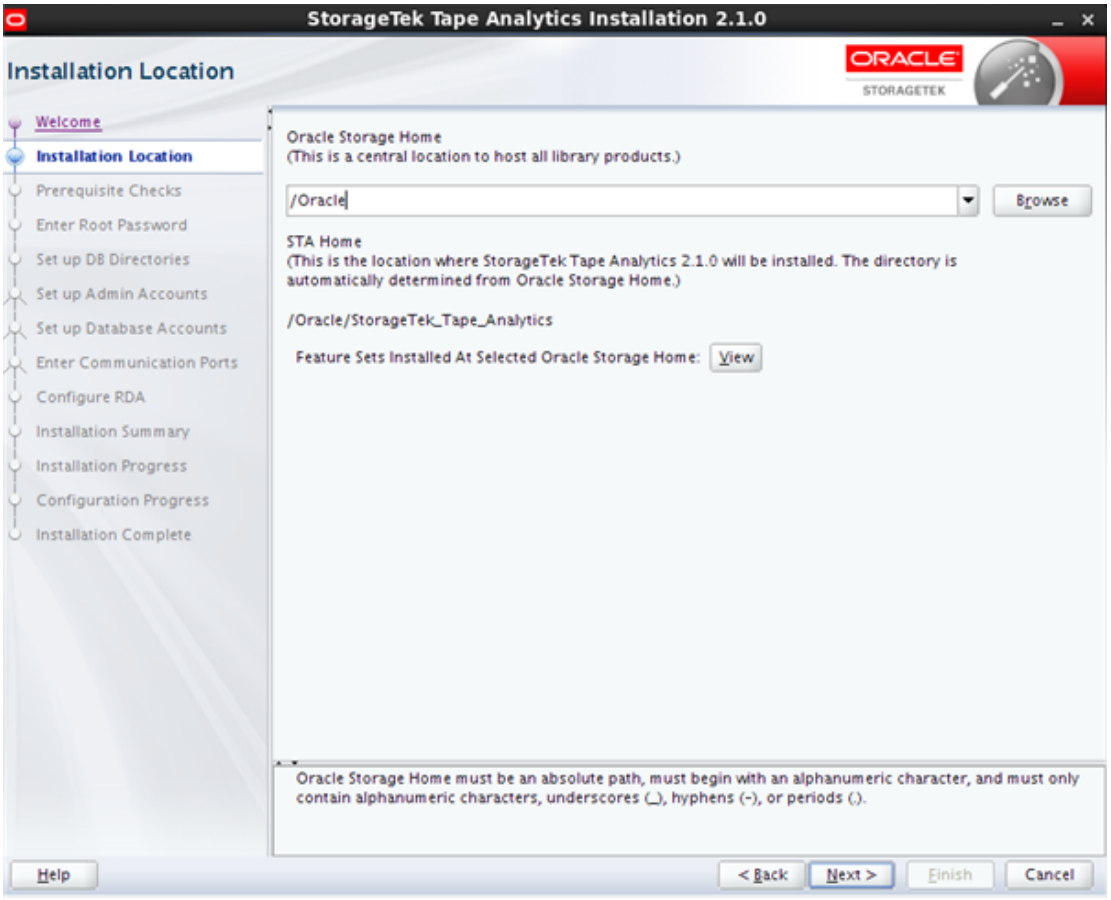
A.2.2.1. Disposición general de la pantalla del instalador

Todas las pantallas del instalador de STA tienen la misma disposición básica. Las partes principales se ilustran y describen a continuación.



Elemento	Nombre	Descripción
A	Título de la pantalla	Título de la pantalla del instalador de STA.
B	Árbol de navegación	Muestra la posición actual en la secuencia de instalación. Los títulos de las pantallas se convierten en enlaces activos a medida que las completa. Puede hacer clic en cualquiera de los enlaces activos para regresar directamente a esa pantalla y revisar o modificar la información introducida.
C	Íconos para expandir y contraer	Haga clic para ocultar o mostrar el árbol de navegación y el panel de mensajes.
D	Barra de control de cambio de tamaño	Haga clic y arrastre para cambiar el tamaño del árbol de navegación o el panel de mensajes.
D	Panel de mensajes	Se incluye solamente en algunas pantallas. Muestra los mensajes de estado relevantes para los procesos realizados en la pantalla.
E	Botones comunes	Los siguientes botones son comunes a todas las pantallas del instalador de STA: • **Help** (Ayuda): haga clic si desea ver ayuda contextual para la pantalla. • **Back** (Atrás): haga clic para ir a la pantalla anterior a fin de revisar o modificar la información introducida. Puede retroceder de a una pantalla a la vez hasta el comienzo de la instalación. • **Next** (Siguiente): haga clic para pasar a la siguiente pantalla después de introducir la información necesaria. • **Finish** (Finalizar): haga clic para completar la instalación. Este botón aparece activado solamente en la pantalla final. • **Cancel** (Cancelar): haga clic para cancelar la instalación en cualquier momento. Si ya se realizó parte de la instalación, el instalador revierte lo que se haya realizado y regresa el servidor al estado original. Se le pedirá que confirme la cancelación.

A.2.3. Ubicación de Instalación



Esta pantalla le permite especificar la ubicación del servidor en la que se instalará STA y el software de Oracle asociado.

No se puede instalar sobre una versión previamente instalada de STA. Para verificar que STA no esté ya instalado en una ubicación específica, puede introducir un directorio en el campo **Oracle Storage Home** (Directorio raíz de almacenamiento de Oracle) y hacer clic en el botón **View** (Ver).

- Si no se ha instalado software en esta ubicación, la lista aparece vacía.
- Si hay software instalado, se lo muestra como aparece en la Figura A.1, “Ejemplo de lista de directorio raíz de almacenamiento de Oracle”.

A.2.3.1. Campos de la pantalla

Oracle Storage Home (Directorio raíz de almacenamiento de Oracle)
Introduzca el directorio en el que se instalará STA y el software asociado de Oracle. Cada paquete de software se instalará en su propio subdirectorio dentro de este directorio. No se puede especificar un directorio en el que ya está instalado STA.

Consulte la Tabla 2.2, “Disposición recomendada para el sistema de archivos” para obtener recomendaciones técnicas sobre este directorio.

Según si el directorio ya existe o no, el usuario y el grupo de instalación de Oracle deben tener los siguientes permisos:

- Si el directorio existe, deben tener permisos completos para él.
- Si el directorio no existe, deben tener permisos completos para el directorio principal, de manera que el instalador de STA pueda crear el directorio raíz de almacenamiento de Oracle.

Debe introducir una ruta de acceso absoluta o hacer clic en el botón **Browse** (Examinar) para navegar hasta el directorio que desea especificar.

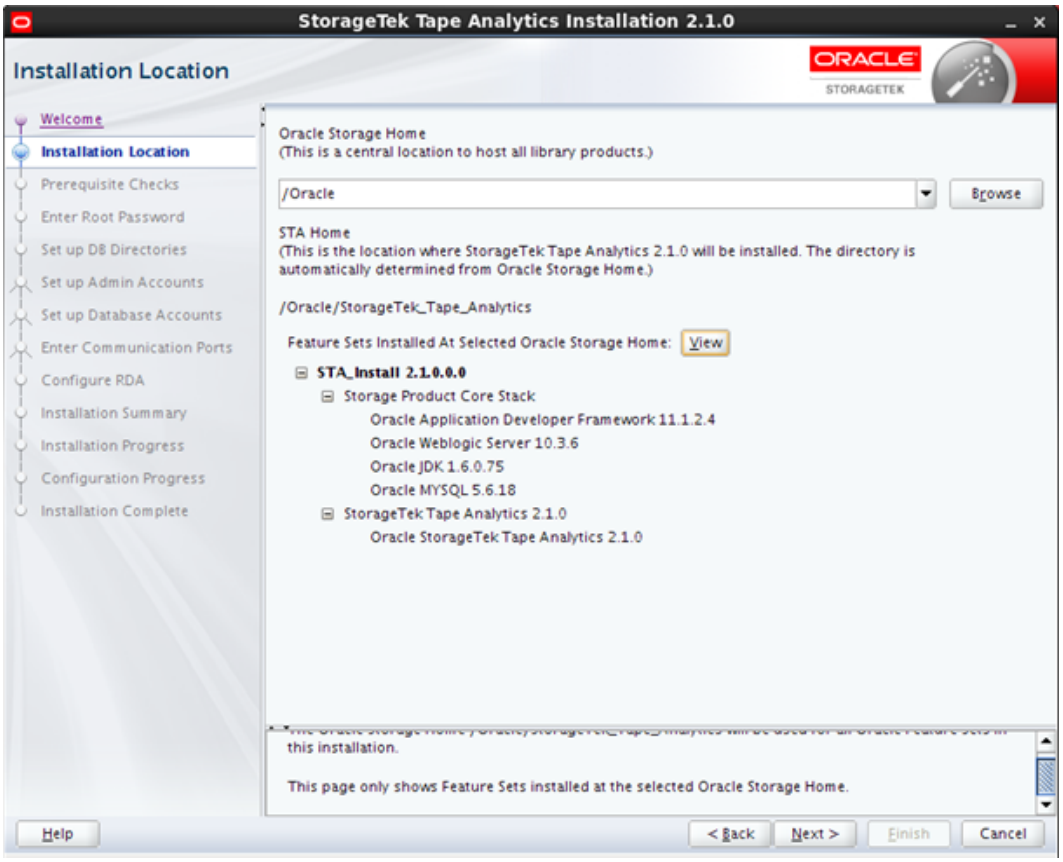
STA Home (Directorio raíz de STA)
Solo visualización. Es el subdirectorio dentro del directorio raíz de almacenamiento de Oracle en el que se instalará STA. Este subdirectorio recibe el nombre *`StorageTek_Tape_Analytics`* y es creado automáticamente durante la instalación.

A.2.3.2. Botones específicos de la pantalla

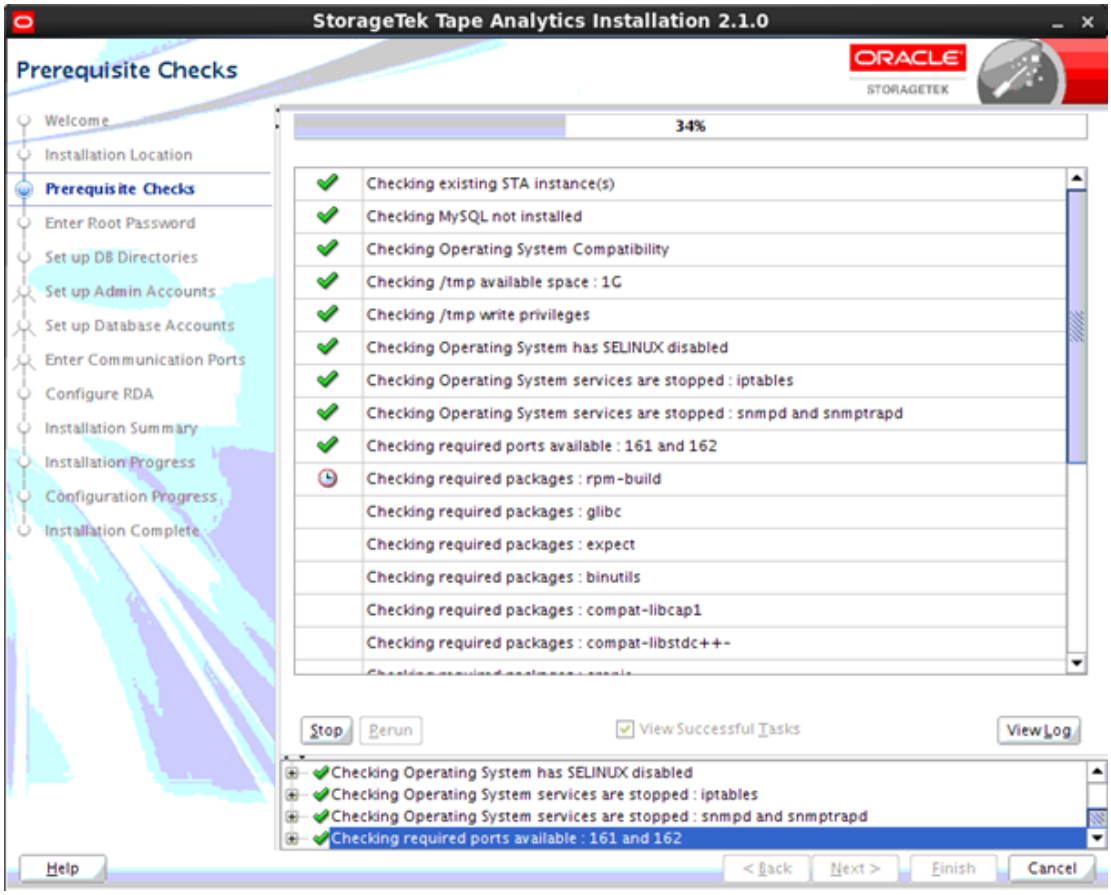
Browse (Examinar)
Haga clic para navegar hasta el directorio que desea especificar.

View/ (Ver/)
Haga clic para mostrar una lista de todo el software actualmente instalado en el directorio raíz de almacenamiento de Oracle especificado. En el caso de nuevas instalaciones, aparece en blanco. En la Figura A.1, “Ejemplo de lista de directorio raíz de almacenamiento de Oracle”, se muestra un ejemplo de la pantalla como se ve después de haber instalado STA.

Figura A.1. Ejemplo de lista de directorio raíz de almacenamiento de Oracle



A.2.4. Comprobaciones de requisitos



El instalador realiza una serie de tareas para verificar que el entorno del servidor cumpla todos los requisitos requeridos y recomendados. Este proceso puede tardar varios minutos.

Los resultados posibles de cada tarea de verificación son los siguientes:

- Correcto — El requisito se cumplió correctamente.
- Advertencia — El requisito recomendado no se cumplió.
- Error — El requisito requerido no se cumplió.

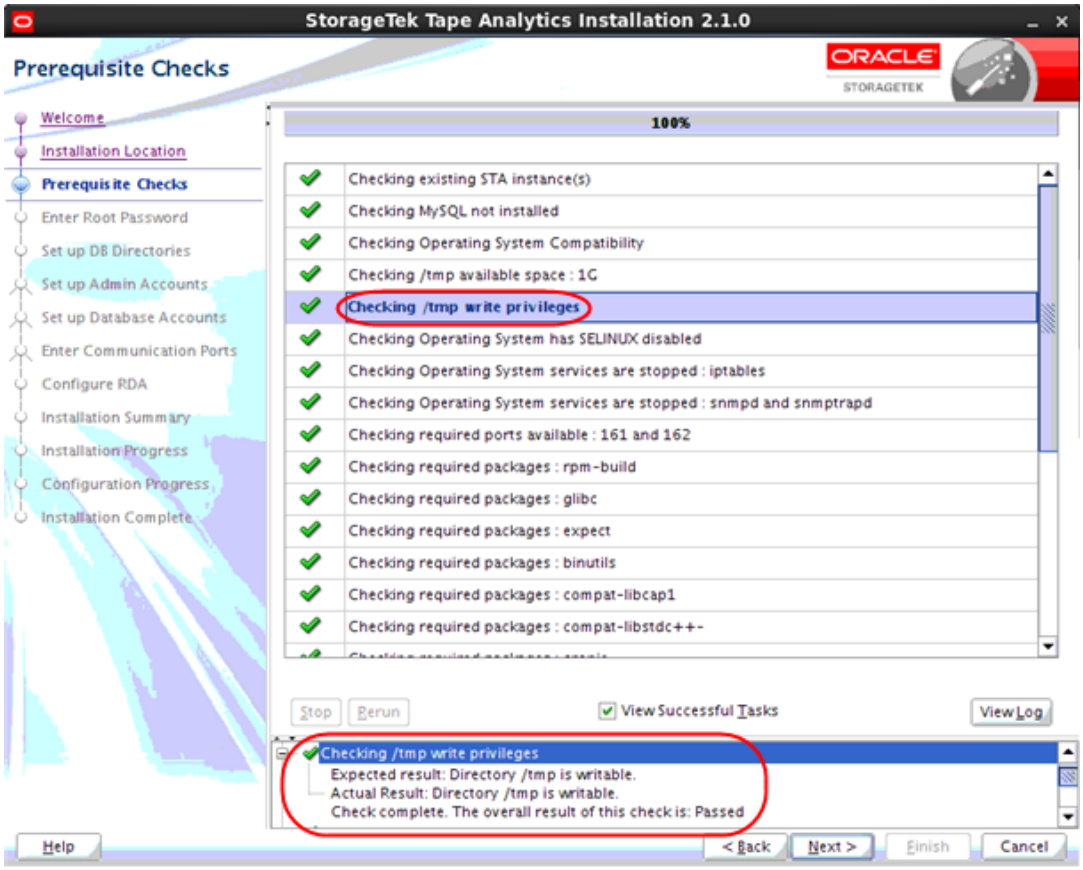
Si hay algún resultado con error, no se puede continuar con la instalación. Asimismo, se recomienda resolver todos los resultados con advertencia antes de continuar. Puede dejar el instalador en esta pantalla mientras resuelve los problemas y, después de resolverlos, regresar y hacer clic en **Rerun** (Volver a ejecutar) para ejecutar el proceso de verificación nuevamente.

En función de la naturaleza de un requisito, tal vez tenga que detener un servicio, cambiar privilegios de usuario o instalar un paquete Yum para resolver problemas. Puede usar

cualquiera de los siguientes métodos para mostrar información detallada que puede ser útil para resolver problemas y determinar qué se debe hacer.

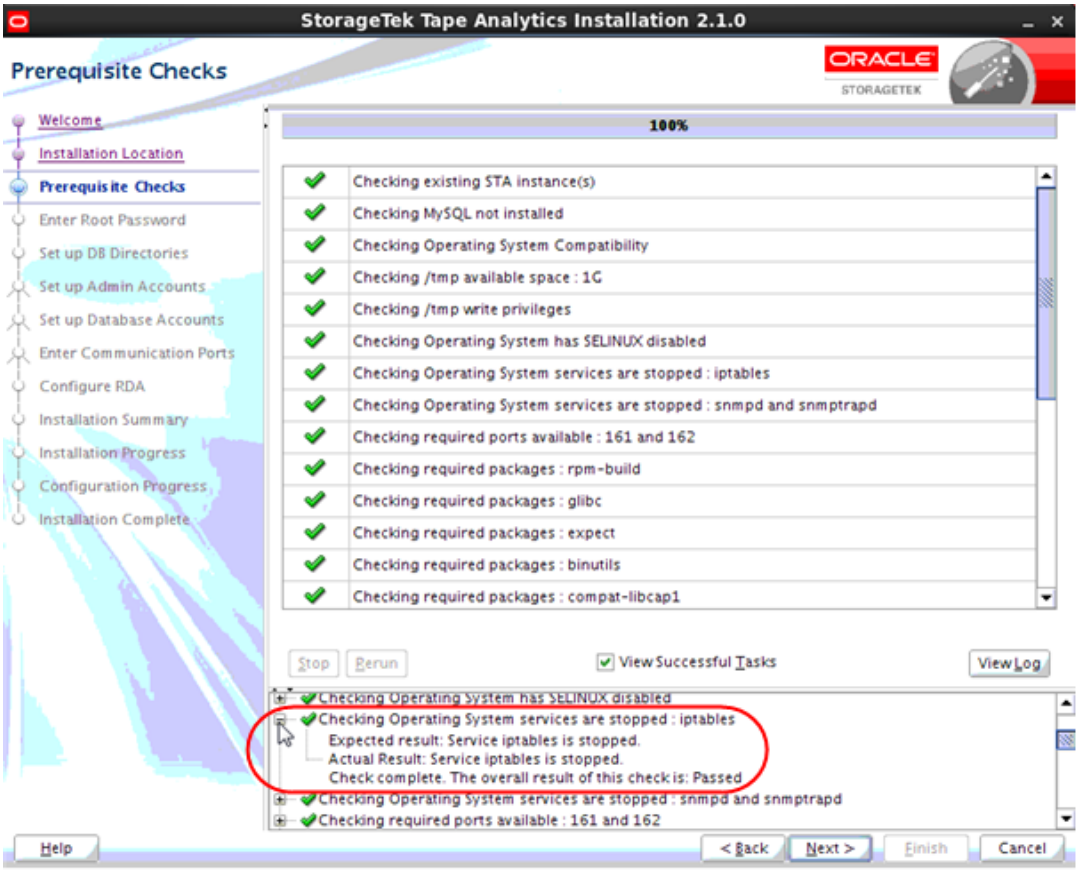
- Seleccione la tarea en la ventana principal. La tarea se resalta en el panel Message (Mensaje) con la información detallada. En la Figura A.2, “Detalle de la tarea que se muestra al seleccionarla en la ventana principal”, se muestra un ejemplo.

Figura A.2. Detalle de la tarea que se muestra al seleccionarla en la ventana principal



- En el panel Message (Mensaje), haga clic en el **ícono para expandir** (+) que se encuentra junto a la tarea cuya información detallada desea ver. La Figura A.3, “Información detallada de la tarea que se muestra al seleccionar el ícono para expandir” es un ejemplo. Haga clic en el **ícono para contraer** (-) para volver a ocultar la información detallada.

Figura A.3. Información detallada de la tarea que se muestra al seleccionar el ícono para expandir



A.2.4.1. Campos de la pantalla

Ninguno

A.2.4.2. Botones específicos de la pantalla

Stop (Parar)
Haga clic para detener el proceso de verificación en la tarea actual. Esto puede resultar útil para ver la información detallada de una tarea seleccionada que ya ha finalizado.

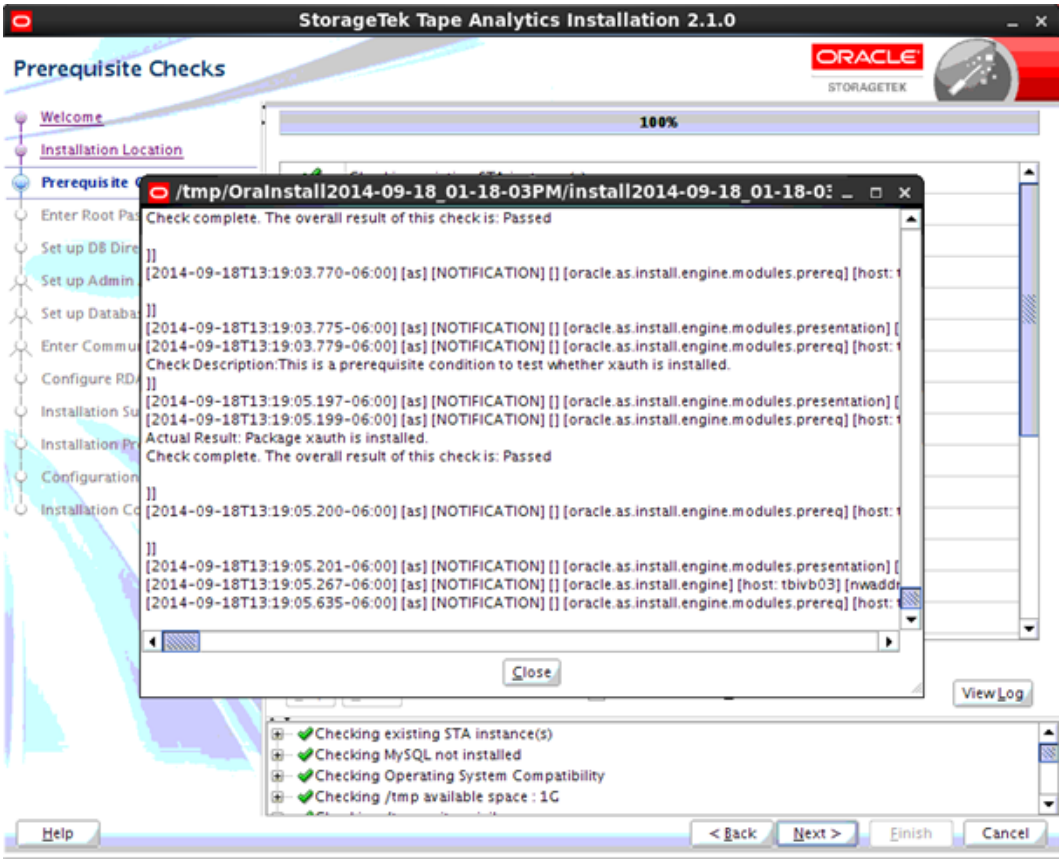
Rerun (Volver a ejecutar)
Haga clic para ejecutar el proceso de verificación nuevamente desde el comienzo. Esto le permite resolver resultados con error o advertencia sin tener que salir del instalador de STA ni reiniciarlo.

View Successful Tasks (Ver tareas correctas)
Seleccione la casilla de verificación para incluir los resultados correctos en la visualización; esta es la configuración predeterminada.

Anule la selección de la casilla de verificación para que se muestren solo los resultados con error o advertencia. Esto le permite filtrar las tareas que se realizaron correctamente para poder concentrarse en las que necesitan atención.

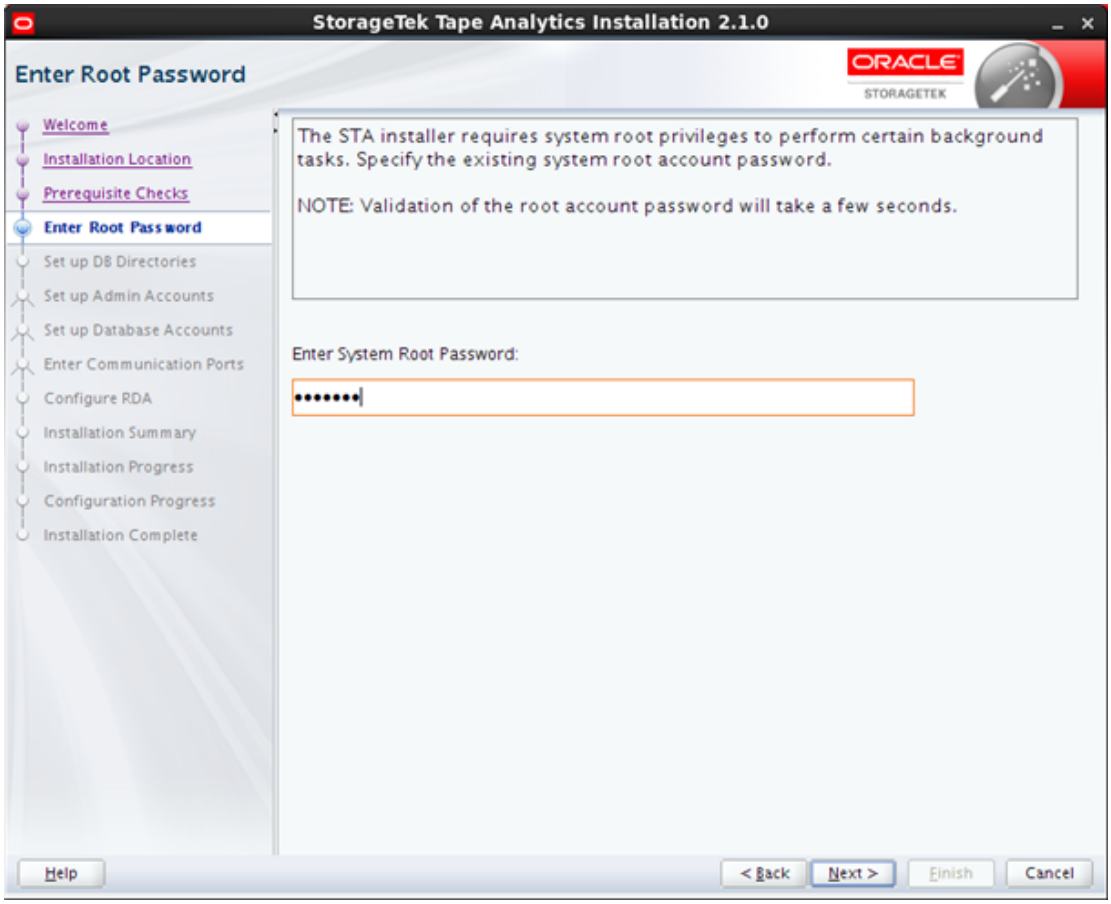
View Log (Ver log)
Haga clic para mostrar el log de verificación de requisitos en otra ventana. En la Figura A.4, “Ejemplo de visualización de log de verificación de requisitos”, se muestra un ejemplo. Haga clic en **Close** (Cerrar) para descartar la ventana del log.

Figura A.4. Ejemplo de visualización de log de verificación de requisitos



También puede ver el log desde la línea de comandos de Linux. Mientras el instalador se ejecuta, los logs se guardan en un subdirectorio dentro de `/tmp`. Consulte Sección 3.4, “Logs de instalación y desinstalación de STA” para obtener información detallada.

A.2.5. Introducción de la contraseña del usuario root



El instalador de STA requiere acceso de root de Linux para realizar la instalación.

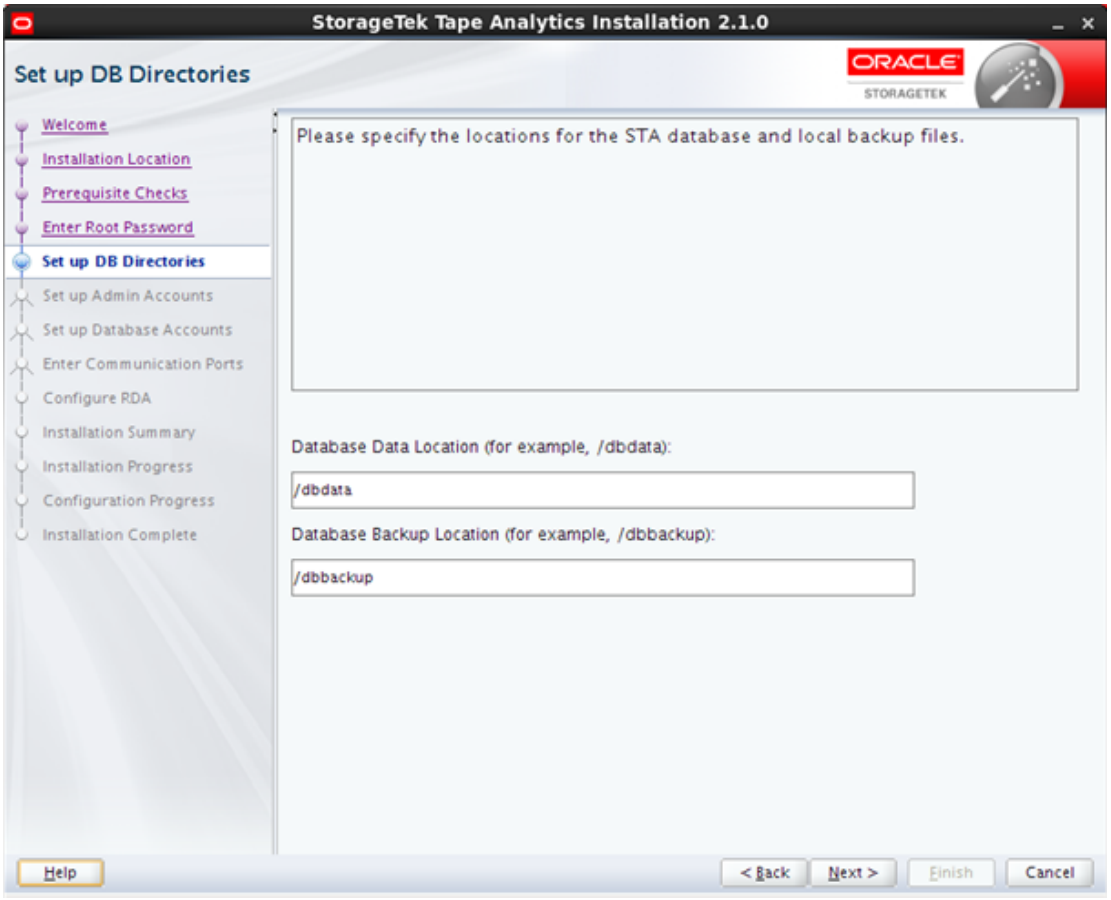
A.2.5.1. Campos de la pantalla

Enter Root Password (Introducir contraseña de usuario root)
Escriba la contraseña del usuario root de Linux. La entrada se muestra enmascarada. La validación de la contraseña puede tardar varios segundos.

