

Oracle® Enterprise Performance Management System

Guía de configuración de seguridad



Versión 11.2
F28802-22
Diciembre de 2023

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Tabla de contenidos

Accesibilidad a la documentación

Comentarios sobre la documentación

1 Acerca de la seguridad de EPM System

Acerca de EPM System	1-1
Presuposición de conocimiento	1-1
Componentes de infraestructura de seguridad	1-2
Autenticación de usuario	1-2
Aprovisionamiento (autorización basada en roles)	1-6
Inicio de Shared Services Console	1-10

2 Activación para SSL de los componentes de EPM System

Suposiciones	2-1
Fuentes de información	2-1
Referencias de ubicaciones	2-2
Acerca de la activación para SSL de los productos de EPM System	2-2
Escenarios de SSL soportados	2-3
Certificados necesarios	2-4
Finalización de SSL en el sistema de descarga de SSL	2-5
Despliegue de SSL completo de EPM System	2-7
Arquitectura de despliegue	2-7
Suposiciones	2-8
Configuración de EPM System para SSL completo	2-9
Nueva configuración de ajustes comunes de EPM System	2-10
Opcional: Instalación del certificado de CA raíz para WebLogic Server	2-11
Instalación del certificado en WebLogic Server	2-12
Configuración de WebLogic Server	2-13
Activación de una conexión de servidor de HFM con una instancia de Oracle Database activada para SSL	2-15

Procedimientos de Oracle HTTP Server	2-21
Configuración de los componentes web de EPM System desplegados en WebLogic Server	2-25
Actualización de la configuración de dominio	2-27
Reinicio de servidores y EPM System	2-28
Prueba del despliegue	2-28
Configuración de directorios de usuario externos activados para SSL	2-29
Finalización de SSL en el servidor web	2-30
SSL para Essbase 11.1.2.4	2-33
Instalación y despliegue de componentes de Essbase	2-35
Uso de certificados CA de terceros de confianza para Essbase	2-36
Establecimiento de una conexión SSL por sesión	2-43
SSL para Essbase 21c	2-44
Instalación y despliegue de componentes de Essbase	2-47
Uso de certificados CA de terceros de confianza para Essbase	2-47
Establecimiento de una conexión SSL por sesión	2-53

3 Habilitación del inicio de sesión único con agentes de seguridad

Métodos de inicio de sesión único soportados	3-1
Inicio de sesión único desde Oracle Access Manager	3-4
OracleAS Single Sign-on	3-5
Prueba del despliegue	3-7
Activación de OSSO para EPM System	3-7
Protección de productos de EPM System para el inicio de sesión único	3-11
Inicio de sesión único basado en cabecera con productos de administración de identidad	3-16
Configuración de EPM System para el inicio de sesión único basado en cabecera con Oracle Identity Cloud Services	3-18
Requisitos previos y direcciones URL de ejemplo	3-18
Activación de la autenticación basada en cabecera para EPM System	3-19
Adición de aplicación y puerta de enlace de EPM System a Oracle Identity Cloud Services	3-19
Configuración de la puerta de enlace de aplicación	3-25
Configuración del directorio de usuario para autorización	3-25
Habilitación del inicio de sesión único en EPM System	3-25
Actualización de la configuración de EPM Workspace	3-25
Inicio de sesión único de SiteMinder	3-26
Inicio de sesión único en Kerberos	3-29
Configuración de EPM System para inicio de sesión único	3-44
Opciones de inicio de sesión único para Smart View	3-45

4 Configuración de directorios de usuario

Directorios de usuario y seguridad de EPM System	4-1
Operaciones relacionadas con la configuración de directorios de usuario	4-2
Oracle Identity Manager y EPM System	4-2
Información sobre Active Directory	4-3
Configuración de OID, Active Directory y otros directorios de usuario basados en LDAP	4-4
Configuración de bases de datos relacionales como directorios de usuario	4-19
Prueba de conexiones de directorios de usuario	4-22
Edición de configuración de directorio de usuario	4-23
Supresión de configuraciones de directorios de usuario	4-24
Administración del orden de búsqueda de directorios de usuario	4-24
Establecimiento de las opciones de seguridad	4-26
Regeneración de claves de cifrado	4-30
Utilización de caracteres especiales	4-31

5 Utilización de un módulo de autenticación personalizado

Descripción general	5-1
Ejemplos y limitaciones de casos de uso	5-3
Requisitos	5-3
Consideraciones de codificación y diseño	5-3
Despliegue del módulo de autenticación personalizado	5-9

6 Pautas para establecer la seguridad de EPM System

Implantación de SSL	6-1
Cambio de la contraseña de administración	6-1
Regeneración de claves de cifrado	6-2
Cambio de contraseñas de base de datos	6-2
Cómo garantizar las cookies	6-3
Reducción del tiempo de espera del símbolo de inicio de sesión único	6-4
Revisión de informes de seguridad	6-4
Personalización del sistema de autenticación para una autenticación compleja	6-4
Desactivación de las utilidades de depuración de EPM Workspace	6-4
Cambio de las páginas de error predeterminadas del servidor web	6-5
Soporte del software de terceros	6-5

A Código de muestra de autenticación personalizado

Código de ejemplo 1	A-1
Código de ejemplo 2	A-2

B **Implantación de una clase de inicio de sesión personalizada**

Código de ejemplo de clase de inicio de sesión personalizada	B-1
Despliegue de una clase de inicio de sesión personalizada	B-4

C **Migración de usuarios y grupos de un directorio de usuario a otro**

Descripción general	C-1
Requisitos	C-1
Procedimiento de migración	C-2
Actualizaciones de producto	C-5

Accesibilidad a la documentación

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

Acceso a Oracle Support

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

Comentarios sobre la documentación

Para hacernos llegar sus comentarios sobre esta documentación, haga clic en el botón Comentarios en la parte inferior de la página de cualquier tema de Oracle Help Center. También puede enviar un correo electrónico a epmdoc_ww@oracle.com.

1

Acerca de la seguridad de EPM System

Consulte también:

- [Acerca de EPM System](#)
- [Presuposición de conocimiento](#)
- [Componentes de infraestructura de seguridad](#)
- [Autenticación de usuario](#)
- [Aprovisionamiento \(autorización basada en roles\)](#)
- [Inicio de Shared Services Console](#)

Acerca de EPM System

Los productos de Oracle Enterprise Performance Management System forman un sistema empresarial que integra módulos de aplicaciones de gestión financiera y planificación con las capacidades de inteligencia empresarial más completas para la generación de informes y análisis. Los principales componentes de los productos de EPM System:

- Oracle Hyperion Foundation Services
- Oracle Essbase
- Oracle Hyperion Financial Management
- Oracle Hyperion Planning

Para obtener información sobre los productos y componentes de cada una de estas familias de productos consulte *Documento de inicio para la instalación de Oracle Hyperion Enterprise Performance Management System*.

Presuposición de conocimiento

Esta guía está destinada a los administradores del sistema que configuran, protegen y gestionan componentes de Oracle Enterprise Performance Management System. Se presupone que dichos administradores cuentan con el siguiente conocimiento:

- Amplio conocimiento de la infraestructura de seguridad de su organización, incluido lo siguiente:
 - Servidores de directorios, por ejemplo, Oracle Internet Directory, Sun Java System Directory Server y Microsoft Active Directory
 - Uso de Secure Socket Layer (SSL) para proteger los canales de comunicación
 - Sistemas de gestión de acceso, por ejemplo, Oracle Access Manager y SiteMinder
 - Infraestructura de inicio de sesión único (SSO), por ejemplo, Kerberos
- Conocimiento de los conceptos de seguridad de EPM System relevantes para su organización

Componentes de infraestructura de seguridad

Oracle Enterprise Performance Management System integra varios componentes de seguridad para garantizar una seguridad sólida de la aplicación. Al integrarse en una infraestructura segura, EPM System ofrece un conjunto seguro de aplicaciones que garantiza la seguridad de los datos y del acceso. Entre los componentes de infraestructura que puede usar para proteger EPM System se incluyen:

- Un sistema de gestión de acceso opcional, por ejemplo, Oracle Access Manager para proporcionar acceso con inicio de sesión único a los componentes de EPM System
- Uso de una infraestructura de inicio de sesión único integrado, por ejemplo, Kerberos.

Puede usar la autenticación de Kerberos con el sistema de gestión de acceso (SiteMinder) para garantizar que los usuarios de Windows puedan iniciar sesión de forma transparente en SiteMinder y en los componentes de EPM System.
- Uso de Secure Socket Layer (SSL) para proteger los canales de comunicación entre los componentes y clientes de EPM System

Autenticación de usuario

La autenticación de usuario permite el inicio de sesión único (SSO) en todos los componentes de Oracle Enterprise Performance Management System mediante la validación de la información de inicio de sesión proporcionada por cada usuario. La autenticación de los usuarios, junto con la autorización específica del componente, otorga al usuario acceso a componentes de EPM System. El proceso de otorgamiento de autorizaciones se denomina aprovisionamiento.

Componentes de autenticación

En las secciones siguientes se describen los componentes compatibles con el inicio de sesión único:

- [Directorio nativo](#)
- [Directorios de usuario externos](#)

Directorio nativo

Directorio nativo hace referencia a la base de datos relacional que Servicios compartidos de Oracle Hyperion utiliza para las tareas de aprovisionamiento y almacenar datos de inicialización, como cuentas de usuario predeterminadas.

Funciones del directorio nativo:

- Mantener y gestionar las cuentas de usuario predeterminadas de EPM System
- Almacenar toda la información de aprovisionamiento de EPM System (relaciones entre usuarios, grupos y roles)

El acceso y la gestión del directorio nativo se realizan a través de Consola de Servicios compartidos de Oracle Hyperion. Consulte "Gestión del directorio nativo" en la *Guía de administración de seguridad de usuarios de Oracle Enterprise Performance Management System*.

Directorios de usuario externos

Los directorios de usuario hacen referencia a un usuario corporativo y sistemas de gestión de identidades compatible con los componentes de EPM System.

Los componentes de EPM System están soportados en varios directorios de usuario, incluidos los directorios de usuario basados en LDAP, por ejemplo, Oracle Internet Directory, Sun Java System Directory Server (anteriormente SunONE Directory Server) y Microsoft Active Directory. También se admiten las bases de datos relacionales como directorios de usuario. Los directorios de usuario que no sean el directorio nativo se denominan directorios de usuario externos a lo largo de este documento.

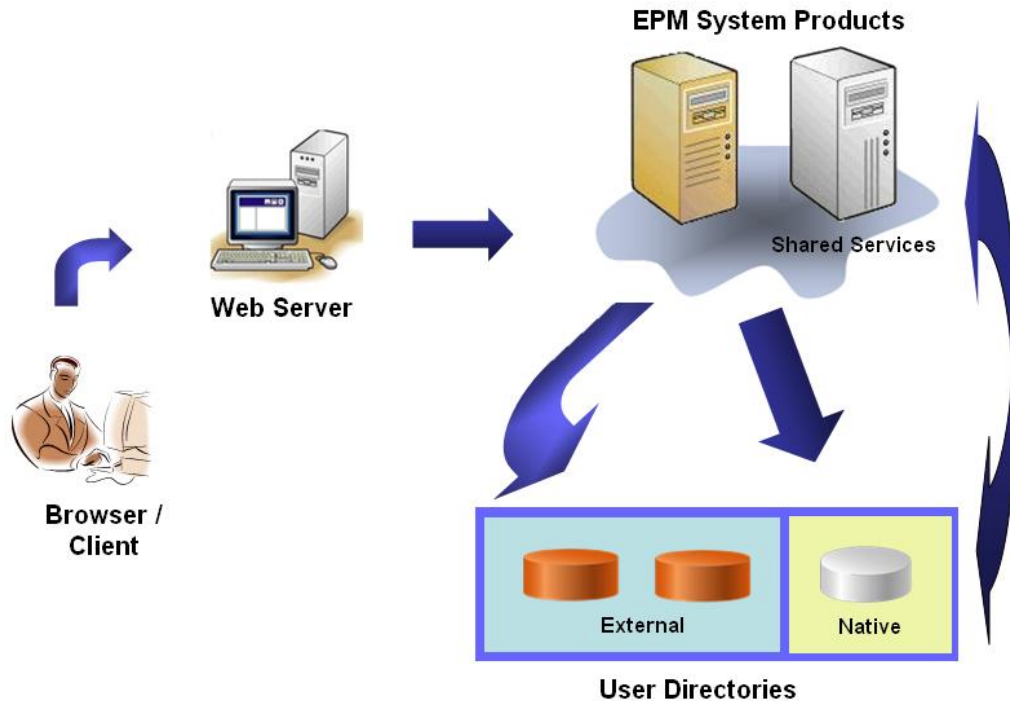
Para obtener una lista de directorios de usuario soportados, consulte la página *Matriz de certificación de Oracle Enterprise Performance Management System* publicada en la página [Configuraciones soportadas del sistema de Oracle Fusion Middleware](#) de Oracle Technology Network (OTN).

En Consola de Servicios compartidos, puede configurar muchos directorios de usuario externo como origen para usuarios y grupos de EPM System. Cada usuario de EPM System debe tener una cuenta única en un directorio de usuario configurado. Normalmente, los usuarios de EPM System se asignan a los grupos para facilitar el aprovisionamiento.

Inicio de sesión único predeterminado de EPM System

EPM System soporta el inicio de sesión único en aplicaciones web de EPM System al permitir a los usuarios autenticados en una aplicación para navegar de forma continua a otras aplicaciones sin volver a introducir credenciales. El inicio de sesión único se implanta al integrar un entorno de seguridad común que gestione la autenticación y el aprovisionamiento de usuarios (autorización basada en roles) en componentes de EPM System.

En la ilustración siguiente se muestra el proceso de inicio de sesión único predeterminado.



1. A través de un explorador, los usuarios obtienen acceso a la pantalla de inicio de sesión del componente de EPM System e introducen un nombre de usuario y contraseña.

El componente de EPM System consulta los directorios de usuario configurados (incluido el directorio nativo) para verificar las credenciales del usuario. Cuando se localiza la cuenta de usuario que coincide con las credenciales indicadas, la búsqueda finaliza y se devuelve la información del usuario al componente de EPM System.

El acceso quedará denegado si no se encuentra ninguna cuenta de usuario en ninguno de los directorios de usuario configurados.
2. Por medio de la información de usuario recuperada, el componente de EPM System obtiene los datos de aprovisionamiento para el usuario del directorio nativo.
3. El componente de EPM System comprueba la lista de control de acceso (ACL) en el componente para determinar los artefactos de aplicación al que puede acceder el usuario.

Después de recibir la información de aprovisionamiento del directorio nativo, el componente de EPM System estará ya disponible para el usuario. En este momento, también se encontrará activado el inicio de sesión único para todos los componentes de EPM System para los que se haya aprovisionado al usuario.

Inicio de sesión único desde sistemas de gestión de acceso

Para proteger aún más los componentes de EPM System, puede implantar un sistema de gestión de acceso soportado como Oracle Access Manager o SiteMinder, que pueden proporcionar al usuario autenticado credenciales para acceder a los componentes de EPM System y controlar el acceso en función de los privilegios de acceso predefinidos.

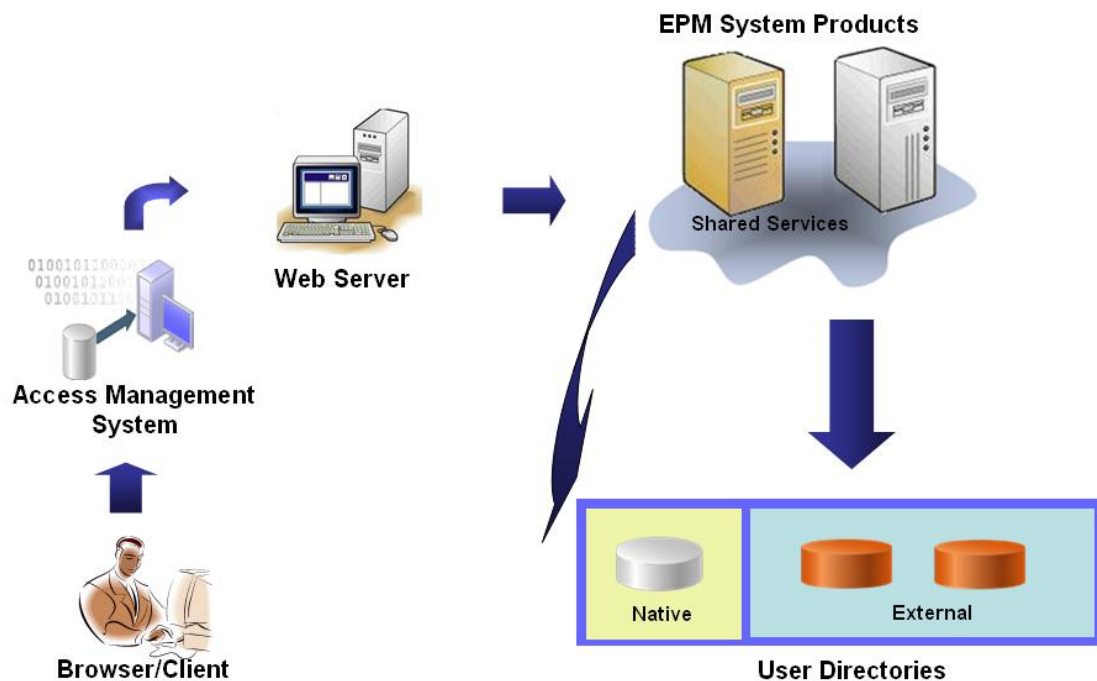
El inicio de sesión único desde agentes de seguridad solo se encuentra disponible para aplicaciones web de EPM System. En este tipo de escenario, los componentes de EPM System utilizan la información de usuario proporcionada por el agente de seguridad para determinar los permisos de acceso de los usuarios. Para mayor seguridad, Oracle recomienda que se bloquee el acceso directo a los servidores por medio de un cortafuegos para que todas las solicitudes se enruten a través de un portal de inicio de sesión único.

El inicio de sesión único desde sistemas de gestión de acceso es compatible si se aceptan las credenciales de usuario autenticadas a través de un mecanismo de inicio de sesión único aceptable. Consulte [Métodos de inicio de sesión único soportados](#). El sistema de gestión de acceso autentifica a los usuarios y transfiere el nombre de inicio de sesión a EPM System. EPM System verifica el nombre de inicio de sesión en los directorios de usuario configurados.

Consulte estos temas.

- [Inicio de sesión único desde Oracle Access Manager](#)
- [OracleAS Single Sign-on](#)
- [Inicio de sesión único de SiteMinder](#)
- [Inicio de sesión único en Kerberos](#)

El siguiente esquema ilustra el concepto:



1. Con un explorador, los usuarios solicitan acceso a un recurso protegido por un sistema de gestión de acceso, por ejemplo, Oracle Access Manager o SiteMinder.

 **Nota:**

Los componentes de EPM System se definen como recursos protegidos por el sistema de gestión de acceso.

El sistema de gestión de acceso intercepta la solicitud y presenta una pantalla de inicio de sesión. Los usuarios introducen un nombre de usuario y contraseña, que se validan con la ayuda de los directorios de usuario configurados en el sistema de gestión de acceso para verificar la autenticidad del usuario. Los componentes de EPM System también se configuran para que funcionen con estos directorios de usuario.

La información sobre el usuario autenticado se transfiere al componente de EPM System, que acepta como válida la información.

El sistema de gestión de acceso transfiere el nombre de inicio de sesión del usuario (valor de `Login Attribute`) al componente de EPM System con un mecanismo de inicio de sesión único aceptable. Consulte [Métodos de inicio de sesión único soportados](#).

2. Para comprobar las credenciales de un usuario, el componente de EPM System intenta localizarlo en un directorio de usuario. Si se encuentra una cuenta de usuario que coincida con dichos datos, se devolverá esta información al componente de EPM System. La seguridad de EPM System establece el símbolo de SSO que permita el inicio de sesión único en los componentes de EPM System.
3. Por medio de la información de usuario recuperada, el componente de EPM System obtiene los datos de aprovisionamiento para el usuario del directorio nativo.

El componente de EPM System se encontrará por fin disponible para el usuario después de recibir esta información de aprovisionamiento. El inicio de sesión único quedará activado para todos los componentes de EPM System para los que se haya aprovisionado al usuario.

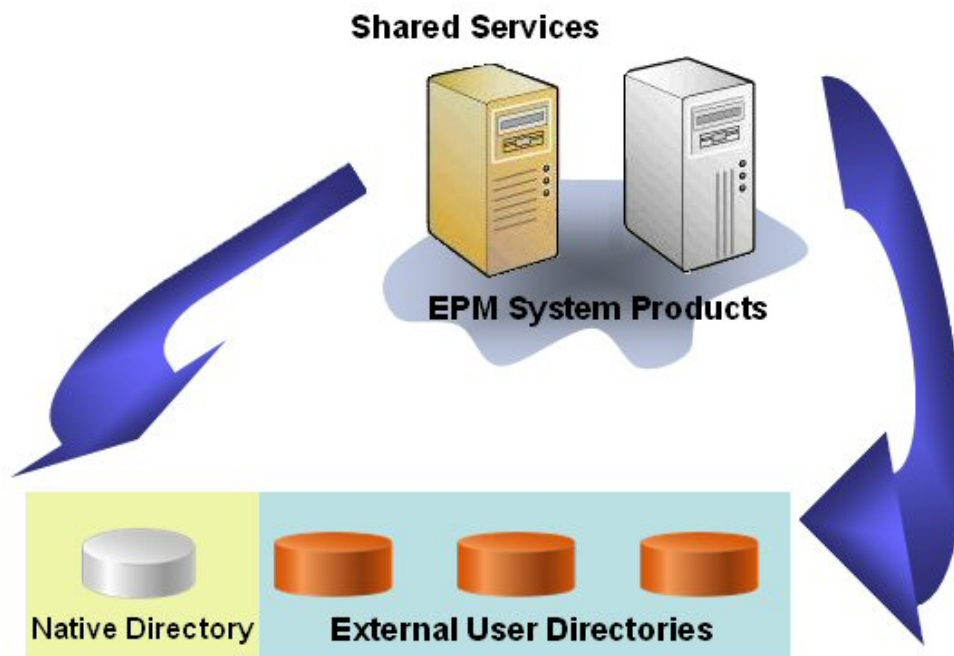
Aprovisionamiento (autorización basada en roles)

La seguridad de Oracle Enterprise Performance Management System determina el acceso de los usuarios a las aplicaciones mediante el concepto de los roles. Las funciones son permisos que determinan dicho acceso a las funciones de las aplicaciones. Algunos componentes de EPM System aplican listas de control de acceso de nivel de objeto para delimitar aún más el acceso de los usuarios a sus artefactos, como informes y miembros.

Cada componente de EPM System proporciona distintas funciones predeterminadas diseñadas según necesidades empresariales concretas. Cada aplicación perteneciente a un componente de EPM System hereda estos roles. Los roles predefinidos de las aplicaciones registradas con Servicios compartidos de Oracle Hyperion están disponibles en Consola de Servicios compartidos de Oracle Hyperion. También puede crear funciones adicionales que se agregan a las funciones predeterminadas para adaptarse a requisitos específicos. Estas funciones se utilizan para tareas de aprovisionamiento. El proceso de conceder a usuarios y grupos funciones específicas pertenecientes a aplicaciones de EPM System y sus recursos se denomina *aprovisionamiento*.

El directorio nativo y los directorios de usuario configurados constituyen orígenes de información sobre usuarios y grupos para el proceso de aprovisionamiento. Puede examinar y aprovisionar usuarios y grupos de todos los directorios de usuario configurados en Shared Services Console. También puede utilizar roles agregados específicos para aplicaciones creadas en el directorio nativo durante el proceso de aprovisionamiento.

Una descripción general ilustrada del proceso de autorización:



1. Después de la autenticación de un usuario, el componente de EPM System consulta los directorios de usuario para determinar sus grupos.
2. El componente de EPM System utiliza la información de grupos y usuarios para recuperar de Servicios compartidos los datos de aprovisionamiento del usuario. El componente utiliza estos datos para determinar a qué recursos puede acceder el usuario.

Las tareas de aprovisionamiento específicas para productos, como el control de acceso, se completan para cada producto. Estos datos se combinan con los de aprovisionamiento para especificar el tipo de acceso.

El aprovisionamiento basado en funciones de los productos de EPM System utiliza estos conceptos.

Roles

Una función es un elemento (similar a la lista de control de acceso) que define los permisos de acceso que se otorgan a usuarios y grupos para realizar distintas funciones en los recursos de EPM System. Un rol es una combinación de recursos o tipos de recursos (elementos a los que los usuarios pueden acceder, por ejemplo, un informe) y acciones que los usuarios pueden realizar en dichos recursos (por ejemplo, ver y editar).

El acceso a los recursos de aplicación de EPM System se restringe. Los usuarios pueden acceder a ellos solo tras asignar un rol que proporcione acceso al usuario o al grupo al que

pertenece el usuario. Las restricciones basadas en funciones permiten a los administradores controlar y administrar el acceso a aplicaciones.