A.2.5.2. Botones específicos de la pantalla

Ninguno

A.2.6. Configuración de directorios de la base de datos



Esta pantalla le permite especificar las ubicaciones para la base de datos de STA y las copias de seguridad locales de la base de datos de STA. El instalador de STA crea estos directorios si todavía no existen.

Consulte *Guía de administración de STA* para obtener información sobre la administración de los servicios y las copias de seguridad de base de datos.

A.2.6.1. Campos de la pantalla

Database Data Location (Ubicación de datos de la base de datos)
Introduzca el directorio en el que se ubicará la base de datos de STA. Este directorio no puede ser el mismo que el de **Database Backup Location** (Ubicación de la copia de seguridad de la base de datos). Debe especificar una ruta de acceso absoluta.

Si el directorio especificado ya contiene un subdirectorio de base de datos (`mysql`), aparece un mensaje de advertencia. Puede especificar otra ubicación para la base de datos o aceptar la entrada actual, en cuyo caso el subdirectorio de base de datos se elimina durante la instalación de STA.

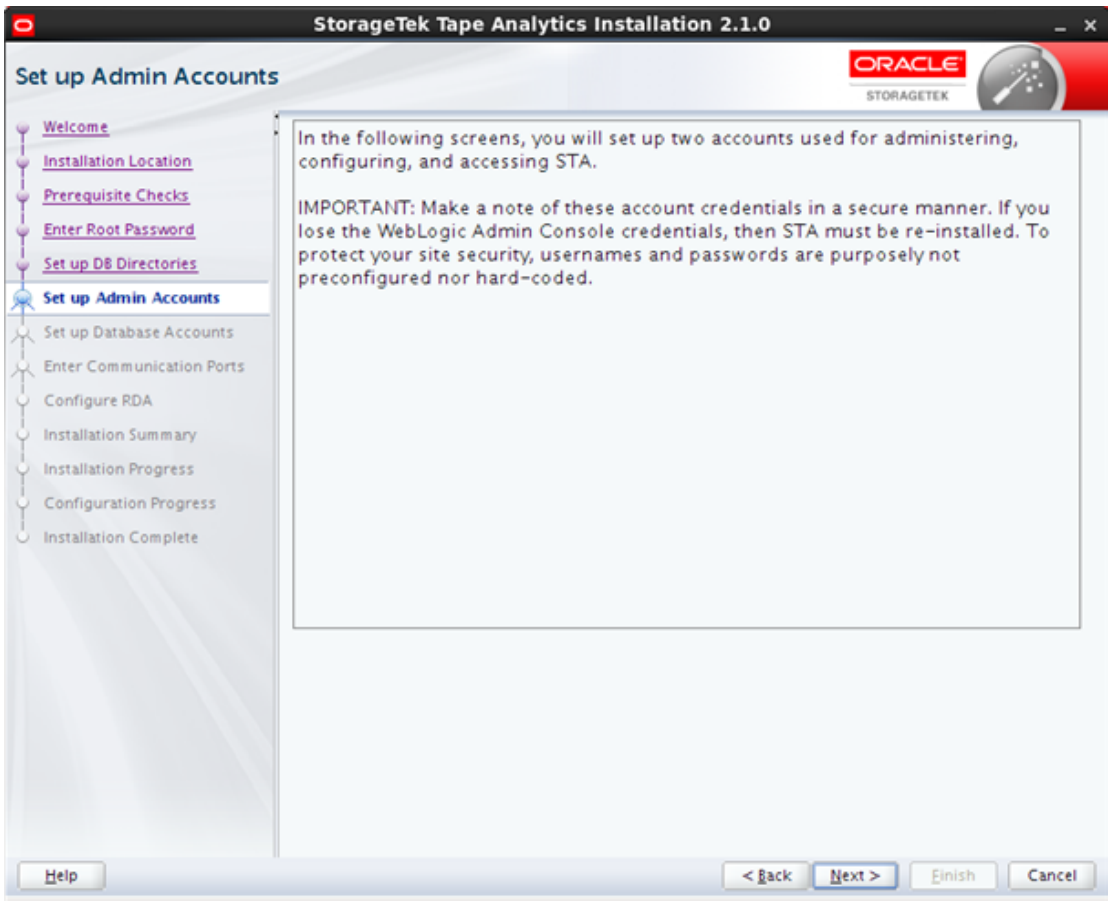
Database Backup Location (Ubicación de la copia de seguridad de la base de datos) Introduzca el directorio en el que se ubicarán las copias de seguridad de la base de datos de STA en el servidor. Este directorio no puede ser el mismo que el de **Database Data Location** (Ubicación de datos de la base de datos). Debe especificar una ruta de acceso absoluta.

Si el directorio especificado ya contiene un subdirectorio de copia de seguridad de base de datos (`local`), aparece un mensaje de advertencia. Puede especificar otra ubicación para las copias de seguridad o aceptar la entrada actual, en cuyo caso el subdirectorio de copias de seguridad se elimina durante la instalación de STA.

A.2.6.2. Botones específicos de la pantalla

Ninguno

A.2.7. Configuración de cuentas de administración



En esta pantalla, se describen los tipos de información que definirá en las siguientes dos pantallas. Lea el texto y, a continuación, haga clic en **Next** (Siguiente) para continuar.

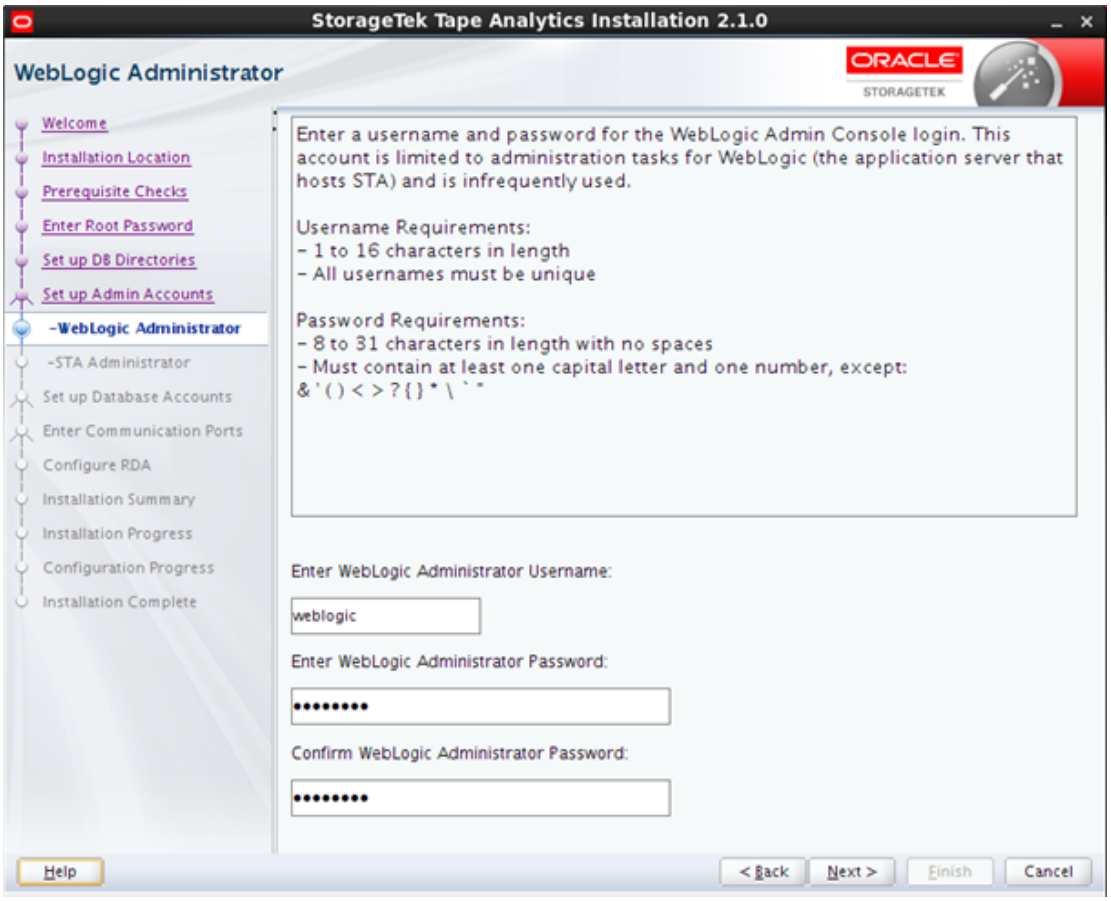
A.2.7.1. Campos de la pantalla

Ninguno

A.2.7.2. Botones específicos de la pantalla

Ninguno

A.2.8. Administrador de WebLogic



WebLogic es el servidor de aplicaciones en el que se aloja STA. La cuenta WebLogic Administrator (Administrador de WebLogic) se usa para iniciar sesión en la consola de administración de WebLogic para configurar y administrar el servidor WebLogic. Esta cuenta no se usa con mucha frecuencia.

La cuenta se crea durante la instalación con las credenciales que usted especifica.

Precaución:

Registre de forma segura estas credenciales de la cuenta, porque, si las pierde, no podrá iniciar sesión en la consola de administración de WebLogic y deberá reinstalar STA.

Para proteger la seguridad del sitio, los nombres de usuario y las contraseñas no se configuran de manera previa ni se codifican.

A.2.8.1. Campos de la pantalla

Enter Username (Introducir nombre de usuario)
Escriba el nombre que desea asignar a la cuenta de administrador de WebLogic.

Los requisitos para los nombres de usuario son los siguientes:

- Debe tener de 1 a 16 caracteres.
- Todos los nombres de usuario deben ser únicos.

Enter Password (Introducir contraseña)
Escriba la contraseña que desea asignar a esta cuenta. La entrada se muestra enmascarada.

Los requisitos para las contraseñas son los siguientes:

- Debe tener de 8 a 31 caracteres.
- Debe incluir al menos un número y una letra mayúscula.
- No debe tener espacios.
- No debe incluir ninguno de los siguientes caracteres especiales:

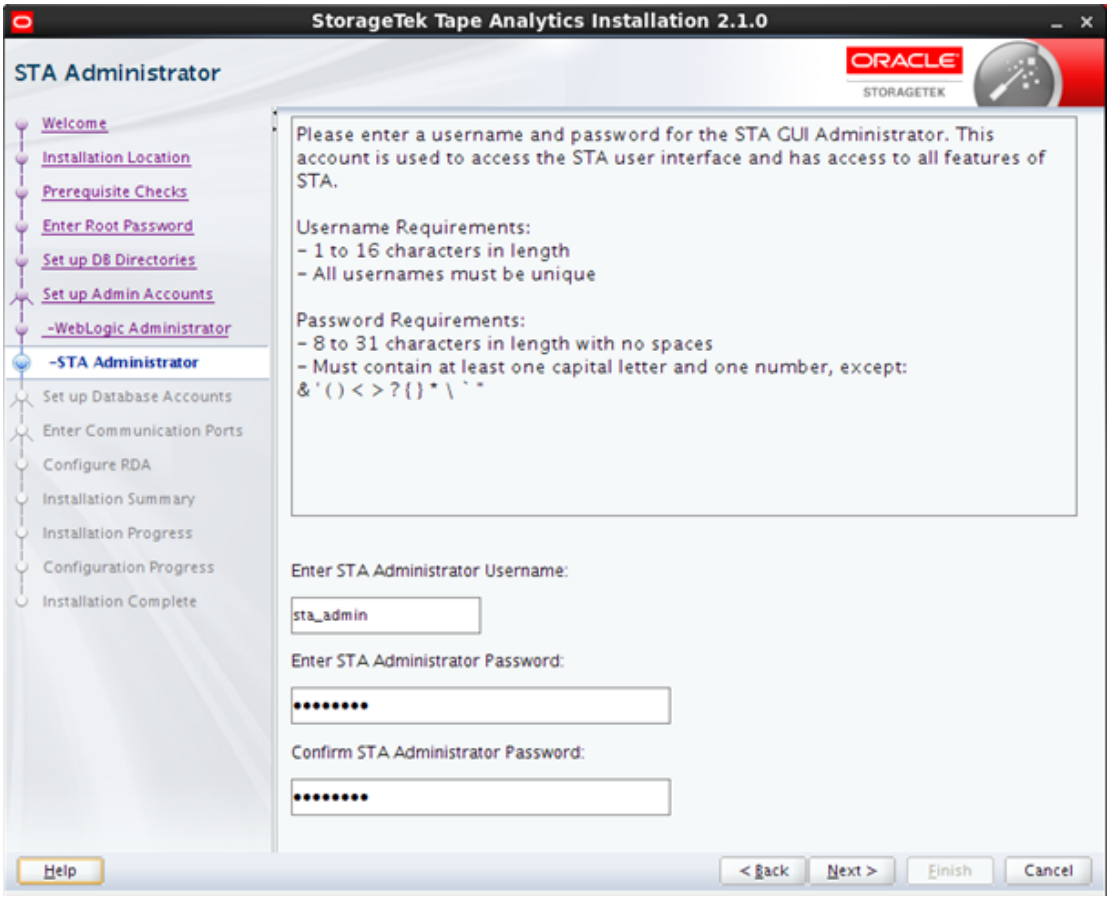
```
& ' ( ) < > ? { } *  / ' "
```

Confirm Password (Confirmar contraseña)
Vuelva a escribir la contraseña para asegurarse de haberla escrito bien.

A.2.8.2. Botones específicos de la pantalla

Ninguno

A.2.9. Administrador de STA



La cuenta de administrador de STA se usa para iniciar sesión en la interfaz de usuario de STA. Este usuario tiene privilegios de administrador para la aplicación STA y, por lo tanto, tiene acceso a todas las pantallas de STA.

La cuenta se crea durante la instalación con las credenciales que usted especifica.

Precaución:

Registre de forma segura estas credenciales de la cuenta, porque si las pierde no podrá iniciar sesión en la interfaz de usuario de STA.

Para proteger la seguridad del sitio, los nombres de usuario y las contraseñas no se configuran de manera previa ni se codifican.

A.2.9.1. Campos de la pantalla

Enter Username (Introducir nombre de usuario)
Escriba el nombre de usuario que desea asignar al administrador de STA.

Los requisitos para los nombres de usuario son los siguientes:

- Debe tener de 1 a 16 caracteres.

- Todos los nombres de usuario deben ser únicos.

Enter Password (Introducir contraseña)
Escriba la contraseña que desea asignar a esta cuenta. La entrada se muestra enmascarada.

Los requisitos para las contraseñas son los siguientes:

- Debe tener de 8 a 31 caracteres.
- Debe incluir al menos un número y una letra mayúscula.
- No debe tener espacios.
- No debe incluir ninguno de los siguientes caracteres especiales:

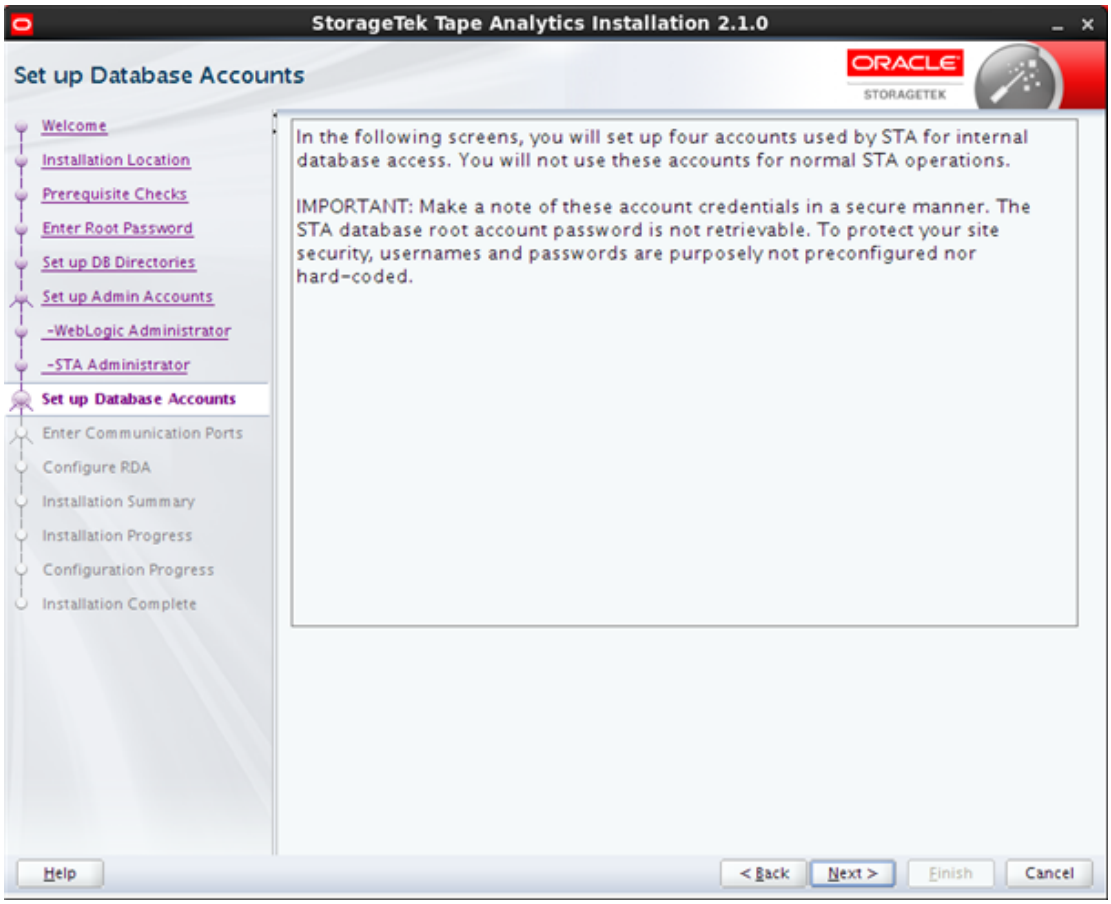
```
& ' ( ) < > ? { } *  / ' "
```

Confirm Password (Confirmar contraseña)
Vuelva a escribir la contraseña para asegurarse de haberla escrito bien.

A.2.9.2. Botones específicos de la pantalla

Ninguno

A.2.10. Configuración de cuentas de base de datos



En esta pantalla, se describen los tipos de información que definirá en las siguientes cuatro pantallas. Lea el texto y, a continuación, haga clic en **Next** (Siguiente) para continuar.

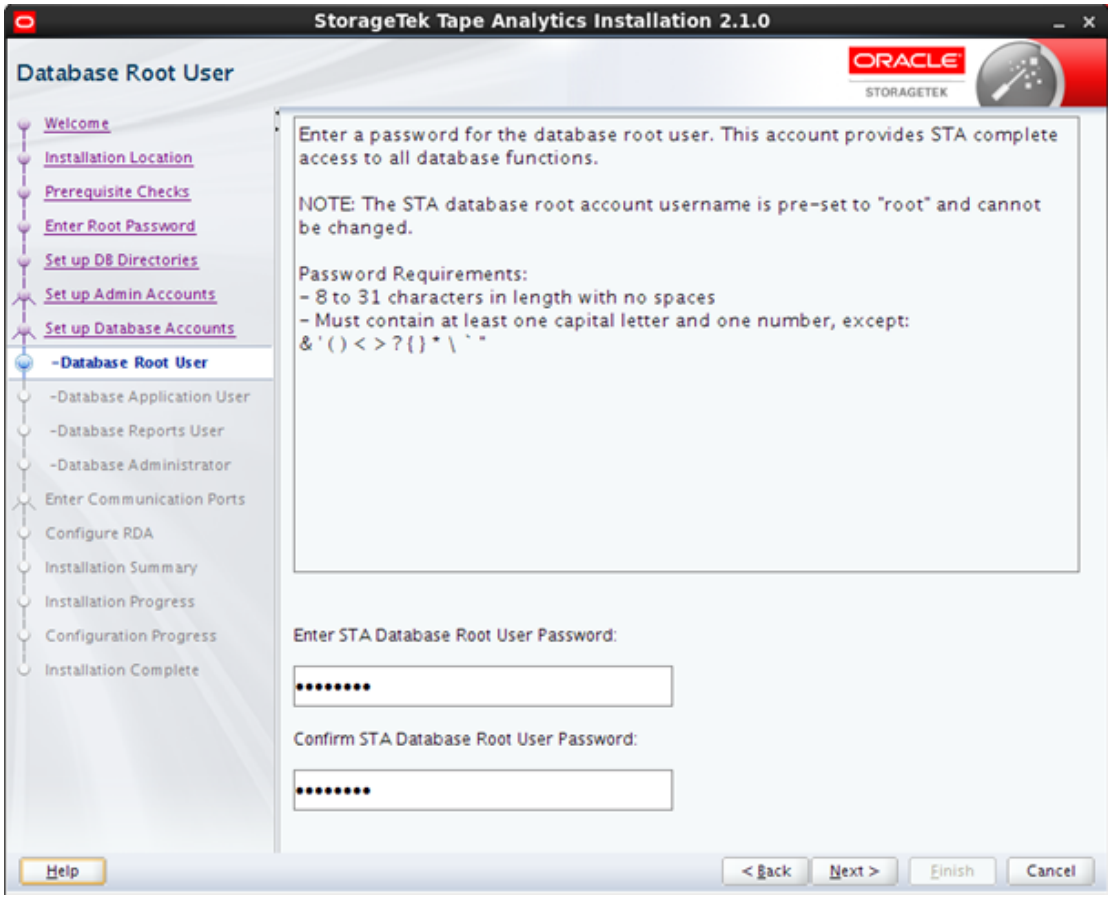
A.2.10.1. Campos de la pantalla

Ninguno

A.2.10.2. Botones específicos de la pantalla

Ninguno

A.2.11. Usuario root de la base de datos



El usuario root de la base de datos de STA es el propietario de la base de datos de STA. Esta cuenta es utilizada internamente por la aplicación de STA para crear la base de datos y proporciona acceso completo a todas las tablas de la base de datos. Esta cuenta no se usa para las operaciones normales de STA.

El nombre de usuario de esta cuenta se define automáticamente como `root` y no se puede cambiar. Se trata de una cuenta de MySQL y es independiente del usuario root de Linux. Esta cuenta se crea durante la instalación con las credenciales que usted especifica.

Nota:

Registre de forma segura las credenciales de la cuenta.

Para proteger la seguridad del sitio, los nombres de usuario y las contraseñas no se configuran de manera previa ni se codifican.

A.2.11.1. Campos de la pantalla

Enter Password (Introducir contraseña)
Escriba la contraseña que desea asignar al usuario root de la base de datos de STA. La entrada se muestra enmascarada.

Los requisitos para las contraseñas son los siguientes:

- Debe tener de 8 a 31 caracteres.
- Debe incluir al menos un número y una letra mayúscula.
- No debe tener espacios.
- No debe incluir ninguno de los siguientes caracteres especiales:

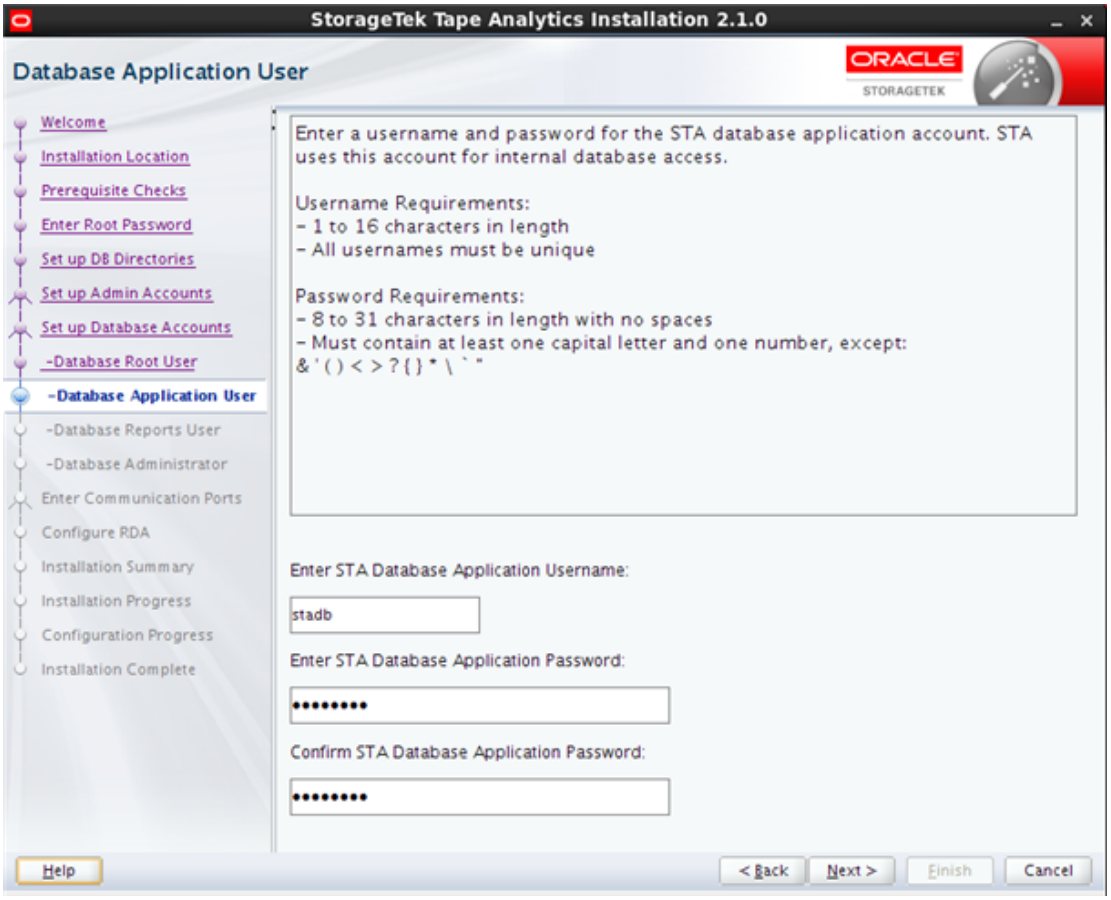
```
& ' ( ) < > ? { } *  / ' "
```

Confirm Password (Confirmar contraseña)
Vuelva a escribir la contraseña para asegurarse de haberla escrito bien.

A.2.11.2. Botones específicos de la pantalla

Ninguno

A.2.12. Usuario de aplicación de base de datos



La cuenta de la aplicación de la base de datos es una cuenta de MySQL que es utilizada internamente por la aplicación de STA para conectarse a la base de datos de STA y actualizarla. La cuenta proporciona acceso de creación, actualización, supresión y lectura para todas las tablas de la base de datos. Esta cuenta no se usa para las operaciones normales de STA.

Esta cuenta se crea durante la instalación con las credenciales que usted especifica.

Nota:

Registre de forma segura las credenciales de la cuenta.

Para proteger la seguridad del sitio, los nombres de usuario y las contraseñas no se configuran de manera previa ni se codifican.

A.2.12.1. Campos de la pantalla

Enter Username (Introducir nombre de usuario)
Escriba el nombre que desea asignar a la cuenta de la aplicación de la base de datos de STA, por ejemplo, *`stadb`*.

Los requisitos para los nombres de usuario son los siguientes:

- Debe tener de 1 a 16 caracteres.
- Todos los nombres de usuario deben ser únicos.

Enter Password (Introducir contraseña)
Escriba la contraseña que desea asignar a la cuenta de la aplicación de la base de datos de STA. La entrada se muestra enmascarada.

Los requisitos para las contraseñas son los siguientes:

- Debe tener de 8 a 31 caracteres.
- Debe incluir al menos un número y una letra mayúscula.
- No debe tener espacios.
- No debe incluir ninguno de los siguientes caracteres especiales:

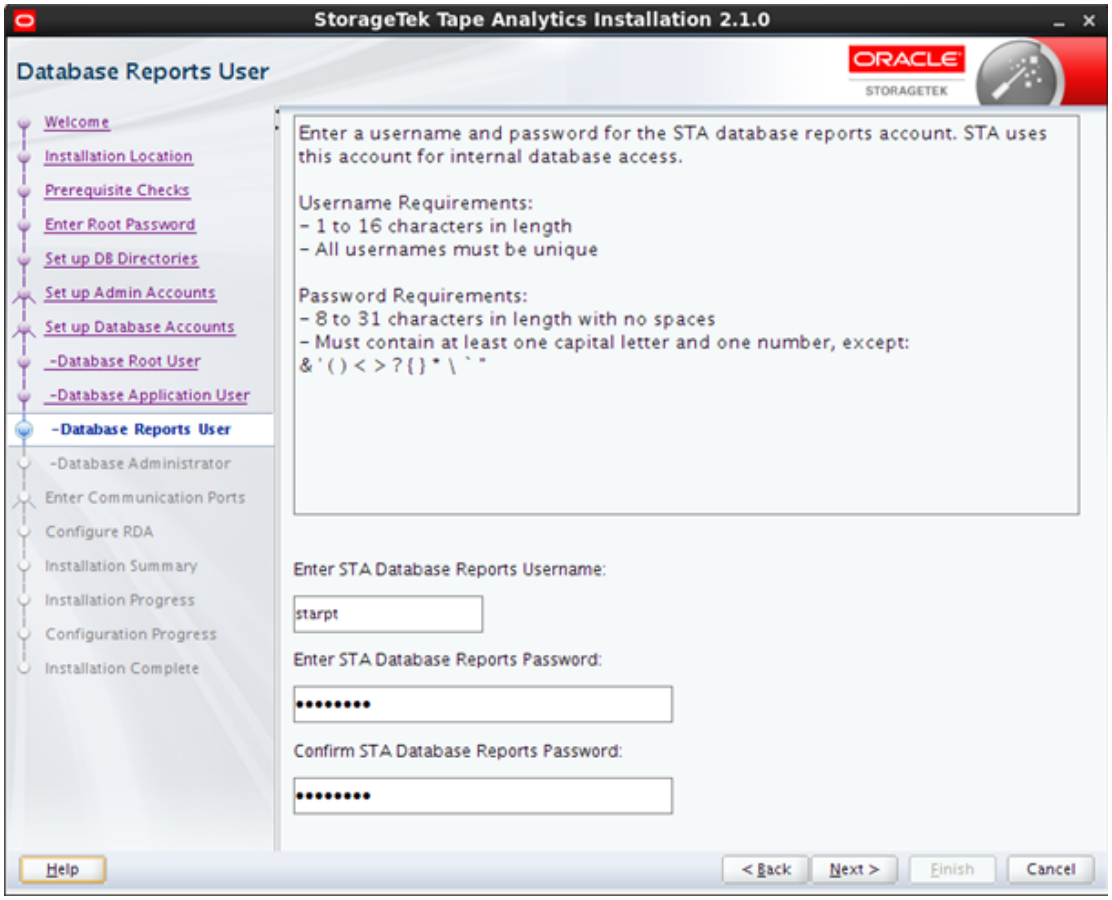
```
& ' ( ) < > ? { } *  / ' "
```

Confirm Password (Confirmar contraseña)
Vuelva a escribir la contraseña para asegurarse de haberla escrito bien.

A.2.12.2. Botones específicos de la pantalla

Ninguno

A.2.13. Usuario de informes de la base de datos



La cuenta de informes de la base de datos de STA es una cuenta de MySQL que es utilizada por las aplicaciones que no son STA y las aplicaciones de terceros para conectarse a la base de datos de STA. La cuenta proporciona acceso de solo lectura a tablas seleccionadas de la base de datos. Esta cuenta no se usa para las operaciones normales de STA.

Esta cuenta se crea durante la instalación con las credenciales que usted especifica.

Nota:

Registre de forma segura las credenciales de la cuenta.

Para proteger la seguridad del sitio, los nombres de usuario y las contraseñas no se configuran de manera previa ni se codifican.