Roles globales

Los roles globales, que son roles de Servicios compartidos válidas para varios productos, permiten a los usuarios realizar determinadas tareas en todos los productos de EPM System. Por ejemplo, el administrador de Servicios compartidos puede aprovisionar a usuarios para todas las aplicaciones de EPM System.

Roles predefinidos

Las funciones predefinidas son funciones integradas en productos de EPM System. No puede suprimirlos. Cada instancia de una aplicación perteneciente a un producto de EPM System hereda todos los roles predefinidos del producto. Para cada una de las aplicaciones, estas funciones se registran con Shared Services al crear la aplicación.

Roles agregados

Las funciones agregadas, también denominadas funciones personalizadas, agregan múltiples funciones predefinidas pertenecientes a una aplicación. Una función agregada puede incluir otras funciones agregadas. Por ejemplo, un gestor de aprovisionamiento o administrador de Servicios compartidos puede crear un rol agregado que combine los roles Planificador y Ver usuario de una aplicación de Oracle Hyperion Planning. Agregar funciones puede simplificar la administración de aplicaciones con varias funciones granulares. Se pueden incluir funciones de Shared Services globales en las funciones agregadas. No se puede crear una función agregada aplicable a varias aplicaciones o productos.

Usuarios

Los directorios de usuario almacenan información sobre aquellos usuarios que pueden acceder a productos de EPM System. Tanto los procesos de autenticación como los de autorización utilizan este tipo de información. Solo se pueden crear y gestionar usuarios del directorio nativo desde Consola de Servicios compartidos.

Se pueden consultar los usuarios de todos los directorios de usuario configurados desde Shared Services Console. Estos usuarios se pueden aprovisionar de forma individual para concederles derechos de acceso sobre aplicaciones de EPM System registradas en Shared Services. Oracle no recomienda el aprovisionamiento de usuarios individuales.

Administrador predeterminado de EPM System

Una cuenta de administrador, con el nombre predeterminado `admin`, se crea en el directorio nativo durante el proceso de despliegue. Es la cuenta de EPM System más importante y solo se debe utilizar para configurar un administrador del sistema, que es el experto en tecnología de la información encargado de la gestión de la seguridad de EPM System y el entorno.

El nombre de usuario y la contraseña del administrador de EPM System se establecen durante el despliegue de Oracle Hyperion Foundation Services. Debido a que esta cuenta no puede estar sujeta a políticas de contraseñas de cuentas corporativas, Oracle recomienda que se desactive tras crear la cuenta del administrador del sistema.

Por lo general, la cuenta de administrador de EPM System predeterminada se usa para realizar estas tareas:

- Configure el directorio corporativo como directorio de usuario externo. Consulte [Configuración de directorios de usuario](#).
- Para crear una cuenta de administrador del sistema, aprovisione un experto en tecnología de la información corporativo con el rol Administrador de Servicios compartidos. Consulte "Aprovisionamiento de usuarios y grupos" en la *Guía de administración de seguridad de usuarios de Oracle Enterprise Performance Management System*.

Administrador del sistema

El administrador del sistema es generalmente un experto en tecnología de la información corporativo que tiene derechos de acceso de lectura, escritura y ejecución a todos los servidores implicados en un despliegue de EPM System.

Por lo general, el administrador del sistema realiza estas tareas:

- Desactive la cuenta del administrador predeterminada de EPM System.
- Cree al menos un administrador funcional.
- Establezca la configuración de seguridad para EPM System con Consola de Servicios compartidos.
- También puede configurar directorio de usuarios como directorio de usuario externo.
- Para supervisar EPM System, ejecute periódicamente la herramienta Análisis de log. En esta guía se describen las tareas que realizan los administradores funcionales.

Procedimientos para crear un administrador funcional:

- Configure el directorio corporativo como directorio de usuario externo. Consulte [Configuración de directorios de usuario](#).
- Aprovisione un usuario o grupo con los roles necesarios para crear un administrador funcional. Consulte "Aprovisionamiento de usuarios y grupos" en la *Guía de administración de seguridad de usuarios de Oracle Enterprise Performance Management System*.

El administrador funcional se debe aprovisionar con estos roles:

- Rol Administrador de LCM de Servicios compartidos
- Rol Administrador y Gestor de aprovisionamiento de cada componente de EPM System desplegado

Administradores funcionales

El administrador funcional es un usuario corporativo experto en EPM System. Normalmente, este usuario está definido en el directorio corporativo configurado en Shared Services como directorio de usuario externo.

El administrador funcional realiza tareas de administración de EPM System tales como crear otros administradores funcionales, configurar la administración delegada, así como crear y aprovisionar aplicaciones y artefactos, y configurar la auditoría de EPM System. En la *Guía de administración de seguridad de usuarios de Oracle Enterprise Performance Management System* se describen las tareas que realizan los administradores funcionales.

Grupos

Los grupos contienen usuarios y también otros grupos. Puede crear y gestionar grupos del directorio nativo desde Consola de Servicios compartidos. Los grupos de todos los directorios de usuario configurados se muestran en Shared Services Console. Puede aprovisionarlos para concederles permisos de acceso a productos de EPM System registrados en Shared Services.

Inicio de Shared Services Console

Utilice una opción de menú de Oracle Hyperion Enterprise Performance Management Workspace para acceder a Oracle Hyperion Shared Services Console.

Para iniciar Shared Services Console:

1. Vaya a:

`http://nombre_servidor_web:número_puerto/workspace`

En la URL, *web_server_name* indica el nombre del equipo en el que se ejecuta el servidor web que utiliza Oracle Hyperion Foundation Services y *port_number* indica el puerto del servidor web, por ejemplo, `https://miservidorweb:19000/workspace`.

Nota:

Si desea acceder a EPM Workspace en entornos seguros, utilice `https` como protocolo (no `http`) y el número de puerto del servidor web seguro. Por ejemplo, utilice una dirección URL como: `https://miservidor:19043/workspace`.

2. Haga clic en **Iniciar aplicación**.

Nota:

Es posible que los bloqueadores de elementos emergentes impidan que se abra EPM Workspace.

3. En **Iniciar sesión**, introduzca su nombre de usuario y contraseña.

Inicialmente, el único usuario con acceso a Shared Services Console es el administrador de Oracle Enterprise Performance Management System cuyo nombre de usuario y contraseña se especificaron durante el proceso de despliegue.

4. Haga clic en **Iniciar sesión**.
5. Seleccione **Navegar**, a continuación, **Administrar** y, finalmente, **Consola de Servicios compartidos**.

2

Activación para SSL de los componentes de EPM System

Consulte también:

- [Suposiciones](#)
- [Fuentes de información](#)
- [Referencias de ubicaciones](#)
- [Acerca de la activación para SSL de los productos de EPM System](#)
- [Escenarios de SSL soportados](#)
- [Certificados necesarios](#)
- [Finalización de SSL en el descargador SSL](#)
- [Despliegue de SSL completo de EPM System](#)
- [Finalización de SSL en el servidor web](#)
- [SSL para Essbase 11.1.2.4](#)
- [SSL para Essbase 21c](#)

Suposiciones

- Ha determinado la topología de despliegue y ha identificado los enlaces de comunicación que se deben proteger mediante SSL.
- Ha obtenido los certificados necesarios de una autoridad de certificación (CA), ya sea conocida o propia, o bien ha creado certificados autofirmados. Consulte [Certificados necesarios](#).
- Conoce los conceptos y procedimientos de SSL, como el de la importación de certificados.

Consulte [Fuentes de información](#) para obtener una lista de documentos de referencia.

Fuentes de información

Para activar SSL para Oracle Enterprise Performance Management System es necesario que prepare componentes como el servidor de aplicaciones, el servidor web, las bases de datos y los directorios de usuario para la comunicación mediante SSL. En este documento se asume que conoce las tareas relacionadas con la activación para SSL esos componentes.

- **Oracle WebLogic Server:** consulte "[Configuración de SSL](#)" en *Securing WebLogic Server Guide* (Guía de protección de Weblogic Server).
- **Oracle HTTP Server:** consulte los temas siguientes en la *Oracle HTTP Server Administrator's Guide*:

- [Gestión de seguridad](#)
- [Activación de SSL para Oracle HTTP Server](#)
- **Directorios de usuario:** consulte la documentación correspondiente al proveedor del directorio de usuario. Algunos enlaces útiles:
 - **Oracle Internet Directory:** consulte [Oracle Internet Directory Administrator's Guide](#) y
 - **Sun Java System Directory Server:** consulte "[Seguridad del servidor de directorios](#)" en *Sun Java System Directory Server Administration Guide* (Guía de administración de Sun Java System Directory Server)
 - **Active Directory:** consulte la documentación de Microsoft.
- **Bases de datos:** consulte la documentación del proveedor de la base de datos.

Referencias de ubicaciones

En este documento se hace referencia a las siguientes ubicaciones de instalación y despliegue:

- *MIDDLEWARE_HOME* hace referencia a la ubicación de los componentes de middleware como Oracle WebLogic Server y, opcionalmente, uno o más directorios *EPM_ORACLE_HOME*. El directorio *MIDDLEWARE_HOME* se define durante la instalación del producto Oracle Enterprise Performance Management System. El directorio *MIDDLEWARE_HOME* predeterminado es `Oracle/Middleware`.

- *EPM_ORACLE_HOME* hace referencia al directorio de instalación que contiene los archivos necesarios para soportar productos de EPM System. *EPM_ORACLE_HOME* reside en *MIDDLEWARE_HOME*. El directorio *EPM_ORACLE_HOME* predeterminado es *MIDDLEWARE_HOME/EPMSys_{tem}11R1*, por ejemplo, `Oracle/Middleware/EPMSystem11R1`.

Los productos de EPM System se instalan en el directorio *EPM_ORACLE_HOME/products*, por ejemplo, `Oracle/Middleware/EPMSystem11R1/products`.

Además, durante la configuración de productos de EPM System, algunos productos despliegan componentes en *MIDDLEWARE_HOME/user_projects/epmsys_{tem}1*, por ejemplo, `Oracle/Middleware/user_projects/epmsystem1`.

- *EPM_ORACLE_INSTANCE* indica una ubicación que se define durante el proceso de configuración donde algunos productos despliegan componentes. La ubicación predeterminada de *EPM_ORACLE_INSTANCE* es *MIDDLEWARE_HOME/user_projects/epmsys_{tem}1*, por ejemplo, `Oracle/Middleware/user_projects/epmsystem1`.

Acerca de la activación para SSL ¿de los productos de EPM System

Durante el proceso de despliegue de Oracle Enterprise Performance Management System, se despliegan automáticamente los productos de EPM System de Oracle para que funcionen tanto en el modo SSL como en el modo sin SSL.

 **Nota:**

- EPM System soporta SSL solo para HTTP y JDBC. No soporta otros estándares (por ejemplo, Thrift y ODBC) para una comunicación segura.
- Para protegerse frente a la vulnerabilidad de Poodle (Relleno de Oracle en cifrado heredado cambiado a versión anterior), que es un ataque al protocolo SSLv3, debe desactivar el soporte SSLv3 en sus servidores y en los exploradores que se usan para acceder a los componentes de EPM System. Consulte la documentación del servidor y del explorador para obtener información sobre la desactivación del soporte SSLv3.
- Los servidores de EPM System puede que no se inicien si desactiva el modo sin SSL tras configurar SSL.
Active la replicación segura para todos los servidores de EPM System en el dominio para que se empiecen a iniciar cuando esté desactivado el modo sin SSL.

Al especificar la configuración común para EPM System, especifique si activar para SSL todas las comunicaciones entre servidores en su despliegue.

Al seleccionar los ajustes SSL durante el proceso de despliegue no configura automáticamente su entorno para SSL. Únicamente se establece un indicador en Servicios compartidos de Oracle Hyperion Registry que indica que todos los componentes de EPM System que emplean Servicios compartidos Registry deben utilizar el protocolo seguro (HTTPS) para las comunicaciones entre servidores. Es necesario llevar a cabo procedimientos adicionales con el fin de activar el entorno para SSL. Estos procedimientos se explican en el presente documento.

 **Nota:**

Al volver a desplegar sus aplicaciones, se borra el servidor de aplicaciones personalizado y la configuración del servidor web que especifique para la activación de SSL.

 **Nota:**

En Enterprise Performance Management System versión 11.2.x, no está soportado Secure Sockets Layer (SSL) para MS SQL Server en la Utilidad de creación de repositorios (RCU).

Escenarios de SSL soportados

Están soportados los siguientes escenarios SSL:

- Terminación SSL en el sistema de carga de SSL. Consulte [Finalización de SSL en el descargador SSL](#).
- Despliegue de SSL completo. Consulte [Despliegue de SSL completo de EPM System](#).

Certificados necesarios

La comunicación SSL usa certificados para crear confianza entre los componentes. Oracle le recomienda que utilice certificados de CA de terceros reconocidas para activar para SSL el entorno de producción de Oracle Enterprise Performance Management System.

Nota:

EPM System soporta el uso de certificados con comodín, lo que puede proteger varios subdominios con un certificado SSL. El uso de un certificado con comodín puede reducir el tiempo y el costo de gestión.

Si está usando certificados con comodín para cifrar la comunicación, debe desactivar la verificación de nombres de host en Oracle WebLogic Server.

Necesita los siguientes certificados para cada servidor que aloje componentes de EPM System:

- Un certificado de CA raíz

Nota:

No tiene que instalar un certificado de CA raíz en el almacén de claves de Java si está usando certificados de una CA de terceros conocida cuyo certificado raíz ya esté instalado en el almacén de claves de Java.

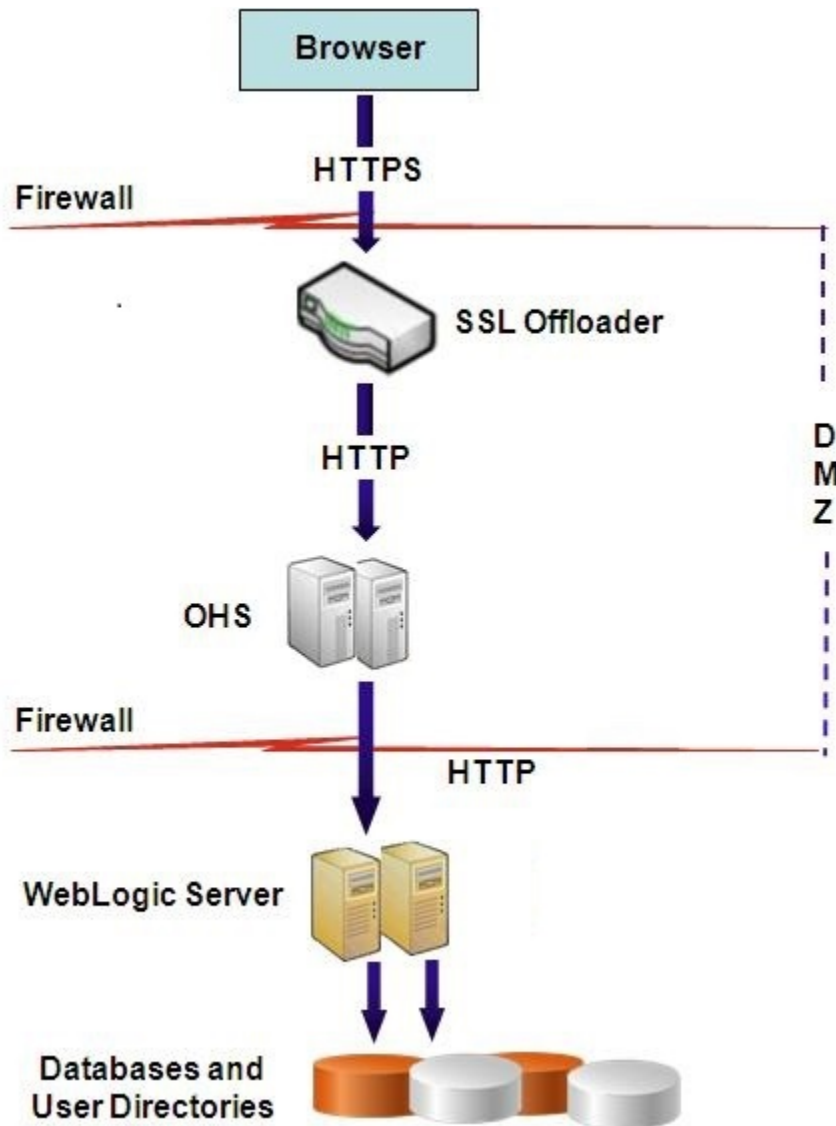
Firefox e Internet Explorer incluyen certificados de CA de terceros conocidas. Si está actuando como su propia CA, debe importar su certificado raíz de CA en el almacén de claves que usan los clientes a los que se acceden desde esos exploradores. Si está actuando como su propia CA, los clientes web no pueden establecer un protocolo de enlace SSL con el servidor si su certificado raíz de CA no está disponible para el explorador desde el que se accede al cliente.

- Los certificados firmados para cada instancia de Oracle HTTP Server en su despliegue
- Un certificado firmado para el equipo host con WebLogic Server. Los servidores gestionados de este equipo también pueden usar este certificado
- Dos certificados para el sistema de descarga/equilibrador de carga de SSL. Uno de estos certificados es para la comunicación externa, y el otro para la comunicación interna

Finalización de SSL en el sistema de descarga de SSL

Arquitectura de despliegue

En este escenario, SSL se usa para proteger el enlace de comunicación entre los clientes de Oracle Enterprise Performance Management System (por ejemplo, un explorador) y un sistema de descarga de SSL. El siguiente esquema ilustra el concepto:



Suposiciones

Sistema de descarga y equilibrador de carga de SSL

Un sistema de descarga de SSL totalmente configurado con un equilibrador de carga debe estar presente en el entorno de despliegue.

El equilibrador de carga se debe configurar para reenviar todas las solicitudes recibidas por los hosts virtuales a instancias de Oracle HTTP Server.

Cuando SSL se está terminando en Oracle HTTP Server (OHS) o en un equilibrador de carga, debe:

- Establecer todas las aplicaciones web lógicas en un host virtual no ssl del equilibrador de carga o de Oracle HTTP Server (por ejemplo, `empinternal.myCompany.com:80`, donde 80 es el puerto no SSL). En la pantalla Configuración, realice estos pasos:
 1. Amplíe la tarea de configuración **Hyperion Foundation**.
 2. Seleccione **Configurar dirección lógica para aplicaciones web**.
 3. Especifique el *nombre de host*, el número de puerto no SSL y el número de puerto SSL.
- Establecer la URL externa en el host virtual compatible con SSL del equilibrador de carga o de Oracle HTTP Server (por ejemplo, `empexternal.myCompany.com:443`, donde 443 es el puerto SSL). En la pantalla Configuración, realice estos pasos:
 1. Amplíe la tarea de configuración **Hyperion Foundation**.
 2. Seleccione **Configurar configuración común**.
 3. Seleccione **Activar descarga de SSL** en Detalles de URL externas.
 4. Especifique el *host de URL externa* y el *puerto de URL externa*.

 **Nota:**

Al volver a desplegar aplicaciones web o volver a configurar un servidor web con **configtool**, se reemplazará la configuración de las aplicaciones web lógicas y de las URL externas.

Hosts virtuales

El SSL finalizado en la configuración del sistema de descarga SSL usa dos alias de servidor, por ejemplo, `epm.myCompany.com` y `empinternal.myCompany.com`, en el sistema de descarga/equilibrador de carga SSL, uno para la comunicación externa entre el sistema de descarga y los exploradores y el otro para la comunicación interna entre los servidores de EPM System. Asegúrese de que los alias del servidor apunten a la dirección IP del equipo y que se puedan resolver mediante la DNS.

Se debe instalar en el sistema de carga/equilibrador de carga un certificado firmado para soportar la comunicación externa entre el sistema de descarga y los exploradores (mediante `epm.myCompany.com`).

Configuración de EPM System

El despliegue predeterminado de los componentes de EPM System soporta la finalización de SSL en el sistema de descarga de SSL. No es necesario realizar ninguna acción adicional.

Al configurar EPM System, asegúrese de que la dirección lógica de sus aplicaciones web apuntan al alias (por ejemplo, `empinternal.myCompany.com`) que se ha creado

para la comunicación interna. Consulte las siguientes fuentes de información para instalar y configurar EPM System:

- *Guía de configuración e instalación de Oracle Enterprise Performance Management System*
- *Documento de inicio para la instalación de Oracle Hyperion Enterprise Performance Management System*
- *Oracle Enterprise Performance Management System Installation and Configuration Troubleshooting Guide (solo disponible en inglés)*

Prueba del despliegue

Tras finalizar el proceso de despliegue, verifique que todo funciona. Para ello, conecte a la URL segura de Oracle Hyperion Enterprise Performance Management Workspace:

```
https://virtual_host_external:SSL_PORT/workspace/index.jsp
```

Por ejemplo, `https://epm.myCompany.com:443/workspace/index.jsp` donde 443 es el puerto SSL.

Despliegue de SSL completo de EPM System

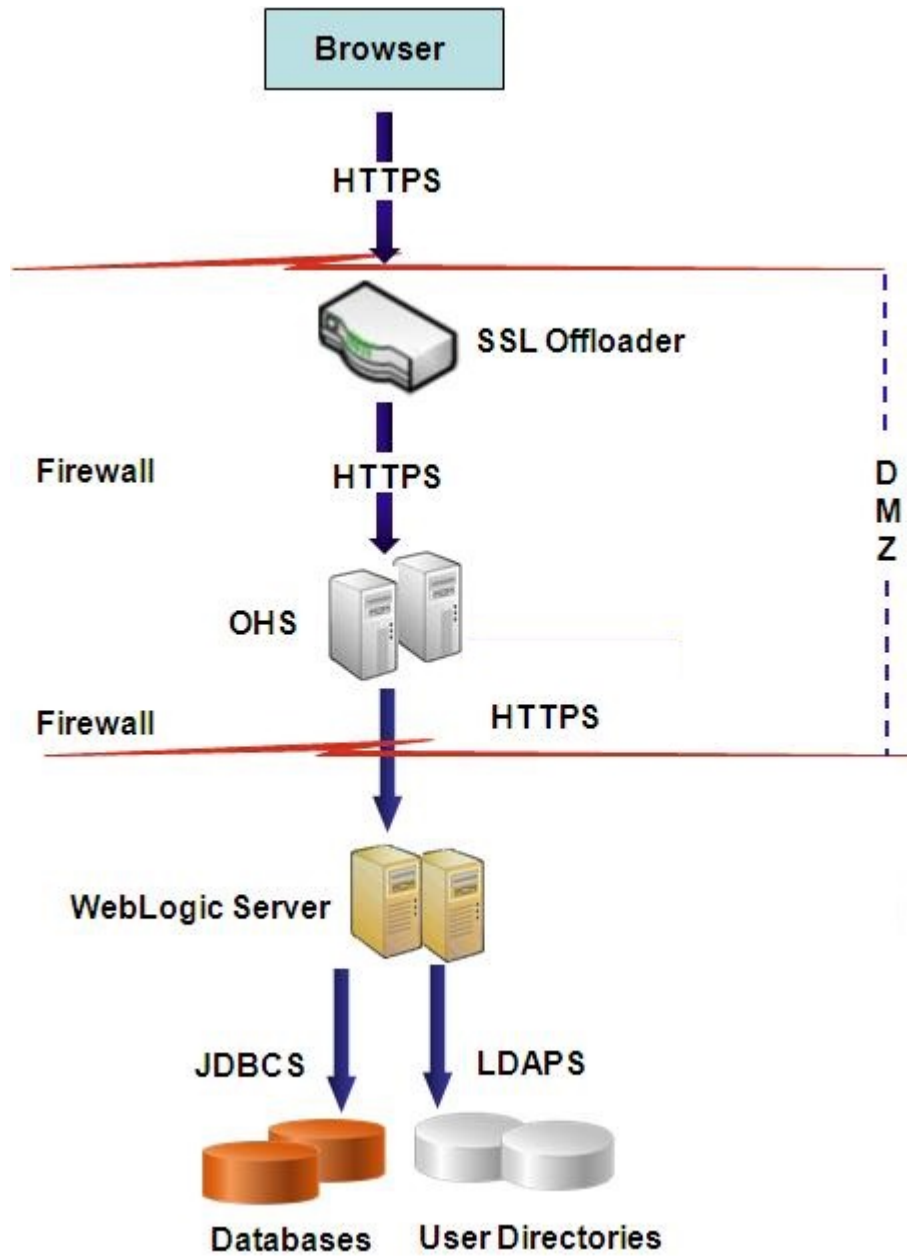
Consulte también:

- [Arquitectura de despliegue](#)
- [Suposiciones](#)
- [Configuración de EPM System para SSL completo](#)

Arquitectura de despliegue

En el modo SSL completo, la comunicación entre todos los canales que se pueden proteger se protegen usando SSL. Este escenario de despliegue de Oracle Enterprise Performance Management System es el más seguro.