A.2.13.1. Campos de la pantalla

Enter Username (Introducir nombre de usuario)
Escriba el nombre que desea asignar a la cuenta de informes de la base de datos de STA, por ejemplo, `starpt`.

Los requisitos para los nombres de usuario son los siguientes:

- Debe tener de 1 a 16 caracteres.
- Todos los nombres de usuario deben ser únicos.

Enter Password (Introducir contraseña)
Escriba la contraseña que desea asignar a esta cuenta. La entrada se muestra enmascarada.

Los requisitos para las contraseñas son los siguientes:

- Debe tener de 8 a 31 caracteres.
- Debe incluir al menos un número y una letra mayúscula.
- No debe tener espacios.
- No debe incluir ninguno de los siguientes caracteres especiales:

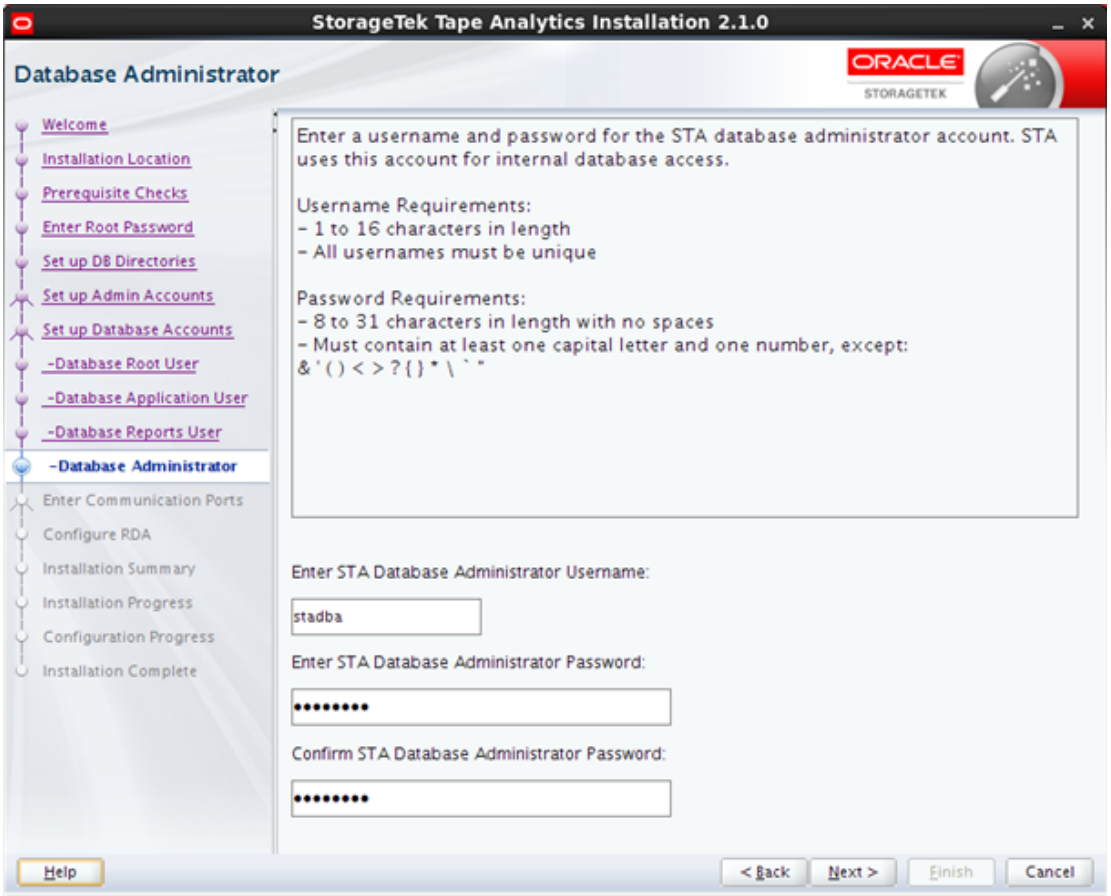
```
& ' ( ) < > ? { } *  / ' "
```

Confirm Password (Confirmar contraseña)
Vuelva a escribir la contraseña para asegurarse de haberla escrito bien.

A.2.13.2. Botones específicos de la pantalla

Ninguno

A.2.14. Administrador de la base de datos



La cuenta de administrador de la base de datos de STA es una cuenta de MySQL que es usada internamente por las utilidades de administración y supervisión de STA para conectarse a la base de datos de STA y configurar y ejecutar copias de seguridad programadas. La cuenta proporciona acceso completo, excepto por la opción "grant" (otorgar), a todas las tablas de la base de datos. Esta cuenta no se usa para las operaciones normales de STA.

Esta cuenta se crea durante la instalación con las credenciales que usted especifica.

Nota:

Registre de forma segura las credenciales de la cuenta.

Para proteger la seguridad del sitio, los nombres de usuario y las contraseñas no se configuran de manera previa ni se codifican.

A.2.14.1. Campos de la pantalla

Enter Username (Introducir nombre de usuario)
Escriba el nombre que desea asignar a la cuenta de administrador de la base de datos de STA, por ejemplo, `stadba`.

Los requisitos para los nombres de usuario son los siguientes:

- Debe tener de 1 a 16 caracteres.
- Todos los nombres de usuario deben ser únicos.

Enter Password (Introducir contraseña)
Escriba la contraseña que desea asignar a esta cuenta. La entrada se muestra enmascarada.

Los requisitos para las contraseñas son los siguientes:

- Debe tener de 8 a 31 caracteres.
- Debe incluir al menos un número y una letra mayúscula.
- No debe tener espacios.
- No debe incluir ninguno de los siguientes caracteres especiales:

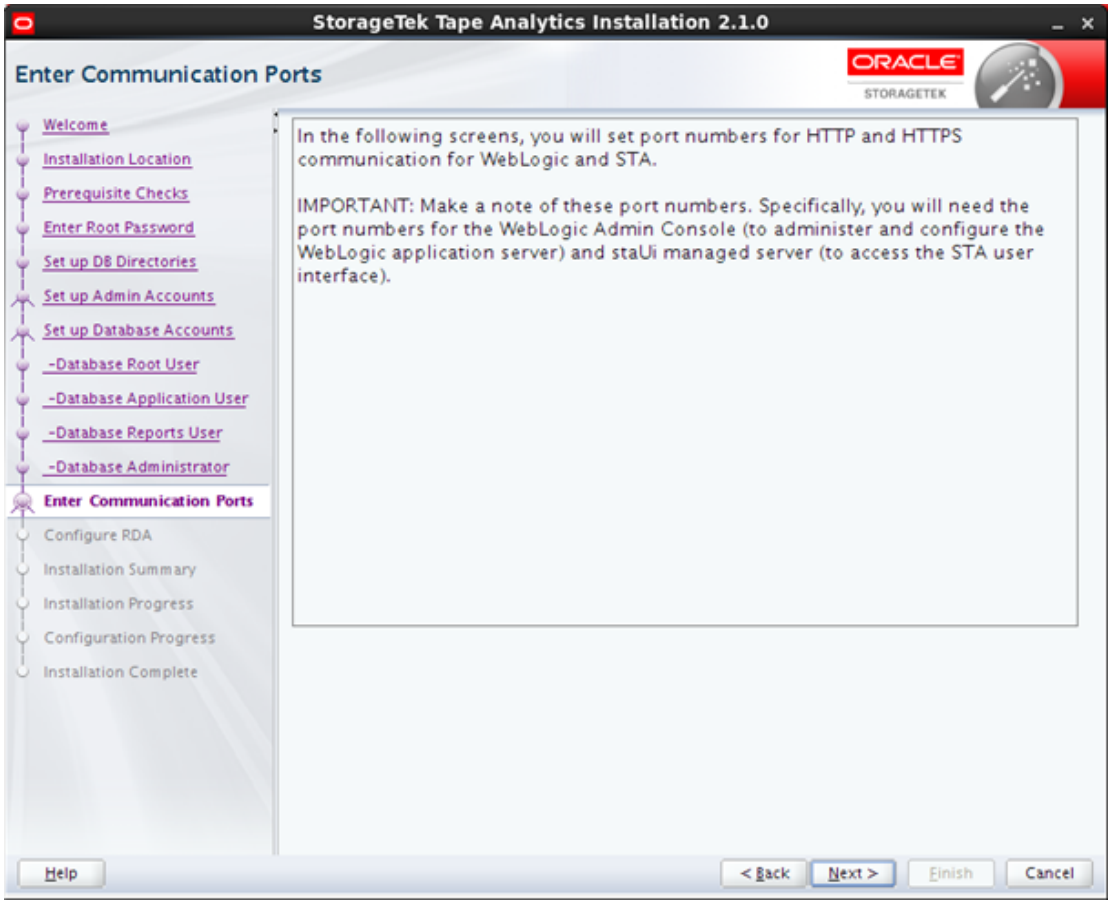
```
& ' ( ) < > ? { } *  / ' "
```

Confirm Password (Confirmar contraseña)
Vuelva a escribir la contraseña para asegurarse de haberla escrito bien.

A.2.14.2. Botones específicos de la pantalla

Ninguno

A.2.15. Introducción de puertos de comunicación



En esta pantalla, se describen los tipos de información que definirá en las siguientes cuatro pantallas. Lea el texto y, a continuación, haga clic en **Next** (Siguiente) para continuar.

Debe proporcionar valores para los puertos internos y externos configurables de WebLogic y STA. Durante la instalación, los puertos se configuran y activan con los valores que especifica. Los números de puerto que especifica deben ser únicos, y los puertos deben estar siempre disponibles y dedicados para STA.

Nota:

Antes de completar estas pantallas, verifique los valores de número de puerto correctos con el administrador de la red. Una vez que STA se haya instalado, los números de puerto no se pueden cambiar sin desinstalar y reinstalar STA.

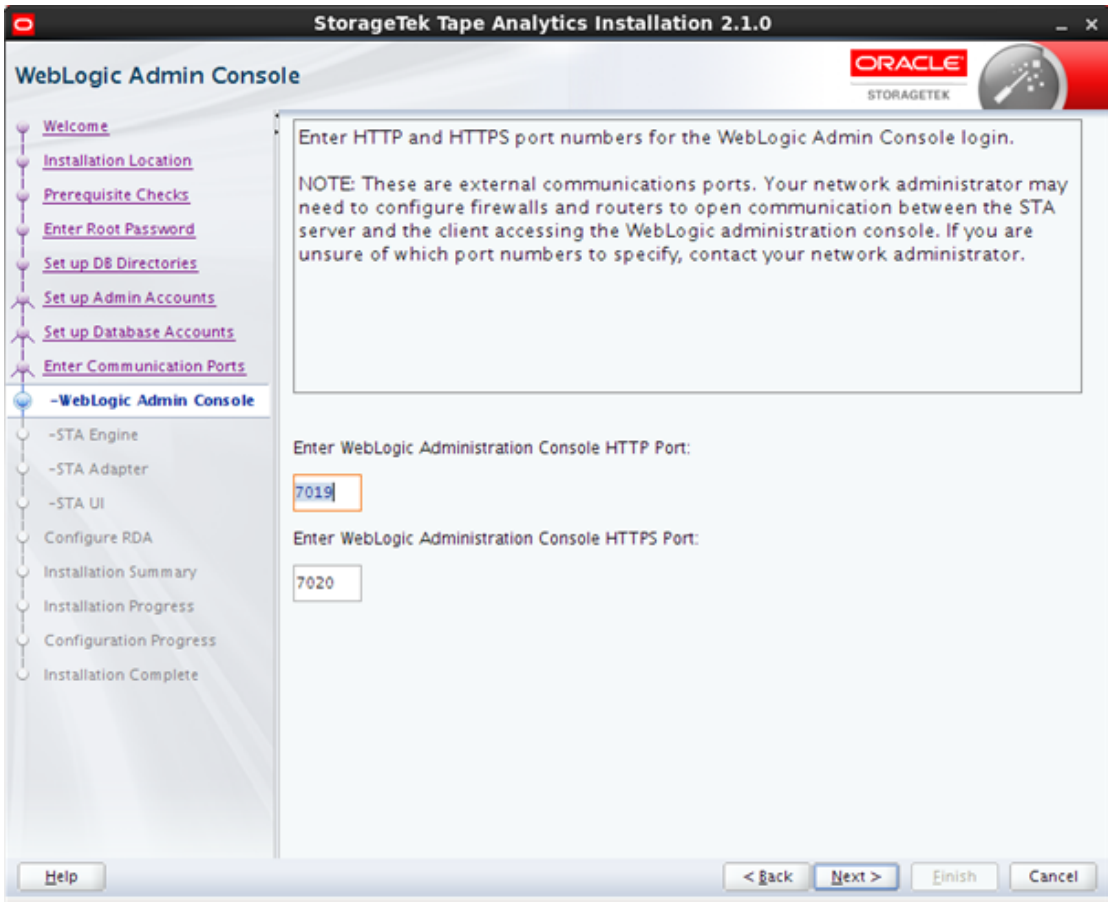
A.2.15.1. Campos de la pantalla

Ninguno

A.2.15.2. Botones específicos de la pantalla

Ninguno

A.2.16. Consola de administración de WebLogic



El número de puerto de la consola de administración de WebLogic se especifica al iniciar sesión en dicha consola, que se usa para administrar y configurar el servidor de aplicaciones de WebLogic.

Nota:

Son puertos de comunicación externos. El administrador de la red puede necesitar configurar firewalls y enrutadores para abrir la comunicación entre el servidor de STA y el cliente que accede a la consola de administración de WebLogic.

Nota:

Registre de forma segura estos números de puerto, ya que no se pueden cambiar una vez que se instala STA.

Para proteger la seguridad del sitio, estos números no se configuran de manera previa ni se codifican.

A.2.16.1. Campos de la pantalla

Enter HTTP Port (Introducir puerto HTTP)
Introduzca el número de puerto HTTP para el acceso no seguro al inicio de sesión de la consola de administración de WebLogic. Normalmente, este puerto es el 7019.

Los números de puerto deben ser únicos y estar disponibles.

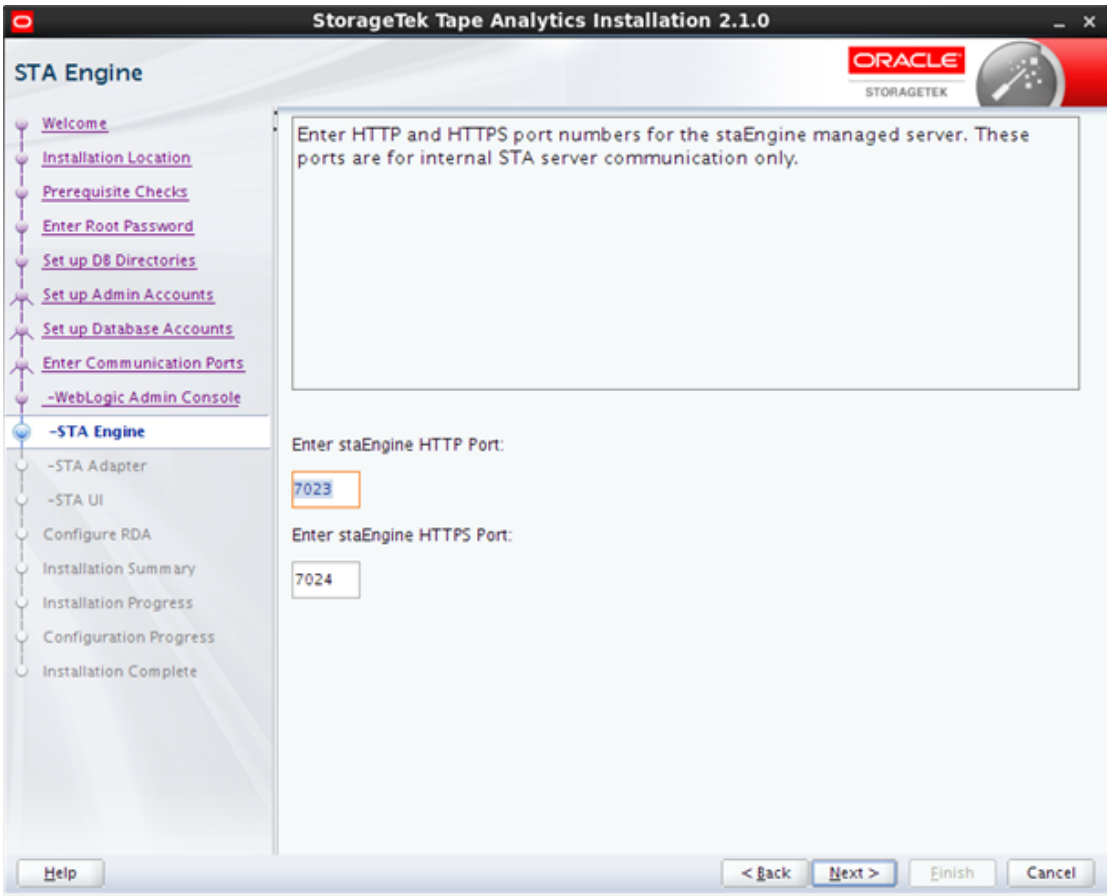
Enter HTTPS Port (Introducir puerto HTTPS)
Introduzca el número de puerto HTTPS para el acceso seguro al inicio de sesión de la consola de administración de WebLogic. Normalmente, este puerto es el 7020.

Los números de puerto deben ser únicos y estar disponibles.

A.2.16.2. Botones específicos de la pantalla

Ninguno

A.2.17. Motor de STA



Los puertos del servidor gestionado staEngine se usan solo para la comunicación interna del servidor de STA.

Nota:

Registre de forma segura estos números de puerto, ya que no se pueden cambiar una vez que se instala STA.

Para proteger la seguridad del sitio, estos números no se configuran de manera previa ni se codifican.

A.2.17.1. Campos de la pantalla

Enter HTTP Port (Introducir puerto HTTP)
Introduzca el número de puerto HTTP para el acceso no seguro al servidor gestionado staEngine. Normalmente, este puerto es el 7023.

Los números de puerto deben ser únicos y estar disponibles.

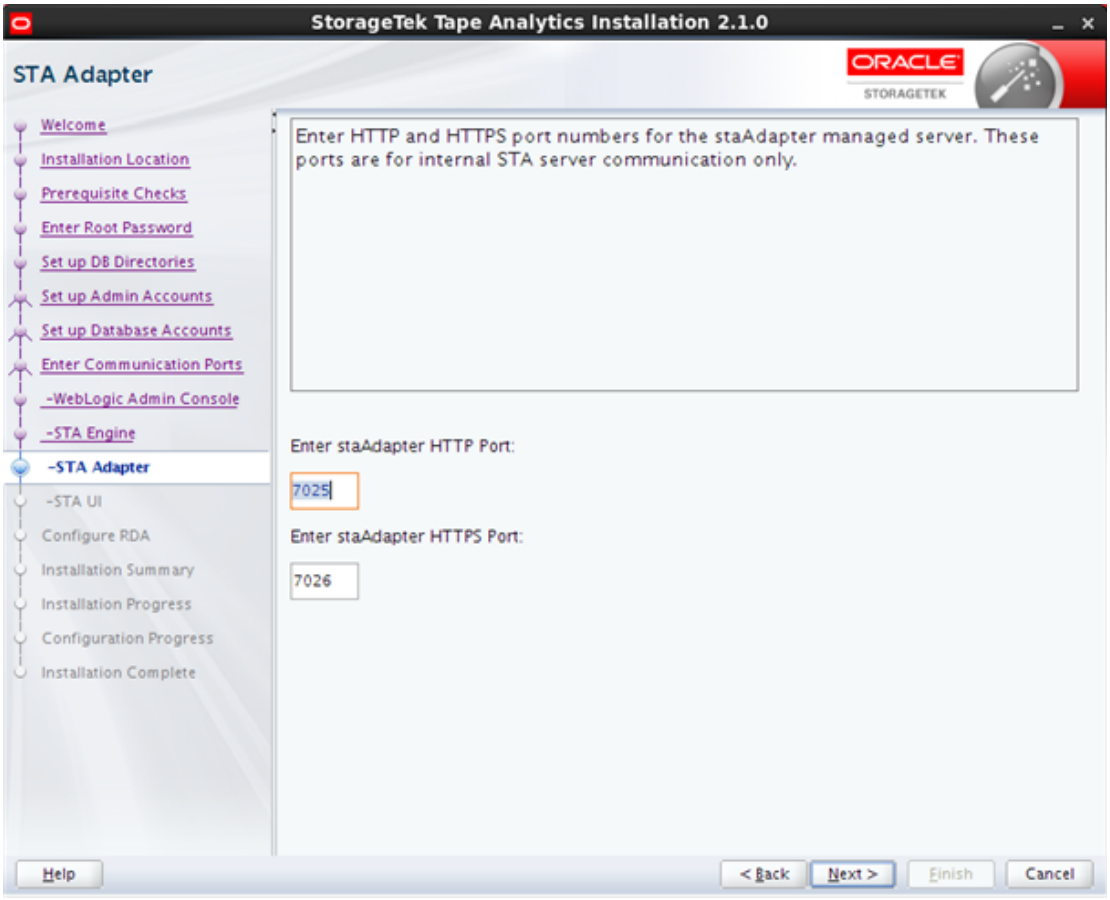
Enter HTTPS Port (Introducir puerto HTTPS)
Introduzca el número de puerto HTTPS para el acceso seguro al servidor gestionado staEngine. Normalmente, este puerto es el 7024.

Los números de puerto deben ser únicos y estar disponibles.

A.2.17.2. Botones específicos de la pantalla

Ninguno

A.2.18. Adaptador de STA



Los puertos del servidor gestionado staAdapter se usan solo para la comunicación de SNMP interna.

Nota:

Registre de forma segura estos números de puerto, ya que no se pueden cambiar una vez que se instala STA.

Para proteger la seguridad del sitio, estos números no se configuran de manera previa ni se codifican.

A.2.18.1. Campos de la pantalla

Enter HTTP Port (Introducir puerto HTTP)
Introduzca el número de puerto HTTP para el acceso no seguro al servidor gestionado staEngine. Normalmente, este puerto es el 7025.

Los números de puerto deben ser únicos y estar disponibles.

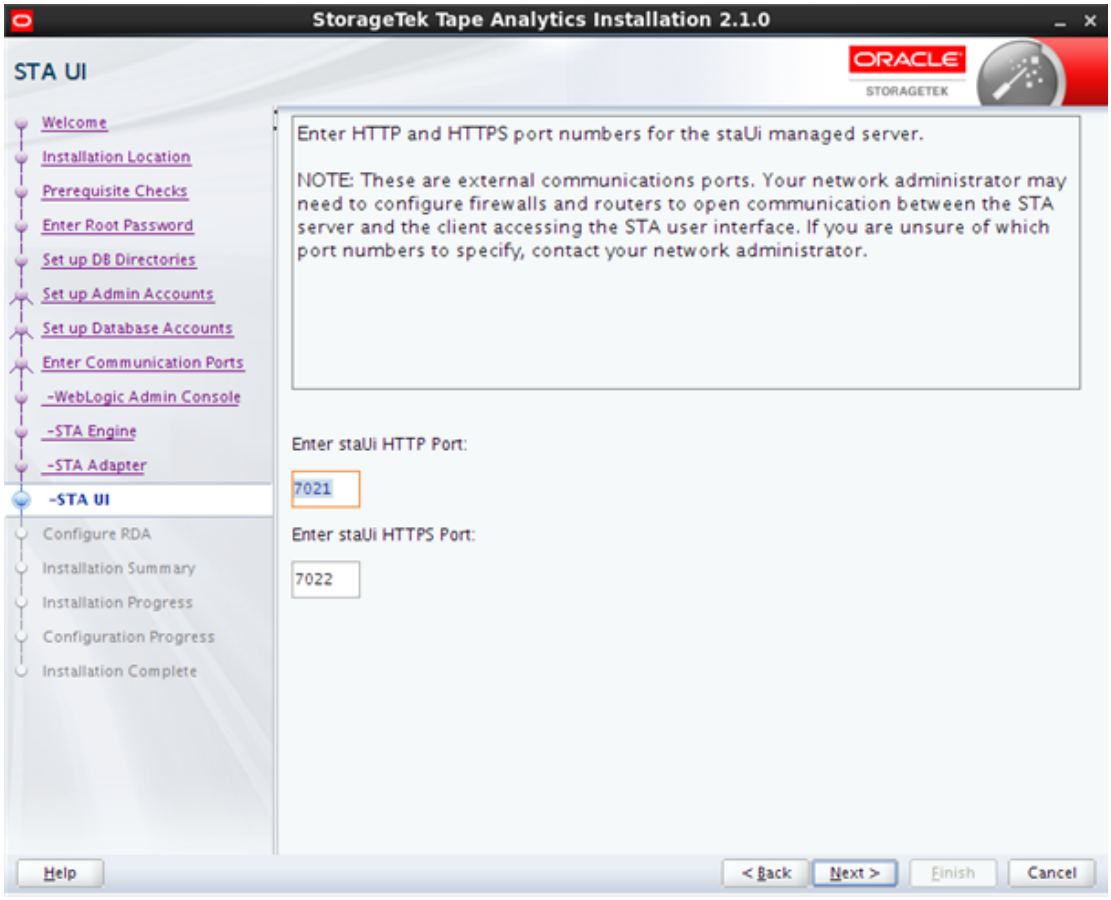
Enter HTTPS Port (Introducir puerto HTTPS)
Introduzca el número de puerto HTTPS para el acceso seguro al servidor gestionado staEngine. Normalmente, este puerto es el 7026.

Los números de puerto deben ser únicos y estar disponibles.

A.2.18.2. Botones específicos de la pantalla

Ninguno

A.2.19. Interfaz de usuario de STA



El número de puerto del servidor gestionado staUi se especifica al iniciar sesión en la interfaz de usuario de la aplicación de STA.

Nota:

Son puertos de comunicación externos. El administrador de la red puede necesitar configurar firewalls y enrutadores para abrir la comunicación entre el servidor de STA y el cliente que accede a la consola de administración de WebLogic.

Nota:

Registre de forma segura estos números de puerto, ya que no se pueden cambiar una vez que se instala STA.

Para proteger la seguridad del sitio, estos números no se configuran de manera previa ni se codifican.

A.2.19.1. Campos de la pantalla

Enter HTTP Port (Introducir puerto HTTP)
Introduzca el número de puerto HTTP para el acceso no seguro al servidor gestionado staUi. Normalmente, este puerto es el 7021.

Los números de puerto deben ser únicos y estar disponibles.

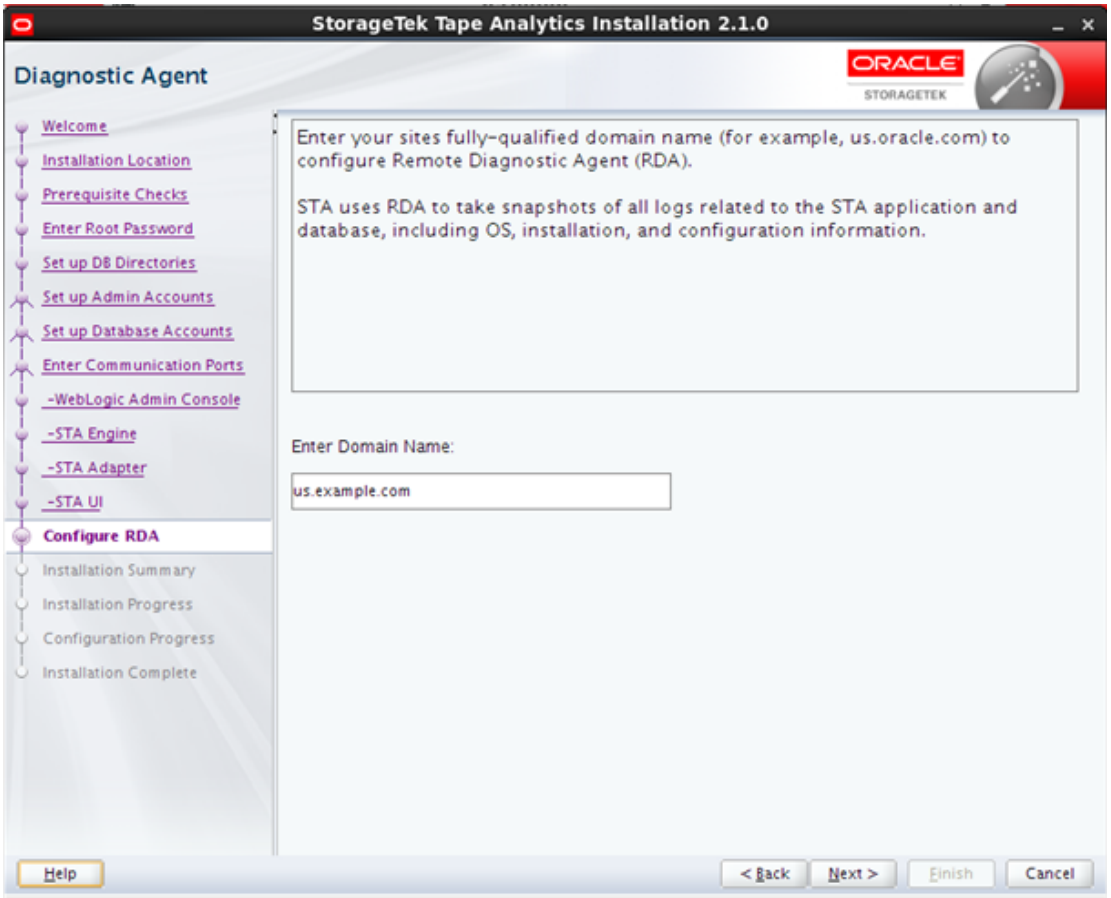
Enter HTTPS Port (Introducir puerto HTTPS)
Introduzca el número de puerto HTTP para el acceso seguro al servidor gestionado staUi. Normalmente, este puerto es el 7022.

Los números de puerto deben ser únicos y estar disponibles.

A.2.19.2. Botones específicos de la pantalla

Ninguno

A.2.20. Agente de diagnóstico



El instalador de STA usa el nombre de dominio completo del sitio para configurar el agente de diagnóstico remoto (RDA) de Oracle.

STA usa RDA para generar instantáneas de todos los logs relacionados con la aplicación y la base de datos de STA, incluida la información del sistema operativo, la instalación y la configuración. Consulte la *Guía del usuario de STA* para obtener información adicional.

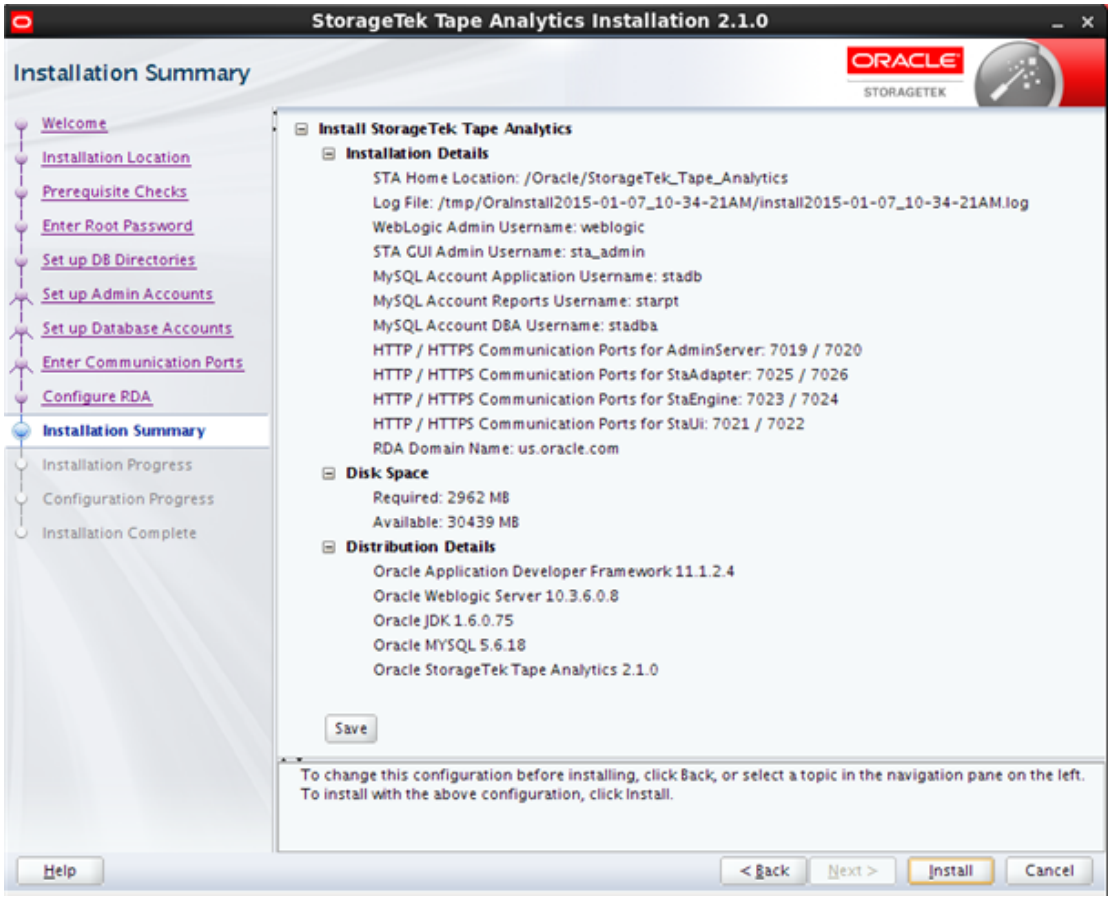
A.2.20.1. Campos de la pantalla

Enter Domain Name (Introducir nombre de dominio)
Introduzca el nombre de dominio completo del sitio, por ejemplo, `us.ejemplo.com`.

A.2.20.2. Botones específicos de la pantalla

Ninguno

A.2.21. Resumen de instalación



En la pantalla, se muestran los siguientes detalles sobre la instalación. Puede guardar esta información en un archivo de texto para tener un registro.

- Installation Details (Detalles de instalación): información que introdujo en las pantallas del instalador.

- Disk Space (Espacio de disco): espacio de disco requerido y disponible, en MB.
- Distribution Details (Detalles de distribución): nombres y números de versión de los paquetes de software que se instalarán.

Continúe de la siguiente manera:

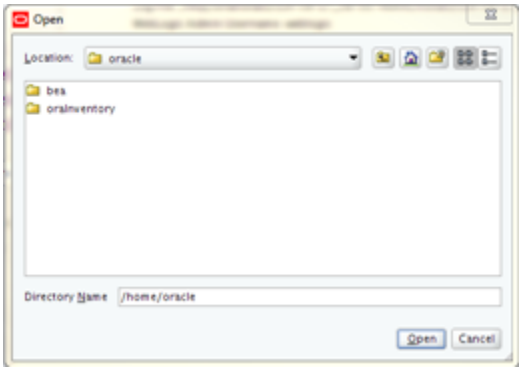
- Para modificar alguno de los detalles de la instalación, haga clic en **Back** (Atrás) para regresar a la pantalla correspondiente o seleccione el enlace de la pantalla en el panel de navegación para ir directamente a esa pantalla.
- Para guardar los detalles que se muestran en un archivo de texto, haga clic en **Save** (Guardar).
- Para instalar usando los valores que se muestran, haga clic en **Install** (Instalar).
- Para cancelar la instalación, haga clic en **Cancel** (Cancelar).

A.2.21.1. Campos de la pantalla

Ninguno

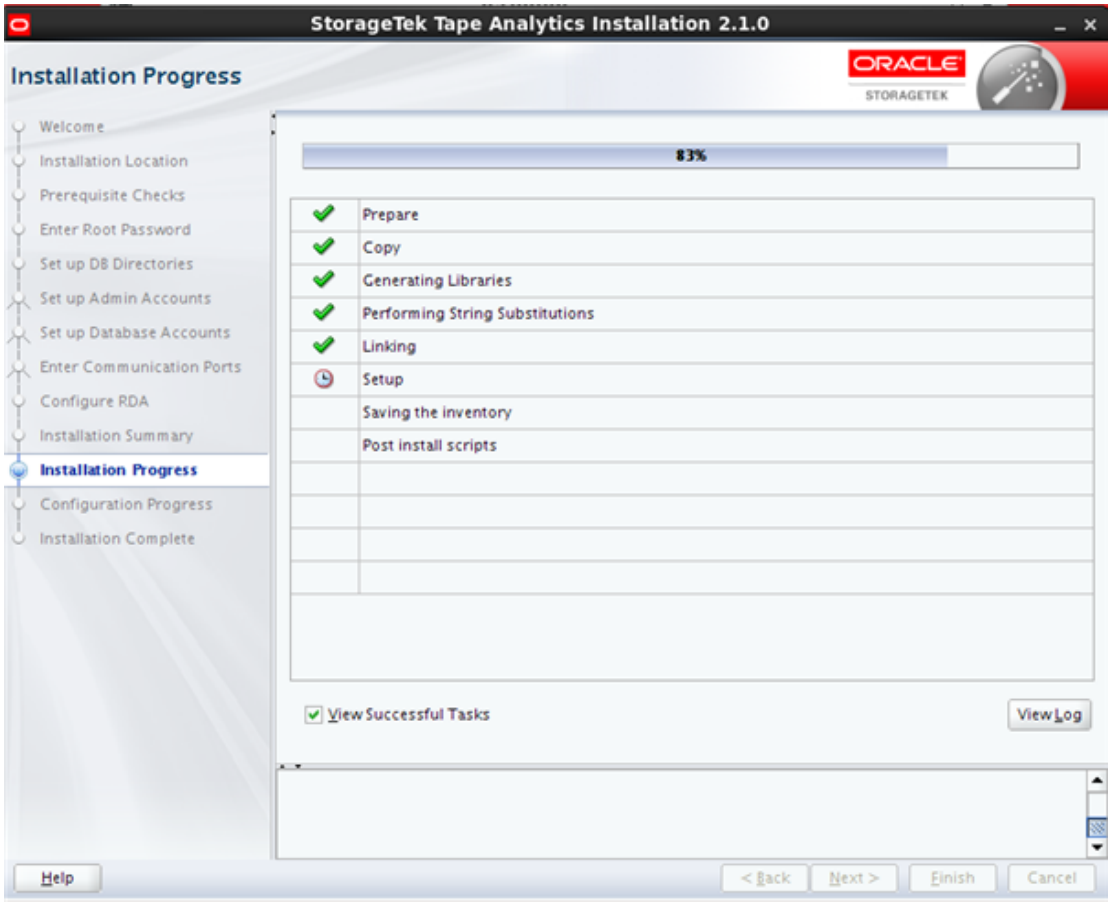
A.2.21.2. Botones específicos de la pantalla

Save (Guardar)
Haga clic para guardar la información que se muestra en un archivo de texto con el nombre *`STA_Installation_Profile_registro de hora.txt`*. En el cuadro de diálogo Open (Abrir), especifique el directorio en donde desea que se guarde el archivo.



Install (Instalar)
Haga clic para comenzar la instalación. Una vez que hace clic en este botón, la instalación no se puede pausar ni cancelar.

A.2.22. Progreso de la instalación



Comienza la instalación de STA, y la pantalla muestra el estado de cada tarea.

Precaución:

No cierre esta ventana; si lo hace, se interrumpe el avance de la instalación y pueden quedar componentes incompletos de la instalación en el servidor.

Si se produce un error en alguna de las tareas, la instalación se detiene y usted debe salir del instalador. Para ello, haga clic en **Cancel** (Cancelar). El instalador revierte la instalación y regresa el servidor a su estado original.

Antes de salir, puede ver detalles adicionales en el panel (Message) Mensaje. Esta información puede ayudarlo a resolver problemas y a determinar cómo proceder. También puede ver el log de la instalación para obtener información adicional.

A.2.22.1. Campos de la pantalla

Ninguno

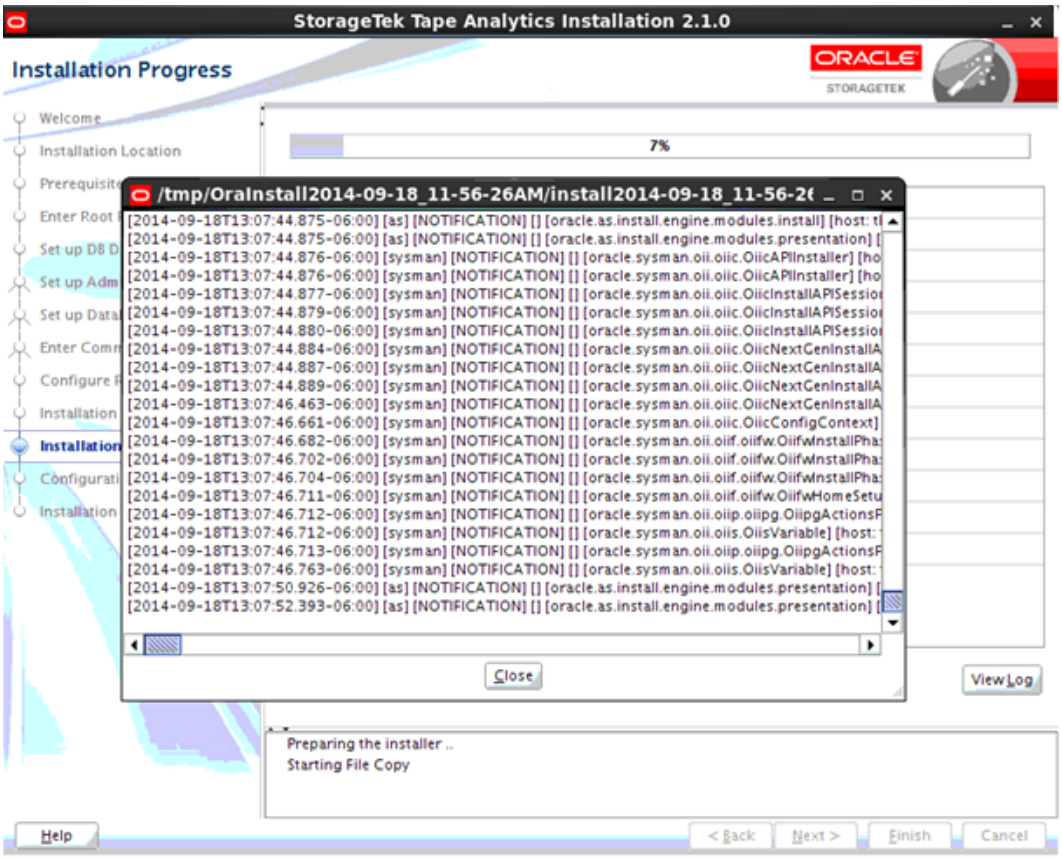
A.2.22.2. Botones específicos de la pantalla

View Successful Tasks (Ver tareas correctas)
Seleccione la casilla de verificación para incluir los resultados correctos en la visualización; esta es la configuración predeterminada.

Anule la selección de la casilla de verificación para que se muestren solo los resultados con error. Esto le permite filtrar las tareas que se realizaron correctamente para poder concentrarse en las que necesitan atención.

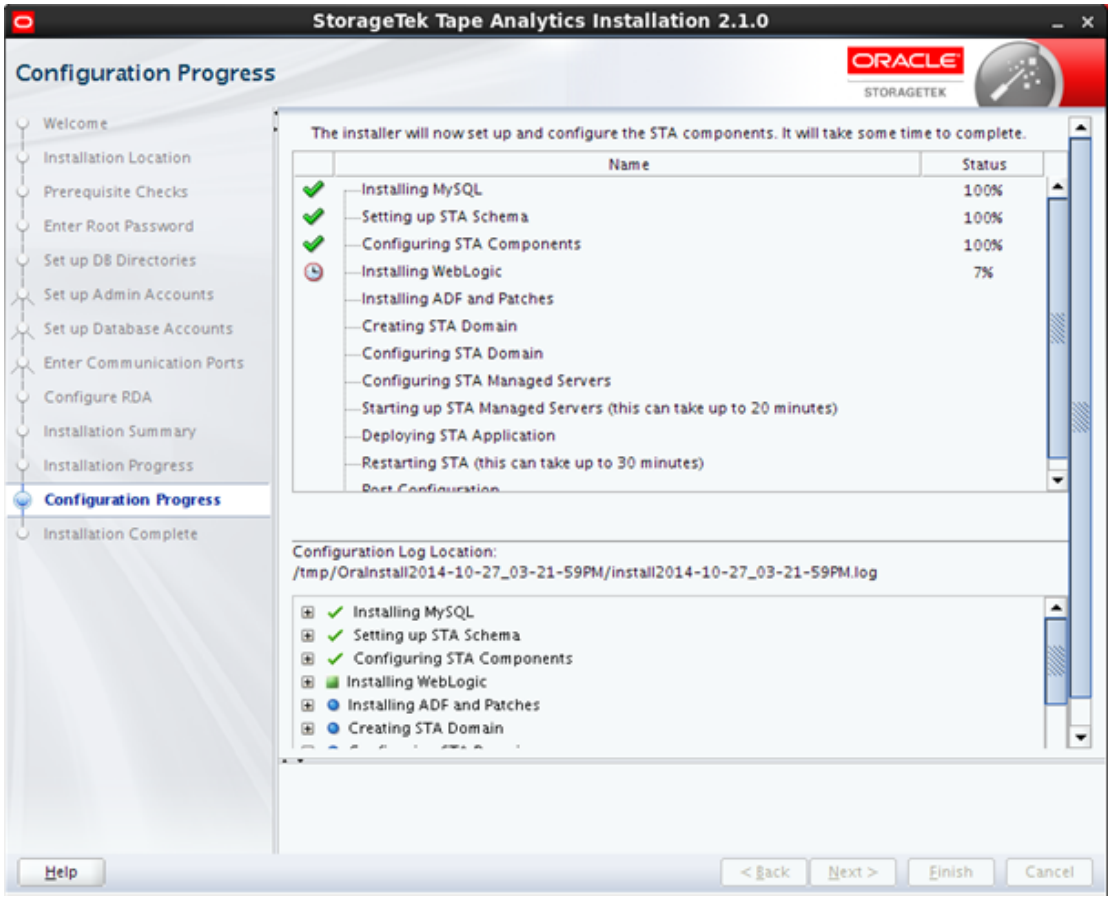
View Log (Ver log)
Haga clic para mostrar el log de la instalación en otra ventana. En la Figura A.5, "Ejemplo de visualización de log de progreso de la instalación", se muestra un ejemplo. Haga clic en **Close** (Cerrar) para descartar la ventana del log.

Figura A.5. Ejemplo de visualización de log de progreso de la instalación



También puede ver el log desde la línea de comandos de Linux. Mientras el instalador se ejecuta, los logs se guardan en un subdirectorio dentro de `/tmp`. Consulte Sección 3.4, "Logs de instalación y desinstalación de STA" para obtener información detallada.

A.2.23. Progreso de la configuración



Comienza la configuración y la implementación de STA, y la pantalla muestra el estado de cada tarea.

Precaución:

No cierre esta ventana; si lo hace, se interrumpe el avance de la configuración y pueden quedar componentes incompletos de la instalación en el servidor.

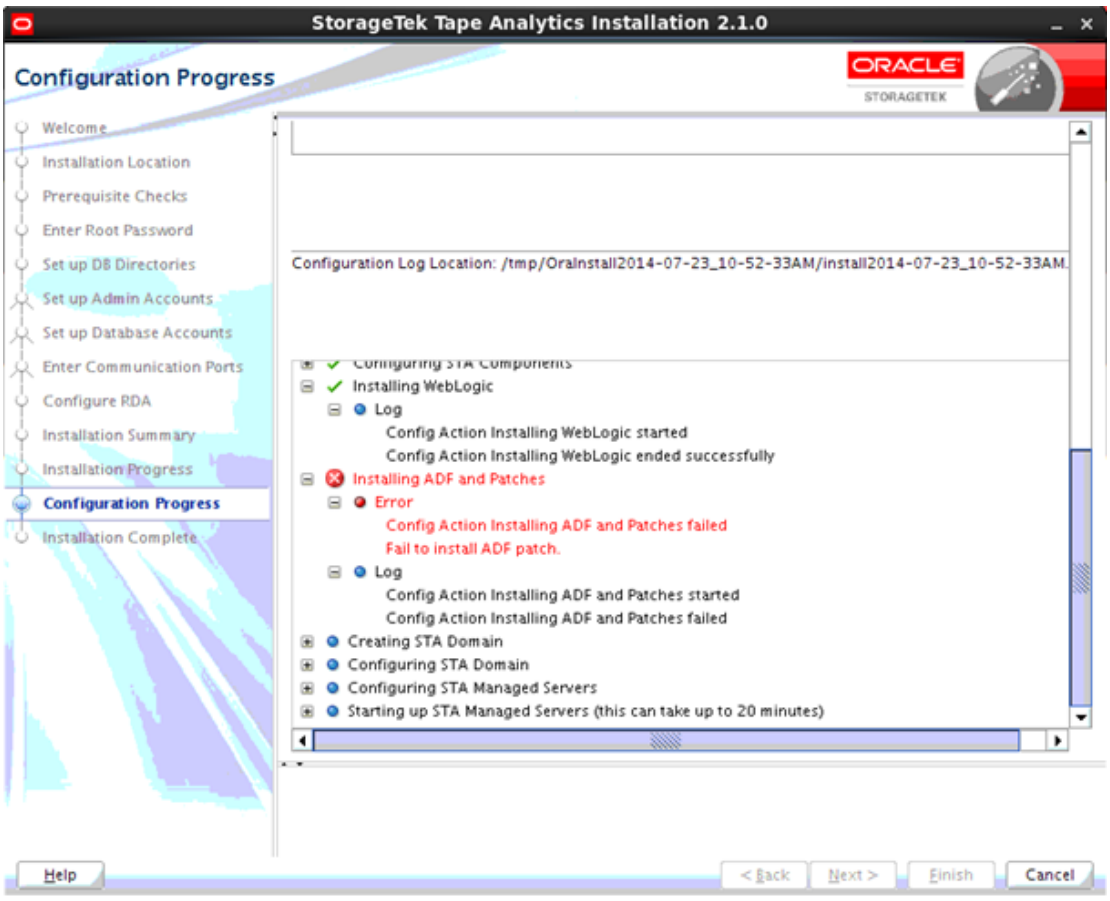
Durante este proceso, se configuran e inician el servidor de WebLogic, los servidores gestionados de STA y la aplicación de STA. Esto puede tardar entre 30 y 60 minutos en finalizar.

Puede ver más detalles de las tareas finalizadas y las que están en curso. En el panel Message (Mensaje), haga clic en el **ícono para expandir** (+) que se encuentra junto a la tarea cuya información detallada desea ver. Haga clic en el **ícono para contraer** (-) para volver a ocultar el detalle. La Figura A.6, “Ejemplo de detalle de progreso de la configuración” es un ejemplo que muestra el detalle de las tareas correctas y las que presentaron errores.

Si una tarea presenta errores, el instalador de STA se cierra, revierte la instalación y regresa el servidor a su estado original. Puede ver el log de la instalación para resolver el

problema. Consulte Sección 3.4, “Logs de instalación y desinstalación de STA” para obtener información detallada.

Figura A.6. Ejemplo de detalle de progreso de la configuración



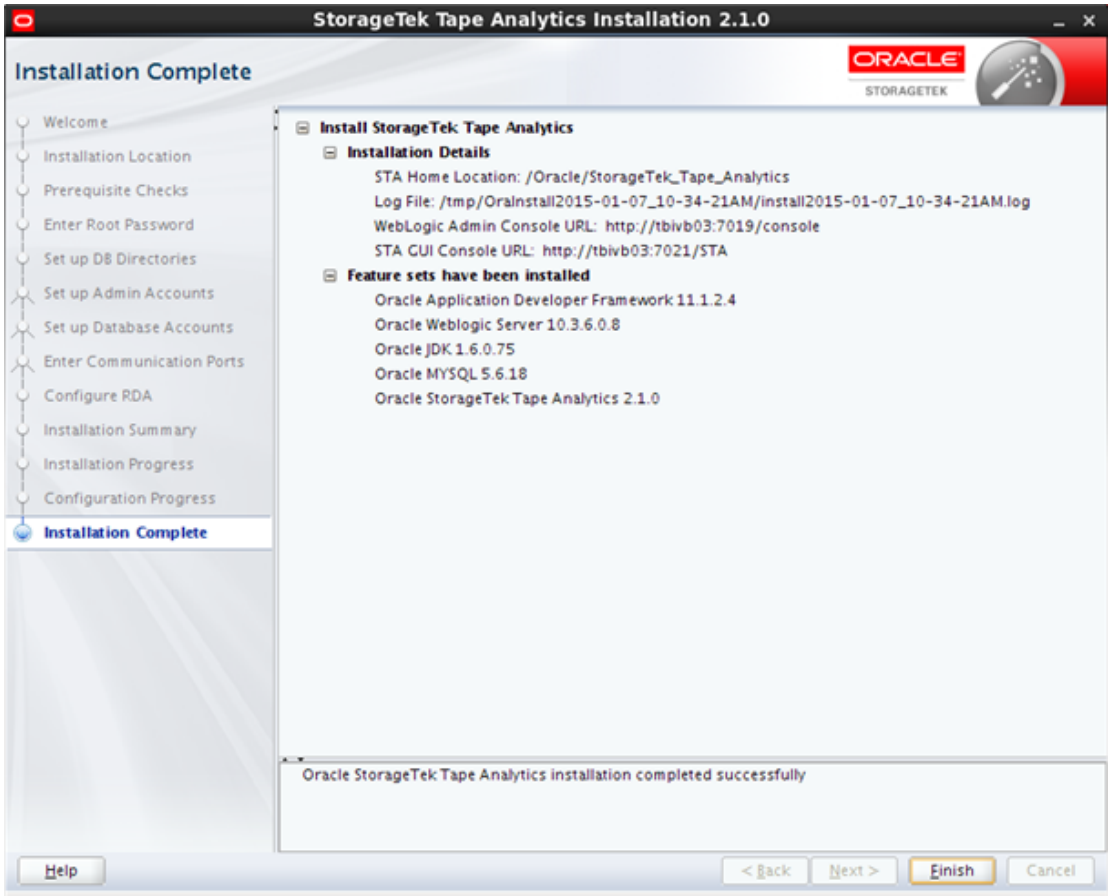
A.2.23.1. Campos de la pantalla

Ninguno

A.2.23.2. Botones específicos de la pantalla

Ninguno

A.2.24. Instalación finalizada



En la pantalla, se muestran los siguientes detalles sobre la instalación finalizada:

- Installation Details (Detalles de la instalación): ubicaciones de la aplicación de STA instalada y el archivo log del instalador, y detalles de conexión para las interfaces de usuario de WebLogic y la aplicación de STA.
- Feature sets have been installed (Conjuntos de funciones instalados): nombres y números de versión de los paquetes de software que se instalaron.

Puede hacer una captura de pantalla de esta información para que le quede un registro. Haga clic en **Finish** (Finalizar) para salir del instalador.

A.2.24.1. Campos de la pantalla

Ninguno

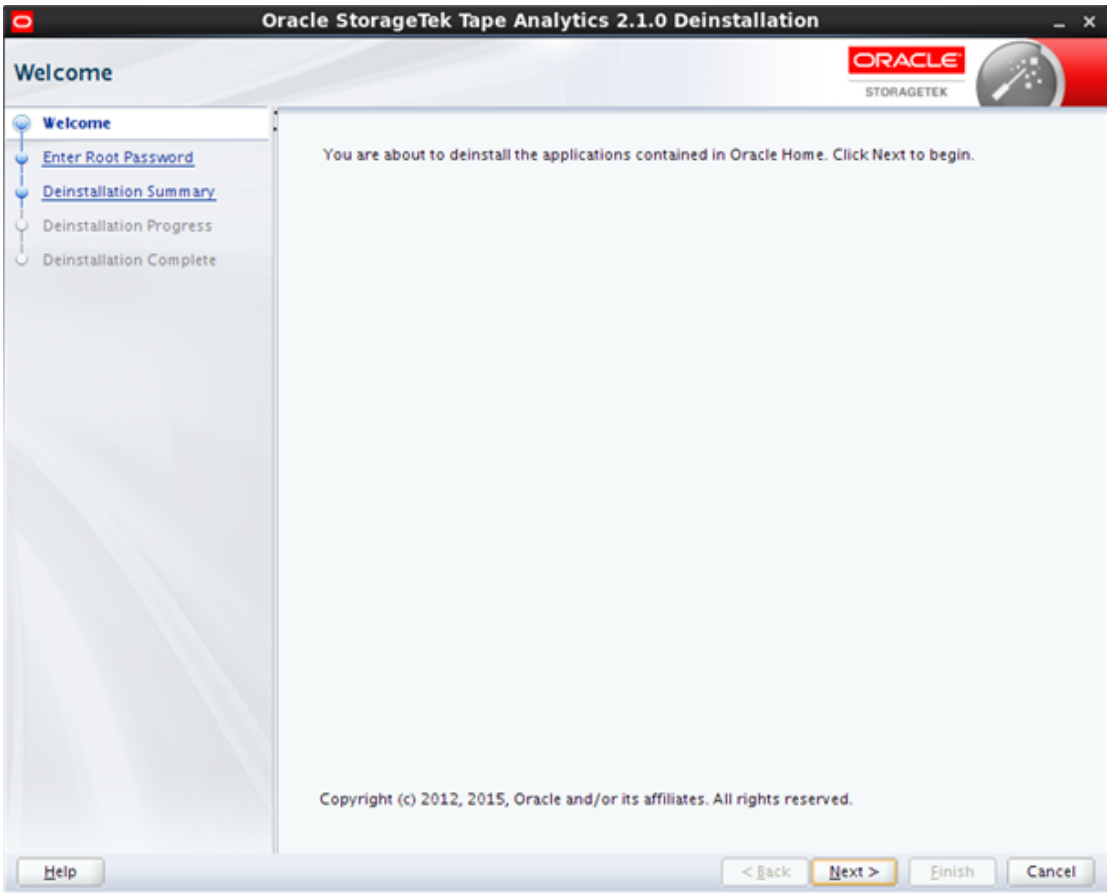
A.2.24.2. Botones específicos de la pantalla

Finish (Finalizar)
Haga clic para salir del instalador de STA.

A.3. Pantallas del desinstalador gráfico de STA

En esta sección, se proporciona referencia detallada para cada una de las pantallas del desinstalador gráfico de STA.

A.3.1. Bienvenido



La pantalla describe las acciones que está por realizar. Lea el texto y haga clic en **Next** (Siguiente) para continuar.

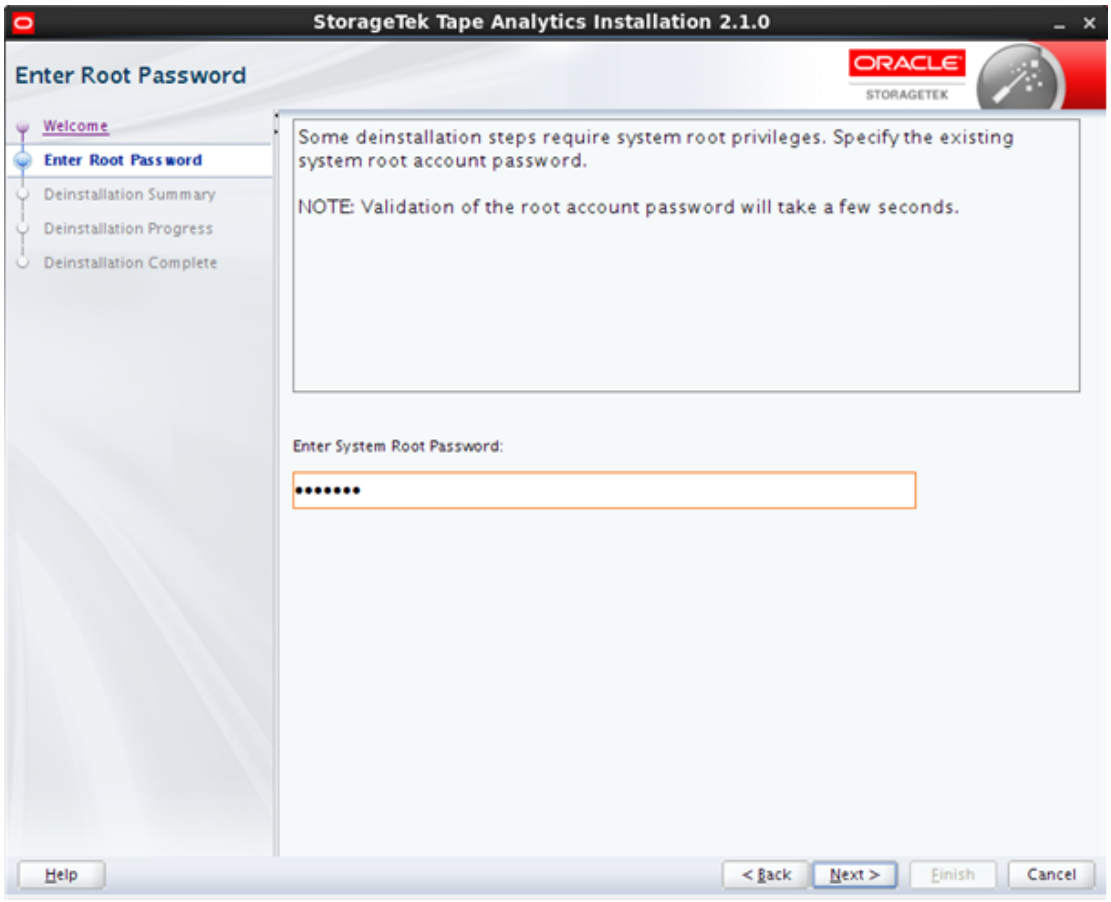
A.3.1.1. Campos de la pantalla

Ninguno

A.3.1.2. Botones específicos de la pantalla

Ninguno

A.3.2. Introducción de la contraseña del usuario root



El desinstalador de STA requiere acceso de root de Linux para realizar las tareas de desinstalación.