El siguiente esquema ilustra el concepto:



Suposiciones

Bases de datos

Los servidores y los clientes de la base de datos tienen SSL activado. Consulte la documentación de la base de datos para obtener información sobre la activación para SSL del servidor y el cliente de la base de datos.

EPM System

Los componentes de Oracle Enterprise Performance Management System, incluidos Oracle WebLogic Server y Oracle HTTP Server, están instalados y desplegados. Es

más, su entorno de EPM System se ha probado para asegurarse de que todo funciona en modo sin SSL. Consulte las siguientes fuentes de información:

- *Guía de configuración e instalación de Oracle Enterprise Performance Management System*
- *Documento de inicio para la instalación de Oracle Hyperion Enterprise Performance Management System*
- *Oracle Enterprise Performance Management System Installation and Configuration Troubleshooting Guide (solo disponible en inglés)*

Si tiene previsto activar para SSL las conexiones de base de datos, durante el proceso de configuración, debe seleccionar el enlace **Opciones avanzadas** en cada pantalla de configuración de base de datos y, a continuación, especificar la configuración especificada, que incluye lo siguiente:

- Seleccione **Usar conexión segura a la base de datos (SSL)** e introduzca una URL de base de datos segura, por ejemplo,

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCPS) (HOST=myDBhost) (PORT=1529) (CONNECT_DATA=(SERVICE_NAME=myDBhost.myCompany.com)))
```
- **Almacén de claves de confianza**
- **Contraseña de almacén de claves de confianza**

Consulte *Guía de configuración e instalación de Oracle Enterprise Performance Management System* para obtener más detalles.

Sistema de descarga y equilibrador de carga de SSL

Un sistema de descarga de SSL totalmente configurado con un equilibrador de carga debe estar presente en el entorno de despliegue.

La configuración completa de SSL usa dos alias de servidor, por ejemplo, `epm.myCompany.com` y `empinternal.myCompany.com`, en el sistema de descarga de SSL. Uno para la comunicación externa entre el sistema de descarga y los exploradores, y el otro para la comunicación interna entre servidores de EPM System. Asegúrese de que los alias del servidor apunten a la dirección IP del equipo y que se puedan resolver mediante la DNS.

El equilibrador de carga se debe configurar para reenviar todas las solicitudes recibidas por los hosts virtuales a instancias de Oracle HTTP Server.

Los dos certificados firmados, uno para soportar la comunicación externa entre el sistema de descarga y los exploradores (mediante `epm.myCompany.com`), y el otro para soportar la comunicación interna (mediante `empinternal.myCompany.com`) entre aplicaciones, se deben instalar en el sistema de carga/equilibrador de carga. Oracle recomienda que estos certificados estén enlazados a los alias del servidor para evitar la exposición de los nombres de servidor y para mejorar la seguridad.

Configuración de EPM System para SSL completo

Consulte también:

- [Nueva configuración de ajustes comunes de EPM System](#)
- [Opcional: Instalación del certificado de CA raíz para WebLogic Server](#)
- [Instalación del certificado en WebLogic Server](#)
- [Configuración de WebLogic Server](#)

- Activación de una conexión de servidor de HFM con una instancia de Oracle Database activada para SSL
- Procedimientos de Oracle HTTP Server
- Configuración de los componentes web de EPM System desplegados en WebLogic Server
- Actualización de la configuración de dominio
- Reinicio de servidores y de EPM System
- Prueba del despliegue
- Configuración de directorios de usuario externos activados para SSL

Nueva configuración de ajustes comunes de EPM System

Durante este proceso, selecciona la configuración que obliga a los componentes de Oracle Enterprise Performance Management System a usar la comunicación de SSL.

Nota:

Si está activando para SSL el servidor web de Oracle Hyperion Financial Management: antes de configurar Financial Management, debe hacer que la cookie sea segura mediante la edición del descriptor de sesión de HFM WebApp en `weblogic.xml`.

1. Expanda el archivo web de Financial Management con una herramienta como 7 Zip. La ubicación de `weblogic.xml` en el archivo es `EPM_ORACLE_HOME\products\FinancialManagement\AppServer\InstallableApps\HFMWebApplication.ear\HFMWeb.war\WEB-INF\weblogic.xml`.
2. Incluya la siguiente directiva en el descriptor de sesión de HFM WebApp en `weblogic.xml`:

```
<cookie-secure>true</cookie-secure>
```
3. Guarde `weblogic.xml`
4. Haga clic en **Sí** cuando 7 Zip consulte si desea actualizar el archivo.

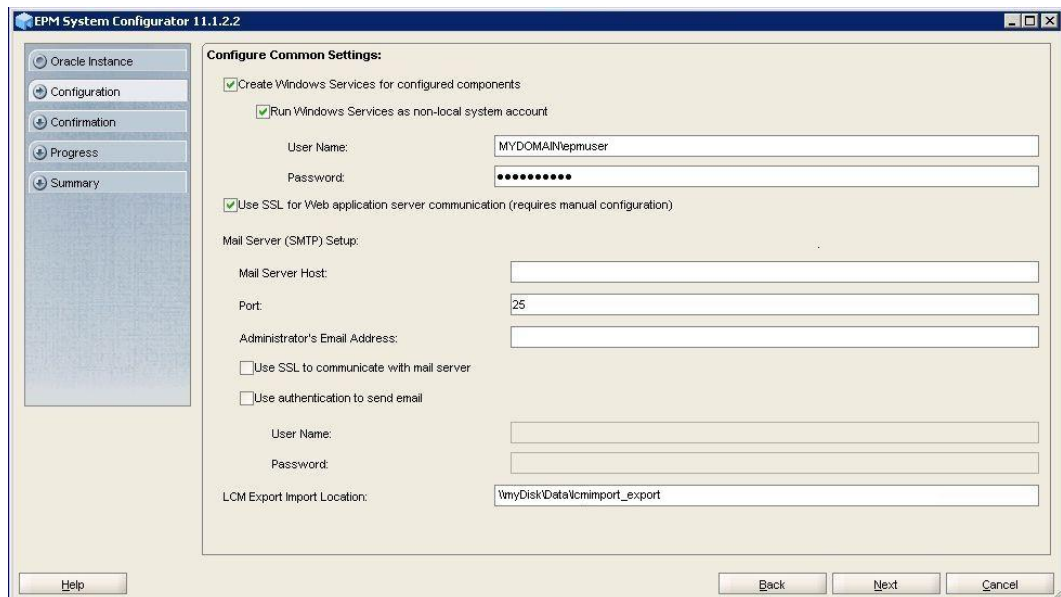
Para volver a configurar EPM System para SSL:

1. Inicie EPM System Configurator.
2. En **Seleccione la instancia de EPM Oracle a la que se debe aplicar la configuración**, realice estos pasos:
 - a. En **Nombre de la instancia de EPM Oracle**, introduzca el nombre de instancia que ha usado al configurar originalmente los componentes de EPM System.
 - b. Haga clic en **Siguiente**.
3. En la pantalla Configuración, realice estos pasos:
 - a. Desmarque **Desactivar todo**.
 - b. Expanda la tarea de configuración de **Hyperion Foundation** y, a continuación, seleccione **Configurar configuración común**.

- c. Haga clic en **Siguiente**.
4. En **Configurar configuración común**, realice estos pasos:

Atención:

Antes de seleccionar la configuración para usar SSL para comunicarse con el servidor de correo electrónico, asegúrese de que el servidor de correo electrónico esté configurado para SSL.



- a. Seleccione **Usar SSL para las comunicaciones del servidor de aplicaciones web de Java (se necesita configuración manual)** para especificar que EPM System debe usar SSL para la comunicación.
- b. **Opcional:** Introduzca información en **Host del servidor de correo** y **Puerto**. Para soportar la comunicación SSL, debe especificar el puerto seguro usado por el servidor de correo SMTP.
- c. **Opcional:** Para soportar la comunicación SSL con el servidor de correo SMTP, seleccione **Usar SSL para comunicación con el servidor de correo**.
- d. Seleccione las opciones o introduzca valores en los demás campos.
- e. Haga clic en **Siguiente**.
5. Haga clic en **Siguiente** en las posteriores pantallas de EPM System Configurator.
6. Cuando termine el proceso de despliegue, aparecerá la pantalla Resumen. Haga clic en **Finalizar**.

Opcional: Instalación del certificado de CA raíz para WebLogic Server

Los certificados raíz de la mayoría de las CA de terceros conocidas ya están instalados en el almacén de claves de JVM. Realice los procedimientos de esta sección si no está usando

certificados de una CA de terceros conocidas (no recomendado). La ubicación del almacén de claves de JVM predeterminada es `MIDDLEWARE_HOME/jdk/jre/lib/security/cacerts`.



Nota:

Realice este procedimiento en cada servidor de Oracle Enterprise Performance Management System.

Para instalar el certificado de CA raíz:

1. Copie el certificado de CA raíz en un directorio local del equipo donde esté instalado Oracle WebLogic Server.
2. En una consola, cambie al directorio `MIDDLEWARE_HOME/jdk/jre/bin`.
3. Ejecute un comando de keytool como el siguiente para instalar el certificado de CA raíz en el almacén de claves de JVM:

```
keytool -import -alias ALIAS -file CA_CERT_FILE -keystore KEYSTORE -storepass KEYSTORE_PASSWORD -trustcacerts
```

Por ejemplo, puede utilizar el siguiente comando para agregar un certificado `CAcert.crt` almacenado en el directorio actual en el almacén de claves de JVM con `Blister` como alias de certificado del almacén de claves. Se asume que se usa la contraseña `example_pwd`.

```
keytool -import -alias Blister -file CAcert.crt -keystore ../lib/security/cacerts -storepass example_pwd -trustcacerts
```



Nota:

En el comando y ejemplo anteriores se usa parte de la sintaxis para importar certificados con keytool. Consulte la documentación de keytool para obtener una lista completa de la sintaxis de importación.

Instalación del certificado en WebLogic Server

La instalación predeterminada de Oracle WebLogic Server usa un certificado de demostración para soportar SSL. Oracle recomienda que instale un certificado de un tercero conocido para reforzar la seguridad de su entorno.

En cada equipo que aloje WebLogic Server, use una herramienta (por ejemplo, keytool) para crear un almacén de claves personalizado con el fin de almacenar el certificado firmado para WebLogic Server y los componentes web de Oracle Enterprise Performance Management System.

Para crear un almacén de claves personalizado e importar el certificado:

1. En una consola, cambie al directorio `MIDDLEWARE_HOME/jdk/jre/bin`.

2. Ejecute un comando de keytool como el siguiente para crear el almacén de claves personalizado (identificado por la directiva `-keystore` en el comando) en un directorio existente:

```
keytool -genkey -dname "cn=myserver, ou=EPM, o=myCompany, c=US" -alias
epm_ssl -keypass password -keystore
C:\oracle\Middleware\EPMSysstem11R1\ssl\keystore -storepass password -
validity 365 -keyalg RSA
```

 **Nota:**

El nombre común (cn) que establezca debe coincidir con el nombre del servidor. Si usa un nombre de dominio completo (FQDN) como cn, debe usar el FQDN al desplegar los componentes web.

3. Genere una solicitud de certificado.

```
keytool -certreq -alias epm_ssl -file C:/certs/epmssl_csr -keypass
password -storetype jks -keystore
C:\oracle\Middleware\EPMSysstem11R1\ssl\keystore -storepass password
```

4. Obtenga un certificado firmado para el equipo con WebLogic Server.
5. Importe el certificado firmado en el almacén de claves:

```
keytool -import -alias epm_ssl -file C:/certs/epmssl.crt -keypass
password -keystore C:\Oracle\Middleware\EPMSysstem11R1\ssl\keystore -
storepass password
```

Configuración de WebLogic Server

Tras desplegar los componentes web de Oracle Enterprise Performance Management System, debe configurarlos para la comunicación SSL.

Para configurar los componentes web para SSL:

1. Para iniciar Oracle WebLogic Server, ejecute `MIDDLEWARE_HOME/user_projects/domains/EPMSysstem/bin/startWebLogic.cmd`:
2. Para iniciar la consola de administración de WebLogic Server, acceda a la dirección URL siguiente:

```
http://SERVER_NAME:Port/console
```

Por ejemplo, para acceder a la consola de WebLogic Server desplegada en el puerto predeterminado en `myServer`, debe usar `http://myServer:7001/console`.

3. En la pantalla Bienvenido, introduzca el nombre de usuario y la contraseña del administrador de WebLogic Server que haya especificado en EPM System Configurator.
4. En **Centro de cambios**, haga clic en **Bloquear y editar**.
5. En el panel izquierdo de la consola, expanda **Entorno** y, a continuación, seleccione **Servidores**.

6. En la pantalla Resumen de servidores, haga clic en el nombre del servidor cuyo SSL desee activar.

Por ejemplo, para activar para SSL los componentes de Oracle Hyperion Foundation Services, use el servidor `EPMServer0`.
7. Desmarque **Puerto de recepción activado** para desactivar el puerto de escucha HTTP.
8. Asegúrese de que está seleccionada la opción **Puerto de recepción SSL activado**.
9. En **Puerto de escucha SSL**, introduzca el puerto de escucha SSL donde este servidor debe escuchar las solicitudes.
10. Para especificar los almacenes de claves de confianza y de identidad que usar, seleccione **Almacenes de claves** para abrir el separador Almacenes de claves.
11. Haga clic en **Cambiar**.
12. Seleccione una opción:
 - **Identidad personalizada y protección personalizada** si no está usando un certificado de servidor de una CA de tercero conocida
 - **Identidad personalizada y protección de estándar de Java** si no está usando un certificado de servidor de una CA de tercero conocida
13. Haga clic en **Guardar**.
14. En **Almacén de claves de identidad personalizado**, introduzca la ruta del almacén de claves donde se haya instalado el certificado de WebLogic Server firmado.
15. En **Tipo de almacén de claves de identidad personalizado**, introduzca `jks`.
16. En **Frase de contraseña de almacén de claves de identidad personalizado y Confirmar frase de contraseña de almacén de claves de identidad personalizado**, introduzca la contraseña del almacén de claves.
17. Si ha seleccionado **Identidad personalizada y protección personalizada en Almacenes de claves**:
 - En **Almacén de claves de confianza personalizado**, introduzca la ruta del almacén de claves personalizado donde esté disponible el certificado raíz de la CA que haya firmado el certificado del servidor.
 - En **Tipo de almacén de claves de confianza personalizado**, introduzca `jks`.
 - En **Frase de contraseña de almacén de claves de confianza personalizado y Confirmar frase de contraseña de almacén de claves de confianza personalizado**, introduzca la contraseña del almacén de claves.
18. Haga clic en **Guardar**.
19. Especifique la configuración de SSL:
 - Seleccione **SSL**.
 - En **Alias de clave privada**, introduzca el alias que haya especificado al importar el certificado de WebLogic Server firmado.
 - En **Frase de contraseña de clave privada y Confirmar frase de contraseña de clave privada**, introduzca la contraseña que se va a usar para recuperar la clave privada.

- Haga clic en **Guardar**.

 **Nota:**

Si está usando certificados SHA-2, debe seleccionar la opción **Usar SSL de JSSE** para cada servidor gestionado que se use para soportar EPM System. Esta opción está disponible en el separador Avanzado de la página SSL. Debe reiniciar WebLogic Server para activar este cambio.

20. Active la replicación segura para el servidor:
 - a. En el panel izquierdo de la consola, expanda **Entorno** y, a continuación, haga clic en **Clusters**.
 - b. En Resumen de clusters, haga clic en el nombre del servidor, por ejemplo, `Foundation Services`, para el que desee activar la replicación segura.

Se muestra el separador Configuración de la pantalla Configuración para el servidor seleccionado.
 - c. Haga clic en **Replicación** para abrir el separador Replicación.
 - d. Seleccione **Replicación bidireccional segura**. Puede que tenga que hacer clic en **Bloquear y editar** antes de poder seleccionar esta opción.
 - e. Haga clic en **Guardar**.
21. Realice del paso 6 al paso 20 para cada servidor gestionado que pertenezca a este host.
22. Active la replicación segura para proporcionar el canal para llamadas de replicación para el cluster.

Consulte el documento 1319381.1 de Oracle Metalink para obtener detalles.
 - En la consola de administración, expanda **Entorno** y, a continuación, seleccione **Clusters**.
 - Seleccione **Replicación**.
 - En **Replicación**, seleccione (marque) **Replicación bidireccional segura**.
 - Haga clic en **Guardar**.
23. En **Centro de cambios**, haga clic en **Activar cambios**.

Activación de una conexión de servidor de HFM con una instancia de Oracle Database activada para SSL

La conexión de red entre el origen de datos de HFM y la instancia de Oracle Database se pueden cifrar mediante SSL. Para que esto funcione, la cartera de Oracle debe configurarse como se describe en la [documentación de Oracle](#). También se debe configurar el listener TNS para que escuche en un nuevo puerto para las conexiones cifradas mediante SSL. Por último, deben cargarse los certificados pertinentes en el almacén de claves y el almacén de confianza de los servidores que alojan el origen de datos de HFM. Las siguientes instrucciones hacen referencia a la [documentación de Oracle Database](#).

Requisitos

Asegúrese de que cumple los siguientes requisitos antes de continuar con los pasos que se indican más abajo:

- Dispone de un servidor de base de datos operativo.
- Se ha asegurado de que ningún cortafuegos local o de red bloquea las comunicaciones con el servidor en el puerto en el que se ejecuta el listener TNS activado para SSL.

En los siguientes ejemplos se ha usado Oracle 12c (12.1.0.2) en MS Windows Server 2016. Estas instrucciones también funcionarán correctamente en una instalación Linux, siempre que las rutas especificadas para los archivos de cartera sean rutas de sistema de archivos de Linux y las sustituciones de variables de entorno se modifiquen según sea pertinente para el shell empleado en el servidor de base de datos. Estas instrucciones se han utilizado con éxito en instancias 19c para desarrollo y soporte.

Los ejemplos de este artículo utilizan certificados autofirmados, pero también puede usar certificados de autoridad de certificación si lo prefiere. Consulte la [documentación de Oracle Database](#) para conocer los pasos exactos que debe seguir para instalar un certificado emitido por una autoridad de certificación.

Configuración de Oracle Database

Para configurar la instancia de Oracle Database, realice los siguientes pasos:

1. Cree una nueva cartera de conexión automática en el servidor de base de datos.

Nota:

Estos pasos solo son necesarios si no se ha creado previamente una cartera de Oracle. Los siguientes pasos no son necesarios si se utiliza la herramienta de interfaz gráfica de usuario de las carteras de Oracle en el servidor de base de datos.

```
C:\> cd %ORACLE_HOME%
C:\oracledb\12.1.0\home> mkdir wallet
C:\oracledb\12.1.0\home> orapki wallet create -wallet wallet -pwd
password1 -auto_login
```

Puede ignorar los mensajes que le pidan que use `-auto_login_local` en la línea de comandos `orapki`. Si se produce un error de autenticación SSL, consulte [Identificador de documento 2238096.1](#) para solucionar el problema.

Asimismo, compruebe el permiso de seguridad del archivo `cwallet.sso` (en el directorio de la cartera) y asegúrese de que el usuario del servicio de listener de Oracle tiene permiso de lectura para este archivo. Sin permiso de lectura, el establecimiento de comunicación SSL fallará más adelante. Esto sucederá si la instancia de Oracle Database se ha instalado con el usuario de Oracle sugerido que no tiene permiso para iniciar sesión. Si la instancia de Oracle Database se ha instalado con el usuario de Oracle, el listener TNS debe ejecutarse como un usuario distinto.

2. Cree un certificado autofirmado y cárguelo en la cartera.

```
C:\oracledb\12.1.0\home> orapki wallet add -wallet wallet -pwd password1 -
dn "CN={FQDN of db server}" -
keysize 1024 -self_signed -validity 3650
```

La contraseña `password1` del ejemplo anterior debe coincidir con la contraseña especificada en el *paso 1*.

3. Exporte el certificado autofirmado recién creado.

```
C:\oracledb\12.1.0\home> orapki wallet export -wallet wallet -pwd
password1 -dn "CN={FQDN of db server}"
-cert %COMPUTERNAME%-certificate.crt
```

4. Copie el archivo de certificado Base64 exportado en los servidores de HFM.

5. Configure los listeners SQL*NET y TNS:

- a.** Identifique un puerto sin utilizar en el servidor de base de datos. En el siguiente ejemplo se crea el nuevo listener en el puerto 1522. El puerto usado habitualmente para las conexiones SSL es el 2484, pero puede usar cualquier puerto disponible. Compruebe que el puerto que desea usar está disponible en el servidor de base de datos antes de continuar y haga los ajustes pertinentes.
- b.** Actualice `SQLNET.ORA`. El elemento `DIRECTORY` de la declaración `WALLET_LOCATION` debe apuntar a la cartera creada en el *paso 1*.

```
SQLNET.AUTHENTICATION_SERVICES= (TCPS, NTS, BEQ)
NAMES.DIRECTORY_PATH= (TNSNAMES, EZCONNECT)
WALLET_LOCATION=
(SOURCE =
(METHOD = FILE)
(METHOD_DATA =
(DIRECTORY = C:\oracledb\12.1.0\home\wallet)
)
)
SSL_CLIENT_AUTHENTICATION = FALSE
```

- c.** Actualice `LISTENER.ORA` para definir un nuevo listener. Use el puerto que se identificó en el *paso 5a*.

```
SID_LIST_LISTENER =
(SID_LIST =
(SID_DESC =
(SID_NAME = CLRExtProc)
(ORACLE_HOME = C:\oracledb\12.1.0\home)
(PROGRAM = extproc)
(ENVS = "EXTPROC_DLLS=ONLY:C:\oracledb\12.1.0\home\bin\oraclr12.dll")
)
)
SSL_CLIENT_AUTHENTICATION = FALSE
WALLET_LOCATION=
(SOURCE =
(METHOD = FILE)
(METHOD_DATA =
```

```
(DIRECTORY = C:\oracledb\12.1.0\home\wallet)
)
)
LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP) (HOST = myServer) (PORT = 1521))
    )
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCPS) (HOST = myServer) (PORT = 1522))
    )
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = IPC) (KEY = EXTPROC1521))
    )
  )
ADR_BASE_LISTENER = C:\oracledb
```

d. Cree una nueva entrada en TNSNAMES.ORA para el nuevo puerto.

```
ORCL_SSL =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCPS) (HOST = myServer) (PORT = 1522))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = myServer_service)
    )
  )
)
```

Debe especificar el mismo puerto que se identificó en el *paso 5a* y se utilizó en el *paso 5c*.

e. Reinicie el listener TNS.

```
C:\oracledb\12.1.0\home>lsnrctl stop
C:\oracledb\12.1.0\home>lsnrctl start
```

f. Compruebe que el nuevo listener TNS funciona.