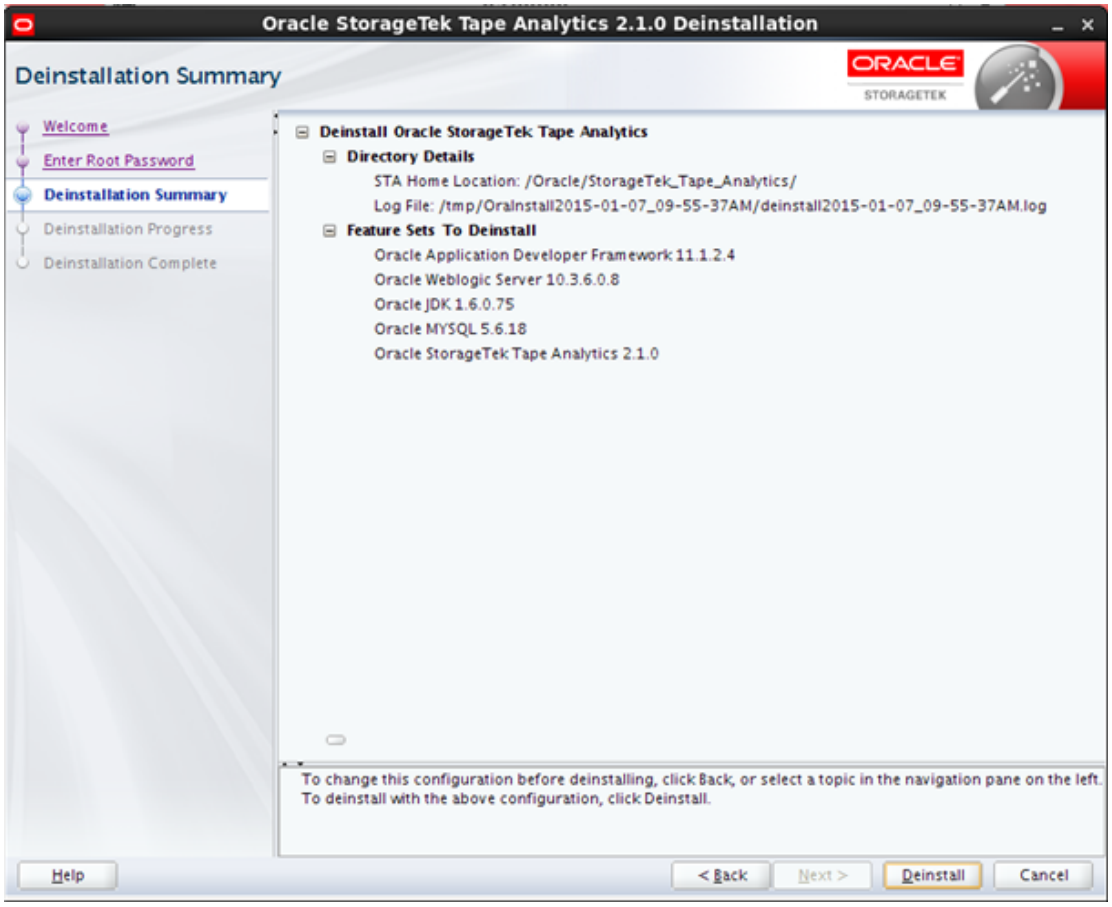
A.3.2.1. Campos de la pantalla

Enter Root Password (Introducir contraseña de usuario root)
Escriba la contraseña del usuario root de Linux. La entrada se muestra enmascarada. La validación de la contraseña puede tardar varios segundos.

A.3.2.2. Botones específicos de la pantalla

Ninguno

A.3.3. Resumen de la desinstalación



La pantalla muestra los siguientes detalles acerca del software que se desinstalará:

- Directory Details (Detalles de directorios): ubicaciones del software de la aplicación de STA y el log de desinstalación.
- Feature Sets to Deinstall (Conjuntos de funciones para desinstalar): nombres y números de versión de los paquetes de software que se desinstalarán.

Verifique esta información y continúe de la siguiente manera:

- Haga clic en **Cancel** (Cancelar) para cancelar la desinstalación y salir del desinstalador.
- Haga clic en **Deinstall** (Desinstalar) para continuar.

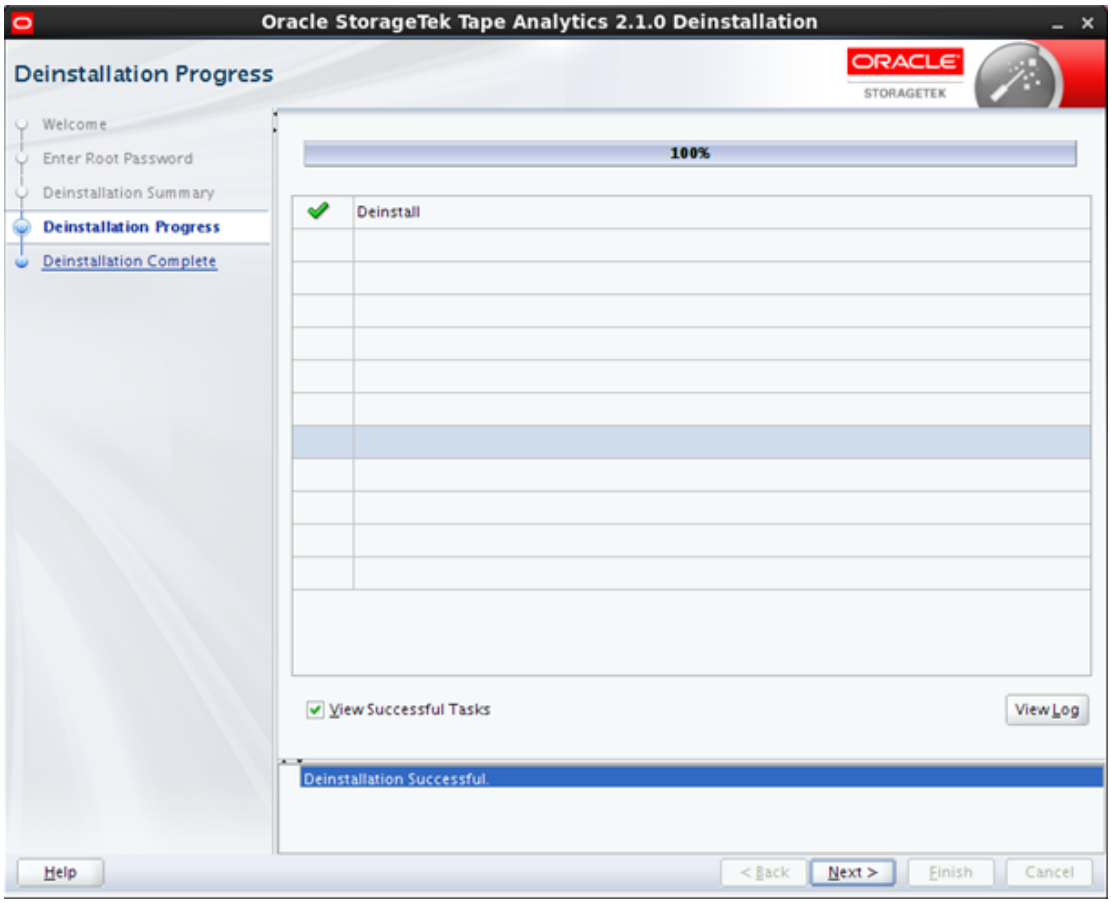
A.3.3.1. Campos de la pantalla

Ninguno

A.3.3.2. Botones específicos de la pantalla

Deinstall (Desinstalar)
Haga clic para comenzar la desinstalación de STA. Una vez que hace clic en este botón, la desinstalación no se puede pausar ni cancelar.

A.3.4. Progreso de la desinstalación



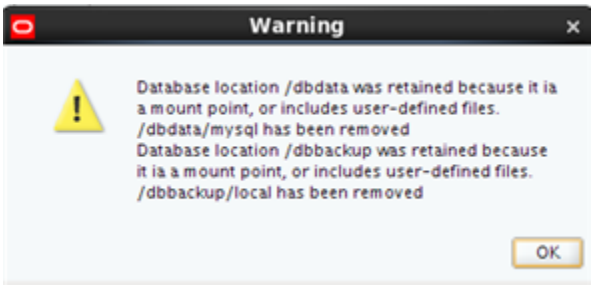
Comienza la desinstalación de STA, y la pantalla muestra el estado de cada tarea.

Precaución:

No cierre esta ventana; si lo hace, se interrumpe el avance de la desinstalación y pueden quedar componentes incompletos de STA en el servidor.

Nota:

Si alguna de las ubicaciones de la base de datos es un punto de montaje en el servidor de STA, aparece el siguiente mensaje para notificarle que el punto de montaje se conservó. Haga clic en **OK** (Aceptar) para descartar el mensaje.



Cuando finaliza la desinstalación, aparece el mensaje "Deinstallation Successful" (Desinstalación correcta) en el panel Message (Mensaje). Haga clic en **Next** (Siguiente) o **Finish** (Finalizar) para pasar a la pantalla final.

Si una tarea presenta errores, el desinstalador de STA se cierra, revierte la desinstalación y regresa el servidor a su estado original. Puede ver el log de la desinstalación para resolver el problema. Consulte Sección 3.4, “Logs de instalación y desinstalación de STA” para obtener información detallada.

A.3.4.1. Campos de la pantalla

Ninguno

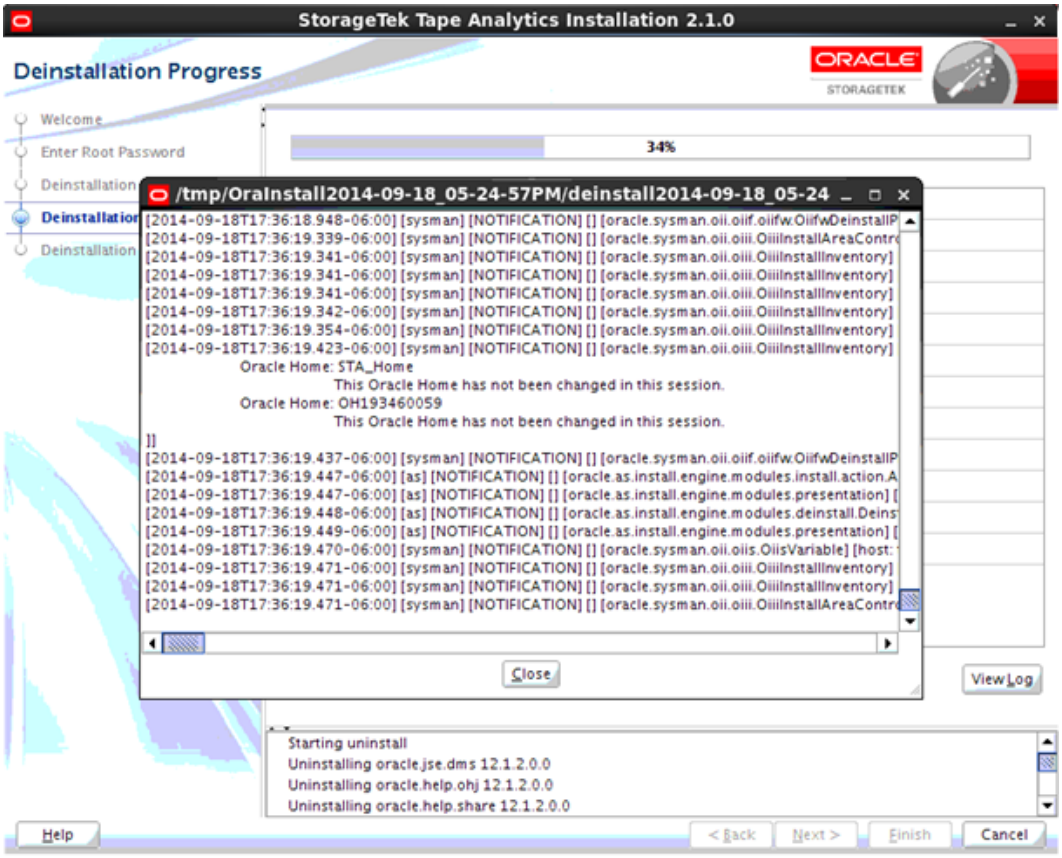
A.3.4.2. Botones específicos de la pantalla

View Successful Tasks (Ver tareas correctas)
Seleccione la casilla de verificación para incluir los resultados correctos en la visualización; esta es la configuración predeterminada.

Anule la selección de la casilla de verificación para que se muestren solo los resultados con error. Esto le permite filtrar las tareas que se realizaron correctamente para poder concentrarse en las que necesitan atención.

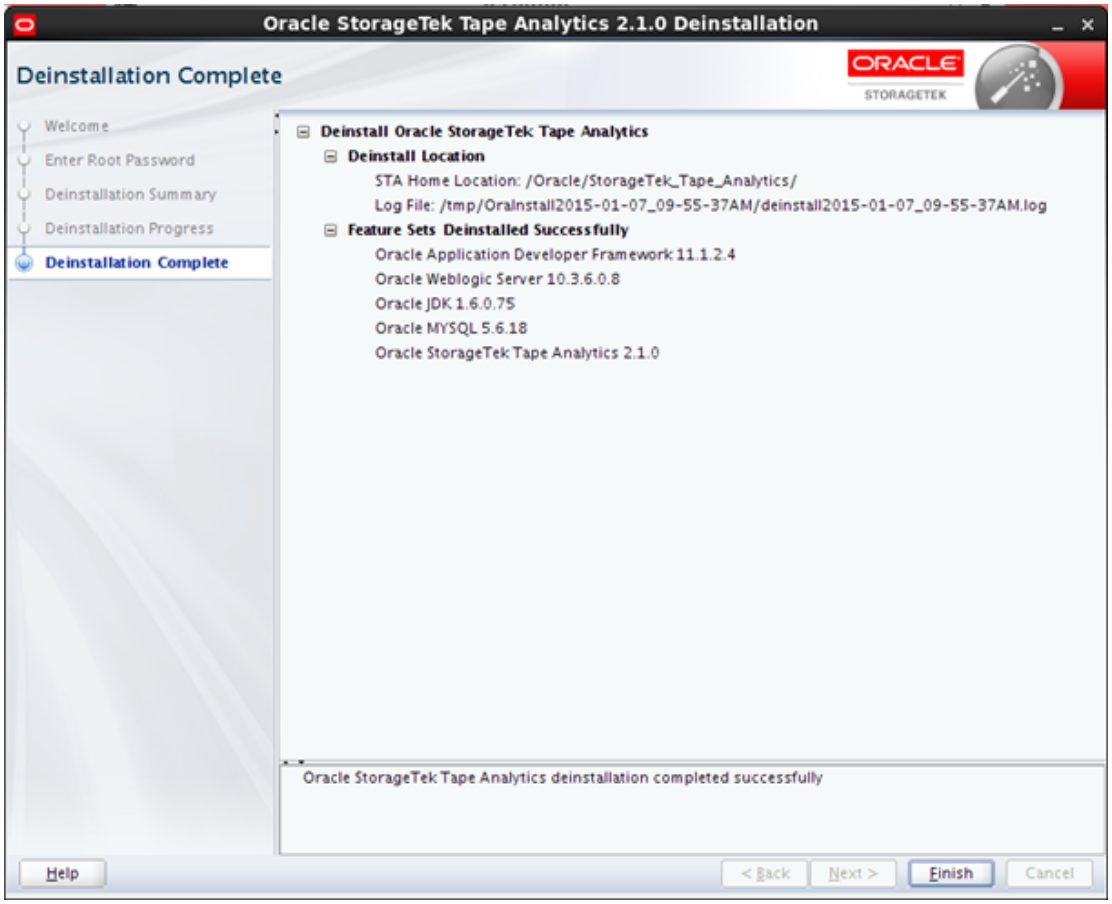
View Log (Ver log)
Haga clic para mostrar el log de la desinstalación en otra ventana. En la Figura A.5, “Ejemplo de visualización de log de progreso de la instalación”, se muestra un ejemplo. Haga clic en **Close** (Cerrar) para descartar la ventana del log.

Figura A.7. Ejemplo de visualización de log de progreso de la desinstalación



También puede ver el log desde la línea de comandos de Linux. Mientras el desinstalador se ejecuta, los logs se guardan en un subdirectorio dentro de `/tmp`. Consulte Sección 3.4, “Logs de instalación y desinstalación de STA” para obtener información detallada.

A.3.5. Desinstalación finalizada



La pantalla muestra los detalles de los paquetes de software que se desinstalaron.

A.3.5.1. Campos de la pantalla

Ninguno

A.3.5.2. Botones específicos de la pantalla

Finish (Finalizar)
Haga clic para salir del desinstalador de STA.

Apéndice B

Instalador y desinstalador en modo silencioso de STA

En este apéndice, se incluyen las siguientes secciones:

B.1. Uso del instalador y el desinstalador en modo silencioso de STA

El modo silencioso le permite omitir la interfaz gráfica de usuario y proporcionar las opciones de instalación o desinstalación de STA en un archivo de propiedades XML llamado *archivo de respuesta*. Para crear el archivo de respuesta, se usa la utilidad de generación de archivos de respuesta, `silentInstallUtility_version.jar`, donde `version` es la versión que tiene descargada de la utilidad.

Este modo es útil para instalaciones desatendidas y para instalar STA en varios equipos. Al usar un archivo de respuesta, puede proporcionar un único conjunto de parámetros y automatizar la instalación. Puede ejecutar el instalador en el modo silencioso desde un script o desde la línea de comandos de Linux.

B.1.1. Requisitos del modo silencioso

Consulte Sección 3.6.2, “Verificación de los requisitos de la instalación” para conocer los requisitos generales para la instalación de STA. Asimismo, el instalador y el desinstalador en modo silencioso de STA tienen los siguientes requisitos específicos para el modo:

- Puede usar el modo silencioso desde clientes telnet, por ejemplo, PuTTY, que no usan el protocolo X11. Sin embargo, debe tener instalado el paquete RPM `xorg-x11-utils` en el servidor de STA.
- Antes de usar el modo silencioso, debe descargar el archivo `silentInstallUtility_version.jar` del sitio web de Oracle Software Delivery Cloud y usarlo para crear el archivo de respuesta con contraseñas cifradas. Consulte

Sección B.3.2, “Creación del archivo de respuesta del instalador en modo silencioso” para obtener instrucciones.

- Para el modo silencioso también se necesita un archivo indicador del inventario central, en el que se especifique la ubicación del directorio del inventario central de Oracle y el grupo de instalación de Oracle. Debe crear el archivo manualmente si aún no existe. Consulte Archivo indicador del inventario central de Oracle para obtener detalles.

B.2. Archivos y utilidades que se usan con el modo silencioso

En esta sección, se describen los conceptos y los términos claves relacionados con la instalación y la desinstalación en modo silencioso.

Archivo indicador del inventario central de Oracle
El instalador y el desinstalador en modo silencioso de STA usan la ubicación del inventario central de Oracle y el grupo de instalación de Oracle especificados en el archivo indicador del inventario central. Consulte Sección 3.1, “Usuarios, grupos y ubicaciones usados por el instalador de STA” para obtener detalles.

De forma predeterminada, el instalador y el desinstalador en modo silencioso usan el archivo indicador `/etc/oraInst.loc`. Al registrar el inventario central de Oracle, el archivo se crea de manera automática con este nombre y en esta ubicación. Consulte Sección 3.6.7, “Registro de la ubicación del inventario central de Oracle” para obtener detalles.

Si la ubicación del inventario central de Oracle *no* está registrada, debe crear el archivo indicador manualmente y asignarle el nombre de archivo `oraInst.loc`. Consulte Sección B.3.1, “Creación del archivo indicador del inventario central de Oracle” para obtener detalles. Puede ubicar el archivo indicador en cualquier directorio, pero si no está en `/etc`, debe usar el parámetro `–invPtrLoc` para especificar la ubicación del archivo cuando ejecute el instalador o el desinstalador en modo silencioso. Consulte –invPtrLoc *pointer_file* para obtener detalles sobre este parámetro.

Archivos de respuesta del instalador y el desinstalador en modo silencioso
Para ejecutarlos desatendidos, el instalador y el desinstalador en modo silencio de STA usan la configuración que se encuentra en el archivo de respuesta que crea. Debe usar el parámetro `–responseFile` para especificar el nombre y la ubicación de este archivo.

El instalador y el desinstalador tienen sus respectivos archivos de respuesta. En el Ejemplo B.1, “Plantilla del archivo de respuesta del instalador en modo silencioso de STA” y el Ejemplo B.2, “Plantilla del archivo de respuesta del desinstalador en modo silencioso de STA”, se muestran el contenido y las entradas requeridas para cada uno. Para crear sus propios archivos de respuesta, puede copiar y pegar cada platilla en un archivo de texto y hacer los cambios apropiados para el sitio.

Para garantizar la seguridad de la contraseña, no introduzca contraseñas sin cifrar en el archivo de respuesta. Después de introducir todos los demás valores de configuración y guardar el archivo, debe usar la utilidad de generación de archivos de respuesta para

insertar contraseñas cifradas en el archivo. Consulte Utilidad de generación de archivos de respuesta del instalador de STA para obtener detalles.

Ejemplo B.1. Plantilla del archivo de respuesta del instalador en modo silencioso de STA

```
[ENGINE]
#DO NOT CHANGE THIS. Response File Version=1.0.0.0.0
[GENERIC]
#The oracle storage home location. This can be an existing Oracle Storage Home or
 #a new Oracle Storage Home
STORAGE_HOME=required
#Root access passsword var.
ROOT ACCESS PASSWORD=
RESPONSEFILE_LOC=
KEYFILE_LOC=
#DBDATA LOC
DBDATA LOC=required
#DBBACKUP LOC
DBBACKUP LOC=required
#Weblogic Admin Name Var
WEBLOGIC ADMIN NAME=required
#Weblogic Admin Password Var
WEBLOGIC ADMIN PASSWORD=
#Weblogic Admin ConfirmPassword Var
WEBLOGIC ADMIN CONFIRMPASSWORD=
#STAGUI Admin Name Var
STAGUI ADMIN NAME=required
#STAGUI Admin Password Var
STAGUI ADMIN PASSWORD=
#STAGUI Admin ConfirmPassword Var
STAGUI ADMIN CONFIRMPASSWORD=
#MySQL root passsword var.
MYSQL ROOT PASSWORD=
#MySQL root confirm passsword var.
MYSQL ROOT CONFIRM PASSWORD=
#MySQL App Name Var
MYSQL APP NAME=required
#MySQL App Password Var
MYSQL APP PASSWORD=
#MySQL App ConfirmPassword Var
MYSQL APP CONFIRMPASSWORD=
#MySQL RPTS Name Var
MYSQL RPTS NAME=required
#MySQL RPTS Password Var
MYSQL RPTS PASSWORD=
#MySQL RPTS ConfirmPassword Var
MYSQL RPTS CONFIRMPASSWORD=
#MySQL DBA Name Var
MYSQL DBA NAME=required
#MySQL DBA Password Var
MYSQL DBA PASSWORD=
#MySQL DBA ConfirmPassword Var
MYSQL DBA CONFIRMPASSWORD=
#ADMINSERVER HTTP Port Var
ADMINSERVER HTTP PORT=7019
#ADMINSERVER HTTPS Port Var
ADMINSERVER HTTPS PORT=7020
#staEngine HTTP Port Var
STAENGINE HTTP PORT=7023
#staEngine HTTPS Port Var
STAENGINE HTTPS PORT=7024
```

```
#staAdapter HTTP Port Var
STAADAPTER HTTP PORT=7025
#staAdapter HTTPS Port Var
STAADAPTER HTTPS PORT=7026
#staUi HTTP Port Var
STAUI HTTP PORT=7021
#staUi HTTPS Port Var
STAUI HTTPS PORT=7022
#Domain name var.
DOMAIN NAME=required
```

Ejemplo B.2. Plantilla del archivo de respuesta del desinstalador en modo silencioso de STA

```
[ENGINE]
#DO NOT CHANGE THIS. Response File Version=1.0.0.0.0
[GENERIC]
#This will be blank when there is nothing to be de-installed in distribution level
SELECTED_DISTRIBUTION=STA_Install~2.1.0.0.0
#Root access passsword var.
DEINSTALL ROOT ACCESS PASSWORD=
RESPONSEFILE_LOC=
KEYFILE_LOC=
```

Utilidad de generación de archivos de respuesta del instalador de STA

La utilidad de generación de archivos de respuesta del instalador le permite insertar contraseñas cifradas en los archivos de respuesta del instalador y el desinstalador en modo silencioso. La utilidad le solicita las contraseñas y las agrega en el archivo especificado en forma cifrada. También guarda un archivo de clave de cifrado en el directorio que usted elija.

Puede descargar la utilidad de generación de archivos de respuesta cuando descarga el instalador de STA. El nombre de la utilidad es *`silentInstallUtility_version.jar`*, donde *`version`* es la versión que tiene descargada de la utilidad.

Después de haber instalado o desinstalado STA correctamente, las contraseñas cifradas se eliminan del archivo de respuesta correspondiente. Para ejecutar nuevamente el instalador o el desinstalador en modo silencioso, puede volver a ejecutar la utilidad de generación para volver a proporcionar las contraseñas cifradas.

La utilidad de generación escribe la ubicación del archivo de respuesta en el contenido del archivo, por lo que no se puede cambiar la ubicación del archivo después de haberlo actualizado con esta utilidad.

Consulte Sección B.3.2, “Creación del archivo de respuesta del instalador en modo silencioso” para obtener instrucciones.

B.3. Tareas del instalador en modo silencioso de STA

Antes de usar estas tareas, debe obtener la información de instalación necesaria, verificar los requisitos y descargar el instalador de STA. Consulte Sección 3.6, “Tareas de instalación de STA” para obtener instrucciones.

A continuación, para instalar STA con el instalador en modo silencioso, use las siguientes tareas en el orden indicado.

- Sección B.3.1, “Creación del archivo indicador del inventario central de Oracle”
- Sección B.3.2, “Creación del archivo de respuesta del instalador en modo silencioso”
- Sección B.3.3, “Ejecución del instalador en modo silencioso”

B.3.1. Creación del archivo indicador del inventario central de Oracle

Use este procedimiento para crear el archivo indicador del inventario central de Oracle si aún no existe.

1. Inicie sesión como usuario de instalación de Oracle.
2. Ejecute el siguiente comando para determinar si ya existe el archivo indicador del inventario central de Oracle.

   ```
   $ cat /etc/oraInst.loc
   ```

   A continuación, se muestran ejemplos de lo que aparece en la pantalla, según si el archivo existe o no.
   - El archivo no existe:

     ```
     cat: /etc/oraInst.loc: No such file or directory
     ```

   - El archivo existe:

     ```
     inventory_loc=/opt/oracle/oraInventory
     inst_group=oinstall
     ```

3. Si el archivo existe, puede abandonar este procedimiento; de lo contrario, pase al siguiente paso.
4. Use un editor de texto para crear el archivo indicador del inventario. Debe tener el nombre *`oraInst.loc`*. Consulte –invPtrLoc *pointer_file* para conocer el contenido de este archivo.
5. Guarde el archivo en el directorio que desee. Si guarda el archivo en el directorio */etc*, el instalador y el desinstalador en modo silencioso de STA lo encontrarán automáticamente; de lo contrario, usted debe especificar la ubicación al ejecutar estas utilidades.

B.3.2. Creación del archivo de respuesta del instalador en modo silencioso

Use este procedimiento para crear el archivo de respuesta del instalador en modo silencioso y agregar contraseñas cifradas en él.

1. Inicie sesión como usuario de instalación de Oracle.
2. Use un editor de texto para crear el archivo de respuesta con el nombre que desee. Consulte el Ejemplo B.1, “Plantilla del archivo de respuesta del instalador en modo silencioso de STA” para ver una plantilla de archivo.

   Copie y pegue la plantilla en un archivo de texto y haga los cambios apropiados para su sitio. Debe proporcionar valores para todas las variables marcadas como "required" (requeridas) y puede cambiar los números de puerto según sea necesario para el sitio.

   - *RESPONSEFILE_LOC*
   - *KEYFILE_LOC*
   - Todas las variables *PASSWORD*
3. Guarde el archivo con un nombre y en una ubicación que desee.
4. Cambie al directorio en el que se descargó la utilidad de generación de archivos de respuesta. El nombre de la utilidad es *silentInstallUtility_version.jar*. Por ejemplo:

   ```
   $ cd /Installers
   ```

5. Ejecute la utilidad de generación de archivos de respuesta.

   ```
   $ java -jar silentInstallUtility_2.1.0.64.124.jar  response_file
   ```

   Donde *response_file* es la ruta de acceso absoluta del archivo de respuesta creado.
6. Responda a cada solicitud con la información correspondiente. Los valores de contraseña que introduce no se muestran en la pantalla. Consulte Sección 3.3.1, “Cuentas de usuario para administrar STA” para conocer los requisitos de contraseñas.

   El Ejemplo B.3, “Ejemplo de ejecución de la utilidad de generación de archivos de respuesta del instalador” es un ejemplo de ejecución de la utilidad de generación de archivos de respuesta.

Ejemplo B.3. Ejemplo de ejecución de la utilidad de generación de archivos de respuesta del instalador

```
$ java -jar silentInstallUtility_2.1.0.64.124.jar /Installers/SilentInstall.rsp
Oracle StorageTek Tape Analytics Silent Installation Utility
------------------------------------------------------------

This utility is used to assist users with the password fields in the Silent
 Installation response file. The silent installation process requireds the
 password fields in the response file requires the password fields to be
 encrypted. The utility will ask the users for the required passwords, and encrypt
 these values, then update the values into the supplied response file.
```

```
Please enter the location to save the key file : /Installers
What is the response file used for? ('i' for Install, 'd' for Deinstall) : i
Enter system root password:
Confirm system root password:
Enter mySQL DB root password:
Confirm mySQL DB root password:
Enter STA user password:
Confirm STA user password:
Enter Weblogic console password:
Confirm Weblogic console password:
Enter STA DB Application password:
Confirm STA DB Application password:
Enter STA DB Report password:
Confirm STA DB Report password:
Enter STA DBA password:
Confirm STA DBA password:
```

7. Una vez que la utilidad finaliza la ejecución, verifique que se haya creado el archivo de clave de cifrado en el directorio en donde se encuentra el archivo de respuesta. Es un archivo oculto que tiene un nombre generado de manera aleatoria que comienza con "sk". Por ejemplo:

```
$ ls -la /Installers/.sk*
-r--------   1 oracle oinstall         17 Sep 22 12:00 .sk1414440339833
```

8. Visualice el archivo de respuesta y verifique los siguientes valores:
   - *RESPONSEFILE_LOC* se actualizó con la ubicación correcta del archivo de respuesta.
   - *KEYFILE_LOC* se actualizó con la ubicación correcta del archivo de clave de cifrado.
   - Todas las contraseñas se actualizaron con un valor cifrado.

   El Ejemplo B.4, “Ejemplo de archivo de instalador después de usar la utilidad de generación” es un ejemplo de la primera parte del archivo, donde se muestran los valores adecuados.

Ejemplo B.4. Ejemplo de archivo de instalador después de usar la utilidad de generación

```
$ view /Installers/SilentInstall.rsp
[ENGINE]
#DO NOT CHANGE THIS. Response File Version=1.0.0.0.0
[GENERIC]
#The oracle storage home location. This can be an existing Oracle Storage Home or
 a new Oracle Storage Home
STORAGE_HOME=/Oracle
#Root access passsword var.
```

```
ROOT ACCESS PASSWORD=JvPABRzrtVP7LZT1Vin0Qg==
RESPONSEFILE_LOC=/Installers/SilentInstall.rsp
KEYFILE_LOC=/Installers/.sk1414705403180
#DBDATA LOC
DBDATA LOC=/dbdata
#DBBACKUP LOC
DBBACKUP LOC=/dbbackup
#Weblogic Admin Name Var
WEBLOGIC ADMIN NAME=weblogic
#Weblogic Admin Password Var
WEBLOGIC ADMIN PASSWORD=k5/c6Oq1KGwQdUje6CfCgA==
#Weblogic Admin ConfirmPassword Var
WEBLOGIC ADMIN CONFIRMPASSWORD=k5/c6Oq1KGwQdUje6CfCgA==
...
```

B.3.3. Ejecución del instalador en modo silencioso

Use este procedimiento para instalar STA con el instalador en modo silencioso.

1. Cambie a la ubicación del instalador de STA. Por ejemplo:

   ```
   $ cd /Installers
   ```

2. Inicie el instalador en modo silencioso de STA. Consulte Sección B.5, “Opciones de comandos del instalador de STA” para obtener definiciones completas de estos parámetros.

   ```
   $ ./sta_installer_linux64_version.bin –silent  –responseFile response_file –
   invPtrLoc pointer_file
   ```

   Donde:

   - *`version`* es la versión del instalador de STA que descargó.
   - *`–silent`* indica el modo silencioso. Este parámetro es obligatorio.
   - *`–responseFile response_file`* especifica la ruta de acceso absoluta del archivo de respuesta del instalador en modo silencioso. Este parámetro es obligatorio.
   - *`–invPtrLoc pointer_file`* especifica la ruta de acceso absoluta del archivo indicador del inventario central de Oracle. Este parámetro se requiere solamente si el archivo no existe en el directorio */etc* o si desea usar otro archivo.

   Por ejemplo:

   ```
   $ ./sta_install_2.1.0.64.124_linux64.bin –silent –responseFile /Installers/
   SilentInstall.rsp -invPtrLoc /opt/oracle/oraInst.loc
   ```

3. El instalador muestra mensajes de estado en la ventana de terminal a medida que realiza los siguientes pasos de instalación. Este proceso puede tardar entre 30 y 60 minutos en finalizar.
   - Realiza comprobaciones de requisitos en el entorno del servidor de STA.
   - Instala los paquetes de software incluidos, entre ellos MySQL, WebLogic y la aplicación de STA.
   - Configura el entorno de STA con los valores que proporcionó en el archivo de respuesta.
   - Inicia la aplicación de STA.

   El Ejemplo B.5, “Mensajes finales de instalación en modo silencioso correcta de STA” muestra los mensajes que aparecen al final de una instalación correcta. El Ejemplo B.6, “Ejemplos de mensajes finales de instalación en modo silencioso con errores de STA” muestra algunos mensajes que pueden aparecer al final de una instalación que falló.

   Ejemplo B.5. Mensajes finales de instalación en modo silencioso correcta de STA

```
...
Started Configuration:Deploying STA Application
Configuration:Deploying STA Application completed successfully
Started Configuration:Restarting STA (this can take up to 30 minutes)
Configuration:Restarting STA (this can take up to 30 minutes) completed
 successfully
Started Configuration:Post Configuration
Successfully moved logs to /var/log/tbi/install.
Configuration:Post Configuration completed successfully
The installation of STA_Install 2.1.0.0.0 completed successfully.
Logs successfully copied to /home/oracle/oraInventory/logs.
$
```

   Ejemplo B.6. Ejemplos de mensajes finales de instalación en modo silencioso con errores de STA

```
[ERROR] Rule_CalculateFreeSpace_Error. Aborting Install
Logs are located here: /tmp/OraInstall2014-09-24_09-29-29AM.
** Error during execution, error code = 256.
$
```

4. Cuando el instalador finalice de manera correcta, verifique que STA se esté ejecutando. Consulte Sección 3.6.5, “Verificación de la instalación” para obtener instrucciones.

B.4. Tareas del desinstalador en modo silencioso de STA

- Sección B.4.1, “Creación del archivo de respuesta del desinstalador en modo silencioso”
- Sección B.4.2, “Ejecución del desinstalador en modo silencioso”

B.4.1. Creación del archivo de respuesta del desinstalador en modo silencioso

Use este procedimiento para crear el archivo de respuesta del desinstalador en modo silencioso y agregar contraseñas cifradas en él.

1. Inicie sesión como usuario de instalación de Oracle.
2. Use un editor de texto para crear el archivo de respuesta del desinstalador con el nombre que desee. Consulte el Ejemplo B.2, “Plantilla del archivo de respuesta del desinstalador en modo silencioso de STA” para ver una plantilla de archivo.

   Copie y pegue la plantilla en un archivo de texto y deje todas las variables en blanco.
3. Guarde el archivo con un nombre y en una ubicación que desee.
4. Cambie al directorio en el que se descargó la utilidad de generación de archivos de respuesta. El nombre de la utilidad es *`silentInstallUtility_version.jar`*. Por ejemplo:

   ```
   $ cd /Installers
   ```

5. Ejecute la utilidad de generación de archivos de respuesta.

   ```
   $ java -jar silentInstallUtility_2.1.0.64.124.jar  response_file
   ```

   Donde *`response_file`* es la ruta de acceso absoluta del archivo de respuesta creado.
6. Responda a cada solicitud con la información correspondiente. Los valores de contraseña que introduce no se muestran en la pantalla.

   El Ejemplo B.7, “Ejemplo de ejecución de la utilidad de generación de archivos de respuesta del desinstalador” es un ejemplo de ejecución de la utilidad.

   ### Ejemplo B.7. Ejemplo de ejecución de la utilidad de generación de archivos de respuesta del desinstalador

   ```
   $ java -jar silentInstallUtility_2.1.0.64.124.jar /Installers/SilentIDeinstall.rsp
   Oracle StorageTek Tape Analytics Silent Installation Utility
   ------------------------------------------------------------

   This utility is used to assist users with the password fields in the Silent
    Installation response file. The silent installation process requireds the
    password fields in the response file requires the password fields to be
    encrypted. The utility will ask the users for the required passwords, and encrypt
    these values, then update the values into the supplied response file.


   Please enter the location to save the key file : /Installers
   ```

```
What is the response file used for? ('i' for Install, 'd' for Deinstall) : d
Enter system root password:
Confirm system root password:
```

7. Una vez que la utilidad finaliza la ejecución, verifique que se haya creado el archivo de clave de cifrado. Es un archivo oculto que tiene un nombre generado de manera aleatoria. Por ejemplo:

```
$ ls -la /Installers/.sk*
-r--------   1 oracle oinstall         17 Sep 22 12:00 .sk1414437879829
```

8. Visualice el archivo de respuesta y verifique los siguientes valores:
   - La contraseña del usuario root del sistema se actualizó con un valor cifrado.
   - *RESPONSEFILE_LOC* se actualizó con la ubicación correcta del archivo de respuesta.
   - *KEYFILE_LOC* se actualizó con la ubicación del archivo de clave de cifrado.

   El Ejemplo B.8, “Ejemplo de archivo de respuesta del desinstalador después de usar la utilidad de generación” es un ejemplo de archivo que muestra los valores correctos.

Ejemplo B.8. Ejemplo de archivo de respuesta del desinstalador después de usar la utilidad de generación

```
$ view /Installers/SilentDeinst.rsp
[ENGINE]
#DO NOT CHANGE THIS. Response File Version=1.0.0.0.0
[GENERIC]
#This will be blank when there is nothing to be de-installed in distribution level
SELECTED_DISTRIBUTION=STA_Install~2.1.0.0.0
#Root access passsword var.
DEINSTALL ROOT ACCESS PASSWORD=zMZJYDbrhiRZUQL35r7uEg==
RESPONSEFILE_LOC=/Installers/silentdeinstall.rsp
KEYFILE_LOC=/Installers/.sk1414700056981
```

B.4.2. Ejecución del desinstalador en modo silencioso

Use este procedimiento para desinstalar STA con el desinstalador en modo silencioso.

1. Inicie sesión como usuario de instalación de Oracle.
2. Cambie al directorio raíz de STA. Por ejemplo:

```
$ cd /Oracle/StorageTek_Tape_Analytics
```

3. Cambie al directorio de las utilidades de STA.

```
$ cd oui/bin
```

4. Inicie el desinstalador en modo silencioso de STA. Consulte Sección B.5, “Opciones de comandos del instalador de STA” para obtener definiciones completas de estos parámetros.

   ```
   $ ./deinstall.sh –silent  –responseFile response_file –invPtrLoc pointer_file
   ```

   Donde:

   - *–silent* indica el modo silencioso. Este parámetro es obligatorio.
   - *–responseFile response_file* especifica la ruta de acceso absoluta del archivo de respuesta del desinstalador de STA. Este parámetro es obligatorio.
   - *–invPtrLoc pointer_file* especifica la ruta de acceso absoluta del archivo indicador del inventario central de Oracle. Este parámetro se requiere solamente si el archivo no existe en el directorio */etc* o si desea usar otro archivo.

   Por ejemplo:

```
$ ./deinstall.sh –silent  –responseFile /Installers/SilentDeinst.rsp –invPtrLoc /opt/oracle/
oraInst.loc
```

5. El desinstalador muestra mensajes de estado en la ventana de terminal a medida que realiza los siguientes pasos de desinstalación. Este proceso puede tardar hasta 30 minutos en terminar.

   El Ejemplo B.9, “Mensajes finales de desinstalación en modo silencioso correcta de STA” muestra los mensajes que aparecen al final de una instalación correcta. El Ejemplo B.10, “Ejemplos de mensajes finales de desinstalación en modo silencioso con errores de STA” muestra algunos mensajes que pueden aparecer al final de una instalación que falló.

Ejemplo B.9. Mensajes finales de desinstalación en modo silencioso correcta de STA

```
...
Reading response file..
Starting silent deinstallation...
-----------20%----------40%----------60%----------80%-------Successfully moved
 logs to /var/log/tbi/install.
s/common/bin/uninstall.sh/mysql was removed, with s/common/bin/uninstall.sh left,
 because there are user defined files in s/common/bin/uninstall.sh or it is a
 mount point.
/dbdata/local was removed, with /dbdata left, because there are user defined files
 in /dbdata or it is a mount point.
100%

The uninstall of STA_Install 2.1.0.0.0 completed successfully.
```

```
Logs successfully copied to /home/oracle/oraInventory/logs.
```

Ejemplo B.10. Ejemplos de mensajes finales de desinstalación en modo silencioso con errores de STA

```
...
Reading response file..
Starting silent deinstallation...
-----------20%----------40%----------60%----------80%-------Internal Error: File
 Copy failed. Aborting Install
Logs are located here: /tmp/OraInstall2014-09-25_10-07-18AM.
```

6. Cuando el desinstalador finalice, verifique que se hayan eliminado los directorios de STA. Consulte Sección 9.2.2, “Verificación de la desinstalación” para obtener instrucciones.

B.5. Opciones de comandos del instalador de STA

En esta sección, se proporciona información de referencia para las opciones del instalador de STA. Las opciones del modo silencioso se usan exclusivamente con el instalador y el desinstalador en modo silencioso. El registro de logs y otras opciones se pueden usar con ambos modos de instalación y desinstalación.

B.5.1. Opciones del modo silencioso

Las siguientes opciones se usan con el instalador y el desinstalador en modo silencioso.

–force
Permite la instalación en modo silencioso en un directorio no vacío.

–invPtrLoc *pointer_file*
Use el archivo indicador del inventario central de Oracle especificado en lugar del que se encuentra en */etc/oraInst.loc*. *pointer_file* debe ser una ruta de acceso absoluta.

El contenido del archivo del inventario central de Oracle es el siguiente:

```
inventory_loc=Oracle_central_inventory_location
inst_group=Oracle_install_group
```

Donde:

- *Oracle_central_inventory_location* es la ruta de acceso absoluta del inventario central de Oracle.
- *Oracle_install_group* es el nombre del grupo de instalación de Oracle.

–response, –responseFile *response_file*
Requerido para el modo silencioso. Ubicación del archivo de respuesta que contiene las entradas para el instalador y el desinstalador de STA en modo silencioso. *response_file* debe ser una ruta de acceso absoluta.

Consulte el Ejemplo B.1, “Plantilla del archivo de respuesta del instalador en modo silencioso de STA” y el Ejemplo B.2, “Plantilla del archivo de respuesta del desinstalador en modo silencioso de STA” para conocer el contenido de los archivos de respuesta del instalador y el desinstalador.

–silent
Requerido para el modo silencioso. Indica que se debe usar el modo silencioso. Las entradas se toman del archivo de respuesta especificado.

B.5.2. Opciones de registro

Las siguientes opciones le permiten controlar los tipos de información que se proporcionan en los logs del instalador y el desinstalador. Se pueden usar tanto en el modo gráfico como en el silencioso.

–debug
Registra información de depuración. Parte de la información de depuración también aparece en la ventana de la consola.

–logLevel *level*
Omite los mensajes de log cuyo nivel de prioridad sea menor que el especificado. Los valores de *`level`* (nivel) son los siguientes:

- severe (grave)
- warning (advertencia)
- info (información)
- config (configuración)
- fine (detallado)
- finer (muy detallado)
- finest (más detallado)

–printdiskusage
Registra información de depuración sobre el uso del disco.

–printmemory
Registra información de depuración sobre el uso de la memoria.

–printtime
Registra información de depuración sobre el tiempo transcurrido.

B.5.3. Otras opciones

Las siguientes opciones de comandos son para uso general. Se pueden usar tanto en el modo gráfico como en el silencioso.

–compatibilityFile *compatibility_file*
Ubicación del archivo que especifica los cambios de dependencias del conjunto de funciones.

–executeSysPrereqs
Ejecuta las comprobaciones de requisitos del entorno del sistema para ejecutar el instalador y sale sin realizar la instalación.

–help
Muestra la ayuda.

–i, –install
Usa el modo gráfico. Este es el valor predeterminado.

–J–Djava.io.tmpdir=*working_directory*
Descomprime el instalador de STA en el directorio de trabajo especificado en lugar de hacerlo en */tmp*. *working_directory* debe ser una ruta de acceso absoluta.

–paramFile *initialization_file*
Use el archivo de inicialización especificado en lugar del que se encuentra en *STA_home/oui/oraparam.ini*. *initialization_file* debe ser una ruta de acceso absoluta.

El instalador de STA usa el archivo que usted especifica para todas las operaciones, incluidas las comprobaciones de requisitos. La ubicación predeterminada es en el directorio *STA_home/oui*.

Apéndice C

Hojas de trabajo de instalación y actualización

Las hojas de trabajo de este apéndice son herramientas de planificación que lo ayudarán a organizar las actividades y la información que debe reunir para realizar una instalación o una actualización de STA. En este apéndice, se incluyen las siguientes secciones:

C.1. Hoja de trabajo de preparación de actualización

La Tabla C.1, “Actividades de preparación de la actualización” se usa solo para actualizaciones de una versión previa de STA. Úsela para llevar un control de las actividades obligatorias y opcionales que realiza con el fin de prepararse para la actualización. Use la columna "Comentarios" para registrar información de planificación especial. Consulte Sección 8.5, “Tareas de preparación de la actualización” para obtener detalles completos sobre estas actividades.

Tabla C.1. Actividades de preparación de la actualización

Actividad	Comentarios	Listo
Verifique que la versión actual de STA sea una versión publicada. **Nota:** Si está actualizando desde STA 1.0.x, debe instalar también una nueva versión de Linux antes de instalar STA 2.1.0.		
Elija el método de actualización de servidor único o de dos servidores.		
Verifique que el sitio y el servidor de destino cumplan los requisitos de STA 2.1.0.		
Determine si será necesario aumentar temporalmente el tamaño del sistema de archivos */tmp* para la actualización.		
Analice los cambios del entorno para STA 2.1.0 a fin de determinar cómo afectan el plan de actualización.		
Asegúrese de que todos los paquetes RPM requeridos estén instalados (solo actualizaciones desde STA 2.0.x).		
Verifique que la versión actual de STA tenga comunicación reciente y correcta con las bibliotecas supervisadas.		
Verifique que STA esté procesando intercambios en todas las bibliotecas supervisadas.		

Actividad	Comentarios	Listo
Mueva a una ubicación segura los logs de instalación y base de datos que desee conservar (opcional).		
Realice una instantánea de logs de servicio en la instalación actual de STA (opcional).		
Descargue los paquetes de logs de servicio que desee conservar (opcional).		
Agregue el prefijo "STA–" al nombre de las plantillas personalizadas (opcional).		
Registre la configuración actual de las plantillas personalizadas que desee conservar (opcional).		
Registre la configuración de políticas de informes ejecutivos que desee conservar (opcional).		

C.2. Hojas de trabajo de instalación y actualización

Estas hojas de trabajo incluyen información requerida por el instalador de STA. Consulte Sección 3.3, “Cuentas y puertos configurados durante la instalación de STA” para obtener detalles completos sobre la información solicitada.

Si está actualizando desde una versión previa de STA, puede usar las columnas "Actual" de las hojas de trabajo para registrar los valores utilizados en la instalación actual. Use las columnas "STA 2.1.0" para registrar los valores que utilizará para STA 2.1.0.

C.2.1. Hoja de trabajo de ubicaciones y usuarios de instalación

La Tabla C.2, “Hoja de trabajo de ubicaciones y usuarios de instalación” incluye las cuentas de usuario y las ubicaciones que se necesitan para ejecutar el instalador de STA.

Tabla C.2. Hoja de trabajo de ubicaciones y usuarios de instalación

Elemento	Descripción	Valor actual	Valor de STA 2.1.0
Grupo de instalación de Oracle	Grupo de Linux utilizado para instalar y actualizar productos de Oracle en el servidor de STA. Nuevo para STA 2.1.0.	–	
Usuario de instalación de Oracle	Usuario de Linux para instalar y actualizar productos de Oracle en el servidor de STA. Nuevo para STA 2.1.0.	–	
Ubicación de inventario central de Oracle	Directorio para llevar un control de la información sobre los productos de Oracle instalados en el servidor de STA. Nuevo para STA 2.1.0.	–	
Ubicación de directorio raíz de almacenamiento de Oracle	Directorio en el que se instalan STA y el software asociado de Oracle. Nuevo para STA 2.1.0.	–	
Ubicación de instalador de STA	Ubicación en la que se descarga el instalador de STA.		

Elemento	Descripción	Valor actual	Valor de STA 2.1.0
Ubicación de datos de base de datos de STA	Ubicación de la base de datos de STA.		
Ubicación de copia de seguridad de base de datos de STA	Ubicación de las copias de seguridad de la base de datos de STA en el servidor de STA.		

C.2.2. Hoja de trabajo de cuentas de usuario

La Tabla C.3, “Hoja de trabajo de cuentas de usuario” incluye las cuentas de usuario que se usan para realizar las actividades de administración de STA y las cuentas de MySQL que usa internamente la aplicación de STA para acceder a la base de datos de STA y administrarla.

Nota:

Los requisitos de contraseña cambiaron para STA 2.1.0. Consulte Sección 3.2, “Requisitos del nombre de usuario y la contraseña” para obtener detalles.

Tabla C.3. Hoja de trabajo de cuentas de usuario

Cuenta	Descripción	Nombre de usuario y contraseña actuales	Nombre de usuario y contraseña de STA 2.1.0
Administración de WebLogic	Se usa para iniciar sesión en la consola de administración de WebLogic. **Precaución**: El nombre de usuario y la contraseña de esta cuenta no se pueden recuperar. Si se pierden estas credenciales, se debe reinstalar STA.		
Administrador de STA	Se usa para iniciar sesión en la aplicación de STA con privilegios de acceso completo.		
Usuario root de la base de datos de STA	Es el propietario de la base de datos de MySQL. El nombre de usuario `root` predefinido no se puede cambiar. **Precaución**: La contraseña de esta cuenta no se puede recuperar.	nombre de usuario = `root`	nombre de usuario = `root`
Usuario de aplicaciones de la base de datos de STA	STA usa esta cuenta para conectarse a la base de datos.		
Usuario de informes de la base de datos de STA	Las aplicaciones que no son de STA y las aplicaciones de terceros usan esta cuenta para conectarse a la base de datos.		
Usuario administrador de la base de datos de STA	Las utilidades de administración y supervisión de STA usan esta cuenta para conectarse a la base de datos, principalmente para realizar copias de seguridad programadas.		

C.2.3. Hojas de trabajo de números de puerto

La Tabla C.4, “Puertos externos no configurables” incluye los puertos externos que usa la aplicación de STA. Estos números de puerto están predefinidos y no se pueden cambiar. Use la columna "Verificado" para registrar si verificó con el administrador de la red que estos puertos estén abiertos y disponibles.

Tabla C.4. Puertos externos no configurables

Descripción del puerto	Protocolo	Puerto de STA 2.1.0	Verificado
Shell seguro. Se usa para iniciar sesión desde el servidor de STA en las bibliotecas supervisadas y la copia de seguridad de la base de datos de STA.	SSH	22	
Se usa para transmitir solicitudes del protocolo simple de administración de redes (SNMP) a las bibliotecas supervisadas.	SNMP	161	
Se usa para recibir notificaciones SNMP (capturas) desde las bibliotecas supervisadas.	SNMPTRAP	162	

La Tabla C.5, “Puertos internos y externos configurables” incluye los puertos internos y externos configurables que usa la aplicación de STA. Use la columna "Verificado" para registrar si verificó con el administrador de la red que estos puertos estén abiertos y disponibles.

Nota:

Los puertos predeterminados de la consola de administración de WebLogic se cambiaron en STA 2.1.0.

Tabla C.5. Puertos internos y externos configurables

Descripción del puerto	Tipo	Protocolo	Puerto predeterminado de STA 2.1.0	Puerto actual	Puerto de STA 2.1.0	Verificado
Puerto no seguro para la consola de administración de WebLogic (el puerto predeterminado para STA 1.0.x y 2.0.x era el 7001)	Externo	HTTP	7019			
Puerto seguro para la consola de administración de WebLogic (el puerto predeterminado para STA 1.0.x y 2.0.x era el 7002)	Externo	HTTPS	7020			
Puerto no seguro para el servidor gestionado staUi, que administra la GUI de STA	Externo	HTTP	7021			
Puerto seguro para el servidor gestionado staUi	Externo	HTTPS	7022			
Puerto no seguro para el servidor gestionado staEngine, que administra los puertos internos básicos de STA	Interno	HTTP	7023			
Puerto seguro para el servidor gestionado staEngine	Interno	HTTPS	7024			
Puerto no seguro para el servidor gestionado staAdapter, que administra la comunicación de SNMP con las bibliotecas supervisadas	Interno	HTTP	7025			
Puerto seguro para el servidor gestionado staAdapter	Interno	HTTPS	7026			

C.2.4. Hoja de trabajo de nombres de dominio

La Tabla C.6, “Nombre de dominio de la empresa” incluye el nombre de dominio completo del sitio que utiliza el agente de diagnóstico remoto (RDA) de Oracle al generar los logs de servicio de STA.

Tabla C.6. Nombre de dominio de la empresa

Información requerida	Valor actual	Valor de STA 2.1.0
Nombre de dominio de la empresa (por ejemplo, us .ejemplo.com)		

C.3. Hoja de trabajo de configuración posterior a la instalación

La Tabla C.7, “Información de configuración de usuarios de SNMP v3” incluye información que se usa para configurar la conexión SNMP entre STA y las bibliotecas supervisadas. Se debe configurar el mismo usuario de SNMP v3 en cada biblioteca supervisada y cada instancia de STA. Consulte Sección 5.1.1.1, “Usuario único de SNMP v3” para obtener detalles completos sobre la información solicitada.

Tabla C.7. Información de configuración de usuarios de SNMP v3

Información requerida	Valores previos	Valores de STA 2.1.0
Nombre de usuario de SNMP v3		
Contraseña de autorización de SNMP v3 (Auth)		
Contraseña de cifrado de privacidad de SNMP v3 (privacidad)		
Comunidad de usuarios de SNMP v2c		
Comunidad de capturas de SNMP v2c		

Apéndice D

Configuración de certificados de seguridad

Oracle proporciona certificados de seguridad autogenerados que se usan con los puertos HTTPS/SSL. Durante la instalación, STA usa la utilidad de herramienta de claves de Java para generar un certificado en el servidor de STA, para lo que usa el nombre de host del servidor. De manera opcional, puede reemplazar el certificado de Oracle por su propio certificado aprobado por una autoridad de certificación seleccionada (por ejemplo, VeriSign).

En este capítulo, se incluye la siguiente sección:

D.1. Tareas de configuración de certificados de seguridad

Si desea usar un certificado de seguridad que no sea el predeterminado, realice estos procedimientos en el orden que se indica.

Nota:

Para estos procedimientos, se usa Mozilla Firefox en una plataforma Windows.

D.1.1. Establecimiento de la conexión HTTPS/SSL inicial

1. Abra un explorador web compatible en el equipo e introduzca la versión HTTPS/SSL de la dirección URL de la aplicación de STA.

   https://*STA_host_name*:*port_number*/**STA/**

   Donde:
   - *host_name* es el nombre de host del servidor de STA.
   - *port_number* es el número de puerto de STA que especificó durante la instalación. El puerto HTTP predeterminado es el 7021; el puerto HTTPS predeterminado es el 7022.
   - *STA* debe estar en mayúsculas.

   Por ejemplo:

   ```
   https://staserver.example.com:7022/STA/
   ```

Aparece la pantalla Connection is Untrusted (La conexión no es de confianza).

2. Seleccione **I Understand the Risks** (Comprendo los riesgos) y, a continuación, haga clic en **Add Exception** (Agregar excepción).

   Aparece la pantalla Add Security Exception (Agregar excepción de seguridad).

3. Haga clic en **View** (Ver).

   Aparece la pantalla Certificate Viewer (Visor de certificados). El certificado *no* aparece como verificado porque no proviene de una autoridad de certificación.

4. Para examinar el certificado, haga clic en el separador **Details** (Detalles).
5. En el panel Certificate Fields (Campos de certificado), seleccione **issuer** (Emisor). A continuación se muestra un ejemplo. CN indica el nombre del servidor en el que se generó el certificado.

   ```
   CN = staserver.example.com
   OU = Tape Systems
   O = Oracle America Inc
   L = Redwood City
   ST = California
   C = USA
   ```

6. Haga clic en **Close** (Cerrar) para regresar a la pantalla Add Security Certificate (Agregar certificado de seguridad).
7. Seleccione **Confirm Security Exception** (Confirmar excepción de seguridad).

   El certificado se agrega al servidor de STA y ahora puede usar HTTPS con el certificado.

D.1.2. Reconfiguración de WebLogic para usar otro certificado de seguridad

1. Abra una ventana de explorador e introduzca la dirección URL de la consola de administración de WebLogic. El puerto HTTP predeterminado es el 7019 y el puerto HTTPS predeterminado es el 7020.

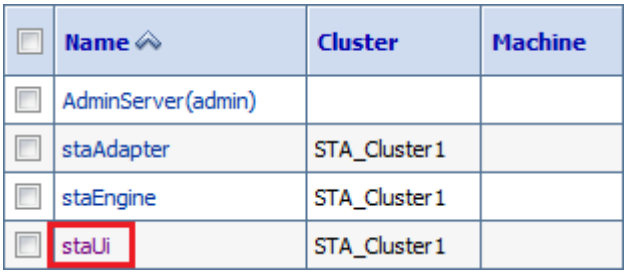
   https://*nombre_de_su_host***:***número de puerto***/console/**

   Por ejemplo:

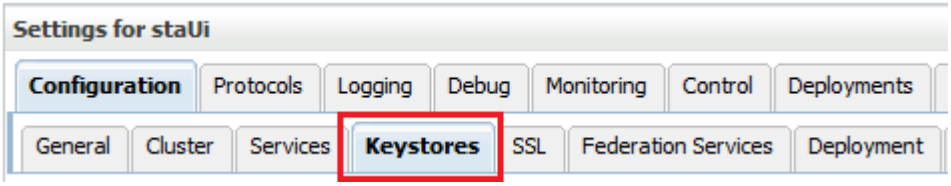
   ```
   https://staserver.company.com:7019/console/
   ```

2. Inicie sesión con el nombre de usuario y la contraseña de la consola de administración de WebLogic que definió durante la instalación de STA.
3. En la sección Domain Structure (Estructura de dominio), seleccione **Environment** (Entorno) y, a continuación, seleccione **Servers** (Servidores).

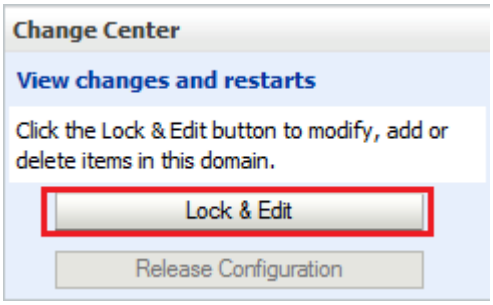
4. En la tabla Servers (Servidores), seleccione el enlace activo **staUi** (seleccione el nombre, no la casilla de control).



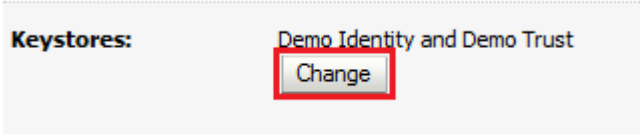
5. Seleccione el separador **Keystores** (Almacén de claves).



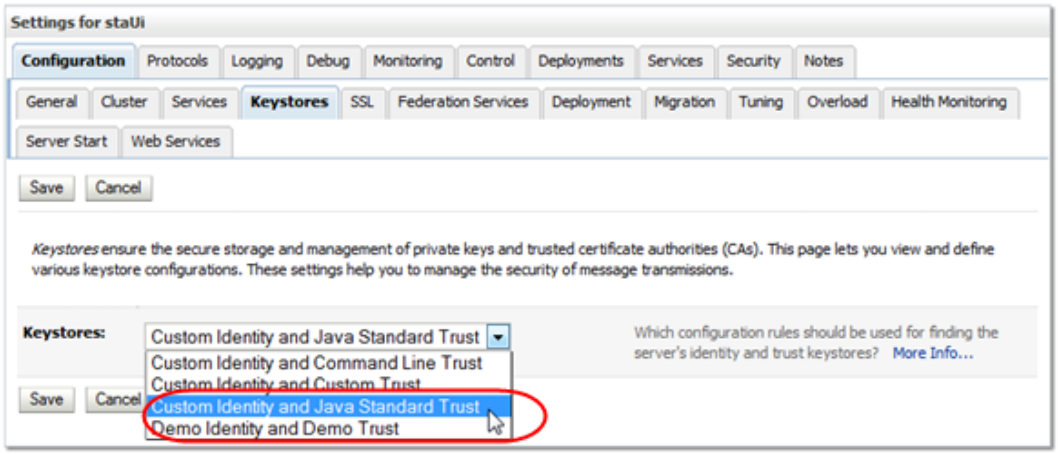
6. En la sección Change Center (Centro de cambios), haga clic en **Lock & Edit** (Bloquear y editar).



7. En la sección Keystores (Almacén de claves), haga clic en **Change** (Cambiar).



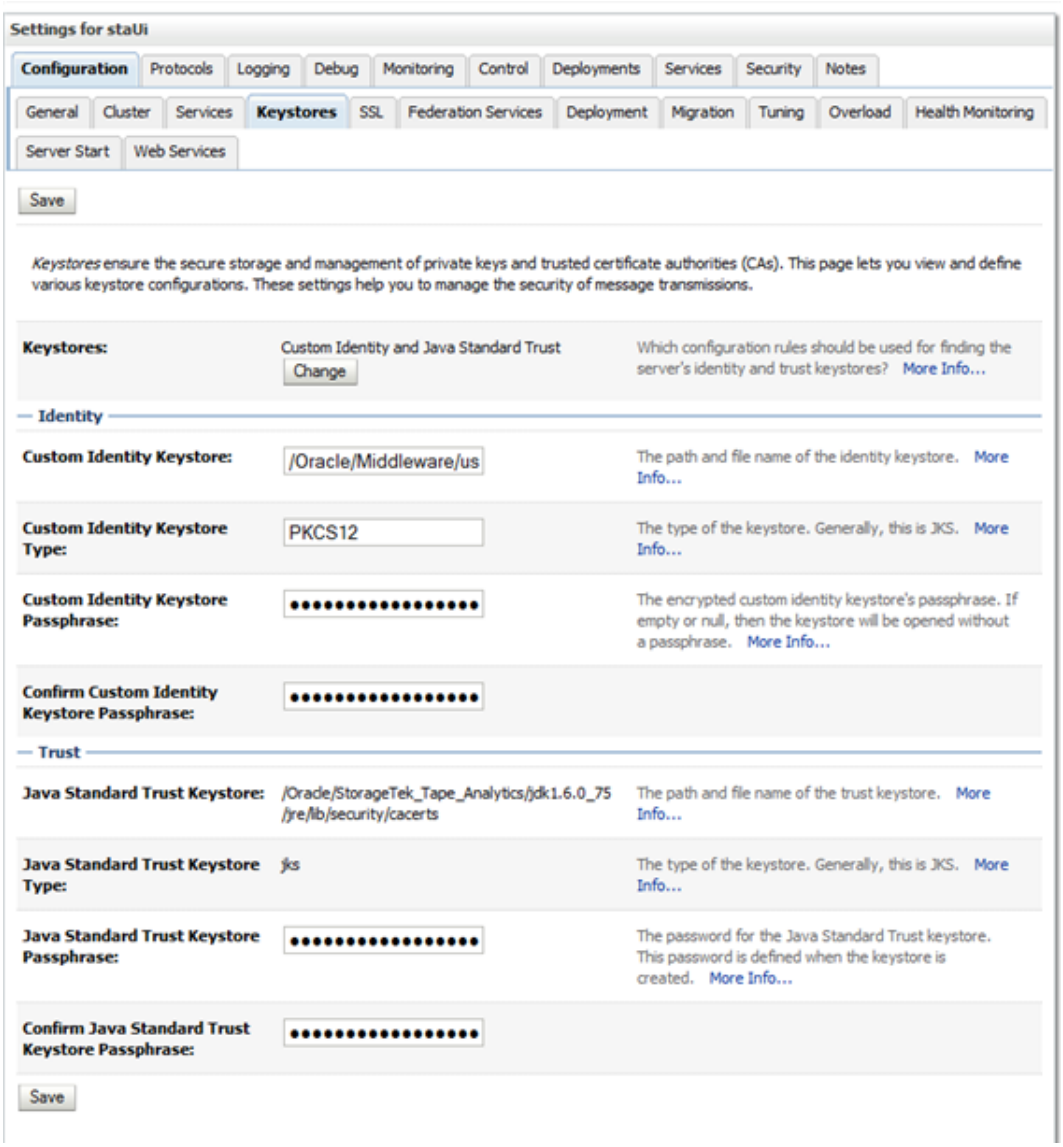
8. En el menú Keystores (Almacén de claves), seleccione **Custom Identity and Java Standard Trust** (Identidad personalizada y protección de estándar de Java).



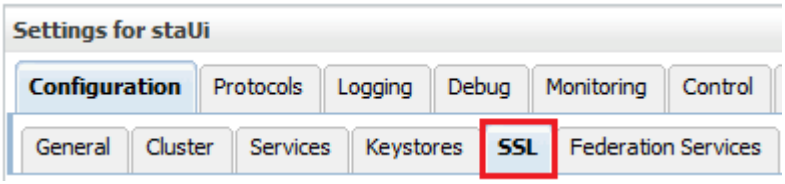
9. Haga clic en **Save** (Guardar).
10. Complete la pantalla Keystores (Almacén de claves) de la siguiente manera:
    - **Custom Identity Keystore** (Almacén de claves de identidad personalizada): ruta de acceso y archivo del archivo de clave privada.
    - **Custom Identity Keystore Type** (Tipo de almacén de claves de identidad personalizada): tipo del almacén de claves. Si se configura para autenticación RACF, introduzca PKCS12.
    - **Custom Identity Keystore Passphrase** (Frase de contraseña de almacén de claves de identidad personalizada): contraseña proporcionada por el administrador del sistema MVS.
    - **Java Standard Trust Keystore Passphrase** (Frase de contraseña de almacén de claves de protección de estándar de Java): nueva contraseña para el archivo de almacén de claves de protección de estándar de Java.

Precaución:

Si olvida estas contraseñas, debe reinstalar STA.



11. Haga clic en **Save** (Guardar).
12. Seleccione el separador **SSL**.

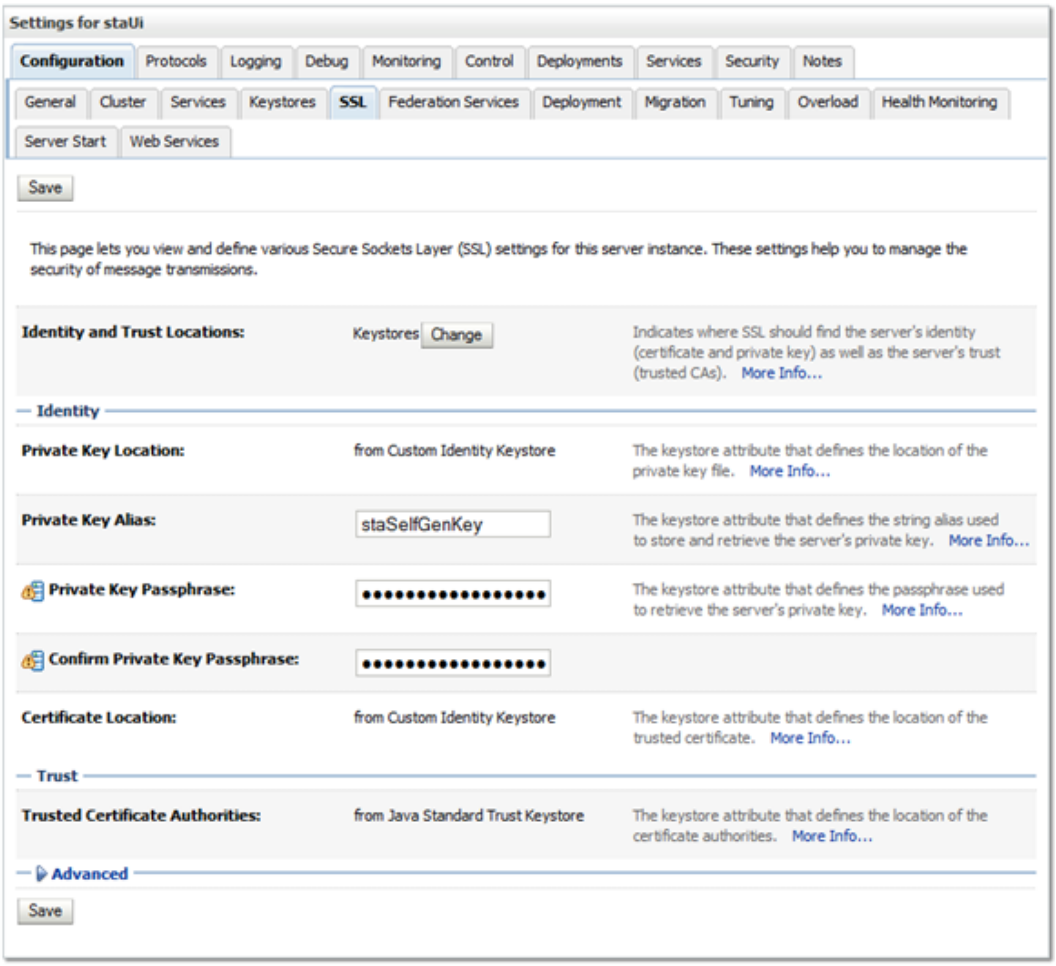


13. Introduzca el alias de la clave privada y la frase de contraseña de la clave privada proporcionados por el programador del sistema MVS.

Nota:

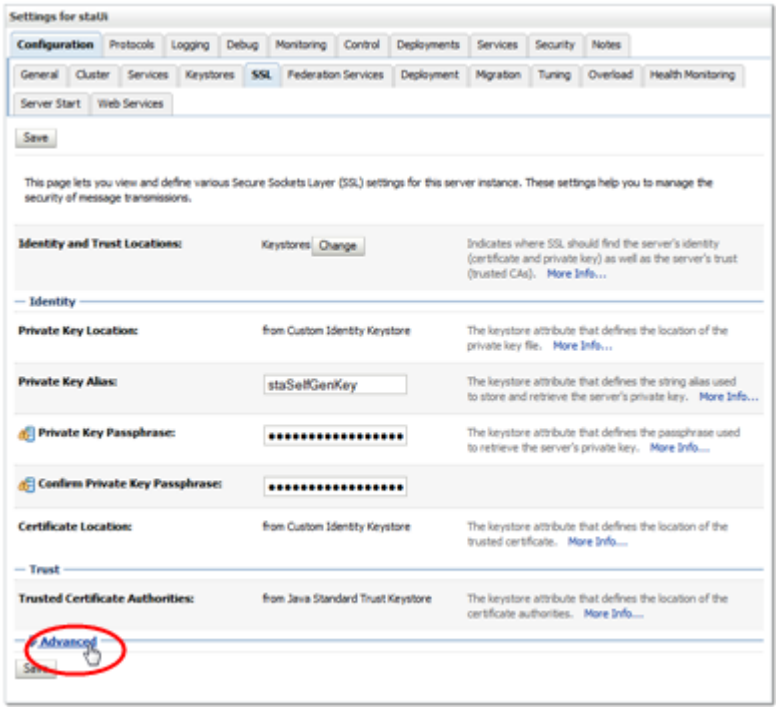
Para determinar el alias de la clave privada, use el comando *keytool* en la línea de comandos del sistema. Por ejemplo:

```
# keytool -list -keystore CLTBI.PKCS12DR.D080411 -storetype PKCS12
Enter keystore password: (password from the MVS sysadmin)
Keystore type: PKCS12
Keystore provider: SunJSSE

Your keystore contains 1 entry

tbiclient, Aug 17, 2011, PrivateKeyEntry,
Certificate fingerprint (MD5):
 9A:F7:D1:13:AE:9E:9C:47:55:83:75:3F:11:0C:BB:46
```

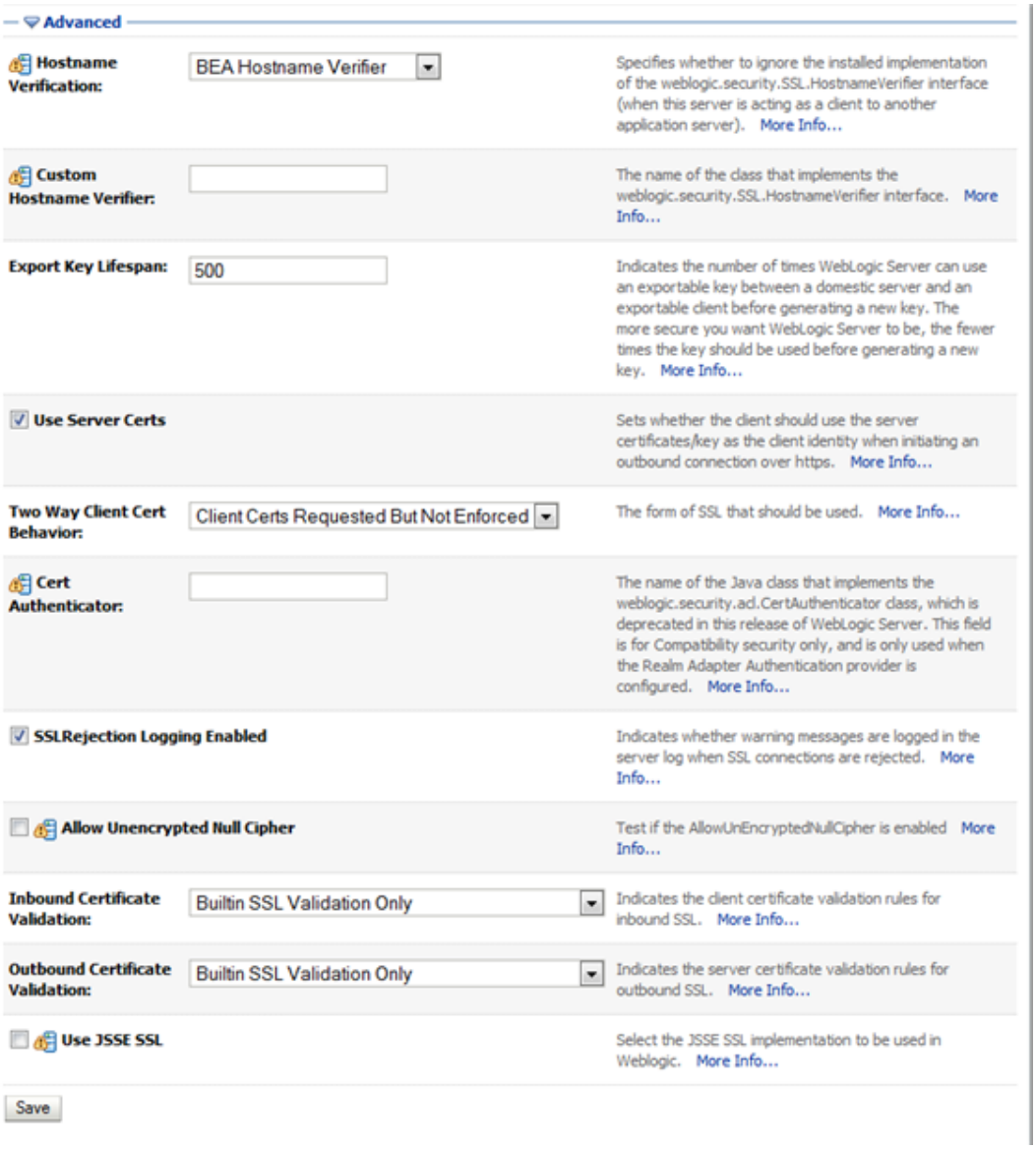


14. Haga clic en **Save** (Guardar).

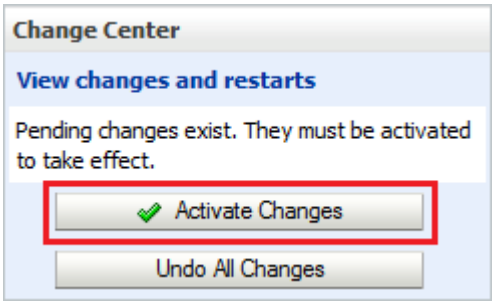
15. En la sección Trusted Certificate Authorities (Autoridades de certificación de confianza), haga clic en **Advanced** (Avanzado).



16. Complete la sección Advanced (Avanzado) de la pantalla SSL de la siguiente manera:
    a. Seleccione el separador **Use Server Certs** (Usar certificados de servidor).
    b. En el menú **Two Way Client Cert Behavior** (Comportamiento de certificado de cliente bidireccional), seleccione Client Certs Requested But Not Enforced (Certificados de cliente solicitados pero no forzados).
    c. En los menús **Inbound Certification Validation** (Validación de certificaciones entrantes) y **Outbound Certificate Validation** (Validación de certificados salientes), seleccione Builtin SSL Validation Only (Solo validación SSL integrada).



17. Haga clic en **Save** (Guardar).
18. En la sección Change Center (Centro de cambios), haga clic en **Activate Changes** (Activar cambios).



19. Cierre la sesión de WebLogic.
20. Detenga STA y reinícielo con el comando *STA*. Consulte información detallada sobre el uso de comandos en *Guía de administración de STA*.

```
# STA stop all
# STA start all
```

D.1.3. Reemplazo del certificado de Oracle

1. Abra un explorador web compatible en el equipo e introduzca la versión HTTPS/SSL de la dirección URL de la aplicación de STA.

   https://*STA_host_name***:***port_number***/STA/**

   Donde:
   - *host_name* es el nombre de host del servidor de STA.
   - *port_number* es el número de puerto de STA que especificó durante la instalación. El puerto HTTP predeterminado es el 7021; el puerto HTTPS predeterminado es el 7022.
   - *STA* debe estar en mayúsculas.

   Por ejemplo:

   ```
   https://staserver.example.com:7022/STA/
   ```

2. Seleccione **I Understand the Risks** (Comprendo los riesgos) en la pantalla This Connection is Untrusted (Esta conexión no es de confianza).
3. Haga clic en **Add Exception** (Agregar excepción).
4. Para especificar un certificado para la organización, haga clic en **Get Certificate** (Obtener certificado) en la pantalla Add Security Certificate (Agregar certificado de seguridad) y seleccione el archivo adecuado.
5. Haga clic en **Confirm Security Exception** (Confirmar excepción de seguridad).

Apéndice E

Configuración de un proveedor de servicios de seguridad para STA

Se debe autenticar a los usuarios para que se les permita el acceso a STA. Puede crear usuarios de manera local desde STA o puede usar proveedores de servicios de seguridad (SSP) externos para proporcionar control de acceso para STA.

En este apéndice, se describe cómo usar OpenLDAP (protocolo ligero de acceso a directorios) de WebLogic y RACF (función de control de acceso a recursos) de IBM para el control de acceso a STA. Incluye las siguientes secciones:

Para crear usuarios con la aplicación de STA, consulte *Guía del usuario de STA*.

E.1. Control de acceso a STA con OpenLDAP de WebLogic

Use este procedimiento para configurar OpenLDAP para STA.

E.1.1. Configuración de OpenLDAP de WebLogic

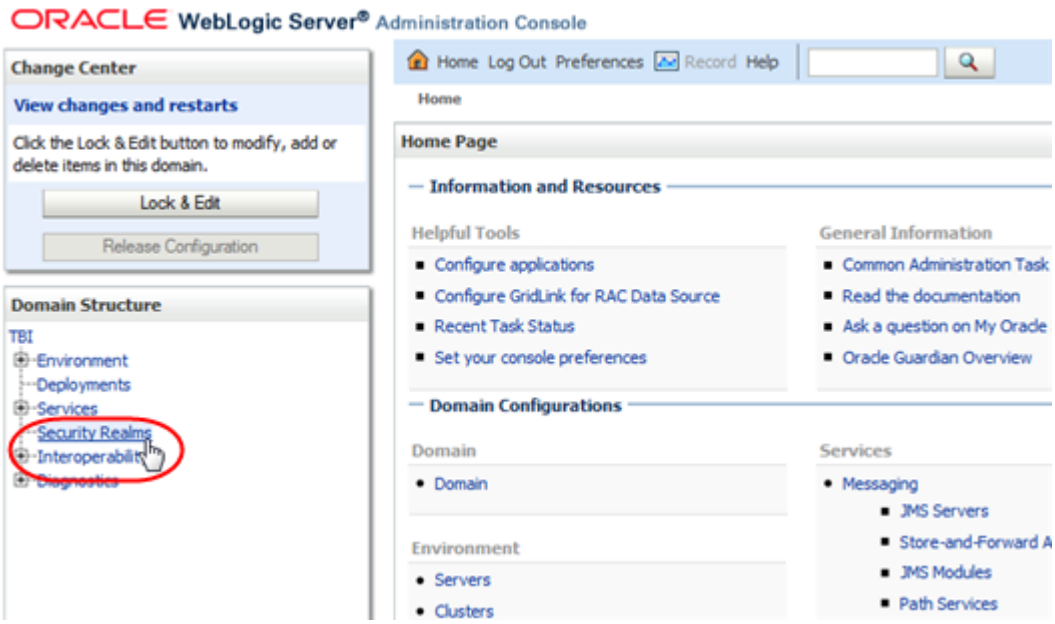
1. Vaya a la pantalla de inicio de sesión de la consola de WebLogic mediante el número de puerto HTTP (el puerto predeterminado de STA 2.1.0 es 7019) o HTTPS (el puerto predeterminado de STA 2.1.0 es 7020) que haya seleccionado durante la instalación de STA.

   https://*yourHostName***:***PortNumber***/console/**

   Por ejemplo:

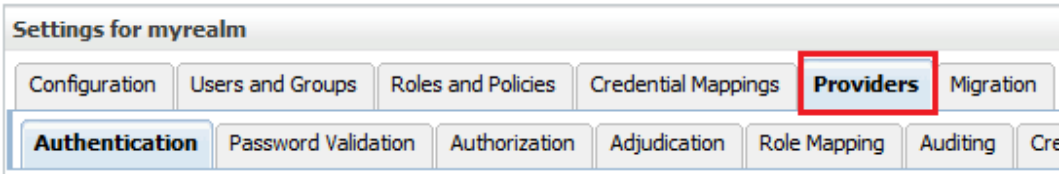
   https://sta_server:7020/console

2. Inicie sesión con el nombre de usuario y la contraseña de la consola de administración de WebLogic que definió durante la instalación de STA.
3. En la sección Domain Structure (Estructura de dominios), haga clic en **Security Realms** (Dominios de seguridad).

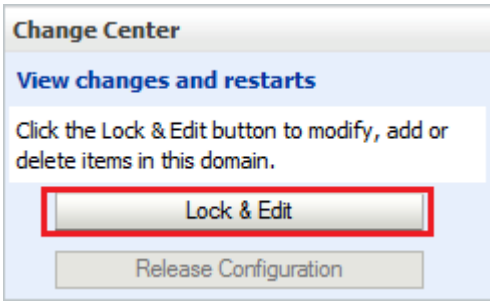


4. En la tabla Realms (Dominios), seleccione el enlace activo **myrealm** (seleccione el enlace, no la casilla de control).

5. Haga clic en el separador **Providers** (Proveedores).

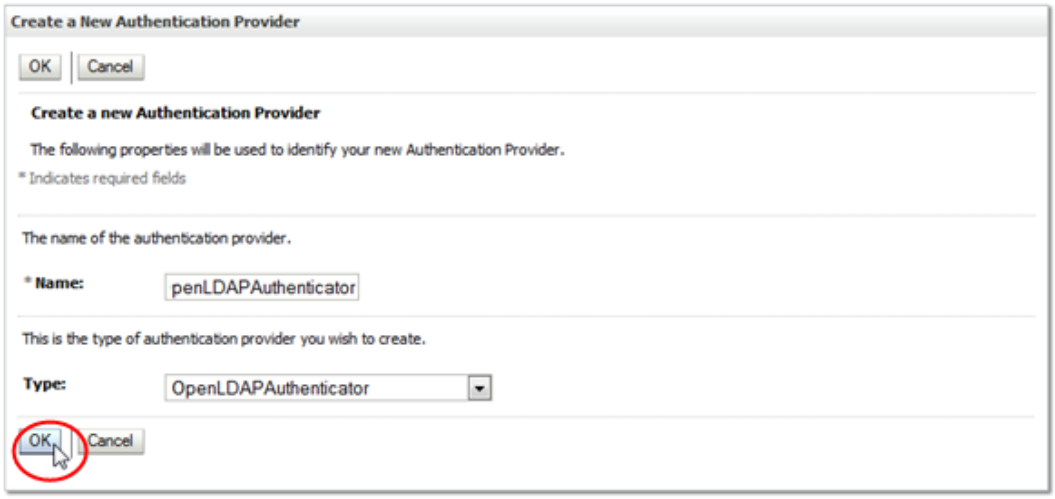


6. En la sección Change Center (Centro de cambios), haga clic en **Lock & Edit** (Bloquear y editar).

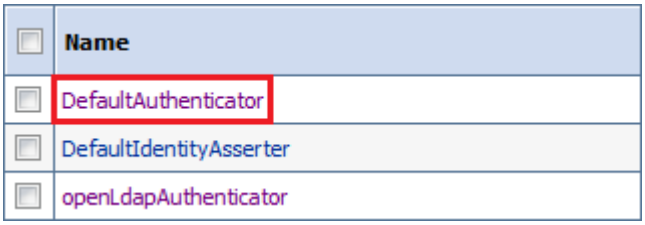


7. En la sección Authentication Providers (Proveedores de autenticación), haga clic en **New** (Nuevo).

8. Introduzca el nombre del proveedor de autenticación que desea crear (por ejemplo, OpenLdapAuthenticator) y seleccione OpenLDAPAuthenticator en el menú **Type** (Tipo). Haga clic en **OK** (Aceptar).

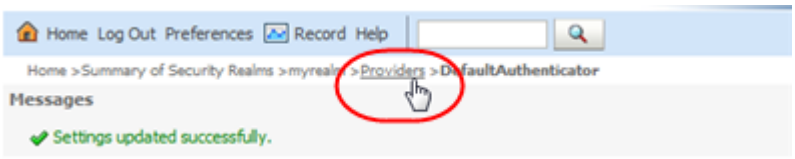


9. Seleccione el enlace activo **DefaultAuthenticator** (seleccione el enlace, no la casilla de control).



10. En el menú **Control Flag** (Indicador de control), seleccione Sufficient (Suficiente) y, a continuación, haga clic en **Save** (Guardar).

11. Seleccione el enlace localizador **Providers** (Proveedores) para regresar a la pantalla Authentication Providers (Proveedores de autenticación).

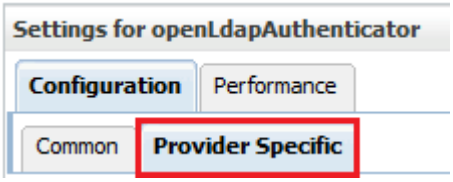


12. En la tabla Authentication Providers (Proveedores de autenticación), seleccione el nombre del autenticador de OpenLDAP que creó en el paso 8 (seleccione el nombre, no la casilla de control).

	Name	Description
☐	DefaultAuthenticator	WebLogic Authentication Provider
☐	DefaultIdentityAsserter	WebLogic Identity Assertion provider
☐	openLdapAuthenticator	Provider that performs LDAP authentication

13. En el menú **Control Flag** (Indicador de control), seleccione Sufficient (Suficiente) y, a continuación, haga clic en **Save** (Guardar).

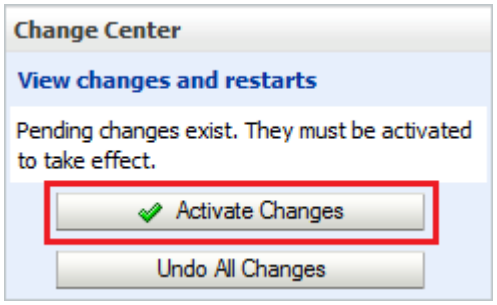
14. Haga clic en el separador **Provider Specific** (Específico del proveedor).



15. Complete los campos de la pantalla en función de los requisitos de la organización. El siguiente ejemplo corresponde al servidor *`lses-ldap1`* y es específico para el entorno de cada cliente.
    - Host = *`lses-ldap1`*
    - Port (Puerto) = *`389`*
    - Principal = déjelo en blanco
    - Credential (Credencial) = déjelo en blanco
    - User Base DN (DN de base de usuarios) = *`ou=people,o=STA,dc=oracle,dc=com`*

- User From Name Filter (Filtro de nombre de usuario remitente) = *(&(cn=%u)(objectclass=inetOrgPerson))*
- User Object Class (Clase de objeto de usuario) = *inetOrgPerson*
- Group Base DN (DN de base de grupos) = *ou=groups,o=STA,dc=oracle,dc=com*
- Group From Name Filter (Filtro de nombre de grupo remitente) = *(&(cn=%g)(objectclass=groupofnames))*

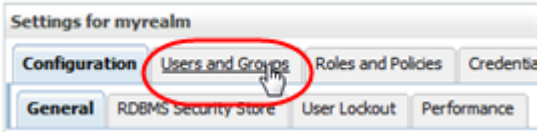
16. Haga clic en **Save** (Guardar).
17. En la sección Change Center (Centro de cambios), haga clic en **Activate Changes** (Activar cambios).



18. Realice los siguientes pasos para probar la configuración.
    a. Cierre la sesión de la consola de administración de WebLogic.
    b. Detenga STA y reinícielo con el comando *STA*. Consulte información detallada sobre el uso de comandos en *Guía de administración de STA*.

```
# STA stop all
# STA start all
```

    c. Inicie sesión en la consola de WebLogic.
    d. En la sección Domain Structure (Estructura de dominios), seleccione **Security Realms** (Dominios de seguridad).
    e. En la tabla Realms (Dominios), seleccione el enlace activo **myrealm** (seleccione el enlace, no la casilla de control).
    f. Haga clic el separador **Users and Groups** (Usuarios y grupos).



    g. En los separadores **Users** (Usuarios) y **Groups** (Grupos), verifique que haya entradas en la columna Provider (Proveedor) para el proveedor OpenLDAP.

E.2. Control de acceso a STA mediante tareas de RACF de IBM

Use los siguientes procedimientos para configurar la autenticación de RACF (Función de control de acceso a recursos) de IBM para STA. Debe completar los procedimientos en el orden indicado.

Nota:

STA admite productos de terceros que sean compatibles con RACF de IBM, por ejemplo, ACF2 y Top Secret de CA. La persona que instala STA, o el administrador de seguridad, es responsable de ejecutar los comandos apropiados para el producto de seguridad instalado.

E.2.1. Tarea 1: Revisión de los requisitos mínimos del mainframe de RACF de IBM

Consulte los requisitos completos de RACF en *Guía de requisitos de STA*.

E.2.2. Tarea 2: Activación de compatibilidad del mainframe para autorizaciones RACF de STA

El lado del mainframe del servicio de RACF para STA se proporciona mediante una rutina CGI que es parte del componente SMC para ELS 7.0 y 7.1. Esta rutina CGI es invocada por el servidor HTTP de SMC y usa los perfiles de RACF definidos en la clase FACILITY.

Para que STA use RACF como medio de autenticación de acceso, se debe configurar en el mainframe una tarea iniciada de SMC que ejecute el servidor HTTP. En el documento *Configuración y gestión de SMC* de ELS puede encontrar los detalles para hacerlo.

Nota:

La tarea iniciada de SMC debe coincidir con la regla de AT-TLS definida. De manera alternativa, permita que la definición de AT-TLS use un nombre de tarea genérico (por ejemplo, SMCW).

Si usa un identificador de STC proporcionado por el valor (por ejemplo, JOBNAME.JOB), se producirá un error en la conexión de la rutina de CGI.

El número de puerto usado para el servidor HTTP debe coincidir con el definido en la consola de WebLogic y el host debe coincidir con el nombre IP del host en el que se ejecuta la tarea de SMC.

Nota:

Se puede usar un SMC existente si existe en el host en el que se realizará la autorización de RACF. En este caso, use el número de puerto del servidor HTTP existente cuando esté realizando la configuración de WebLogic.

E.2.3. Tarea 3: Configuración de AT-TLS

AT-TLS es una solución de cifrado para aplicaciones TCP/IP que es transparente para el servidor de aplicaciones y el cliente. El cifrado y el descifrado de paquetes se realizan en el espacio de direcciones z/OS TCPIP en el nivel del protocolo TCP. Los requisitos de AT-TLS para la autorización de RACF se describen en *Guía de requisitos de STA*.

Los siguientes comandos de RACF indican el estado de los diversos objetos de RACF que se definen en el proceso de configuración:

- *RLIST STARTED PAGENT.* STDATA ALL*
- *RLIST DIGTRING *ALL*
- *RLIST FACILITY IRR.DIGTCERT.LISTRING ALL*
- *RLIST FACILITY IRR.DIGCERT.LST ALL*
- *RLIST FACILITY IRR.DIGCERT.GENCERT ALL*
- *RACDCERT ID(stcuser) LIST*
- *RACDCERT ID(stcuser) LISTRING(keyringname)*
- *RACDCERT CERTAUTH LIST*

Para configurar AT-TLS, haga lo siguiente:

1. Especifique el siguiente parámetro en el juego de datos del perfil TCPIP para activar AT-TLS:

   ```
   TCPCONFIG TTLS
   ```

   Esta declaración se puede colocar en el archivo TCP OBEY.
2. Configuración del agente de políticas (PAGENT)

   El espacio de direcciones del agente de políticas controla cuál es el tráfico de TCP/IP que se cifra.
   a. Introduzca la tarea JCL iniciada por PAGENT.

      Por ejemplo:

      ```
      //PAGENT PROC
      //*
      //PAGENT EXEC PGM=PAGENT,REGION=0K,TIME=NOLIMIT,
      // PARM='POSIX(ON) ALL31(ON) ENVAR("_CEE_ENVFILE=DD:STDENV")/-d1'
      //*
      //STDENV DD DSN=pagentdataset,DISP=SHR//SYSPRINT DD SYSOUT=*
      ```

```
//SYSOUT DD SYSOUT=*
//*
//CEEDUMP DD SYSOUT=*,DCB=(RECFM=FB,LRECL=132,BLKSIZE=132)
```

b. Introduzca las variables del entorno *PAGENT*. El juego de datos *pagentdataset* contiene las variables del entorno *PAGENT*.

   Por ejemplo:

```
LIBPATH=/lib:/usr/lib:/usr/lpp/ldapclient/lib:.
PAGENT_CONFIG_FILE=/etc/pagent.conf
PAGENT_LOG_FILE=/tmp/pagent.log
PAGENT_LOG_FILE_CONTROL=3000,2
_BPXK_SETIBMOPT_TRANSPORT=TCPIP
TZ=MST7MDT
```

   En este ejemplo, */etc/pagent.conf* contiene los parámetros de configuración de *PAGENT*. Use su propia zona horaria para el parámetro *TZ*.

c. Configure *PAGENT*.

   Por ejemplo:

```
TTLSRule TBI-TO-ZOS
{
 LocalAddr localtcpipaddress
 RemoteAddr remotetcpipaddress
 LocalPortRange localportrange
 RemotePortRange remoteportrange
 Jobname HTTPserverJobname
 Direction Inbound
 Priority 255
 TTLSGroupActionRef gAct1~TBI_ICSF
 TTLSEnvironmentActionRef eAct1~TBI_ICSF
 TTLSConnectionActionRef cAct1~TBI_ICSF
}
TTLSGroupAction gAct1~TBI_ICSF
{
 TTLSEnabled On
 Trace 2
}
TTLSEnvironmentAction eAct1~TBI_ICSF
{
 HandshakeRole Server
 EnvironmentUserInstance 0
 TTLSKeyringParmsRef keyR~ZOS
```

```
}
TTLSConnectionAction cAct1~TBI_ICSF
{
 HandshakeRole ServerWithClientAuth
 TTLSCipherParmsRef cipher1~AT-TLS__Gold
 TTLSConnectionAdvancedParmsRef cAdv1~TBI_ICSF
 CtraceClearText Off
 Trace 2
}
TTLSConnectionAdvancedParms cAdv1~TBI_ICSF
{
 ApplicationControlled Off
 HandshakeTimeout 10
 ResetCipherTimer 0
 CertificateLabel certificatelabel
 SecondaryMap Off
}
TTLSKeyringParms keyR~ZOS
{
 Keyring keyringname
}
TTLSCipherParms cipher1~AT-TLS__Gold
{
 V3CipherSuites TLS_RSA_WITH_3DES_EDE_CBC_SHA
 V3CipherSuites TLS_RSA_WITH_AES_128_CBC_SHA
}
```

donde:

- *`localtcpipaddress`*: dirección TCP/IP local del servidor HTTP
- *`remotetcpipaddress`*: dirección TCP/IP remota del cliente de STA. Puede ser ALL (Todas) para todas las direcciones de TCP/IP
- *`localportrange`*: puerto local del servidor HTTP (especificado en el inicio de HTTP o SMC)
- *`remoteportrange`*: rango de puertos remotos (1024-65535 para todos los puertos efímeros)
- *`HTTPserverJobname`*: nombre de trabajo del servidor HTTP
- *`certificatelabel`*: etiqueta proveniente de la definición del certificado
- *`keyringname`*: nombre proveniente de la definición del archivo de claves RACF

3. Active las clases de RACF. Se pueden usar los paneles de RACF o la CLI.

   Las clases de RACF incluyen:

   - *`DIGTCERT`*
   - *`DIGTNMAP`*

- *DIGTRING*

  La clase *SERVAUTH* debe ser RACLISTed para evitar que *PORTMAP* y *RXSERV* finalicen de manera anormal.

```
SETROPTS RACLIST(SERVAUTH)
RDEFINE SERVAUTH **UACC(ALTER) OWNER (RACFADM)
RDEFINE STARTED PAGENT*.* OWNER(RACFADM) STDATA(USER(TCPIP) GROUP(STCGROUP)
RDEFINE FACILITY IRR.DIGTCERT.LISTRING UACC(NONE) OWNER(RACFADM)
RDEFINE FACLITY IRR.DIGTCERT.LIST UACC(NONE) OWNER(RACFADM)
RDEFINE FACILITY IRR.DIGTCERT.GENCERT UACC(NONE) OWNER (RACFADM)
```

4. Definición de archivos de claves y certificados de RACF
   a. Introduzca los siguientes comandos de RACF para crear archivos de claves y certificados:

```
RACDCERT ID(stcuser) ADDRING(keyringname)
```

   donde:

   - *stcuser*: ID de usuario de RACF asociado con el espacio de direcciones de TCPIP
   - *keyringname*: nombre del archivo de claves, debe coincidir con el archivo de claves especificado en la configuración de PAGENT

```
RACDCERT ID(stcuser) GENCERT CERTAUTH SUBJECTSDN(CN('serverdomainname')
 O('companyname') OU('unitname') C('country')) WITHLABEL('calabel') TRUST
 SIZE(1024) KEYUSAGE(HANDSHAKE,DATAENCRYPT,CERTSIGN)
```

   Nota:

   Se trata del certificado de la autoridad de certificación para el sistema de STA.

   donde:

   - *stcuser*: ID de usuario de RACF asociado con el espacio de direcciones de TCPIP
   - *serverdomainname*: nombre de dominio del servidor z/OS (por ejemplo, *MVSA .COMPANY.COM*)
   - *companyname*: nombre de la organización
   - *unitname*: nombre de la unidad organizativa
   - *country*: país
   - *calabel*: etiqueta de la autoridad de certificación (por ejemplo, CATBISERVER)

```
RACDCERT ID(stcuser) GENCERT SUBJECTSDN(CN('serverdomainname')
 O('companyname') OU('unitname') C('country')) WITHLABEL('serverlabel') TRUST
 SIZE(1024) SIGNWITH(CERTAUTH LABEL('calabel'))
```

Nota:

Es el certificado SERVER.

donde:

- *stcuser*: ID de usuario de RACF asociado con el espacio de direcciones de TCPIP
- *serverdomainname*: nombre de dominio del servidor z/OS (por ejemplo, MVSA .COMPANY.COM)
- *companyname*: nombre de la organización
- *unitname*: nombre de la unidad organizativa
- *country*: país
- *serverlabel*: etiqueta del certificado del servidor (por ejemplo, TBISERVER)
- *calabel*: etiqueta de la autoridad de certificación, especificada en la definición del certificado de CA

```
RACDCERT ID(stcuser) GENCERT SUBJECTSDN(CN('clientdomainname')
 O('companyname') OU('unitname') C('country')) WITHLABEL('clientlabel') TRUST
 SIZE(1024) SIGNWITH(CERTAUTH LABEL('calabel'))
```

Nota:

Es el certificado CLIENT.

donde:

- *stcuser*: ID de usuario de RACF asociado con el espacio de direcciones de TCPIP
- *clientdomainname*: nombre de dominio del cliente de STA (por ejemplo, *TBIA .COMPANY.COM*)
- *companyname*: nombre de la organización
- *unitname*: nombre de la unidad organizativa
- *country*: país
- *clientlabel*: etiqueta del certificado del servidor: TBICLIENT
- *calabel*: etiqueta de la autoridad de certificación, especificada en la definición del certificado de CA

b. Conecte los certificados de la autoridad de certificación, del servidor y del cliente al patrón de claves especificado en la configuración de PAGENT:

```
RACDCERT ID(stcuser) CONNECT(CERTAUTH LABEL('calabel') RING('keyringname')
 USAGE(CERTAUTH))
```

donde:

- *stcuser*: ID de usuario de RACF asociado con el espacio de direcciones de TCPIP
- *calabel*: etiqueta de la autoridad de certificación, especificada en la definición del certificado de CA
- *keyringname*: nombre del archivo de claves, debe coincidir con el archivo de claves especificado en la configuración de PAGENT

```
RACDCERT ID(stcuser) CONNECT(ID(stcuser) LABEL('serverlabel')
 RING('keyingname') DEFAULT USEAGE(PERSONAL)
```

donde:

- *stcuser*: ID de usuario de RACF asociado con el espacio de direcciones de TCPIP
- *serverlabel*: etiqueta del certificado del servidor
- *keyringname*: nombre del archivo de claves, debe coincidir con el archivo de claves especificado en la configuración de PAGENT

```
RACDCERT ID(stcuser) CONNECT(ID(stcuser) LABEL('clientlabel')
 RING('keyingname') USEAGE(PERSONAL)
```

donde:

- *stcuser*: ID de usuario de RACF asociado con el espacio de direcciones de TCPIP
- *clientlabel*: etiqueta del certificado del cliente
- *keyringname*: nombre del archivo de claves, debe coincidir con el archivo de claves especificado en la configuración de PAGENT

c. Exporte los certificados de la autoridad de certificación y el cliente que se deben transmitir a STA:

```
RACDCERT EXPORT (LABEL('calabel')) CERTAUTH DSN('datasetname') FORMAT(CERTB64)
```

donde:

- *calabel*: etiqueta de la autoridad de certificación, especificada en la definición del certificado de CA
- *datasetname*: juego de datos para recibir el certificado exportado

```
RACDCERT EXPORT (LABEL('clientlabel')) ID(stcuser) DSN('datasetname')
 FORMAT(PKCS12DER) PASSWORD(' password ')
```

donde:

- *clientlabel*: etiqueta del certificado del cliente
- *stcuser*: ID de usuario de RACF asociado con el espacio de direcciones de TCPIP
- *datasetname*: juego de datos para recibir el certificado exportado
- *password*: contraseña para el cifrado de datos. Se necesita cuando se recibe el certificado en STA. La contraseña debe tener ocho caracteres o más.

Los juegos de datos de exportación ahora se transmiten a STA y se puede usar FTP. El certificado de CA se transmite con una conversión de EBCDIC a ASCII. El certificado CLIENT se transmite como archivo BINARY y contiene el certificado del cliente y la clave privada correspondiente.

E.2.4. Tarea 4: Creación de los perfiles de RACF usados por la rutina CGI

Los perfiles se definen en la clase FACILITY. El primero de los perfiles se llama *SMC .ACCESS.STA* y determina si el usuario tiene acceso a la aplicación de STA.

Los usuarios que necesitan tener acceso a STA deben tener acceso READ a este perfil. Los demás perfiles se muestran como *SMC.ROLE.nnn* y se usan para determinar cuáles son los roles que tiene el usuario cuando inicia sesión.

Nota:

El único rol definido para STA es *StorageTapeAnalyticsUser*. Para obtener este rol, debe solicitar que su ID de usuario se agregue al perfil *SMC.ROLE.STORAGETAPEANALYTICSUSER* con acceso READ.

E.2.5. Tarea 5: Importación del archivo del certificado y el archivo de la clave privada (opcional)

Este procedimiento puede ser valioso para probar que las claves públicas y privadas se hayan generado correctamente, y que los identificadores y las contraseñas de los usuarios se hayan definido con los permisos apropiados.

La prueba se puede hacer con cualquier explorador; en el ejemplo se usa Firefox.

1. En el menú **Herramientas** de Firefox, seleccione **Opciones**.
2. Seleccione el separador **Opciones avanzadas** y, a continuación, seleccione el separador **Cifrado**.
3. Haga clic en **Ver certificados**.
4. En el cuadro de diálogo **Gestor de certificados**, seleccione el separador **Autoridades** y, a continuación, seleccione el archivo de certificado que desea importar.
5. Haga clic en **Importar**.

6. Seleccione el separador **Sus certificados** e introduzca el archivo de claves privadas que desea importar.
7. Haga clic en **Importar**.
8. Haga clic en **Aceptar** para guardar y cerrar el cuadro de diálogo.

E.2.6. Tarea 6: Prueba de la rutina de CGI

Para probar la rutina de CGI desde un explorador, introduzca la siguiente dirección URL, donde *host*, *port*, *userid* y *password* están configurados con los valores apropiados.

https://*host***:***port***/smcgsaf?type=authentication&userid=***userid***&password=***password***&roles=StorageTapeAnalyticsUser**

La salida resultante indica si el usuario está autorizado o no para acceder a STA y el rol *StorageTapeAnalyticsUser*.

Nota:

La función de autorización RACF de STA no admite el cambio de la contraseña de ID de usuarios del mainframe. Si la contraseña de un ID de usuario caduca, STA así lo indica y la contraseña se debe restablecer por medio de los canales normales del mainframe antes de intentar iniciar sesión en STA nuevamente.

E.2.7. Tarea 7: Configuración de RACF/SSP para la consola de WebLogic

El proveedor de servicios de seguridad RACF (o RACF SSP) debe instalarse como complemento en WebLogic.

Si se instaló RACF SSP, el instalador de STA debe colocarlo en la ubicación apropiada de WebLogic. Si no se instaló, coloque el archivo de seguridad *jar* de RACF en el directorio, de la siguiente manera:

/Oracle_storage_home/Middleware/wlserver_10.3/server/lib/mbeantypes/staRACF.jar

donde *Oracle_storage_home* es la ubicación del directorio raíz de almacenamiento de Oracle especificada durante la instalación de STA.

E.2.8. Tarea 8: Configuración de SSL entre STA y RACF

1. Instale los PTF requeridos en el sistema MVS. Estos PTF posibilitan la autenticación con RACF u otro software de seguridad de terceros al iniciar sesión en STA. Consulte los requisitos de PTF en *Guía de requisitos de STA*.

   Application Transparent TLS (AT-TLS) se configuró en MVS para que el número de puerto definido para el servidor HTTP de SMC y WebLogic se cifre en el servidor.

Antes de continuar, asegúrese de tener dos archivos: el certificado del servidor de MVS (en formato ASCII) y la clave privada del cliente de STA (en formato binario PKCS12). El administrador del sistema de MVS le entregó la contraseña del archivo PKCS12.

2. Coloque el certificado en */Oracle_storage_home/Middleware/user_projects/domains/tbi/cert*.

   donde *Oracle_storage_home* es la ubicación del directorio raíz de almacenamiento de Oracle especificada durante la instalación de STA.

3. Convierta el certificado del formato DER al formato PEM.

   ```
   openssl pkcs12 -clcerts -in PKCS12DR.xxxxxx -out mycert.pem
   ```

   Se le solicitará que introduzca la contraseña de importación (que se le entregó con el certificado), una nueva contraseña de PEM y que verifique la contraseña.

4. Con el comando de la herramienta de claves de Java, importe el archivo del certificado al archivo */Oracle_storage_home/Middleware/jdk1.6.0_xx/jre/lib/security/cacerts*.

   ```
   # /Oracle_storage_home/Middleware/jdk1.6.0_xx/jre/bin/keytool -importcert -alias
    tbiServer -file certificate -keystore /Oracle/Middleware/jdk1.6.0_xx/jre/lib/
   security/cacerts -storetype jks
   ```

E.2.9. Tarea 9: Configuración del servidor de WebLogic

Para configurar WebLogic para la autenticación de RACF, siga el procedimiento indicado en Sección D.1.2, “Reconfiguración de WebLogic para usar otro certificado de seguridad”.

E.2.10. Tarea 10: Instalación de RACF/SSP en la consola de WebLogic

1. Vaya a la pantalla de inicio de sesión de la consola de WebLogic mediante el número de puerto HTTP (el puerto predeterminado de STA 2.1.0 es 7019) o HTTPS (el puerto predeterminado de STA 2.1.0 es 7020) que haya seleccionado durante la instalación de STA.

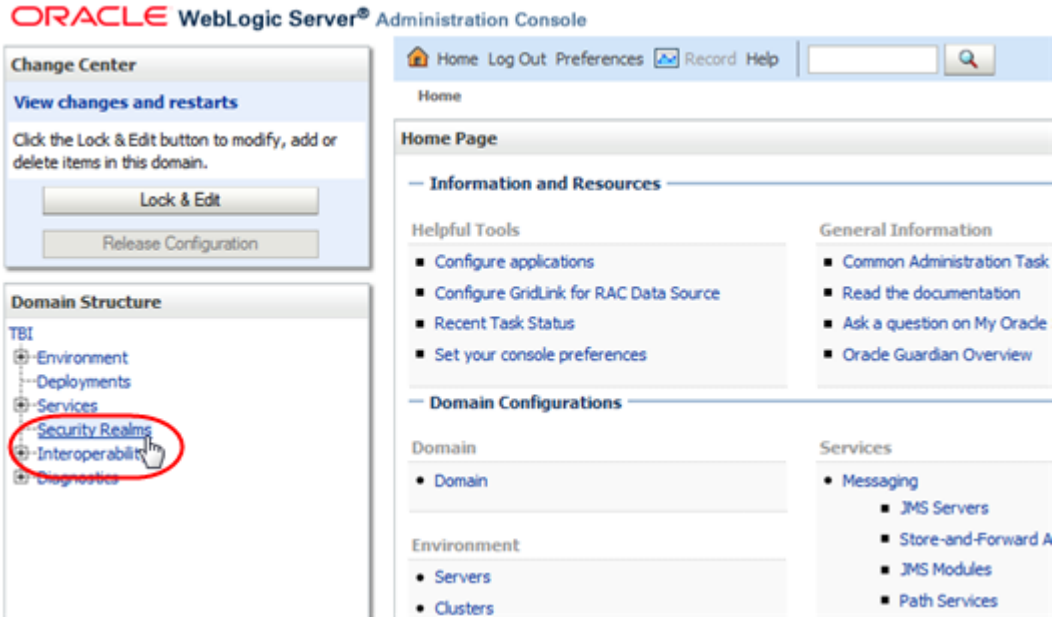
   ```
   https://yourHostName:PortNumber/console/
   ```

   Por ejemplo:

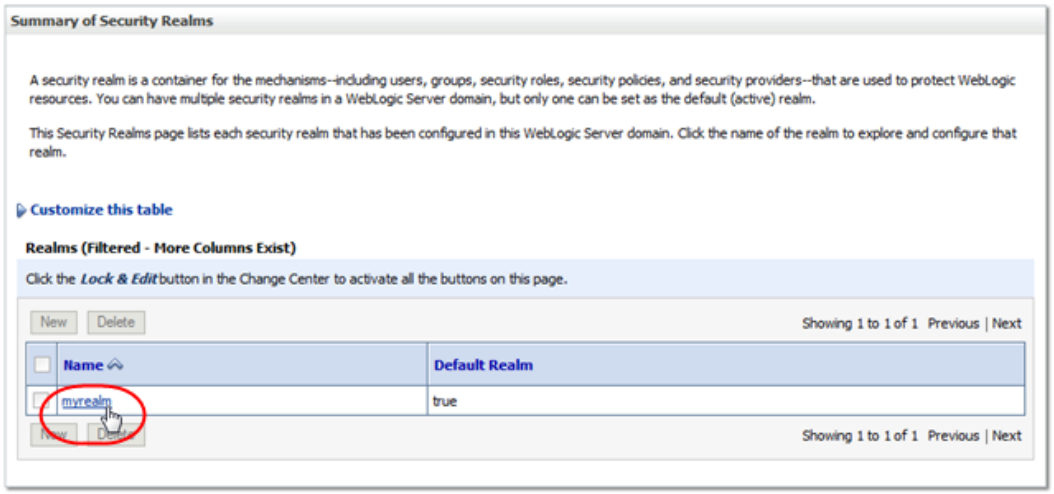
   ```
   https://sta_server:7020/console/
   ```

2. Inicie sesión con el nombre de usuario y la contraseña de la consola de administración de WebLogic que definió durante la instalación de STA.

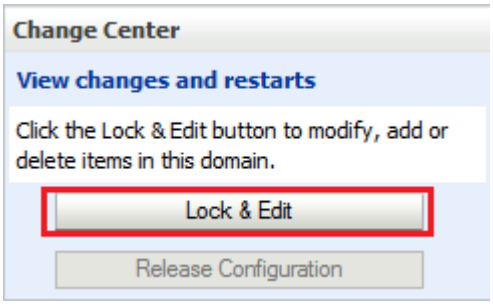
3. En la sección Domain Structure (Estructura de dominios), seleccione **Security Realms** (Dominios de seguridad).



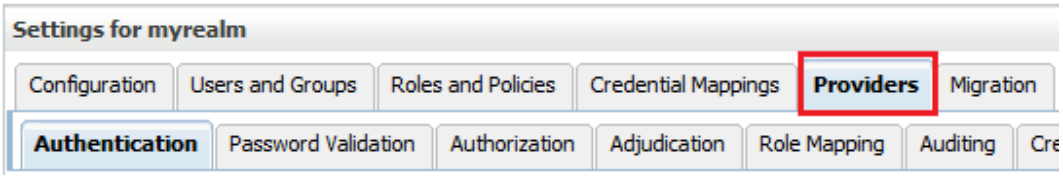
4. En la sección Realms (Dominios), seleccione el enlace activo **myrealm** (seleccione el nombre, no la casilla de control).



5. En la sección Change Center (Centro de cambios), haga clic en **Lock & Edit** (Bloquear y editar).



6. Seleccione el separador **Providers** (Proveedores).

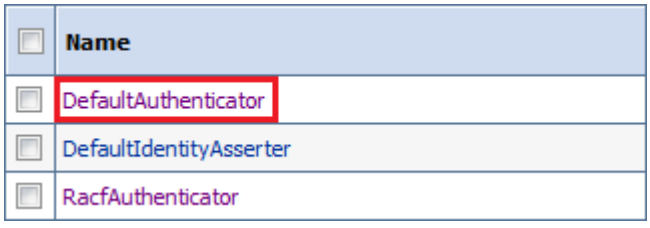


7. En la sección Authentication Providers (Proveedores de autenticación), haga clic en **New** (Nuevo).

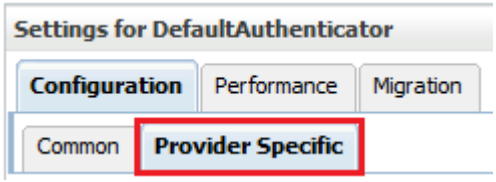
8. Introduzca el nombre del proveedor de autenticación que desea agregar (por ejemplo, *`STA RacfAuthenticator`*) y seleccione *`RacfAuthenticator`* en el menú **Type** (Tipo). Haga clic en **OK** (Aceptar).

> **Nota:**
>
> El archivo jar de RACF debería aparecer en el menú **Type** (Tipo). Si no es así, detenga STA y reinícielo con el comando *`STA`*. Consulte información detallada sobre el uso de comandos en *Guía de administración de STA*.

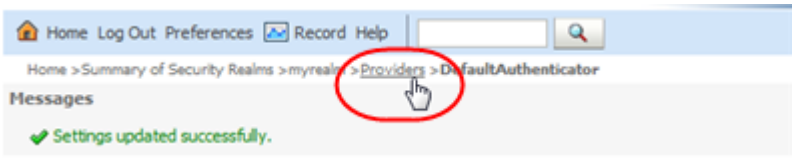
9. Verifique que el proveedor RACF esté incluido en la tabla Authentication Providers (Proveedores de autenticación). *`DefaultAuthenticator`* y *`DefaultIdentityAsserter`* deben ser siempre los dos primeros proveedores de esta lista.
10. Seleccione el enlace activo **DefaultAuthenticator** (seleccione el nombre, no la casilla de control).



11. En el menú **Control Flag** (Indicador de control), seleccione Sufficient (Suficiente) y, a continuación, haga clic en **Save** (Guardar).
12. Haga clic en el separador **Provider Specific** (Específico del proveedor) y, a continuación, en **Save** (Guardar).



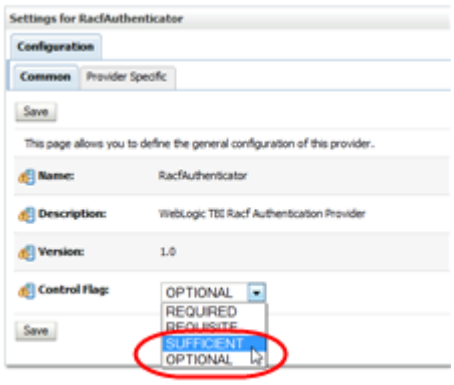
13. Haga clic en el enlace localizador **Providers** (Proveedores) para regresar a la pantalla Authentication Providers (Proveedores de autenticación).



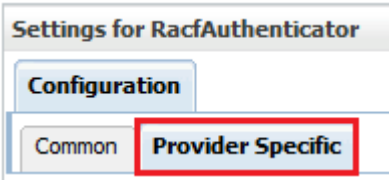
14. En la tabla Authentication Providers (Proveedores de autenticación), seleccione el nombre del autenticador de RACF que creó en el paso 8 (seleccione el nombre, no la casilla de control).

	Name	Description
☐	DefaultAuthenticator	WebLogic Authentication Provider
☐	DefaultIdentityAsserter	WebLogic Identity Assertion provider
☐	RacfAuthenticator	WebLogic TBI Racf Authentication Provider

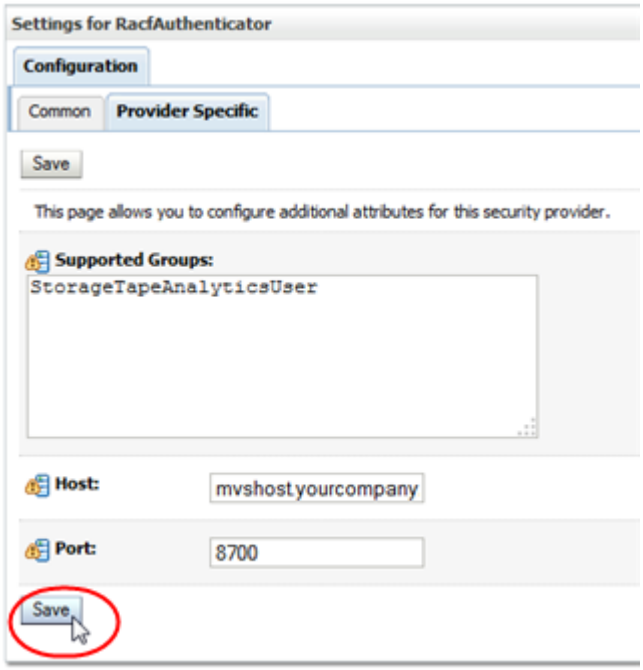
15. En el menú **Control Flag** (Indicador de control), seleccione *`Sufficient`* (Suficiente) y, a continuación, haga clic en **Save** (Guardar).



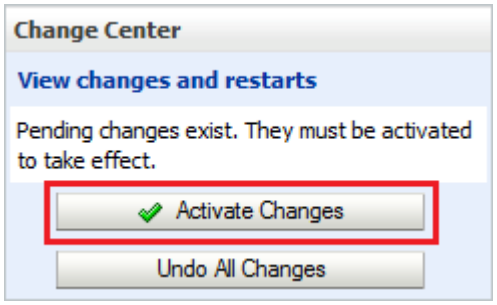
16. Haga clic en el separador **Provider Specific** (Específico del proveedor).



17. Introduzca el nombre del host (por ejemplo, *`mvshost.yourcompany.com`*) y el número de puerto (por ejemplo, *`8700`*) en donde se está ejecutando el sistema MVS y haga clic en **Save** (Guardar).



18. En la sección Change Center (Centro de cambios), haga clic en **Activate Changes** (Activar cambios).



19. Cierre la sesión de la consola de administración de WebLogic.
20. Detenga STA y reinícielo con el comando *`STA`*. Consulte información detallada sobre el uso de comandos en *Guía de administración de STA*.

```
# STA stop all
# STA start all
```

Apéndice F

Configuración del modo SNMP v2c

Si STA supervisará alguna biblioteca configurada para SNMP v2c, debe configurar el modo SNMP v2c.

STA siempre intenta comunicarse con las bibliotecas mediante el protocolo SNMP v3 recomendado. Si no es posible la comunicación SNMP v3 (por ejemplo, si SNMP v3 no está configurado en una biblioteca), STA usará SNMP v2c en caso de que se lo haya activado como se indica en las instrucciones de este apéndice.

El proceso de configuración de SNMP v3 se describe en el Capítulo 5, *Configuración de SNMP en las bibliotecas* y el Capítulo 6, *Configuración de conexiones de bibliotecas en STA*. En este apéndice, se describen los procedimientos que son diferentes para la configuración de SNMP v2c.

En este apéndice, se incluye la siguiente sección:

- Tareas de configuración de SNMP v2c

F.1. Tareas de configuración de SNMP v2c

F.1.1. Configuración del modo SNMP v2c

Use este procedimiento para configurar STA y las bibliotecas con el fin de que usen SNMP v2c para las comunicaciones de SNMP.

1. En el Capítulo 5, *Configuración de SNMP en las bibliotecas*, siga todos los procedimientos que se muestran en la Tabla 5.1, “Tareas para configurar bibliotecas para STA”, excepto:
   - Reemplace "Creación del destinatario de capturas de SNMP v3 de STA" [84] por Sección F.1.2, “Creación del destinatario de capturas SNMP v2c de STA en la biblioteca”
   - Después de completar el proceso que se describe en la Tabla 5.1, “Tareas para configurar bibliotecas para STA”, siga con Sección F.1.3, “Activación del modo SNMP v2c para STA”
2. Configure SNMP v2c en STA. Consulte el Capítulo 6, *Configuración de conexiones de bibliotecas en STA* [89] para obtener instrucciones.

F.1.2. Creación del destinatario de capturas SNMP v2c de STA en la biblioteca

Use este procedimiento para definir el servidor de STA como destinatario autorizado de capturas SNMP v2c y para definir las capturas que envía la biblioteca. En función del modelo de biblioteca, puede usar la CLI de la biblioteca, SL Console o la interfaz de explorador de SL150. Tenga en cuenta los siguientes puntos:

- Use comas para separar los niveles de captura.
- Para evitar registros duplicados, no defina el servidor de STA como destinatario de capturas en varias instancias. Por ejemplo, no cree una definición de destinatario de capturas de SNMP v3 y SNMP v2c para el servidor de STA.
- Es posible que el nivel de captura 4 no sea compatible con versiones de firmware de biblioteca antiguas. Sin embargo, siempre se lo puede especificar al crear destinatarios de capturas.
- Para evitar errores de introducción en la CLI, puede escribir primero el comando en un archivo de texto y, a continuación, copiarlo y pegarlo en la CLI. Si necesita ayuda con los comandos de la CLI, escriba *`help snmp`*.

Con la CLI de la biblioteca (todas las bibliotecas, excepto SL150)

1. Cree un destinatario de capturas de SNMP v2c.

   ```
   snmp addTrapRecipient trapLevel 1,2,3,4,11,13,14,21,25,27,41,45,
    61,63,65,81,85,100 host STA_server_IP version v2c community community_name
   ```

   Donde:
   - *`STA_server_IP`*: dirección IP del servidor de STA.
   - *`community_name`*: comunidad de capturas SNMP v2c. Puede ser *`public`* (pública) u otro nombre.

   Por ejemplo:

   ```
   SL3000> snmp addTrapRecipient trapLevel 1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100
    host 192.0.2.20 version v2c community public
   ```

2. Genere una lista de los destinatarios de capturas para verificar que el servidor de STA se haya agregado correctamente.

   ```
   snmp listTrapRecipients
   ```

Con SL Console (solo bibliotecas SL500)

1. En el menú **Tools** (Herramientas), seleccione **System Detail** (Detalle del sistema).

2. En el árbol de navegación, seleccione **Library** (Biblioteca).
3. Seleccione el separador **SNMP** y, a continuación, seleccione el separador **Add Trap Recipients** (Agregar destinatarios de capturas).
4. Introduzca la siguiente información:
   - *Host*: dirección IP del servidor de STA.
   - *TrapLevel* (Nivel de captura): lista de los niveles de captura que la biblioteca debe enviar a STA, separados por coma: 1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100.
   - *Version* (Versión): seleccione *v2c*.
   - *Community* (Comunidad): puede ser *public* u otro nombre.
5. Haga clic en **Apply** (Aplicar) para agregar el destinatario de capturas.

Con la interfaz de usuario de SL150

1. En el árbol de navegación, seleccione **SNMP**.
2. En la sección (o el separador) SNMP Trap Recipients (Destinatarios de capturas SNMP), seleccione **Add Trap Recipient** (Agregar destinatario de capturas).
3. Complete los campos de Add Trap Recipient (Agregar destinatario de capturas) de la siguiente manera:
   - *Host Address* (Dirección de host): dirección IP del servidor de STA.
   - *Trap Level* (Nivel de captura): lista de los niveles de captura que la biblioteca debe enviar a STA, separados por coma: 1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100.
   - *Version* (Versión): seleccione *v2c*.
   - *Community Name* (Nombre de la comunidad): puede ser *public* u otro nombre.
4. Haga clic en **OK** (Aceptar) para agregar el destinatario de capturas.

F.1.3. Activación del modo SNMP v2c para STA

1. Establezca una sesión de terminal con el servidor de STA e inicie sesión como usuario root del sistema.
2. Cambie al directorio de archivos de configuración de STA.

   ```
   # cd /Oracle_storage_home/Middleware/user_projects/domains/TBI
   ```

3. Edite el archivo de propiedades de la versión de SNMP.

   ```
   # vi TbiSnmpVersionSupport.properties
   ```

4. Verifique que el valor del parámetro SNMP v2c sea *true*.

   ```
   V2c=true
   ```

5. Guarde el archivo y ciérrelo.

6. Si en el paso 4 cambió el valor del parámetro SNMP v2c, detenga todos los procesos de STA y reinícielos.

```
# STA stop all
# STA start all
```

Índice