```
C:\oracledb\12.1.0\home>tnsping orcl_ssl
TNS Ping Utility for 64-bit Windows: Version 12.1.0.2.0 -
Production on 10-SEP-2019 15:43:22
Copyright (c) 1997, 2014, Oracle. All rights reserved.
Used parameter files:
C:\oracledb\12.1.0\home\network\admin\sqlnet.ora
Used TNSNAMES adapter to resolve the alias
Attempting to contact (DESCRIPTION = (ADDRESS = (PROTOCOL = TCPS)
(HOST = myServer)
(PORT = 1522)) (CONNECT_DATA = (SERVER = DEDICATED)
(SERVICE_NAME = myServer_service)))
OK (130 msec)
```

Configuración de un servidor de HFM para usar conexiones SSL de base de datos

Adición del certificado de la base de datos al almacén de confianza en los servidores de HFM

Los siguientes pasos deben realizarse en todos los servidores de EPM en los que se ejecute el origen de datos de HFM. La variable de entorno `%MW_HOME%` que se usa más abajo es la ubicación de la instalación de Oracle Middleware. Esta variable de entorno no se crea de forma predeterminada durante la instalación de EPM, y se utiliza aquí para mostrar el directorio principal de la instalación de EPM.

La ubicación de la instalación de EPM se especifica mediante la variable de entorno `EMP_ORACLE_HOME`. En el siguiente ejemplo se coloca el almacén de claves y los almacenes de confianza en un directorio que comparte ubicación con la instalación de EPM, pero los archivos de almacén de claves y almacenes de confianza pueden estar en cualquier ubicación del sistema de archivos del servidor de HFM.

1. Cree un nuevo directorio en `%MW_HOME%` para guardar el almacén de claves Java y el almacén de confianza PKCS12.
 - a. `cd %MW_HOME%`
 - b. `mkdir certs`
2. Copie el cacerts del archivo de almacén de claves Java del JDK.
 - a. `cd %MW_HOME%\certs`
 - b. `copy %MW_HOME%\jdk1.8.0_181\jre\lib\security\cacerts testing_cacerts`
El motivo por el que se copia el almacén de claves del JDK y se utiliza esa copia en lugar del almacén de claves predeterminado del JDK es el siguiente: si se cambia la versión del JDK y se suprime la versión anterior, se perderán las claves y los certificados insertados en el almacén de claves predeterminado.
3. Copie el certificado Base 64 en `%MW_HOME%\certs`.
4. Importe el certificado en el archivo de almacén de claves Java `testing_cacerts`.
 - a. Por ejemplo, `keytool -importcert -file bur00cbb-certificate.crt -keystore testing_cacerts -alias "myserver"`
 - i. Deberá especificar la contraseña para el almacén de claves.
 - ii. Debe reemplazar "myserver" por el dominio completo del servidor de base de datos.
 - b. Cuando se le pregunte si se debe confiar o no en el certificado, escriba **y**.
5. Cree el almacén de confianza en formato PKCS12 a partir del archivo de almacén de claves Java del JDK. Por ejemplo:

```
keytool -importkeystore -srckeystore testing_cacerts -srcstoretype JKS -
deststoretype PKCS12 -destkeystore testing_cacerts.pfx
```

Actualización de las conexiones JDBC de HFM para usar SSL

1. Vuelva a configurar la conexión JDBC de base de datos de HFM para usar SSL.
 - a. Inicie la herramienta de configuración de EPM.

- i. Seleccione los nodos **Configurar base de datos** y **Desplegar en servidor de aplicaciones** en el nodo **Financial Management**.
 - ii. Haga clic en **Siguiente**.
 - iii. Realice todos estos pasos para la conexión JDBC de HFM
 - i. Introduzca el puerto SSL, el nombre del servicio, el nombre de usuario y la contraseña para la conexión en las columnas de puerto, nombre de servicio, nombre de usuario y contraseña.
 - ii. Haga clic en (+) para abrir las **opciones avanzadas de base de datos**.
 - iii. Seleccione la casilla de verificación **Usar conexiones seguras**.
 - iv. Introduzca la ubicación del almacén de claves Java creado en el *paso 2*.
 - v. Haga clic en **Aplicar**.
 - vi. Haga clic en (+) para abrir las **opciones avanzadas de base de datos**.
 - vii. Haga clic en **Editar y usar URL de JDBC modificada**. Tenga en cuenta que no se deben hacer cambios en la URL de JDBC que se muestra.
 - viii. Haga clic en **Aplicar**.
 - ix. Haga clic en **Siguiente**.
 - b. Realice los pasos restantes para desplegar la aplicación de HFM como se describe en la documentación de EPM.
 2. Abra un shell o una ventana de comandos para actualizar manualmente el registro de EPM de forma que la conexión de ODBC que utilice el origen de datos se pueda activar para SSL.
Ejecute cada uno de los siguientes comandos:

```
epmsys_registry.bat addproperty FINANCIAL_MANAGEMENT_PRODUCT/  
DATABASE_CONN/@ODBC_TRUSTSTORE "C:  
\Oracle\Middleware\certs\testing_cacerts.pfx"  
epmsys_registry.bat addencryptedproperty  
FINANCIAL_MANAGEMENT_PRODUCT/DATABASE_CONN  
/@ODBC_TRUSTSTOREPASSWORD <truststorepassword>  
epmsys_registry.bat addproperty FINANCIAL_MANAGEMENT_PRODUCT/  
DATABASE_CONN  
/@ODBC_VALIDATESERVERCERTIFICATE false
```

En los ejemplos anteriores, la ruta C:\Oracle\Middleware es el valor de %MW_HOME% en los pasos 1, 2 y 3.

La propiedad FINANCIAL_MANAGEMENT_PRODUCT/DATABASE_CONN/@ODBC_VALIDATESERVERCERTIFICATE solo debe definirse como false si se utiliza un certificado autofirmado. El valor de FINANCIAL_MANAGEMENT_PRODUCT/DATABASE_CONN/@ODBC_TRUSTSTOREPASSWORD debe ser la contraseña del almacén de claves Java original que se copió en el *paso 2*.

Actualización de la entrada de nombres TNS utilizada por HFM

Edite `TNSNAMES.ORA` para crear una nueva entrada y renombrar la entrada antigua. En el siguiente ejemplo se muestra un archivo `TNSNAMES.ORA` actualizado en el servidor de HFM con los cambios necesarios aplicados. Estos cambios se deben realizar porque HFM busca y utiliza una entrada de nombres TNS llamada `HFMTNS`. Es necesario cambiar el protocolo y el puerto de esta entrada para que `XFMDDataSource` funcione correctamente.

```
HFMTNS_UNENC =
(DESCRIPTION =
(ADDRESS_LIST =
(ADDRESS = (PROTOCOL = TCP) (HOST = myserver) (PORT = 1521))
)
(CONNECT_DATA =
(SERVICE_NAME = myserver_service)
(SERVER = DEDICATED)
)
)
HFMTNS =
(DESCRIPTION =
(ADDRESS_LIST =
(ADDRESS = (PROTOCOL = TCPS) (HOST = myserver) (PORT = 1522))
)
(CONNECT_DATA =
(SERVICE_NAME = myserver_service)
(SERVER = DEDICATED)
)
)
```

La entrada `HFMTNS` original se ha renombrado como `HFMTNS_UNENC`. El nuevo valor `HFMTNS` se ha obtenido copiando `HFMTNS_UNENC` y renombrándolo como `HFMTNS`. Después se ha actualizado el protocolo a `TCPS` y cambiado el puerto a `1522`. El puerto especificado debe ser el mismo puerto indicado en el archivo `TNS_LISTENER.ORA`.

Procedimientos de Oracle HTTP Server

Creación de una cartera e instalación del certificado para Oracle HTTP Server

Se instala automáticamente una cartera predeterminada con Oracle HTTP Server. Debe configurar una cartera real para cada instancia de Oracle HTTP Server en su despliegue.

Nota: A partir de las versiones 11.2.x, Oracle Wallet Manager no se instala con Oracle HTTP Server. Oracle Wallet Manager solo se instalará si instala el cliente de Oracle Database. Deberá usar el gestor de carteras disponible con el cliente de Database para crear la cartera e importar el certificado. Si está configurando Oracle HTTP Server para SSL, asegúrese de instalar siempre el cliente de 64 bits de Oracle Database como parte de la instalación de los productos de EPM System.

Para crear e instalar un certificado de Oracle HTTP Server:

1. En cada equipo que aloje Oracle HTTP Server, inicie Wallet Manager.

Seleccione **Inicio**, **Todos los programas**, **Oracle-OHxxxxxx**, **Herramientas de gestión integradas** y, a continuación, **Wallet Manager**.

xxxxxx es el número de instancia de Oracle HTTP Server.

2. Cree una cartera nueva vacía.
 - a. En Oracle Wallet Manager, seleccione **Cartera** y, a continuación, **Nueva**.
 - b. Haga clic en **Sí** para crear un directorio de carteras predeterminado o **No** para crear el archivo de carteras en la ubicación que elija.
 - c. En **Contraseña de cartera** y **Confirmar contraseña** en la pantalla Nueva cartera, introduzca la contraseña que desea usar.
 - d. Haga clic en **Aceptar**.
 - e. En el cuadro de diálogo de confirmación, haga clic en **No**.
3. **Opcional:** Si no está usando una CA que conozca Oracle HTTP Server, importe el certificado de la CA raíz en la cartera.
 - a. En Oracle Wallet Manager, haga clic con el botón derecho en **Certificados de confianza** y seleccione **Importar certificado de confianza**.
 - b. Busque y seleccione el certificado de CA raíz.
 - c. Seleccione **Abrir**.
4. Cree una solicitud de certificado.
 - a. En Oracle Wallet Manager, haga clic con el botón derecho en **Certificado: [vacío]** y seleccione **Agregar solicitud de certificado**.
 - b. En Crear solicitud de certificado, introduzca la información necesaria.

Para el nombre común, introduzca el alias de servidor completo, por ejemplo, `epm.myCompany.com` o `epminternal.myCompany.com`, disponible en el archivo `hosts` de su sistema.
 - c. Haga clic en **Aceptar**.
 - d. En el cuadro de diálogo de confirmación, haga clic en **Aceptar**.
 - e. Haga clic con el botón derecho en la solicitud de certificado que haya creado y, a continuación, seleccione **Exportar solicitud de certificado**.
 - f. Especifique un nombre para el archivo de solicitud de certificado.
5. Con los archivos de solicitud de certificado, obtenga los certificados firmados de la CA.
6. Importe los certificados firmados.
 - a. En Oracle Wallet Manager, haga clic con el botón derecho en la solicitud de certificado que se ha usado para obtener el certificado firmado y, a continuación, seleccione **Importar certificado de confianza**.
 - b. En Importar certificado, haga clic en **Aceptar** para importar el certificado de un archivo.
 - c. En Importar certificado, seleccione el archivo de certificado y, a continuación, haga clic en **Abrir**.
7. Guarde la cartera en una ubicación práctica, por ejemplo, `EPM_ORACLE_INSTANCE/httpConfig/ohs/config/OHS/ohs_component/keystores/epmsystem`.

8. Seleccione **Cartera** y, a continuación, **Inicio de sesión automático** para activarlo.

Configuración de Oracle Wallet con ORAPKI (en Linux)

Para configurar Oracle Wallet con la línea de comandos ORAPKI, lleve a cabo los pasos siguientes:

1. Cree una carpeta para su cartera:

```
$ mkdir /MIDDLEWARE_HOME/oracle_common/wallet
```

2. Agregue la ubicación de la utilidad orapki a su ruta:

```
$ export PATH=$PATH:$MIDDLEWARE_HOME/oracle_common/bin
```

3. Cree una cartera para guardar su certificado:

```
>$ MIDDLEWARE_HOME/oracle_common/bin/orapki wallet create -wallet  
[wallet_location] -auto_login
```

Este comando le pide que introduzca y vuelva a introducir una contraseña de cartera si no se ha especificado ninguna contraseña en la línea de comandos. Crea una cartera en la ubicación especificada para `-wallet`.

4. Genere una solicitud de firma de certificado (CSR) y agréguela a su cartera:

```
$ MIDDLEWARE_HOME/oracle_common/bin/orapki wallet add -wallet  
[wallet_location] -dn 'CN=<CommonName>,OU=<OrganizationUnit>,  
O=<Company>, L=<Location>, ST=<State>, C=<Country>' -keysize 512|1024|  
2048|4096 -pwd [Wallet_Password]
```

5. Agregue el certificado raíz y el certificado intermedio al almacén de claves de confianza.

```
$ MIDDLEWARE_HOME/oracle_common/bin/orapki wallet add -wallet  
[wallet_location] -trusted_cert -cert [certificate_location] [-pwd]
```

6. Utilice su autoridad de certificación (CA) para firmar la solicitud de firma de certificado (CSR). Para exportar la solicitud de certificado de una Oracle Wallet:

```
$ MIDDLEWARE_HOME/oracle_common/bin/orapki wallet export -wallet  
[wallet_location] -dn 'CN=<CommonName>,OU=<OrganizationUnit>,  
O=<Company>, L=<Location>, ST=<State>, C=<Country>' -request  
[certificate_request_filename] [-pwd]
```

7. Importe la CSR firmada a la cartera:

```
$ MIDDLEWARE_HOME/oracle_common/bin/orapki wallet add -wallet  
[wallet_location] -user_cert -cert [certificate_location] [-pwd]
```

8. Para mostrar el contenido de una cartera:

```
$ MIDDLEWARE_HOME/oracle_common/bin/orapki wallet display -wallet  
[wallet_location] [-pwd]
```

Activación para SSL de Oracle HTTP Server

Tras volver a configurar el servidor web en cada equipo que aloje Oracle HTTP Server, actualice el archivo de configuración de Oracle HTTP Server mediante el reemplazo de la ubicación de la cartera predeterminada por la cartera que haya creado.

Para configurar Oracle HTTP Server para SSL:

1. Vuelva a configurar el servidor web en cada equipo host de Oracle HTTP Server de su despliegue.
2. Inicie EPM System Configurator para la instancia.
3. En la pantalla de selección de la tarea de configuración, realice estos pasos y, a continuación, haga clic en **Siguiente**.
 - a. Borre la selección de **Desactivar todo**.
 - b. Expanda el grupo de tareas **Hyperion Foundation** y, a continuación, seleccione **Configurar servidor web**.
4. En **Configurar servidor web**, haga clic en **Siguiente**.
5. En **Confirmación**, haga clic en **Siguiente**.
6. En **Resumen**, haga clic en **Finalizar**.

7. Con un editor de texto, abra `EPM_ORACLE_INSTANCE/httpConfig/ohs/config/fmwconfig/components/OHS/ohs_component/ssl.conf`.
8. Asegúrese de que el puerto SSL que está usando aparece en `OHS Listen port` y que es similar al siguiente:

Si está usando 19443 como puerto de comunicación SSL, las entradas deben ser como las siguientes:

```
Listen 19443
```

9. Establezca el valor del parámetro `SSLSessionCache` en `none`.
10. Actualice los valores de configuración de cada instancia de Oracle HTTP Server en su despliegue.
 - a. Con un editor de texto, abra `EPM_ORACLE_INSTANCE/httpConfig/ohs/config/fmwconfig/components/OHS/ohs_component/ssl.conf`.
 - b. Busque la directiva `SSLWallet` y cambie su valor para que apunte a la cartera donde haya instalado el certificado. Si ha creado la cartera en `EPM_ORACLE_INSTANCEhttpConfig/ohs/config/OHS/ohs_component/keystores/epmsystem`, su directiva `SSLWallet` puede ser como la que se muestra a continuación:

```
SSLWallet "${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/${COMPONENT_NAME}/keystores/epmsystem"
```

- c. Guarde y cierre `ssl.conf`.
11. Actualice `mod_wl_ohs.conf` en cada instancia de Oracle HTTP Server en su despliegue.

- a. Con un editor de texto, abra `EPM_ORACLE_INSTANCE/httpConfig/ohs/config/fmwconfig/components/OHS/ohs_component/mod_wl_ohs.conf`.
- b. Asegúrese de que la directiva `WLSSLWallet` apunte a la instancia de Oracle Wallet donde se haya almacenado el certificado SSL.

```
WLSSLWallet MIDDLEWARE_HOME/ohs/bin/wallets/myWallet
```

Por ejemplo, `C:/Oracle/Middleware/ohs/bin/wallets/myWallet`

- c. Establezca el valor de la directiva `SecureProxy` en `ON`.

```
SecureProxy ON
```

- d. Asegúrese de que las definiciones de `LocationMatch` para los componentes desplegados de Oracle Enterprise Performance Management System son similares a los del siguiente ejemplo de Servicios compartidos de Oracle Hyperion, en el que se asume un cluster de Oracle WebLogic Server (en `myserver1` y `myserver2` con el puerto SSL 28443):

```
<LocationMatch /interop/>
  SetHandler weblogic-handler
  pathTrim /
  WeblogicCluster myServer1:28443,myServer2:28443
  WLProxySSL ON
</LocationMatch>
```

- e. Guarde y cierre `mod_wl_ohs.conf`.

Configuración de los componentes web de EPM System desplegados en WebLogic Server

Tras desplegar los componentes web de Oracle Enterprise Performance Management System, debe configurarlos para la comunicación SSL.

Para configurar los componentes web para SSL:

1. Para iniciar Oracle WebLogic Server, ejecute un archivo almacenado en `EPM_ORACLE_INSTANCE/domains/EPMSysystem/bin/startWebLogic.cmd`:
2. Para iniciar la consola de administración de WebLogic Server, acceda a la dirección URL siguiente:

```
http://SERVER_NAME:Port/console
```

Por ejemplo, para acceder a la consola de WebLogic Server desplegada en el puerto predeterminado en `myServer`, debe usar `http://myServer:7001/console`.

3. En la pantalla Bienvenido, introduzca el nombre y la contraseña de usuario para acceder a `EPMSysystem`. El nombre de usuario y la contraseña se especifican en EPM System Configurator durante el proceso de configuración.
4. En **Centro de cambios**, haga clic en **Bloquear y editar**.

5. En el panel izquierdo de la consola, expanda **Entorno** y, a continuación, seleccione **Servidores**.
6. En la pantalla Resumen de servidores, haga clic en el nombre del servidor cuyo SSL desee activar.

Por ejemplo, si ha instalado todos los componentes de Oracle Hyperion Foundation Services, puede activar SSL en estos servidores:

- CalcManager
 - FoundationServices
7. Desmarque **Puerto de recepción activado** para desactivar el puerto de escucha HTTP.
 8. Asegúrese de que está seleccionada la opción **Puerto de recepción SSL activado**.
 9. En **Puerto de escucha SSL**, introduzca el puerto de escucha SSL de WebLogic Server.
 10. Especifique los almacenes de claves de confianza e identidad que vaya a usar.
 - Seleccione **Almacenes de claves** para abrir el separador Almacenes de claves.
 - En **Almacenes de claves**, seleccione una opción:
 - a. Seleccione **Almacenes de claves** para abrir el separador Almacenes de claves.
 - b. En **Almacenes de claves**, seleccione una opción:
 - **Identidad personalizada y protección personalizada** si no está usando un certificado de servidor de una CA de tercero conocida
 - **Identidad personalizada y protección de estándar de Java** si no está usando un certificado de servidor de una CA de tercero conocida
 - c. En **Almacén de claves de identidad personalizado**, introduzca la ruta del almacén de claves donde se haya instalado el certificado de WebLogic Server firmado.
 - d. En **Tipo de almacén de claves de identidad personalizado**, introduzca `jks`.
 - e. En **Frase de contraseña de almacén de claves de identidad personalizado** y **Confirmar frase de contraseña de almacén de claves de identidad personalizado**, introduzca la contraseña del almacén de claves.
 - f. Si ha seleccionado **Identidad personalizada y protección personalizada** en **Almacenes de claves**:
 - En **Almacén de claves de confianza personalizado**, introduzca la ruta del almacén de claves personalizado donde esté disponible el certificado raíz de la CA que haya firmado el certificado del servidor.
 - En **Tipo de almacén de claves de confianza personalizado**, introduzca `jks`.
 - En **Frase de contraseña de almacén de claves de confianza personalizado** y **Confirmar frase de contraseña de almacén de claves de confianza personalizado**, introduzca la contraseña del almacén de claves.
 - g. Haga clic en **Guardar**.

11. Especifique la configuración de SSL.
 - Seleccione **SSL**.
 - En **Alias de clave privada**, introduzca el alias que haya especificado al importar el certificado de WebLogic Server firmado.
 - En **Frase de contraseña de clave privada y Confirmar frase de contraseña de clave privada**, introduzca la contraseña que se va a usar para recuperar la clave privada.
 - Solo aplicación web de **Oracle Hyperion Provider Services**: si está usando certificados con comodín para cifrar la comunicación entre WebLogic Server y otros componentes de servidor de EPM System, desactive la verificación del nombre de host para la aplicación web Provider Services.
 - Seleccione **Avanzadas**.
 - En **Verificación de nombre de host**, seleccione **Ninguna**.
 - Haga clic en **Guardar**.
12. En **Centro de cambios**, haga clic en **Activar cambios**.

Actualización de la configuración de dominio

Este proceso actualiza la configuración del dominio Cree una copia de seguridad completa del despliegue antes de iniciar este procedimiento. Oracle recomienda que pruebe este procedimiento en un despliegue de prueba antes de realizar cambios en un despliegue de producción.

Para actualizar la configuración del dominio:

1. Desplácese al directorio `MIDDLEWARE_HOME/oracle_common/bin` directory:
`cd MIDDLEWARE_HOME/oracle_common/bin`
2. Defina `ORACLE_HOME`, `WL_HOME` y `JAVA_HOME`.
`set ORACLE_HOME= /Oracle/Middleware`
`set WL_HOME= /Oracle/Middleware/wlserver`
`set JAVA_HOME= /Oracle/Middleware/jdk`
3. En la Consola de WebLogic, active el puerto HTTP para el servidor de administración.
4. Cree un almacén de claves mediante un comando similar al siguiente:
`libovdconfig.bat -host HOSTNAME -port 7001 -userName USERNAME -domainPath %MWH%\user_projects\domains\EPMSYSTEM -createKeystore`

En este comando, reemplace `HOSTNAME` y `USERNAME` por el nombre de host del servidor de WebLogic y el nombre de usuario del administrador, respectivamente. Asegúrese de que la salida indica que se ha creado correctamente el almacén de claves de OVD.

5. Exporte el certificado SSL de AdminServer.

Note:

Este paso solo es aplicable para un LDAP embebido (autenticador predeterminado). Para otros LDAP, el certificado se debe exportar utilizando los comandos específicos de LDAP adecuados. El formato de archivo del certificado debe ser **X.509 codificado en Base64**

- a. Utilizando Internet Explorer, acceda a la consola de administración de WebLogic conectándose a `https://HOSTNAME:7002/console`
 - b. Haga clic en **Ver certificado** y, después, en **Detalles**, y seleccione **Copiar en archivo** para exportar el certificado SSL.
 - c. Guarde el certificado como un archivo de certificado **X.509 codificado en Base64** en un directorio local; por ejemplo, como `C:\certificate\slc17rby.cer`.
 - d. Mueva el certificado a un servidor.
6. Mediante keytool, importe el certificado en el almacén de claves que ha creado en el paso 4. Utilice comandos similares al siguiente (suponiendo que `JAVA_HOME`, y el ejecutable keytool, esté en la ruta de acceso):
- ```
export PATH=$JAVA_HOME/bin:$PATH

keytool -importcert -keystore
DOMAIN_HOME\config\fmwconfig\ovd\default\keystores/adapters.jks -
storepass PASSWORD -alias wcp_ssl -file CERTIFICATE_PATH -noprompt, por
ejemplo:

keytool -importcert -keystore %MWH%
\user_projects\domains\EPMSysystem\config\fmwconfig\ovd\default\keystore
s/adapters.jks -storepass examplePWD -alias wcp_ssl -file
C:\certificate\slc17rby.cer -noprompt
```

 **Note:**

- La contraseña utilizada en este comando debe coincidir con la contraseña utilizada al generar el almacén de claves en el paso 4.
- `CERTIFICATE_PATH` es la ubicación y el nombre del certificado
- alias puede ser cualquier alias de su elección.

Al importar correctamente el archivo, keytool muestra el mensaje `Certificate was added to keystore`.

7. En la consola de WebLogic, active el puerto SSL para el servidor de administración, además del puerto HTTP.
8. Reinicie el servidor de administración de Weblogic y los servidores administrados.
9. Inicie sesión en Oracle Hyperion Enterprise Performance Management Workspace utilizando una conexión de seguridad para verificar que todo está funcionando.

## Reinicio de servidores y EPM System

Reinicie todos los servidores del despliegue y, a continuación, inicie Oracle Enterprise Performance Management System en cada servidor.

## Prueba del despliegue

Tras finalizar el despliegue SSL, verifique que todo funciona.

Para probar el despliegue:

1. Con un explorador, acceda a la URL segura de Oracle Hyperion Enterprise Performance Management Workspace:

Si ha usado `epm.myCompany.com` como alias de servidor para la comunicación externa y 4443 como puerto SSL, la URL de EPM Workspace URL será

```
https://epm.myCompany.com:4443/workspace/index.jsp
```

2. En la pantalla de inicio de sesión, introduzca un nombre de usuario y contraseña.
3. Haga clic en **Iniciar sesión**.
4. Verifique que puede acceder de forma segura a los componentes de Oracle Enterprise Performance Management System desplegados.

## Configuración de directorios de usuario externos activados para SSL

### Suposiciones

- Los directorios de usuario externos que tenga previsto configurar en Consola de Servicios compartidos de Oracle Hyperion están activados para SSL.
- Si no ha utilizado un certificado de una CA de terceros conocida para activar para SSL el directorio de usuario, tendrá una copia del certificado raíz de la CA que firmó el certificado del servidor.

### Importar el certificado de CA raíz

Si no ha utilizado un certificado de una CA de terceros conocida para activar para SSL el directorio de usuario, debe importar el certificado raíz de la CA que firmó el certificado del servidor en los siguientes almacenes de claves:



#### Nota:

Durante el despliegue de la aplicación, WebLogic agrega la directiva - `Djavax.net.ssl.trustStore` que apunta a `DemoTrust.jks` en `setDomainEnv.sh` o `setDomainEnv.cmd`. Elimine `-Djavax.net.ssl.trustStore` de `setDomainEnv.sh` o `setDomainEnv.cmd` si no está usando el certificado de WebLogic predeterminado.

Utilice una herramienta, como `keytool`, para importar el certificado de CA raíz.

- Todos los servidores de Oracle Enterprise Performance Management System:  
**Almacén de claves de JVM:** `MIDDLEWARE_HOME/jdk/jre/lib/security/cacerts`
- El almacén de claves que usa JVM en cada equipo host de componente de EPM System. De forma predeterminada, los componentes de EPM System utilizan el almacén de claves siguiente:

```
MIDDLEWARE_HOME/jdk/jre/lib/security/cacerts
```

### Configurar directorios de usuario externos

Los directorios de usuario se configuran con la Consola de Servicios compartidos. Al configurar los directorios de usuario, debe seleccionar la opción `SSL activado` que indica a la seguridad de EPM System que utilice el protocolo seguro para comunicarse con el directorio de usuario. Puede activar para SSL una conexión entre la seguridad de EPM System y los directorios de usuarios activados para LDAP, por ejemplo, Oracle Internet Directory y Microsoft Active Directory.

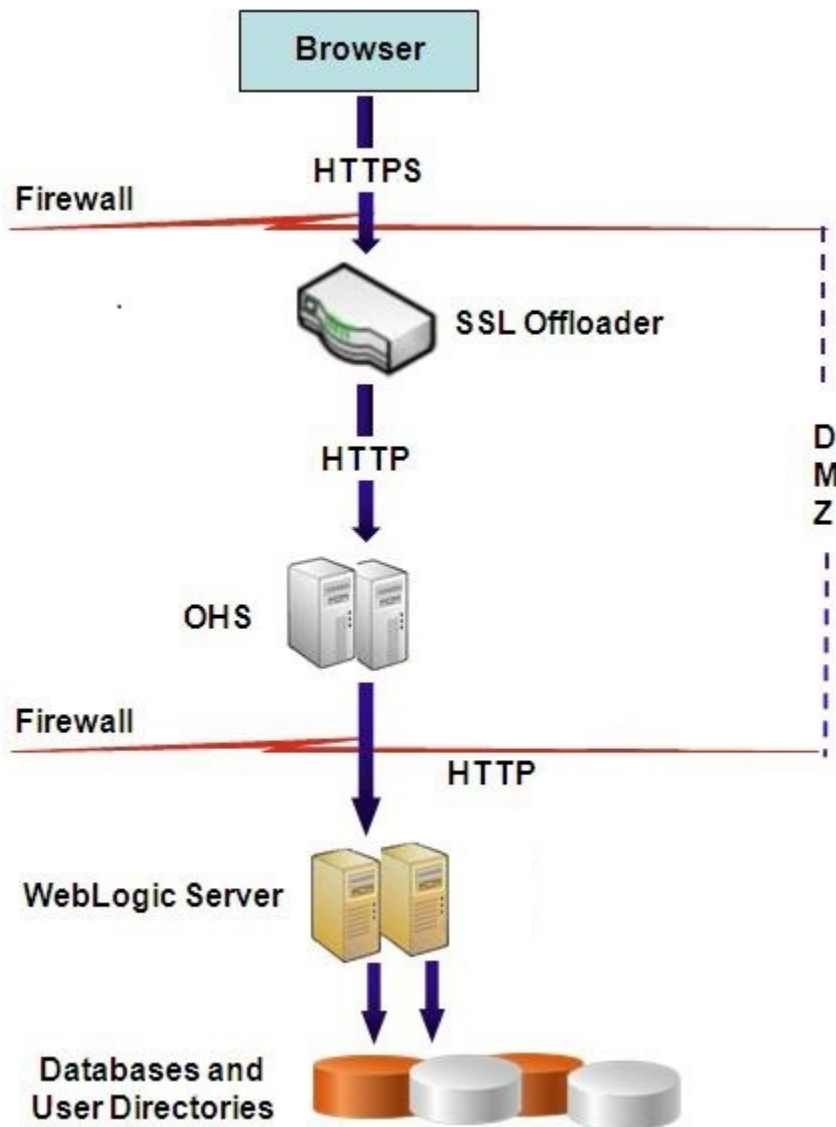
Consulte la sección sobre configuración de directorios de usuario en *Guía de administración de seguridad de usuarios de Oracle Enterprise Performance Management System*.

## Finalización de SSL en el servidor web

### Arquitectura de despliegue

En este escenario, SSL se usa para proteger el enlace de comunicación entre los clientes de Oracle Enterprise Performance Management System (por ejemplo, un explorador) y Oracle HTTP Server. El siguiente esquema ilustra el concepto:





### Suposiciones

Esta configuración usa dos alias de servidor, por ejemplo, `epm.myCompany.com` y `empinternal.myCompany.com`, en el servidor web, uno para la comunicación externa entre el servidor web y los exploradores y el otro para la comunicación interna entre los servidores de EPM System. Asegúrese de que los alias del servidor apunten a la dirección IP del equipo y que se puedan resolver mediante la DNS.

Se debe instalar en el servidor web un certificado firmado para soportar la comunicación externa con los exploradores (por ejemplo, mediante `epm.myCompany.com`) en el servidor web (donde se define el host virtual que soporta la comunicación externa). Este host virtual debe terminar SSL y reenviar solicitudes HTTP a Oracle HTTP Server.

Cuando SSL se está terminando en Oracle HTTP Server (OHS) o en un equilibrador de carga, debe:

- Establecer todas las aplicaciones web lógicas en un host virtual no ssl del equilibrador de carga o de Oracle HTTP Server (por ejemplo, `empinternal.myCompany.com:80`, donde 80 es el puerto no SSL). En la pantalla Configuración, realice estos pasos:

1. Amplíe la tarea de configuración **Hyperion Foundation**.
  2. Seleccione **Configurar dirección lógica para aplicaciones web**.
  3. Especifique el *nombre de host*, el número de puerto no SSL y el número de puerto SSL.
- Establecer la URL externa en el host virtual compatible con SSL del equilibrador de carga o de Oracle HTTP Server (por ejemplo, `empexternal.myCompany.com:443`, donde 443 es el puerto SSL). En la pantalla Configuración, realice estos pasos:
    1. Amplíe la tarea de configuración **Hyperion Foundation**.
    2. Seleccione **Configurar configuración común**.
    3. Seleccione **Activar descarga de SSL** en Detalles de URL externas.
    4. Especifique el *host de URL externa* y el *puerto de URL externa*.

 **Nota:**

Al volver a desplegar aplicaciones web o volver a configurar un servidor web con **configtool**, se reemplazará la configuración de las aplicaciones web lógicas y de las URL externas.

### Configuración de EPM System

El despliegue predeterminado de los componentes de EPM System soporta la finalización de SSL en el servidor web. No es necesario realizar ninguna acción adicional.

Al configurar EPM System, asegúrese de que las aplicaciones web lógicas apunten al host virtual (por ejemplo, `empinternal.myCompany.com`) que se ha creado para la comunicación interna. Consulte las siguientes fuentes de información para instalar y configurar EPM System:

- *Guía de configuración e instalación de Oracle Enterprise Performance Management System*
- *Documento de inicio para la instalación de Oracle Hyperion Enterprise Performance Management System*

### Prueba del despliegue

Tras finalizar el proceso de despliegue, verifique que todo funciona. Para ello, conecte a la URL segura de Oracle Hyperion Enterprise Performance Management Workspace:

```
https://virtual_host_external:SSL_PORT/workspace/index.jsp
```

Por ejemplo, `https://epm.myCompany.com:443/workspace/index.jsp` donde 443 es el puerto SSL.

## SSL para Essbase 11.1.2.4

### Descripción general

En esta sección se explican los procedimientos para reemplazar los certificados predeterminados que se usan para proteger la comunicación entre una instancia de Oracle Essbase y componentes como MaxL, Oracle Essbase Administration Services Server, Oracle Essbase Studio Server, Oracle Hyperion Provider Services, Oracle Hyperion Foundation Services, Oracle Hyperion Planning, Oracle Hyperion Financial Management y el registro de servicios compartidos de Oracle Hyperion.

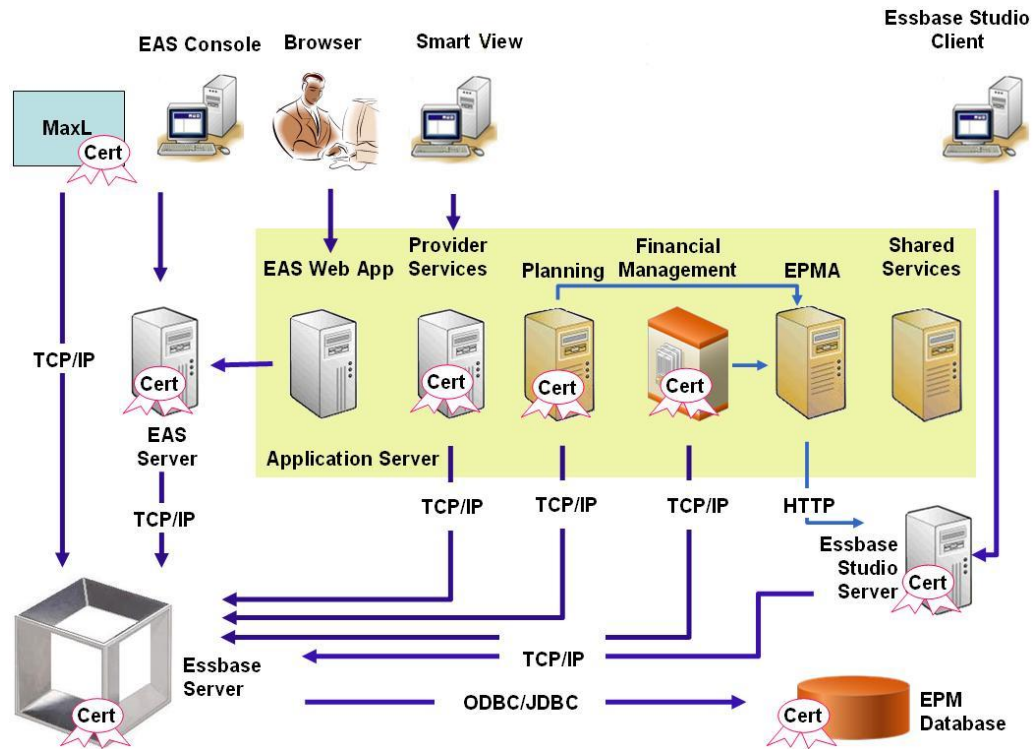
### Despliegue predeterminado

Essbase se puede desplegar para funcionar en modo SSL y no SSL. El agente de Essbase escucha en un puerto no seguro; también se puede configurar para escuchar en un puerto seguro. Todas las conexiones que acceden al puerto seguro se consideran conexiones SSL. Si un cliente se conecta al agente de Essbase en el puerto que no es SSL, la conexión se considera como una conexión no SSL. Los componentes pueden establecer conexiones no SSL y SSL simultáneas a un agente Essbase.

Puede controlar SSL en cada sesión. Para ello, especifique el protocolo y el puerto seguro al iniciar sesión. Consulte [Establecimiento de una conexión SSL por sesión](#).

Si SSL está activado, se cifra toda la comunicación en una instancia de Essbase para garantizar la seguridad de los datos.

Los despliegues predeterminados de los componentes de Essbase en modo seguro usan certificados autofirmados para activar la comunicación SSL, principalmente para realizar pruebas. Oracle le recomienda que utilice certificados de CA de terceros conocidas para activar para SSL los entornos de producción de Essbase.



Normalmente, Oracle Wallet almacena el certificado que activa la comunicación SSL con clientes que usan Essbase RTC y un almacén de claves Java almacena el certificado que permite la comunicación SSL con componentes que utilizan JAPI para la comunicación. Para establecer la comunicación SSL, los clientes y las herramientas de Essbase almacenan el certificado raíz de la CA que ha firmado los certificados del servidor y del agente de Essbase. Consulte [Certificados necesarios y su ubicación](#).

### Certificados necesarios y su ubicación

Oracle recomienda el uso de certificados de CA de terceros conocidas para activar para SSL Essbase en un entorno de producción. Puede usar los certificados autofirmados predeterminados para realizar pruebas.

#### Nota:

Essbase soporta el uso de certificados con comodín, lo que puede proteger varios subdominios con un certificado SSL. El uso de un certificado con comodín puede reducir el tiempo y el costo de gestión.

Los certificados con comodín no se pueden usar si está activada la comprobación del nombre de host.

Necesita los siguientes certificados:

- Un certificado de CA raíz.  
Los componentes que usen Essbase RTC para establecer una conexión a Essbase necesitan que el certificado de autoridad de certificación raíz se almacene en una cartera de Oracle. Los componentes que usen JAPI para establecer una conexión necesitan que el certificado de CA raíz se almacene en

un almacén de claves Java. En la tabla siguiente se indican los certificados necesarios y sus ubicaciones.

 **Nota:**

No tiene que instalar un certificado de CA raíz si está usando certificados de una CA de terceros conocida cuyo certificado raíz ya esté instalado en Oracle Wallet.

- Certificado firmado para el servidor de Essbase y el agente de Essbase.

**Tabla 2-1 Certificados necesarios y sus ubicaciones**

| Componente <sup>1</sup>                                          | Almacén de claves                                                                                   | Certificado <sup>2</sup>                                                                                                                          |
|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| MaxL                                                             | Oracle Wallet                                                                                       | Certificado de CA raíz                                                                                                                            |
| Servidor de Administration Services                              | Oracle Wallet                                                                                       | Certificado de CA raíz                                                                                                                            |
| Provider Services                                                | Oracle Wallet                                                                                       | Certificado de CA raíz                                                                                                                            |
| Base de datos de Oracle Enterprise Performance Management System | Oracle Wallet                                                                                       | Certificado de CA raíz                                                                                                                            |
| Servidor de Essbase Studio                                       | Almacén de claves Java                                                                              | Certificado de CA raíz                                                                                                                            |
| Planning                                                         | <ul style="list-style-type: none"> <li>• Oracle Wallet</li> <li>• Almacén de claves Java</li> </ul> | Certificado de CA raíz                                                                                                                            |
| Financial Management                                             | Almacén de claves Java                                                                              | Certificado de CA raíz                                                                                                                            |
| Essbase (servidor y agente) <sup>3</sup>                         | <ul style="list-style-type: none"> <li>• Oracle Wallet</li> <li>• Almacén de claves Java</li> </ul> | <ul style="list-style-type: none"> <li>• Certificado de CA raíz</li> <li>• Certificado firmado para el servidor y el agente de Essbase</li> </ul> |
| Repositorio de Servicios compartidos de Oracle Hyperion          |                                                                                                     |                                                                                                                                                   |

<sup>1</sup> Solo necesita una instancia del almacén de claves para soportar varios componentes que usen un almacén de claves similar.

<sup>2</sup> Varios componentes pueden usar un certificado raíz instalado en un almacén de claves.

<sup>3</sup> Los certificados se deben instalar en la instancia de Oracle Wallet predeterminada y en el almacén de claves Java.

## Instalación y despliegue de componentes de Essbase

El proceso de configuración permite seleccionar un puerto de agente seguro (el valor predeterminado es 6423), que puede cambiar al configurar Oracle Essbase. De forma predeterminada, el proceso de despliegue instala los certificados autofirmados necesarios para crear un despliegue seguro funcional para las pruebas.

EPM System Installer instala una instancia de Oracle Wallet y un certificado autofirmado en `ARBOR_PATH` en el equipo que aloja la instancia de Essbase si se instala Oracle HTTP Server. En despliegues de un solo host, todos los componentes de Essbase comparten este certificado.

## Uso de certificados CA de terceros de confianza para Essbase

### Creación de solicitudes de certificados y obtención de certificados

Genere una solicitud de certificado para obtener un certificado para el servidor que aloja el servidor de Oracle Essbase y el agente de Essbase. Una solicitud de certificado contiene información cifrada específica de su nombre distintivo (DN). Usted envía la solicitud del certificado a una autoridad de firma para obtener un certificado SSL.

Utilice una herramienta como keytool u Oracle Wallet Manager para crear una solicitud de certificado. Para obtener información detallada sobre la creación de una solicitud de certificado, consulte la documentación de la herramienta que esté usando.

Si está usando keytool, use un comando como el siguiente para crear una solicitud de certificado:

```
keytool -certreq -alias essbase_ssl -file C:/certs/essabse_server_csr -
keypass password -storetype jks -keystore
C:\oracle\Middleware\EPMSystem11R1\Essbase_ssl\keystore -storepass
password
```

### Obtención e instalación del certificado de CA raíz

El certificado de CA raíz verifica la validez del certificado que se usa para soportar SSL. Contiene la clave pública con la que se hace coincidir la clave privada que se ha usado para verificar el certificado. Puede obtener el certificado de CA raíz de la autoridad de certificación que haya firmado sus certificados SSL.

Instale el certificado raíz de la CA que haya firmado el certificado de servidor de Essbase en clientes que conecten al servidor o al agente de Essbase. Asegúrese de que el certificado raíz esté instalado en el almacén de claves adecuado para el cliente. Consulte [Certificados necesarios y su ubicación](#).



#### Nota:

Varios componentes pueden usar un certificado CA raíz instalado en un equipo de servidor.

### Oracle Wallet

Consulte la [Certificados necesarios y su ubicación](#) para obtener una lista de los componentes que exigen el certificado raíz de CA en una instancia de Oracle Wallet. Puede crear una cartera o instalar el certificado en la cartera de demostración donde esté instalado el certificado autofirmado predeterminado.

Consulte la documentación de Oracle Wallet Manager para obtener procedimientos detallados para crear carteras e importar el certificado de CA raíz.

### Almacén de claves Java

Consulte la [Certificados necesarios y su ubicación](#) para obtener una lista de los componentes que exigen el certificado de CA raíz en un almacén de claves Java.

Puede agregar el certificado en el almacén de claves donde esté instalado el certificado autofirmado predeterminado o crear un almacén de claves para almacenar el certificado.

 **Nota:**

Los certificados de CA raíz de muchas de las CA de terceros conocidas ya están instalados en el almacén de claves de Java.

Consulte la documentación de la herramienta que esté usando para obtener instrucciones detalladas. Si está usando keytool, use un comando, como el siguiente, para importar el certificado raíz:

```
keytool -import -alias blister_CA -file c:/certs/CA.crt -keypass
password -trustcacerts -keystore
C:\Oracle\Middleware\EPMSysstem11R1\Essbase_ssl
\keystore -storepass password
```

### Instalación de certificados firmados

Usted instala los certificados SSL firmados en el servidor que aloja el servidor de Essbase y el agente de Essbase. Los componentes que usen Essbase RTC (API de C) para establecer una conexión al servidor o al agente de Essbase necesitan que el certificado se almacene en una instancia de Oracle Wallet con el certificado de CA raíz. Los componentes que usen JAPI para establecer una conexión al servidor o al agente de Essbase necesitan que el certificado de CA raíz y el certificado SSL firmado se almacene en un almacén de claves Java. Para conocer los procedimientos detallados, consulte estas fuentes de información:

- Documentación de Oracle Wallet Manager
- Documentación o ayuda en línea de la herramienta, por ejemplo, keytool, que usa para importar el certificado

Si está usando keytool, use un comando, como el siguiente, para importar el certificado

```
keytool -import -alias essbase_ssl -file C:/certs/essbase_ssl.crt -keypass
password -keystore
C:\Oracle\Middleware\EPMSysstem11R1\Essbase_ssl\keystore -storepass password
```

### Actualización de los valores del registro del servidor de Essbase

#### Windows

1. En un símbolo del sistema, cambie el directorio a *EPM\_ORACLE\_INSTANCE/epmsystem1/bin*.
2. Ejecute estos comandos para actualizar el Registro de Windows:
 

```
epmsys_registry.bat updateproperty "#<Object ID>/@EnableSecureMode" true
epmsys_registry.bat updateproperty "#<Object ID>/@EnableClearMode" false
```

Asegúrese de sustituir <Object ID> por el ID de componente del servidor de Essbase, el cual está disponible en el informe del registro que se genera al completar el proceso de configuración del servidor de Essbase.

#### Linux

1. En una consola, cambie el directorio a `EPM_ORACLE_INSTANCE/epmsystem1/bin`.
2. Ejecute estos comandos para actualizar el registro:

```
epmsys_registry.sh updateproperty "#<Object ID>/@EnableSecureMode"
true
```

```
epmsys_registry.sh updateproperty "#<Object ID>/@EnableClearMode"
false
```

Asegúrese de sustituir `<Object ID>` por el ID de componente del servidor de Essbase, el cual está disponible en el informe del registro que se genera al completar el proceso de configuración del servidor de Essbase.

### Actualización de la configuración Essbase de Essbase

Puede personalizar la configuración de SSL para el servidor y los clientes de Essbase especificando valores para ellos en `essbase.cfg`.

- Configuración para activar el modo seguro
- Configuración para activar el modo Clear
- Modo preferido para comunicarse con los clientes (solo usado por los clientes)
- Puerto seguro
- Conjuntos de cifrado
- Ruta de Oracle Wallet



#### Nota:

En `essbase.cfg`, asegúrese de agregar los parámetros necesarios que falten, en concreto, `EnableSecureMode` y `AgentSecurePort`, y establezca sus valores.

Para actualizar `essbase.cfg`:

1. Copie la cartera de Oracle con certificados para el servidor de Essbase en `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin/wallet`. Esta es la única ubicación de Oracle Wallet que es aceptable para el servidor de Essbase.
2. Con un editor de texto, abra `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin/essbase.cfg`.
3. Introduzca la configuración según sea necesario. Se usa de forma implícita la configuración predeterminada de Essbase. Si necesita cambiar el comportamiento predeterminado, agregue la configuración para el comportamiento personalizado en `essbase.cfg`. Por ejemplo, `EnableClearMode` se aplica de forma predeterminada, por el que se activa el servidor de Essbase para comunicarse a través de un canal no cifrado. Para desactivar la disponibilidad del servidor de Essbase a través de un canal no cifrado, debe especificar `EnableClearMode FALSE` en `essbase.cfg`. Consulte la siguiente tabla.



**Tabla 2-2 Configuración de SSL de Essbase**

| Valor                            | Descripción <sup>1</sup>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EnableClearMode <sup>2</sup>     | <p>Activa la comunicación sin cifrado entre las aplicaciones de Essbase y el agente de Essbase. Si esta propiedad está establecida en FALSE, Essbase no gestiona solicitudes que no sean SSL.</p> <p><b>Valor predeterminado:</b> EnableClearMode TRUE</p> <p><b>Ejemplo:</b> EnableClearMode FALSE</p>                                                                                                                                                                                                     |
| EnableSecureMode                 | <p>Activa la comunicación cifrada de SSL entre el cliente de Essbase y el agente de Essbase. Esta propiedad se debe establecer en TRUE para soportar SSL.</p> <p><b>Valor predeterminado:</b> FALSE</p> <p><b>Ejemplo:</b> EnableSecureMode TRUE</p>                                                                                                                                                                                                                                                        |
| SSLCipherSuites                  | <p>Lista de conjuntos de cifrado, en orden de preferencia, que usar para la comunicación SSL. El agente de Essbase usa uno de los conjuntos de cifrado para la comunicación SSL. Al primer conjunto de cifrado se le asigna la máxima prioridad cuando el agente elige un conjunto de cifrado.</p> <p><b>Valor predeterminado:</b> SSL_RSA_WITH_RC4_128_MD5</p> <p><b>Ejemplo:</b> SSLCipherSuites<br/>SSL_RSA_WITH_AES_256_CBC_SHA256,SSL_RSA_WITH_AES_256_GCM_SHA384</p>                                  |
| APSRESOLVER                      | <p>URL de Oracle Hyperion Provider Services. Si utiliza varios servidores de Provider Services, separe cada URL con un punto y coma.</p> <p><b>Ejemplo:</b> APSRESOLVER https://<br/>exampleAPShost1:PORT/aps;https://<br/>exampleAPShost2:PORT/aps</p>                                                                                                                                                                                                                                                     |
| AgentSecurePort                  | <p>Puerto seguro en el que escucha el agente.</p> <p><b>Valor predeterminado:</b> 6423</p> <p><b>Ejemplo:</b> AgentSecurePort 16001</p>                                                                                                                                                                                                                                                                                                                                                                     |
| WalletPath                       | <p>Ubicación de la instancia de Oracle Wallet (menos de 1.024 caracteres) que almacena el certificado de la CA raíz y del certificado firmado.</p> <p><b>Valor predeterminado:</b> ARBORPATH/bin/wallet</p> <p><b>Ejemplo:</b> WalletPath/usr/local/wallet</p>                                                                                                                                                                                                                                              |
| ClientPreferredMode <sup>3</sup> | <p>Modo (Secure o Clear) para la sesión de cliente. Si esta propiedad está establecida en Secure, se usa el modo SSL para todas las sesiones.</p> <p>Si esta propiedad se establece en Clear, se elige el transporte en función de si la solicitud de inicio de sesión del cliente contiene la palabra clave de transporte seguro. Consulte <a href="#">Establecimiento de una conexión SSL por sesión</a>.</p> <p><b>Valor predeterminado:</b> CLEAR</p> <p><b>Ejemplo:</b> ClientPreferredMode SECURE</p> |

**Tabla 2-2 (Continuación) Configuración de SSL de Essbase**

| Valor | Descripción <sup>1</sup>                                                                                                                          |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <sup>1</sup> El valor predeterminado se aplica si estas propiedades no están disponibles en <code>essbase.cfg</code> .                            |
|       | <sup>2</sup> Essbase deja de estar operativo si <code>EnableClearMode</code> y <code>EnableSecureMode</code> se definen como <code>FALSE</code> . |
|       | <sup>3</sup> Los clientes usan esta opción para determinar si se debe establecer una conexión segura o no segura con Essbase.                     |

4. Guarde y cierre `essbase.cfg`.

### Actualización de nodos de Essbase distribuidos para SSL



#### Nota:

Esta sección se aplica solamente a despliegues distribuidos de Essbase

Asegúrese de que la carpeta de la cartera (por ejemplo, `WalletPath/usr/local/wallet`) que contiene el certificado de autoridad de certificación raíz y el certificado firmado se encuentra en la ubicación necesaria en cada nodo distribuido.

1. Copie la carpeta de la cartera a estas ubicaciones en cada nodo distribuido:
  - `EPM_ORACLE_HOME/common/EssbaseRTC/11.1.2.0/bin`
  - `EPM_ORACLE_HOME/common/EssbaseRTC-64/11.1.2.0/bin`
2. Copie la carpeta de la cartera a estas ubicaciones, si están presentes, en cada nodo distribuido:
  - `EPM_ORACLE_HOME/products/Essbase/EssbaseServer/bin`
  - `EPM_ORACLE_HOME/products/Essbase/EssbaseServer-32/bin`
  - `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin`
3. Copie `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin/essbase.cfg` a estas ubicaciones en cada nodo distribuido:
  - `EPM_ORACLE_HOME/common/EssbaseRTC/11.1.2.0/bin`
  - `EPM_ORACLE_HOME/common/EssbaseRTC-64/11.1.2.0/bin`
4. Copie `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin/essbase.cfg` a estas ubicaciones, si están presentes, en cada nodo distribuido:
  - `EPM_ORACLE_HOME/products/Essbase/EssbaseServer/bin`
  - `EPM_ORACLE_HOME/products/Essbase/EssbaseServer-32/bin`
  - `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin`
5. Copie la carpeta de la cartera a estas ubicaciones de instalación de cliente de Essbase en cada nodo distribuido:
  - `EPM_ORACLE_HOME/products/Essbase/EssbaseClient/bin`
  - `EPM_ORACLE_HOME/products/Essbase/EssbaseClient-32/bin`

**6. Copie `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin/essbase.cfg` a estas ubicaciones de instalación de cliente de Essbase en cada nodo distribuido:**

- `EPM_ORACLE_HOME/products/Essbase/EssbaseClient/bin`
- `EPM_ORACLE_HOME/products/Essbase/EssbaseClient-32/bin`

**7. Agregue estas propiedades al archivo `essbase.properties`:**

- `essbase.ssleverywhere=true`
- `olap.server.ssl.alwaysSecure=true`
- `APSRESOLVER=http[s]://host:httpsPort/aps`  
Asegúrese de sustituir este valor por la URL pertinente.

Actualice el archivo `essbase.properties` en estas ubicaciones, si están presentes, en cada nodo distribuido:

- `EPM_ORACLE_HOME/common/EssbaseJavaAPI/11.2.0/bin/essbase.properties`
- `EPM_ORACLE_HOME/products/Essbase/aps/bin/essbase.properties`
- `EPM_ORACLE_INSTANCE/aps/bin/essbase.properties`

**8. Copie `EPM_ORACLE_HOME/products/Essbase/aps/bin/essbase.properties` en el directorio `EPM_ORACLE_HOME/products/Essbase/eas`, si está disponible, en cada nodo distribuido.**

**9. Solo para Oracle Hyperion Planning:** agregue estas tres propiedades al archivo `essbase.properties`:

- `essbase.ssleverywhere=true`
- `olap.server.ssl.alwaysSecure=true`
- `APSRESOLVER=APS_URL`  
Sustituya `APS_URL` por la URL de Provider Services. Si utiliza varios servidores de Provider Services, separe cada URL con un punto y coma. Por ejemplo, `https://exampleAPShost1:PORT/aps;https://exampleAPShost2:PORT/aps`.

Debe actualizar el archivo `essbase.properties` en estas ubicaciones en cada nodo distribuido:

- `EPM_ORACLE_HOME/products/Planning/config/essbase.properties`
- `EPM_ORACLE_HOME/products/Planning/lib/essbase.properties`

**10. Solo para Oracle Hyperion Financial Reporting:** agregue estas tres propiedades al archivo `EPM_ORACLE_HOME/products/financialreporting/bin/EssbaseJAPI/bin/essbase.properties`:

- `essbase.ssleverywhere=true`
- `olap.server.ssl.alwaysSecure=true`
- `APSRESOLVER=APS_URL`  
Sustituya `APS_URL` por la URL de Provider Services. Si utiliza varios servidores de Provider Services, separe cada URL con un punto y coma. Por ejemplo, `https://exampleAPShost1:PORT/aps;https://exampleAPShost2:PORT/aps`.

 **Nota:**

En entornos de Secure Sockets Layer, Financial Reporting necesita el nombre de cluster de Essbase para establecer la conexión. Se produce un fallo en la conexión si se utiliza el nombre de host para conectar.

11. a. Defina las variables de entorno:
  - **Windows:** Cree una nueva variable de sistema llamada `API_DISABLE_PEER_VERIFICATION` y establezca su valor en 1.
  - **Linux:** Agregue la directiva `API_DISABLE_PEER_VERIFICATION=1` en `setCustomParamsPlanning.sh`.
- b. Agregue la directiva `API_DISABLE_PEER_VERIFICATION=1` en `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin/setEssbaseenv.bat` o `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin/setEssbaseenv.sh`.

Defina variables de entorno:

### Personalización de las propiedades SSL de clientes de JAPI

Hay varias propiedades predeterminadas predefinidas para los componentes de Essbase que se basan en JAPI. Las propiedades predeterminadas se pueden sustituir mediante la inclusión de propiedades en `essbase.properties`.

 **Nota:**

Solo unas pocas propiedades SSL identificadas en la siguiente tabla se externalizan en `essbase.properties`. Debe agregar las propiedades que no estén externalizadas.

Para actualizar las propiedades SSL de los clientes de JAPI:

1. Con un editor de texto, abra `EPM_ORACLE_HOME/common/EssbaseJavaAPI/11.1.2.0/bin/essbase.properties`.
2. Actualice las propiedades según sea necesario. Consulte la tabla siguiente para consultar una descripción de las propiedades de cliente JAPI personalizable. Si no se ha incluido una propiedad que desee en `essbase.properties`, agréguela.

**Tabla 2-3 Propiedades de SSL predeterminadas para clientes de JAPI**

| Propiedad                                 | Descripción                                                                                                                                                                                                          |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>olap.server.ssl.alwaysSecure</code> | Establece el modo que deben usar los clientes en todas las instancias de Essbase. Cambie el valor de esta propiedad a <code>true</code> para aplicar el modo SSL.<br><b>Valor predeterminado:</b> <code>false</code> |

**Tabla 2-3 (Continuación) Propiedades de SSL predeterminadas para clientes de JAPI**

| Propiedad                                      | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>olap.server.ssl.securityHandler</code>   | Nombre de paquete para gestionar el protocolo. Puede cambiar este valor para indicar otro identificador.<br><b>Valor predeterminado:</b><br><code>java.protocol.handler.pkgs</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <code>olap.server.ssl.securityProvider</code>  | Oracle utiliza la implantación del protocolo SSL de Sun. Puede cambiar este valor para indicar otro proveedor.<br><b>Valor predeterminado:</b><br><code>com.sun.net.ssl.internal.www.protocol</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <code>olap.server.ssl.supportedCiphers</code>  | Lista separada por comas de cifrados adicionales que se van a activar para una comunicación segura. Debe especificar solo cifrados que soporte Essbase.<br><b>Ejemplo:</b><br><code>SSL_RSA_WITH_AES_256_CBC_SHA256,SSL_RSA_WITH_AES_256_GCM_SHA384</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <code>olap.server.ssl.trustManagerClass</code> | La clase TrustManager que usar para validar el certificado SSL mediante la verificación de la firma y la comprobación de la fecha de caducidad del certificado.<br>De manera predeterminada, esta propiedad no se establece para aplicar todas las comprobaciones de verificación.<br>Para no aplicar comprobaciones de verificación, establezca el valor de este parámetro en <code>com.essbase.services.olap.security.EssDefaultTrustManager</code> , que es la clase TrustManager predeterminada que permite que todas las comprobaciones de validación sean correctas.<br>Para implantar una clase TrustManager personalizada, especifique un nombre de clase completo de la clase TrustManager que implante la interfaz <code>javax.net.ssl.X509TrustManager</code> .<br><b>Ejemplo:</b> <code>com.essbase.services.olap.security.EssDefaultTrustManager</code> |

3. Guarde y cierre `essbase.properties`.
4. Reinicie todos los componentes de Essbase.

## Establecimiento de una conexión SSL por sesión

Los componentes de Oracle Essbase, por ejemplo, MaxL, pueden controlar SSL en el nivel de sesión mediante la conexión al agente de Essbase con `secure` como palabra clave de

transporte. Por ejemplo, puede establecer una conexión segura entre MaxL y el agente de Essbase mediante la ejecución de uno de los siguientes comandos desde una consola de MaxL:

```
login admin example_password on hostA:PORT:secure
```

```
login admin example_password on hostA:secure
```

El control por sesión tiene prioridad sobre los valores de configuración especificados en `essbase.cfg`. Si no se especifica ninguna palabra clave de transporte, los clientes de Essbase usan el valor establecido para `ClientPreferredMode` para determinar si iniciar una conexión segura con Essbase. Si la opción `ClientPreferredMode` no está establecida en `Secure`, la comunicación se produce a través de un canal no seguro.

## SSL para Essbase 21c

### Descripción general

En esta sección se explican los procedimientos para reemplazar los certificados predeterminados que se usan para proteger la comunicación entre una instancia de Oracle Essbase y componentes como MaxL, Oracle Essbase Administration Services Server, Oracle Hyperion Provider Services, Oracle Hyperion Foundation Services, Oracle Hyperion Planning, Oracle Hyperion Financial Management y Oracle Hyperion Shared Services Registry.

#### Nota:

Essbase Administration Services (EAS) Lite no utiliza el puerto SSL del servidor HTTP (por ejemplo, 443) configurado mediante EPM Configurator. La URL segura del archivo `easconsole.jnlp` se define de forma predeterminada en el puerto no SSL (80).

**Solución alternativa:** reemplace el puerto no SSL predeterminado de la URL segura identificada en `easconsole.jnlp` por la URL segura actualizada:

URL segura predeterminada: `https://myserver:SECURE_PORT/easconsole/console.html`. Ejemplo, `https://myserver:80/easconsole/console.html`

URL segura predeterminada: `https://myserver:SECURE_PORT/easconsole/console.html`. Ejemplo, `https://myserver:443/easconsole/console.html`

Consulte el artículo de My Oracle Support (MOS) [ID de documento 1926558.1 - SSL Port Not Included In easconsole.jnlp of the EAS Web Console](#) para obtener más información.

### Despliegue predeterminado

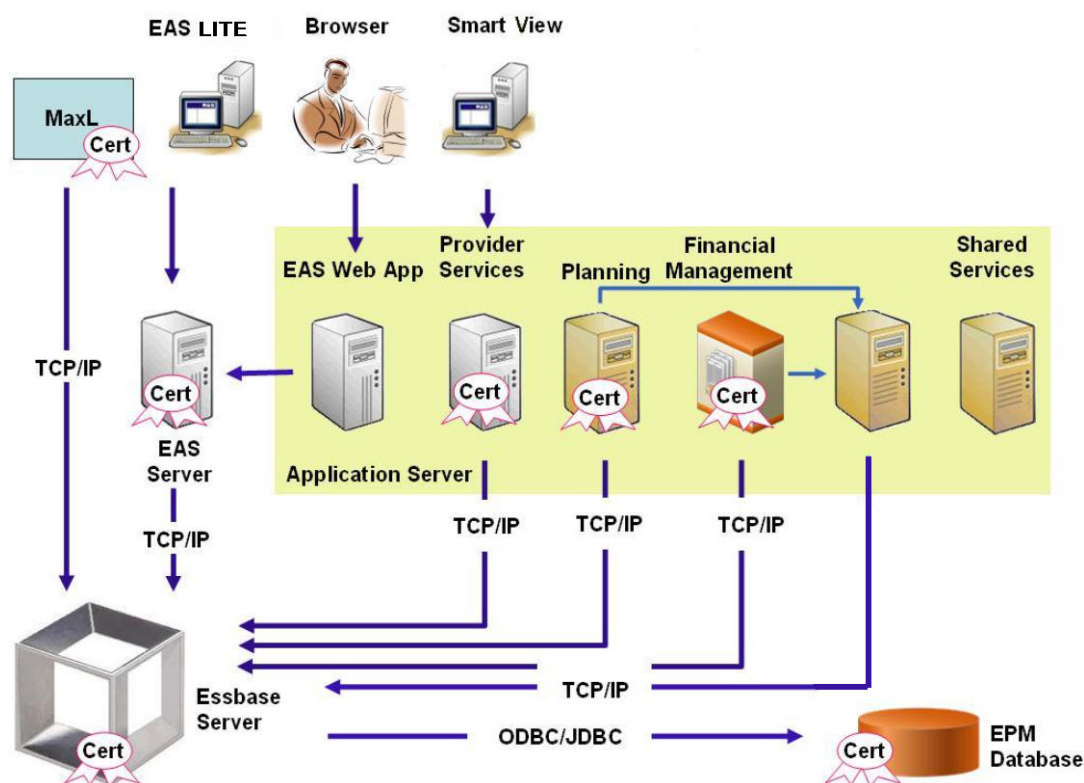
Essbase se puede desplegar para funcionar en modo SSL y no SSL. El agente de Essbase escucha en un puerto no seguro; también se puede configurar para escuchar en un puerto seguro. Todas las conexiones que acceden al puerto seguro se consideran conexiones SSL. Si un cliente se conecta al agente de Essbase en el

puerto que no es SSL, la conexión se considera como una conexión no SSL. Los componentes pueden establecer conexiones no SSL y SSL simultáneas a un agente Essbase.

Puede controlar SSL en cada sesión. Para ello, especifique el protocolo y el puerto seguro al iniciar sesión. Consulte [Establecimiento de una conexión SSL por sesión](#).

Si SSL está activado, se cifra toda la comunicación en una instancia de Essbase para garantizar la seguridad de los datos.

Los despliegues predeterminados de los componentes de Essbase en modo seguro usan certificados autofirmados para activar la comunicación SSL, principalmente para realizar pruebas. Oracle le recomienda que utilice certificados de CA de terceros conocidas para activar para SSL los entornos de producción de Essbase.



Normalmente, Oracle Wallet almacena el certificado que activa la comunicación SSL con clientes que usan Essbase RTC y un almacén de claves Java almacena el certificado que permite la comunicación SSL con componentes que utilizan JAPI para la comunicación. Para establecer la comunicación SSL, los clientes y las herramientas de Essbase almacenan el certificado raíz de la CA que ha firmado los certificados del servidor y del agente de Essbase.

### Certificados necesarios y su ubicación

Oracle recomienda el uso de certificados de CA de terceros conocidas para activar para SSL Essbase en un entorno de producción. Puede usar los certificados autofirmados predeterminados para realizar pruebas.

 **Nota:**

Essbase soporta el uso de certificados con comodín, lo que puede proteger varios subdominios con un certificado SSL. El uso de un certificado con comodín puede reducir el tiempo y el costo de gestión.

Los certificados con comodín no se pueden usar si está activada la comprobación del nombre de host.

Necesita los siguientes certificados:

- Un certificado de CA raíz.  
Los componentes que usen Essbase RTC para establecer una conexión a Essbase necesitan que el certificado de autoridad de certificación raíz se almacene en una cartera de Oracle. Los componentes que usen JAPI para establecer una conexión necesitan que el certificado de CA raíz se almacene en un almacén de claves Java. En la tabla siguiente se indican los certificados necesarios y sus ubicaciones.

 **Nota:**

No tiene que instalar un certificado de CA raíz si está usando certificados de una CA de terceros conocida cuyo certificado raíz ya esté instalado en Oracle Wallet.

- Certificado firmado para el servidor de Essbase y el agente de Essbase.

**Tabla 2-4 Certificados necesarios y sus ubicaciones**

| Componente <sup>1</sup>                                          | Almacén de claves                                                                                   | Certificado <sup>2</sup>                                                                                                                          |
|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| MaxL                                                             | Oracle Wallet                                                                                       | Certificado de CA raíz                                                                                                                            |
| Servidor de Administration Services                              | Oracle Wallet                                                                                       | Certificado de CA raíz                                                                                                                            |
| Provider Services                                                | Oracle Wallet                                                                                       | Certificado de CA raíz                                                                                                                            |
| Base de datos de Oracle Enterprise Performance Management System | Oracle Wallet                                                                                       | Certificado de CA raíz                                                                                                                            |
| Planning                                                         | <ul style="list-style-type: none"> <li>• Oracle Wallet</li> <li>• Almacén de claves Java</li> </ul> | Certificado de CA raíz                                                                                                                            |
| Financial Management                                             | Almacén de claves Java                                                                              | Certificado de CA raíz                                                                                                                            |
| Essbase (servidor y agente) <sup>3</sup>                         | <ul style="list-style-type: none"> <li>• Oracle Wallet</li> <li>• Almacén de claves Java</li> </ul> | <ul style="list-style-type: none"> <li>• Certificado de CA raíz</li> <li>• Certificado firmado para el servidor y el agente de Essbase</li> </ul> |
| Repositorio de Servicios compartidos de Oracle Hyperion          |                                                                                                     |                                                                                                                                                   |



**Tabla 2-4 (Continuación) Certificados necesarios y sus ubicaciones**

| Componente <sup>1</sup>                                                                                                                | Almacén de claves | Certificado <sup>2</sup> |
|----------------------------------------------------------------------------------------------------------------------------------------|-------------------|--------------------------|
| <sup>1</sup> Solo necesita una instancia del almacén de claves para soportar varios componentes que usen un almacén de claves similar. |                   |                          |
| <sup>2</sup> Varios componentes pueden usar un certificado raíz instalado en un almacén de claves.                                     |                   |                          |
| <sup>3</sup> Los certificados se deben instalar en la instancia de Oracle Wallet predeterminada y en el almacén de claves Java.        |                   |                          |

## Instalación y despliegue de componentes de Essbase

El proceso de configuración permite seleccionar un puerto de agente seguro (el valor predeterminado es 6423), que puede cambiar al configurar Oracle Essbase. De forma predeterminada, el proceso de despliegue instala los certificados autofirmados necesarios para crear un despliegue seguro funcional para las pruebas.

EPM System Installer instala una instancia de Oracle Wallet y un certificado autofirmado en *ARBOR\_PATH* en el equipo que aloja la instancia de Essbase si se instala Oracle HTTP Server. En despliegues de un solo host, todos los componentes de Essbase comparten este certificado.

## Uso de certificados CA de terceros de confianza para Essbase

### Creación de solicitudes de certificados y obtención de certificados

Genere una solicitud de certificado para obtener un certificado para el servidor que aloja el servidor de Oracle Essbase y el agente de Essbase. Una solicitud de certificado contiene información cifrada específica de su nombre común (CN=) del servidor. Usted envía la solicitud del certificado a una autoridad de firma para obtener un certificado SSL.

Utilice una herramienta como keytool u Oracle Wallet Manager para crear una solicitud de certificado. Para obtener información detallada sobre la creación de una solicitud de certificado, consulte la documentación de la herramienta que esté usando.

### Ejemplos utilizando la herramienta de claves:

Cree un almacén de claves Java (JKS) y genere una clave privada:

```
keytool.exe -genkey -dname "cn=myserver, ou=EPM, o=Oracle, c=US"
-alias essbase_ssl -keypass password -keystore
C:\oracle\Middleware\EPMSys11R1\ssl\EPM.JKS -storepass password
-validity 365 -keyalg RSA -keysize 2048 -sigalg SHA256withRSA -noprompt
```

Genere una solicitud de certificado:

```
keytool -certreq -alias essbase_ssl -file
C:\oracle\Middleware\EPMSys11R1\ssl\essbase_server.csr -keypass password
-keystore C:\oracle\Middleware\EPMSys11R1\ssl\EPM.JKS -storepass password
```

Exporte su clave privada (necesitará la utilidad `openssl` para realizar estos pasos):

1. `openssl.exe pkcs12 -in C:\oracle\Middleware\EPMSys11R1\ssl\EPM.JKS -passin pass:password -legacy -nocerts -out c:\Apache24\ssl\Apache24.key -passout pass:password`
2. Firme la Solicitud de certificado que se acaba de generar utilizando su CA (autoridad de certificación) y péguela en el siguiente archivo:  
C:\oracle\Middleware\EPMSys11R1\ssl\essbase.cer.

### Obtención e instalación del certificado de CA raíz

El certificado de CA raíz verifica la validez del certificado que se usa para soportar SSL. Contiene la clave pública con la que se hace coincidir la clave privada que se ha usado para verificar el certificado. Puede obtener el certificado de CA raíz de la autoridad de certificación que haya firmado sus certificados SSL.

Instale el certificado raíz de la CA que haya firmado el certificado de servidor de Essbase en clientes que conecten al servidor o al agente de Essbase. Asegúrese de que el certificado raíz esté instalado en el almacén de claves adecuado para el cliente. Consulte [Certificados necesarios y su ubicación](#).



#### Nota:

Varios componentes pueden usar un certificado CA raíz instalado en un equipo de servidor.

### Instalación de certificados firmados por CA

Para instalar certificados firmados por CA, consulte los siguientes enlaces:

- [Configuración de la conexión TLS de Weblogic TLS para Essbase](#)
- [Actualización de certificados TLS](#)

Actualice el archivo `tls.properties` ubicado en

```
%EPM_HOME%\essbase\bin\tls_tools.properties:
certCA=c:\ssl\ca.crt;c:\ssl\intermediate.crt;c:\ssl\
\essbase.key;c:\ssl\essbase.cer;
```

Donde:

```
C:\ssl\ca.crt - root CA certificate.
C:\ssl\intermediate.crt - intermediate CA certificate.
C:\ssl\essbase.key - your private key generated in the previous step.
C:\ssl\essbase.cer - your server's signed certificate issued by your
CA.
```

Ejecute lo siguiente para actualizar el servidor de Essbase con los nuevos certificados:

```
set ORACLE_HOME=c:\OracleSSL
set EPM_HOME=%ORACLE_HOME%
set WL_HOME=%ORACLE_HOME%\wlserver
set JAVA_HOME=%ORACLE_HOME%\jdk
```

```
set DOMAIN_HOME=%ORACLE_HOME%\user_projects\domains\essbase_domain
%EPM_HOME%\essbase\bin\tls_tools.properties:
%ORACLE_HOME%\jdk\bin\java.exe -Xmx256m -jar %ORACLE_HOME%
\essbase\lib\tlsTools.jar %EPM_HOME%\essbase\bin\tls_tools.properties
```

### Actualización de la configuración Essbase de Essbase

Puede personalizar la configuración de SSL para el servidor y los clientes de Essbase especificando valores para ellos en `essbase.cfg`.

- Configuración para activar el modo seguro
- Configuración para activar el modo Clear
- Modo preferido para comunicarse con los clientes (solo usado por los clientes)
- Puerto seguro
- Conjuntos de cifrado
- Ruta de Oracle Wallet

#### Nota:

En `essbase.cfg`, asegúrese de agregar los parámetros necesarios que faltan, en concreto, `EnableSecureMode` y `AgentSecurePort`, y establezca sus valores.

Para actualizar `essbase.cfg` ubicado en:

```
ESSBASE_DOMAIN_HOME\config\fmwconfig\essconfig\essbase
```

1. Introduzca la configuración según sea necesario. Se usa de forma implícita la configuración predeterminada de Essbase. Si necesita cambiar el comportamiento predeterminado, agregue la configuración para el comportamiento personalizado en `essbase.cfg`. Por ejemplo, `EnableClearMode` se aplica de forma predeterminada, por el que se activa el servidor de Essbase para comunicarse a través de un canal no cifrado. Para desactivar la disponibilidad del servidor de Essbase a través de un canal no cifrado, debe especificar `EnableClearMode FALSE` en `essbase.cfg`. Consulte la siguiente tabla:

**Tabla 2-5 Configuración de SSL de Essbase**

| Valor                                    | Descripción <sup>1</sup>                                                                                                                                                                                                                                                                                                         |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>EnableClearMode<sup>2</sup></code> | Activa la comunicación sin cifrado entre las aplicaciones de Essbase y el agente de Essbase. Si esta propiedad está establecida en <code>FALSE</code> , Essbase no gestiona solicitudes que no sean SSL.<br><b>Valor predeterminado:</b> <code>EnableClearMode TRUE</code><br><b>Ejemplo:</b> <code>EnableClearMode FALSE</code> |
| <code>EnableSecureMode</code>            | Activa la comunicación cifrada de SSL entre el cliente de Essbase y el agente de Essbase. Esta propiedad se debe establecer en <code>TRUE</code> para soportar SSL.<br><b>Valor predeterminado:</b> <code>FALSE</code><br><b>Ejemplo:</b> <code>EnableSecureMode TRUE</code>                                                     |

**Tabla 2-5 (Continuación) Configuración de SSL de Essbase**

| Valor                            | Descripción <sup>1</sup>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SSLCipherSuites                  | <p>Lista de conjuntos de cifrado, en orden de preferencia, que usar para la comunicación SSL. El agente de Essbase usa uno de los conjuntos de cifrado para la comunicación SSL. Al primer conjunto de cifrado se le asigna la máxima prioridad cuando el agente elige un conjunto de cifrado.</p> <p><b>Valor predeterminado:</b> <code>SSL_RSA_WITH_RC4_128_MD5</code></p> <p><b>Ejemplo:</b> <code>SSLCipherSuites</code><br/><code>SSL_RSA_WITH_AES_256_CBC_SHA256,SSL_RSA_WITH_AES_256_GCM_SHA384</code></p>              |
| APSPRESOLVER                     | <p>URL de Oracle Hyperion Provider Services. Si utiliza varios servidores de Provider Services, separe cada URL con un punto y coma.</p> <p><b>Ejemplo:</b> <code>https://exampleAPShost1:PORT/essbase;https://exampleAPShost2:PORT/essbase</code></p>                                                                                                                                                                                                                                                                         |
| AgentSecurePort                  | <p>Puerto seguro en el que escucha el agente.</p> <p><b>Valor predeterminado:</b> <code>6423</code></p> <p><b>Ejemplo:</b> <code>AgentSecurePort 16001</code></p>                                                                                                                                                                                                                                                                                                                                                              |
| WalletPath                       | <p>Ubicación de la instancia de Oracle Wallet (menos de 1.024 caracteres) que almacena el certificado de la CA raíz y del certificado firmado.</p> <p><b>Valor predeterminado:</b> <code>ARBORPATH/bin/wallet</code></p> <p><b>Ejemplo:</b> <code>WalletPath/usr/local/wallet</code></p>                                                                                                                                                                                                                                       |
| ClientPreferredMode <sup>3</sup> | <p>Modo (Secure o Clear) para la sesión de cliente. Si esta propiedad está establecida en Secure, se usa el modo SSL para todas las sesiones. Si esta propiedad se establece en Clear, se elige el transporte en función de si la solicitud de inicio de sesión del cliente contiene la palabra clave de transporte seguro. Consulte <a href="#">Establecimiento de una conexión SSL por sesión</a>.</p> <p><b>Valor predeterminado:</b> <code>CLEAR</code></p> <p><b>Ejemplo:</b> <code>ClientPreferredMode SECURE</code></p> |

- <sup>1</sup> El valor predeterminado se aplica si estas propiedades no están disponibles en `essbase.cfg`.
- <sup>2</sup> Essbase deja de estar operativo si `EnableClearMode` y `EnableSecureMode` se definen como `FALSE`.
- <sup>3</sup> Los clientes usan esta opción para determinar si se debe establecer una conexión segura o no segura con Essbase.

2. Guarde y cierre `essbase.cfg`.

### Actualización de nodos de Essbase distribuidos para SSL



**Nota:**

Esta sección se aplica solamente a despliegues distribuidos de Essbase

Asegúrese de que la carpeta de la cartera (por ejemplo, `WalletPath/usr/local/wallet`) que contiene el certificado de autoridad de certificación raíz y el certificado firmado se encuentra en la ubicación necesaria en cada nodo distribuido.

**1. Importe todos los certificados de CA nuevos utilizando las herramientas de TLS.**

Para obtener más información, consulte los siguientes enlaces:

- [Configuración de la conexión TLS de Weblogic TLS para Essbase](#)
- [Actualización de certificados TLS](#)

**2. Vaya a la ubicación de origen:**

`ESSBASE_DOMAIN_HOME\config\fmwconfig\essconfig\essbase` y modifique las siguientes propiedades en el archivo `essbase.properties`:

- `essbase.ssleverywhere=true`
- `olap.server.ssl.alwaysSecure=true`
- `APRESOLVER=APS_URL`  
Reemplace `APS_URL` por la URL de Provider Services. Si utiliza varios servidores de Provider Services, separe cada URL utilizando un punto y coma.  
  
`https://exampleAPShost1:PORT/essbase;https://exampleAPShost2:PORT/essbase.`

**3. Copie la carpeta `Wallet`, la carpeta `Walletssl`, el archivo `essbase.cfg` y el archivo `essbase.properties` en las siguientes rutas de destino.**

**Tabla 2-6 Rutas de destino**

| Rutas de destino                                                             | Wallet | Walletssl | essbase.cfg | essbase.properties |
|------------------------------------------------------------------------------|--------|-----------|-------------|--------------------|
| <code>EPM_ORACLE_HOME\common\EssbaseRTC-21c\11.1.2.0\bin</code>              | Sí     | Sí        | Sí          | Sí                 |
| <code>EPM_ORACLE_HOME\common\EssbaseJavaAPI-21c\11.1.2.0\bin</code>          | Sí     | Sí        | Sí          | Sí                 |
| <code>ESSBASE_DOMAIN_HOME\config\fmwconfig\essconfig\aps</code>              | Sí     | Sí        | Sí          | Sí                 |
| <code>ESSBASE_DOMAIN_HOME\config\fmwconfig\essconfig\essbase</code>          | Sí     | Sí        | Sí          | Sí                 |
| <code>MIDDLEWARE_HOME\essbase\products\Essbase\template_files\essbase</code> | Sí     | Sí        | Sí          | Sí                 |
| <code>MIDDLEWARE_HOME\essbase\products\Essbase\EssbaseServer\bin</code>      | Sí     | Sí        | Sí          | Sí                 |
| <code>MIDDLEWARE_HOME\essbase\products\Essbase\aps\bin</code>                | Sí     | Sí        | Sí          | Sí                 |
| <code>MIDDLEWARE_HOME\essbase\products\Essbase\eas</code>                    | Sí     | Sí        | Sí          | Sí                 |
| <code>MIDDLEWARE_HOME\essbase\common\EssbaseJavaAPI\bin</code>               | Sí     | Sí        | Sí          | Sí                 |

Tabla 2-6 (Continuación) Rutas de destino

| Rutas de destino                                                                                                                                                                                                                                                                                                                                                                      | Wallet | Wallet<br>ssl | essbase.cfg | essbase.<br>properties |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|---------------|-------------|------------------------|
| <p><b>Solo para Oracle Hyperion Financial Reporting</b><br/>EPM_ORACLE_HOME/products/<br/>financialreporting/bin/EssbaseJAPI/bin/</p> <p><b>Nota:</b> En entornos completos de Secure Sockets Layer, Financial Reporting necesita el nombre de cluster de Essbase para establecer una conexión. Se produce un fallo en la conexión si se utiliza el nombre de host para conectar.</p> | Sí     | Sí            | Sí          | Sí                     |
| <p><b>Solo para Oracle Hyperion Planning</b><br/>EPM_ORACLE_HOME/products/Planning/config/<br/>EPM_ORACLE_HOME/products/Planning/lib/</p>                                                                                                                                                                                                                                             | Sí     | Sí            | Sí          | Sí                     |

4. Defina las variables de entorno:

- **Windows:** Cree una nueva variable de sistema llamada `API_DISABLE_PEER_VERIFICATION` y establezca su valor en 1.
- **Linux:** Agregue la directiva `API_DISABLE_PEER_VERIFICATION=1` en `setCustomParamsPlanning.sh`.

**Personalización de las propiedades SSL de clientes de JAPI**

Hay varias propiedades predeterminadas predefinidas para los componentes de Essbase que se basan en JAPI. Las propiedades predeterminadas se pueden sustituir mediante la inclusión de propiedades en `essbase.properties`.



**Nota:**

Solo unas pocas propiedades SSL identificadas en la siguiente tabla se externalizan en `essbase.properties`. Debe agregar las propiedades que no estén externalizadas.

Para actualizar las propiedades SSL de los clientes de JAPI:

1. Con un editor de texto, abra `EPM_ORACLE_HOME/common/EssbaseJavaAPI-21c/11.2.0/bin/essbase.properties`.
2. Actualice las propiedades según sea necesario. Consulte la tabla siguiente para consultar una descripción de las propiedades de cliente JAPI personalizable. Si no se ha incluido una propiedad que desee en `essbase.properties`, agréguela.

**Tabla 2-7 Propiedades de SSL predeterminadas para clientes de JAPI**

| Propiedad                                      | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>olap.server.ssl.alwaysSecure</code>      | <p>Establece el modo que deben usar los clientes en todas las instancias de Essbase. Cambie el valor de esta propiedad a <code>true</code> para aplicar el modo SSL.</p> <p><b>Valor predeterminado:</b> <code>false</code></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <code>olap.server.ssl.securityHandler</code>   | <p>Nombre de paquete para gestionar el protocolo. Puede cambiar este valor para indicar otro identificador.</p> <p><b>Valor predeterminado:</b> <code>java.protocol.handler.pkgs</code></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <code>olap.server.ssl.securityProvider</code>  | <p>Oracle utiliza la implantación del protocolo SSL de Sun. Puede cambiar este valor para indicar otro proveedor.</p> <p><b>Valor predeterminado:</b><br/><code>com.sun.net.ssl.internal.www.protocol</code></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <code>olap.server.ssl.supportedCiphers</code>  | <p>Lista separada por comas de cifrados adicionales que se van a activar para una comunicación segura. Debe especificar solo cifrados que soporte Essbase.</p> <p><b>Ejemplo:</b><br/><code>SSL_RSA_WITH_AES_256_CBC_SHA256,SSL_RSA_WITH_AES_256_GCM_SHA384</code></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <code>olap.server.ssl.trustManagerClass</code> | <p>La clase <code>TrustManager</code> que usar para validar el certificado SSL mediante la verificación de la firma y la comprobación de la fecha de caducidad del certificado. De manera predeterminada, esta propiedad no se establece para aplicar todas las comprobaciones de verificación.</p> <p>Para no aplicar comprobaciones de verificación, establezca el valor de este parámetro en <code>com.essbase.services.olap.security.EssDefaultTrustManager</code>, que es la clase <code>TrustManager</code> predeterminada que permite que todas las comprobaciones de validación sean correctas.</p> <p>Para implantar una clase <code>TrustManager</code> personalizada, especifique un nombre de clase completo de la clase <code>TrustManager</code> que implante la interfaz <code>javax.net.ssl.X509TrustManager</code>.</p> <p><b>Ejemplo:</b><code>com.essbase.services.olap.security.EssDefaultTrustManager</code></p> |

3. Guarde y cierre `essbase.properties`.
4. Reinicie todos los componentes de Essbase.

## Establecimiento de una conexión SSL por sesión

Los componentes de Oracle Essbase, por ejemplo, MaxL, pueden controlar SSL en el nivel de sesión mediante la conexión al agente de Essbase con `secure` como palabra clave de transporte. Por ejemplo, puede establecer una conexión segura entre MaxL y el agente de

Essbase mediante la ejecución de uno de los siguientes comandos desde una consola de MaxL:

```
login admin example_password on hostA:PORT:secure
```

```
login admin example_password on hostA:secure
```

El control por sesión tiene prioridad sobre los valores de configuración especificados en `essbase.cfg`. Si no se especifica ninguna palabra clave de transporte, los clientes de Essbase usan el valor establecido para `ClientPreferredMode` para determinar si iniciar una conexión segura con Essbase. Si la opción `ClientPreferredMode` no está establecida en `Secure`, la comunicación se produce a través de un canal no seguro.



# 3

## Habilitación del inicio de sesión único con agentes de seguridad

### Consulte también:

- [Métodos de inicio de sesión único soportados](#)
- [Inicio de sesión único desde Oracle Access Manager](#)
- [OracleAS Single Sign-on](#)
- [Protección de productos de EPM System para el inicio de sesión único](#)
- [Inicio de sesión único basado en cabecera con productos de administración de identidad](#)
- [Configuración de EPM System para inicio de sesión único basado en cabecera con Oracle Identity Cloud Services](#)
- [Inicio de sesión único de SiteMinder](#)
- [Inicio de sesión único en Kerberos](#)
- [Configuración de EPM System para inicio de sesión único](#)
- [Opciones de inicio de sesión único para Smart View](#)

## Métodos de inicio de sesión único soportados

El inicio de sesión único exige que la solución de gestión de identidad web transfiera el nombre de inicio de sesión de los usuarios autenticados a Oracle Enterprise Performance Management System. Puede usar los siguientes métodos de EPM System estándar para integrar EPM System con soluciones de inicio de sesión basadas en web comerciales y personalizadas.

- [Cabecera HTTP](#)
- [Clase de inicio de sesión personalizada](#)
- [Cabecera de autorización HTTP](#)
- [Obtener usuario remoto de solicitud HTTP](#)
- [Autenticación basada en cabecera con productos de administración de identidad](#)

### ▲ Atención:

Como medida de seguridad, Oracle recomienda que implante la autenticación de certificado de cliente (SSL bidireccional) entre el servidor web y el servidor de aplicaciones si su organización utiliza métodos que lleven la identidad de usuario en la cabecera para la propagación de la identidad.

## Cabecera HTTP

Si está usando Oracle Single Sign-on (OSSO), SiteMinder u Oracle Access Manager como solución de gestión de identidad web, la seguridad de EPM System selecciona automáticamente la cabecera HTTP personalizada para transferir el nombre de inicio de sesión de los usuarios autenticados a los componentes de EPM System.

El nombre de inicio de sesión de un usuario de productos de EPM System viene determinado por el valor `Login Attribute` especificado al configurar los directorios de usuario en Servicios compartidos de Oracle Hyperion. Consulte la sección sobre configuración de OID, Active Directory y otros directorios de usuarios basados en LDAP en la *Guía de administración de seguridad de usuarios de Oracle Enterprise Performance Management System* para obtener una descripción breve de `Login Attribute`.

La cabecera HTTP debe contener el valor del atributo que se haya establecido como atributo de inicio de sesión. Por ejemplo, si `uid` es el valor de `Login Attribute`, la cabecera HTTP deberá llevar el valor de dicho atributo `uid`.

Consulte la documentación suministrada con la solución de gestión de identidades web para obtener información detallada sobre la definición y la generación de cabeceras HTTP personalizadas.

La seguridad de EPM System analiza la cabecera HTTP y valida el nombre de inicio de sesión que lleva en los directorios de usuario configurados en Servicios compartidos.

## Clase de inicio de sesión personalizada

Cuando un usuario inicia sesión, la solución de gestión de identidades web autentifica al usuario contrastando sus datos con un servidor de directorios y encapsula las credenciales de dicho usuario en un mecanismo de SSO a fin de activar el inicio de sesión único en sistemas descendente. Si la solución de gestión de identidades web utiliza un mecanismo no soportado por los productos de EPM System o si el valor del `Login Attribute` no se encuentra disponible en el mecanismo de inicio de sesión único, deberá utilizar una clase de inicio de sesión personalizada para derivar y transferir el valor del `Login Attribute` a los productos de EPM System.

Con una clase de inicio de sesión personalizada se permite a EPM System integrar con agentes de seguridad que usen la autenticación basada en certificados X509. Para utilizar este mecanismo de autenticación se requiere la implantación de API de Servicios compartidos estándar a fin de definir la interfaz de inicio de sesión único entre los componentes de EPM System y la solución de gestión de identidades web. La clase de inicio de sesión personalizada debe pasar el valor del atributo de inicio de sesión a los productos de EPM System. Consulte la sección sobre configuración de OID, Active Directory y otros directorios de usuarios basados en LDAP en *Guía de administración de seguridad de usuarios de Oracle Enterprise Performance Management System* para obtener una descripción breve de `Login Attribute`. Para conocer los pasos de implantación y código de ejemplo, consulte [Implantación de una clase de inicio de sesión personalizada](#).

Para poder utilizar una clase de inicio de sesión personalizada (el nombre predeterminado es

`com.hyperion.css.sso.agent.X509CertificateSecurityAgentImpl`), debe encontrarse disponible una implantación de la interfaz

`com.hyperion.css.CSSSecurityAgentIF` en la ruta de clase. `CSSSecurityAgentIF`

define el método que utiliza la función de recuperación del nombre de usuario y la contraseña (opcional). Si la interfaz devuelve una contraseña nula, la autenticación de seguridad considerará al proveedor como usuario de confianza y verificará su existencia entre los proveedores configurados. Si la interfaz devuelve un valor no nulo para la contraseña, EPM System intentará autenticar la solicitud utilizando el nombre de usuario y la contraseña devueltas por esta implantación.

`CSSSecurityAgentIF` comprende dos métodos: `getUserName` y `getPassword`.

### Método `getUserName`

Este método devuelve el nombre de usuario para su autenticación.

```
java.lang.String getUserName(
 javax.servlet.http.HttpServletRequest req,
 javax.servlet.http.HttpServletResponse res)
 throws java.lang.Exception
```

El parámetro `req` identifica la solicitud HTTP que lleva la información necesaria para determinar el nombre de usuario. El parámetro `res` no se utiliza (configuración predefinida para compatibilidad con versiones anteriores).

### Método `getPassword`

Este método devuelve una contraseña en texto no cifrado para la autenticación. La recuperación de la contraseña es opcional.

```
java.lang.String getPassword(
 javax.servlet.http.HttpServletRequest req,
 javax.servlet.http.HttpServletResponse res)
 throws java.lang.Exception
```

El parámetro `req` identifica la solicitud HTTP que lleva la información necesaria para determinar la contraseña. El parámetro `res` no se utiliza (configuración predefinida para compatibilidad con versiones anteriores).

### Cabecera de autorización HTTP

La seguridad de EPM System soporta el uso de una cabecera de autorización HTTP para transferir el valor de `Login Attribute` a los productos de EPM System desde las soluciones de gestión de identidad web. Los productos de EPM System analizarán la cabecera de autorización para recuperar el nombre de inicio de sesión del usuario.

### Obtener usuario remoto de solicitud HTTP

La seguridad de EPM System soporta el uso de una solicitud HTTP para transferir el valor de `Login Attribute` a los productos de EPM System desde las soluciones de gestión de identidad web. Utilice este método de inicio de sesión único si la solución de gestión de identidades web transfiere la solicitud HTTP que contiene el valor de `Login Attribute`, que se establece con la función `setRemoteUser`.

### Autenticación basada en cabecera con productos de administración de identidad

EPM System soporta cualquier producto de administración de identidad, como Oracle Identity Cloud Services, Microsoft Azure AD, Okta, que soporten la autenticación basada en cabecera. El flujo de trabajo conceptual es el siguiente:

- Una puerta de enlace de aplicación que actúa como proxy inverso protege los componentes de EPM System al restringir el acceso a la red no autenticado.
- La puerta de enlace de la aplicación intercepta las solicitudes HTTPS a componentes de EPM System y garantiza que el producto de administración de identidad autentique los usuarios antes de reenviar las solicitudes a componentes de EPM System.
- Mientras se reenvían las solicitudes a componentes de EPM System, la puerta de enlace de aplicación propaga la identidad de usuario autenticado al componente de EPM System a través de solicitudes de cabecera HTTP.

Para soportar este escenario de autenticación, se debe configurar EPM System para trabajar con la identidad de usuario autenticada que se haya propagado a través de las solicitudes de cabecera HTTP.

## Inicio de sesión único desde Oracle Access Manager

Oracle Enterprise Performance Management System se integra con Oracle Access Manager al aceptar una cabecera HTTP personalizada (nombre predeterminado `HYPLOGIN`) que contenga el valor de atributo de inicio de sesión. El atributo de inicio de sesión se establece al configurar un directorio de usuario externo en Servicios compartidos de Oracle Hyperion. Consulte la sección sobre configuración de OID, Active Directory y otros directorios de usuarios basados en LDAP en *Guía de administración de seguridad de usuarios de Oracle Enterprise Performance Management System* para obtener una descripción breve de `Login Attribute`.

Puede usar cualquier nombre de cabecera que proporcione el valor del atributo de inicio de sesión a EPM System. Use el nombre de cabecera al configurar Servicios compartidos para el inicio de sesión único de Oracle Access Manager.

EPM System usa el valor del atributo de inicio de sesión para autenticar en el directorio de usuario configurado (en este caso, el directorio de usuario en el que Oracle Access Manager autentifica a los usuarios) y, a continuación, genera un símbolo de inicio de sesión único de EPM que activa dicho inicio de sesión en EPM System. La información de aprovisionamiento del usuario se comprueba en el directorio nativo para autorizar al usuario a los recursos de EPM System.



#### Nota:

La consola de Oracle Essbase Administration Services, que es un cliente grueso, no soporta el inicio de sesión único desde Oracle Access Manager.

Encontrará información sobre la configuración de Oracle Access Manager y la realización de tareas como la configuración de la cabecera HTTP y los dominios de políticas en la documentación de Oracle Access Manager. En esta guía se asume que

hay un despliegue de Oracle Access Manager en funcionamiento donde ha realizado las siguientes tareas:

- Configurar los dominios de políticas necesarios para los componentes de EPM System.
- Configurar una cabecera HTTP para transferir el valor del atributo de inicio de sesión a EPM System.
- Proteger los recursos de EPM System mostrados en [Recursos que proteger](#). Oracle Access Manager pide las solicitudes para acceder a los recursos protegidos.
- Desproteger los recursos de EPM System mostrados en [Recursos que desproteger](#). Oracle Access Manager pide las solicitudes para acceder a los recursos desprotegidos.

Para configurar EPM System para el inicio de sesión único desde Oracle Access Manager:

1. Agregue el directorio de usuario que Oracle Access Manager usa para autenticar a los usuarios como un directorio de usuario externo en EPM System. Consulte la sección sobre configuración de OID, Active Directory y otros directorios de usuarios basados en LDAP en *Guía de administración de seguridad de usuarios de Oracle Enterprise Performance Management System*.

 **Nota:**

Asegúrese de que la casilla de verificación **De confianza** de la pantalla Información de conexión para indicar que el directorio de usuario es una fuente de inicio de sesión único de confianza.

2. Configure EPM System para el inicio de sesión único. Consulte [Configuración de EPM System para inicio de sesión único](#).

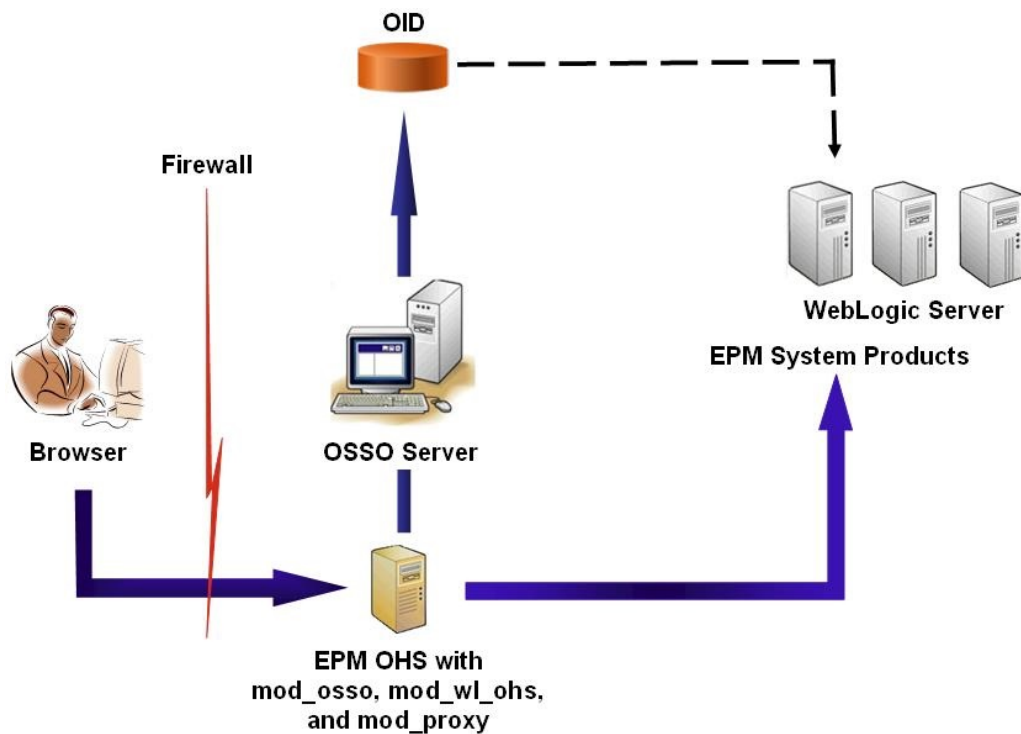
Seleccione Oracle Access Manager en la lista **Agente o proveedor de inicio de sesión único**. Si la cabecera HTTP de Oracle Access Manager usa un nombre que no sea `HYPLOGIN`, introduzca el nombre de la cabecera personalizada en el cuadro de texto junto a la lista **Mecanismo de inicio de sesión único**.

3. Solo Oracle Data Relationship Management:
  - a. Configure Data Relationship Management para la autenticación de Servicios compartidos.
  - b. Active el inicio de sesión único en la consola de Data Relationship Management.  
Consulte la documentación de Data Relationship Management para obtener información detallada.

## OracleAS Single Sign-on

La solución OracleAS Single Sign-on (OSSO) ofrece acceso con inicio de sesión único a las aplicaciones web mediante Oracle Internet Directory (OID) como directorio de usuario. Los usuarios utilizan un nombre de usuario y una contraseña definidos en un OID para iniciar sesión en los productos de Oracle Enterprise Performance Management System.

### Flujo de procesos



El proceso de OSSO:

1. Con una URL de EPM System, por ejemplo, `http://OSSO_OHS_Server_NAME:OSSO_OHS_Server_PORT/interop/index.jsp`, los usuarios acceden a un componente de EPM System que esté definido como aplicación protegida de OSSO.
2. Como la URL está protegida con OSSO, `mod_osso`, desplegado en Oracle HTTP Server, intercepta la solicitud. Con `mod_osso`, Oracle HTTP Server comprueba si hay una cookie válida. Si no hay una cookie válida disponible en la solicitud, Oracle HTTP Server redirige a los usuarios al servidor de OSSO, que solicita a los usuarios las credenciales, que se autentica en OID.
3. El servidor de OSSO crea `obSSOCookie` y devuelve el control al módulo `mod_osso` en la instancia de Oracle HTTP Server, que establece `obSSOCookie` en el explorador. También redirige la solicitud al recurso de EPM System mediante `mod_wl_ohs` (Oracle WebLogic Server). Antes de reenviar la solicitud a un recurso de EPM System, Oracle HTTP Server establece la cabecera de `Proxy-Remote-User`, que usa la seguridad de EPM System para activar el inicio de sesión único.
4. El componente EPM System verifica que el usuario cuya identidad se recupera de `Proxy-Remote-User` esté presente en OID. Para que este proceso funcione, la instancia de OID que se haya configurado con el servidor de OSSO se debe configurar como directorio de usuario externo en Servicios compartidos de Oracle Hyperion.

### Requisitos

1. Una infraestructura de Oracle Application Server totalmente funcional.

Para establecer una infraestructura de Oracle Application Server, instale y configure Oracle Identity Management Infrastructure 10.1.4. Asegúrese de que

OSSO está activado. En la instalación de Oracle Identity Management Infrastructure 10.1.4 se incluyen los siguientes componentes para soportar OSSO.

- Servidor de Oracle 10g OSSO.
- Una instancia de OID, que el servidor de OSSO usa para validar las credenciales. Consulte las guías siguientes:
  - *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*
  - *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*
- Oracle HTTP Server como frontend para el servidor de OSSO. Esta instalación incluye `mod_osso`, que permite definir las aplicaciones de socio para OSSO.

 **Nota:**

Esta instancia de Oracle HTTP Server forma parte de la infraestructura de OSSO; no se usa directamente para configurar OSSO para los componentes de EPM System.

Durante el proceso de instalación, asegúrese de que `mod_osso` se haya registrado con el servidor de OSSO como aplicación de socio.

2. Un despliegue de EPM System totalmente funcional.  
Al configurar el servidor web para los componentes de EPM System, EPM System Configurator configura `mod_wl_ohs.conf` en Oracle HTTP Server para realizar proxy de las solicitudes a WebLogic Server:

## Prueba del despliegue

Tras finalizar el despliegue SSL, verifique que todo funciona.

Para probar el despliegue:

1. Con un explorador, acceda a la URL segura de Oracle Hyperion Enterprise Performance Management Workspace:

Si ha usado `epm.myCompany.com` como alias de servidor para la comunicación externa y 4443 como puerto SSL, la URL de EPM Workspace URL será

`https://epm.myCompany.com:4443/workspace/index.jsp`

2. En la pantalla de inicio de sesión, introduzca un nombre de usuario y contraseña.
3. Haga clic en **Iniciar sesión**.
4. Verifique que puede acceder de forma segura a los componentes de Oracle Enterprise Performance Management System desplegados.

## Activación de OSSO para EPM System

En esta sección se asume que ha configurado completamente la infraestructura de OSSO. Consulte la *Oracle Application Server Administrator's Guide*.

## Registro del servidor web de EPM System como aplicación de socio

La herramienta de registro de inicio de sesión único de Oracle Identity Manager (`ssoreg.sh` o `ssoreg.bat`) se usa para registrar el servidor web de Oracle Enterprise Performance Management System como aplicación de socio en Oracle HTTP Server que aplica front-end al servidor de OSSO.

Realice este procedimiento en el servidor que aloja la instancia de Oracle HTTP Server que aplica front-end al servidor de OSSO. Con este proceso se genera y almacena un `osso.conf` ofuscado en la ubicación que elija.

Para registrar el servidor web de EPM System como aplicación de socio:

1. Abra una consola en el servidor que aloja la instancia de Oracle HTTP Server que aplica front-end al servidor de OSSO y vaya al directorio `ORACLE_HOME/sso/bin` de Oracle HTTP Server, por ejemplo a `C:/OraHome_1/sso/bin` (Windows).
2. Ejecute un comando similar al siguiente con la opción `-remote_midtier`:

```
ssoreg.bat -site_name epm.myCompany.com
-mod_osso_url http://epm.myCompany.com:19400
-config_mod_osso TRUE
-update_mode CREATE
-remote_midtier
-config_file C:\OraHome_1\myFiles\osso.conf
```

A continuación se explican los parámetros usados en este comando. En esta descripción, la aplicación de socio hace referencia a la instancia de Oracle HTTP Server que se usa como servidor web de EPM System.

- Con `-site_name` se identifica el sitio web de la aplicación de socio, por ejemplo, `epm.myCompany.com`.
- `-mod_osso_url` indica la dirección URL de la aplicación de socio, con formato `PROTOCOL://HOST_NAME:PORT`. Esta es la URL en la que el servidor web de EPM System acepta las solicitudes de cliente entrantes, por ejemplo, `http://epm.myCompany.com:19000`.
- Con `-config_mod_osso` se identifica que la aplicación de socio usa `mod_osso`. Debe incluir el parámetro `config_mod_osso` para generar `osso.conf`.
- Con `-update_mode` se indica el modo de actualización. Utilice `CREATE`, el valor predeterminado, para generar un nuevo registro.
- Con `-remote_midtier` se especifica que la aplicación de socio de `mod_osso` está en un nivel medio remoto. Utilice esta opción cuando la aplicación de socio esté en otro directorio `ORACLE_HOME` distinto al servidor de OSSO.
- `-virtualhost` indica que la dirección URL de la aplicación de socio es un host virtual. No use este parámetro si no está usando un host virtual. Si está registrando una dirección URL de aplicación de socio vinculada a un host virtual, debe definir el host virtual en `httpd.conf`. Consulte [Opcional: Definición del host virtual](#).
- `-config_file` indica la ruta donde se va a generar el archivo `osso.conf`.



### Opcional: Definición del host virtual

Si ha usado una dirección URL de host virtual al registrar la aplicación de socio, debe definir el host virtual al actualizar `httpd.conf` en la instancia de Oracle HTTP Server que se usa como servidor web de EPM System.

Para definir un host virtual:

1. Con un editor de texto, abra `EPM_ORACLE_INSTANCE/httpConfig/ohs/config/OHS/ohs_component/httpd.conf`.
2. Agregue una definición similar a la siguiente. En esta definición se asume que el servidor web se está ejecutando en el servidor virtual `epm.myCompany.com` del puerto `epm.myCompany.com:19400`. Modifique la configuración para adaptarla a sus necesidades.

```
NameVirtualHost epm.myCompany.com:19400
Listen 19400
<VirtualHost epm.myCompany.com:19400>
DocumentRoot "C:/Oracle/Middleware/user_projects/epmsystem1/httpConfig/ohs
/config/OHS/ohs_component/private-docs"
include "${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}
/${COMPONENT_NAME}/mod_osso.conf"
</VirtualHost>
```

### Creación de `mod_osso.conf`

Cree `mod_osso.conf` en la instancia de Oracle HTTP Server que aplica front-end al servidor web de EPM System.

Para crear `mod_osso.conf`:

1. Con un editor de texto, cree un archivo.
2. Copie el siguiente contenido en el archivo y modifíquelo para su entorno.

```
LoadModule osso_module C:/Oracle/Middleware/ohs/ohs/modules/mod_osso.so
<IfModule mod_osso.c>
OsoIpCheck off
OsoIdleTimeout off
OsoSecureCookies off
OsoConfigFile C:/Oracle/Middleware/user_projects/epmsystem1/
httpConfig/
ohs/config/OHS/ohs_component/osso/osso.conf
```

3. En la definición `<IfModule mod_osso.c>`, incluya definiciones de ubicación similares a las siguientes para identificar cada recurso que tenga previsto proteger con OSSO.

```
<Location /interop/>
require valid user
AuthType Oso
</Location>
</IfModule>
```

4. Guarde el archivo como `mod_osso.conf`.

### Reubicación de `osso.conf`

El proceso de registro del servidor web de EPM System como aplicación de socio (consulte [Registro del servidor web de EPM System como aplicación de socio](#)) crea un archivo `osso.conf` ofuscado en la ubicación identificada por la directiva `config_file`.

Para reubicar `osso.conf`:

1. Busque el archivo `osso.conf` que se ha creado al registrar el servidor web de EPM System como aplicación de socio (consulte [Registro del servidor web de EPM System como aplicación de socio](#)).
2. Copie `osso.conf` en el directorio (en la instancia de Oracle HTTP Server que aplica front-end al servidor OSSO) identificado por la propiedad `OssosConifgFile` definida en `mod_osso.conf` (consulte [Creación de `mod\_osso.conf`](#)).

### Configuración de EPM System para OSSO

Configure el OID que está integrado con la solución OSSO como directorio de usuario externo en EPM System y, a continuación, active el inicio de sesión único.

Para configurar EPM System para OSSO:

1. Configure la instancia de OID que utiliza la solución OSSO como directorio de usuario externo. Consulte la sección sobre configuración de OID, Active Directory y otros directorios de usuarios basados en LDAP en *Guía de administración de seguridad de usuarios de Oracle Enterprise Performance Management System*.
2. Active el inicio de sesión único en EPM System. [Configuración de EPM System para inicio de sesión único](#)

#### Nota:

Para configurar OSSO como solución de gestión de identidad, debe elegir **Other** en **Agente o proveedor de inicio de sesión único**, **Custom HTTP Header** en **Mecanismo de inicio de sesión único** e introduzca `Proxy-Remote-User` como nombre de la cabecera HTTP personalizada.

3. Aprovechone como mínimo un usuario de OID como administrador de Servicios compartidos de Oracle Hyperion.
4. Reinicie los productos de EPM System y las aplicaciones personalizadas que utilicen las API de seguridad de Shared Services.

#### Nota:

Asegúrese de que la instancia de OID configurada con Servicios compartidos se esté ejecutando antes de iniciar los productos de EPM System.

### Opcional: Activación de mensajes de depuración en el servidor de OSSO

Para registrar los mensajes de depuración en el servidor de OSSO, modifique `policy.properties`. Los mensajes de depuración se escriben en `ORACLE_HOME/sso/log/ssoServer.log`.

Para registrar los mensajes de depuración:

1. Con un editor de texto, abra `ORACLE_HOME/sso/conf/policy.properties`, por ejemplo, `C:\OraHome_1\sso\conf\policy.properties`, en el servidor de OSSO.
2. Establezca el valor de la propiedad `debugLevel` en `DEBUG`.

```
debugLevel = DEBUG
```

3. Guarde y cierre `policy.properties`.

### Opcional: Activación de mensajes de depuración para recursos protegidos

Para registrar los mensajes de depuración de OSSO para recursos protegidos con `mod_osso.conf`, modifique `httpd.conf` en el servidor web de EPM System. Los mensajes de depuración se escriben en `EPM_ORACLE_INSTANCE/httpConfig/ohs/diagnostics/logs/OHS/ohs_component/ohs_component.log`.

Para registrar los mensajes de depuración para los recursos protegidos:

1. Con un editor de texto, abra `EPM_ORACLE_INSTANCE/httpConfig/ohs/config/OHS/ohs_component/httpd.conf`.
2. Establezca el valor de la propiedad `OraLogSeverity` en `TRACE`.

```
OraLogSeverity TRACE:32
```

3. Guarde y cierre `httpd.conf`.

## Protección de productos de EPM System para el inicio de sesión único

Debe proteger los recursos de Oracle Enterprise Performance Management System de forma que las solicitudes de inicio de sesión único de los usuarios se redireccionen al agente de seguridad correspondiente (OAM, OSSO o SiteMinder).

Oracle HTTP Server utiliza `mod_osso` para redireccionar a los usuarios al servidor de OSSO. Esto sólo ocurre si se ha configurado la protección de las URL solicitadas en `mod_osso`. Consulte [Gestión de seguridad](#) en la *Oracle HTTP Server Administrator's Guide*.

Si desea obtener información sobre la protección de recursos para el inicio de sesión único de SiteMinder, consulte la documentación de SiteMinder.

### Solo para OAM : evitar que las cabeceras predeterminadas se agreguen a las respuestas

De forma predeterminada, OAM agrega dos cabeceras; Pragma: sin caché, y Control de caché: sin caché para las URL protegidas. Puesto que estas cabeceras entran en conflicto con las directivas de almacenamiento en caché similares agregadas por EPM System y las

aplicaciones web, es posible que los navegadores no almacenen en caché el contenido de las URL protegidas, lo que causa un rendimiento más lento.

Para obtener información detallada acerca de cómo evitar que estas cabeceras de OAM se agreguen a las respuestas, consulte "Ajuste de agentes OAM" en la sección "Oracle Access Management Performance Tuning" de *Guía del administrador de Fusion Middleware para Oracle Access Manager con Oracle Security Token Service*.

### Recursos que proteger

En la siguiente tabla se muestran los contextos que se deben proteger. La sintaxis para proteger un recurso (mediante `interop` como ejemplo) para OSSO:

```
<Location /interop>
Require valid-user
AuthType Basic
order deny,allow
deny from all
allow from myServer.myCompany.com
satisfy any
</Location>
```

El parámetro `allow from` especifica los servidores desde los que se podrá evitar la protección del contexto.

Para Oracle Hyperion Enterprise Performance Management Workspace y Oracle Hyperion Financial Reporting, solo debe establecer los parámetros indicados en el siguiente ejemplo:

```
<Location /workspace>
Require valid-user
AuthType Basic
</Location>
```

**Tabla 3-1 Recursos de EPM System que proteger**

| Producto de EPM System                   | Contexto que proteger                                                                                    |
|------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Servicios compartidos de Oracle Hyperion | <ul style="list-style-type: none"> <li>• /interop</li> <li>• /interop/.../*</li> </ul>                   |
| EPM Workspace                            | <ul style="list-style-type: none"> <li>• /workspace</li> <li>• /workspace/.../*</li> </ul>               |
| Financial Reporting                      | <ul style="list-style-type: none"> <li>• /hr</li> <li>• /hr/.../*</li> </ul>                             |
| Oracle Hyperion Planning                 | <ul style="list-style-type: none"> <li>• /HyperionPlanning</li> <li>• /HyperionPlanning/.../*</li> </ul> |
| Oracle Integrated Operational Planning   | <ul style="list-style-type: none"> <li>• /interlace</li> <li>• /interlace/.../*</li> </ul>               |

**Tabla 3-1 (Continuación) Recursos de EPM System que proteger**

| Producto de EPM System                                                | Contexto que proteger                                                                                                                                                                                                           |
|-----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Oracle Hyperion Financial Management                                  | <ul style="list-style-type: none"> <li>• /hfmadf</li> <li>• /hfmadfe/.../*</li> <li>• /hfmofficeprovider</li> <li>• /hfmofficeprovider/.../*</li> <li>• /hfmsmartviewprovider</li> <li>• /hfmsmartviewprovider/.../*</li> </ul> |
| Oracle Hyperion Financial Reporting Web Studio                        | /frdesigner/**                                                                                                                                                                                                                  |
| Oracle Data Relationship Management                                   | <ul style="list-style-type: none"> <li>• /drm-web-client</li> <li>• /drm-web-client/.../*</li> </ul>                                                                                                                            |
| Oracle Essbase Administration Services                                | <ul style="list-style-type: none"> <li>• /hbrlauncher</li> <li>• /hbrlauncher/.../*</li> </ul>                                                                                                                                  |
| Oracle Hyperion Financial Data Quality Management                     | <ul style="list-style-type: none"> <li>• /HyperionFDM</li> <li>• /HyperionFDM/.../*</li> </ul>                                                                                                                                  |
| Oracle Hyperion Calculation Manager                                   | <ul style="list-style-type: none"> <li>• /calcmgr</li> <li>• /calcmgr/.../*</li> </ul>                                                                                                                                          |
| Oracle Hyperion Provider Services                                     | <ul style="list-style-type: none"> <li>• /aps</li> <li>• /aps/.../*</li> </ul>                                                                                                                                                  |
| Oracle Hyperion Profitability and Cost Management                     | <ul style="list-style-type: none"> <li>• /profitability</li> <li>• /profitability/.../*</li> </ul>                                                                                                                              |
| Account Reconciliation Manager                                        | <ul style="list-style-type: none"> <li>• /arm</li> <li>• /arm/.../*</li> </ul>                                                                                                                                                  |
| Oracle Hyperion Financial Close Management                            | <ul style="list-style-type: none"> <li>• /fcc</li> <li>• /fcc/.../*</li> </ul>                                                                                                                                                  |
| Oracle Hyperion Financial Data Quality Management, Enterprise Edition | <ul style="list-style-type: none"> <li>• /aif</li> <li>• /aif/.../*</li> </ul>                                                                                                                                                  |
| Oracle Hyperion Tax Governance Tax Operations                         | /tss<br>/taxop                                                                                                                                                                                                                  |
| Oracle Hyperion Tax Provision Supplemental Data Manager               | /taxprov<br><ul style="list-style-type: none"> <li>• /sdm*</li> <li>• /sdm/**</li> <li>• /sdm/./**</li> <li>• /SDM-Datamodel-context-root/**</li> </ul>                                                                         |
| Oracle Essbase                                                        | <ul style="list-style-type: none"> <li>• /essbase/.../*</li> <li>• /essbase/**</li> <li>• /essbase*</li> </ul>                                                                                                                  |

**Recursos que desproteger**

En la siguiente tabla se muestran los contextos que no se deben proteger. La sintaxis para desproteger un recurso (mediante /interop/framework(.\*) , por ejemplo) para OSSO:

```
<LocationMatch /interop/framework(.*)>
 Require valid-user
 AuthType Basic
 allow from all
```

```
satisfy any
</LocationMatch>
```

**Tabla 3-2 Recursos de EPM System que desproteger**

| Producto de EPM System | Contextos que desproteger                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Servicios compartidos  | <ul style="list-style-type: none"> <li>• /interop/framework</li> <li>• /interop/framework*</li> <li>• /interop/framework.*</li> <li>• /interop/framework/.../*</li> <li>• /interop/Audit</li> <li>• /interop/Audit*</li> <li>• /interop/Audit.*</li> <li>• /interop/Audit/.../*</li> <li>• /interop/taskflow</li> <li>• /interop/taskflow*</li> <li>• /interop/taskflow/.../*</li> <li>• /interop/WorkflowEngine</li> <li>• /interop/WorkflowEngine/*</li> <li>• /interop/WorkflowEngine/.../*</li> <li>• /interop/TaskReceiver</li> <li>• /framework/lcm/HSSMigration</li> </ul>                     |
| EPM Workspace          | <ul style="list-style-type: none"> <li>• /epmstatic/.../*</li> <li>• /workspace/bpmstatic/.../*</li> <li>• /workspace/static/.../*</li> <li>• /workspace/cache/.../*</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Planning               | <ul style="list-style-type: none"> <li>• /HyperionPlanning/Smartview</li> <li>• /HyperionPlanning/faces/PlanningCentral</li> <li>• /HyperionPlanning/servlet/HspDataTransfer</li> <li>• /HyperionPlanning/servlet/HspLCMServlet</li> <li>• /HyperionPlanning/servlet/HspADMServlet/.../*</li> <li>• /HyperionPlanning/servlet/HspADMServlet/**</li> <li>• /HyperionPlanning/servlet/HspADMServlet*</li> <li>• /HyperionPlanning/servlet/HspAppManagerServlet/.../*</li> <li>• /HyperionPlanning/servlet/HspAppManagerServlet/**</li> <li>• /HyperionPlanning/servlet/HspAppManagerServlet*</li> </ul> |

**Tabla 3-2 (Continuación) Recursos de EPM System que desproteger**

| Producto de EPM System                              | Contextos que desproteger                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Financial Reporting                                 | <ul style="list-style-type: none"> <li>• /hr/common/HRLogon.jsp</li> <li>• /hr/services</li> <li>• /hr/services/*</li> <li>• /hr/services/.../*</li> <li>• /hr/modules/com/hyperion/reporting/web/reportViewer/HRStaticReport.jsp</li> <li>• /hr/modules/com/hyperion/reporting/web/repository/HRObjectListXML.jsp</li> <li>• /hr/modules/com/hyperion/reporting/web/reportViewer/HRHtmlReport.jsp</li> <li>• /hr/modules/com/hyperion/reporting/web/bookViewer/HRBookTOCFns.jsp</li> <li>• /hr/modules/com/hyperion/reporting/web/bookViewer/HRBookPdf.jsp</li> </ul> |
| Data Relationship Management<br>Calculation Manager | /drm-migration-client <ul style="list-style-type: none"> <li>• /calcmgr/importexport.postExport.do</li> <li>• /calcmgr/common.performAction.do</li> <li>• /calcmgr/lcm.performAction.do*</li> <li>• /calcmgr/lcm.performAction.do/*</li> </ul>                                                                                                                                                                                                                                                                                                                         |
| Administration Services                             | <ul style="list-style-type: none"> <li>• /eas</li> <li>• /easconsole</li> <li>• /easdocs</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Financial Management                                | <ul style="list-style-type: none"> <li>• /hfm/EIE/EIEListener.asp</li> <li>• /hfmapplicationsservice</li> <li>• /oracle-epm-fm-webservices</li> <li>• /hfmlcmsservice</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                       |
| Financial Close Management                          | <ul style="list-style-type: none"> <li>• /FCC-DataModel-context-root</li> <li>• /oracle-epm-erpi-webservices/*</li> <li>• /ARM-DataModel-context-root</li> <li>• /oracle-epm-erpi-webservices/**</li> <li>• /arm/batch/armbatchexecutionservlet</li> <li>• /ARM-DataModel-context-root</li> </ul>                                                                                                                                                                                                                                                                      |

Tabla 3-2 (Continuación) Recursos de EPM System que desproteger

| Producto de EPM System           | Contextos que desproteger                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Integrated Operational Planning  | <ul style="list-style-type: none"> <li>• /interlace/services/</li> <li>• /interlace/services/*</li> <li>• /interlace/services/*</li> <li>• /interlace/services/.../*</li> <li>• /interlace/anteros</li> <li>• /interlace/anteros/*</li> <li>• /interlace/anteros/*</li> <li>• /interlace/anteros/.../*</li> <li>• /interlace/interlace</li> <li>• /interlace/interlace/*</li> <li>• /interlace/interlace/*</li> <li>• /interlace/interlace/.../*</li> <li>• /interlace/WebHelp</li> <li>• /interlace/WebHelp/*</li> <li>• /interlace/WebHelp/*</li> <li>• /interlace/WebHelp/.../*</li> <li>• /interlace/html</li> <li>• /interlace/html/*</li> <li>• /interlace/html/*</li> <li>• /interlace/html/.../*</li> <li>• /interlace/email-book</li> <li>• /interlace/email-book/*</li> <li>• /interlace/email-book/*</li> <li>• /interlace/email-book/.../*</li> </ul> |
| Rentabilidad y gestión de costes | <ul style="list-style-type: none"> <li>• /profitability/cesagent</li> <li>• /profitability/lcm</li> <li>• /profitability/control</li> <li>• /profitability/ApplicationListener</li> <li>• /profitability/HPMApplicationListener</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Oracle Essbase                   | <ul style="list-style-type: none"> <li>• /essbase/agent/.../*</li> <li>• /essbase/jet/logout.html</li> <li>• /essbase/jet/.+\. (js   css   gif   jpe?g   png)\$</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| FDME                             | <ul style="list-style-type: none"> <li>• /aif/services/FDMRuleService</li> <li>• /aif/services/RuleService</li> <li>• /aif/LCMServlet</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## Inicio de sesión único basado en cabecera con productos de administración de identidad

### Requisitos

- Oracle Enterprise Performance Management System totalmente configurado. El servidor de directorios del producto de administración de identidad debe configurarse en EPM System como un directorio de usuarios para autorizar usuarios.



- Un producto de administración de identidad totalmente configurado (Microsoft Azure AD, Okta, etc.) que soporte la autenticación basada en cabecera.

Los siguientes procesos genéricos están implicados en la configuración de EPM System para el inicio de sesión único con un producto de administración de identidad compatible. Dado que los pasos específicos implicados dependen del producto que utilice, consulte los manuales de su producto de administración de identidad para ver los pasos detallados.

Para saber más sobre los pasos detallados de la configuración de autenticación basada en cabecera con Oracle Identity Cloud Services, consulte [Configuración de EPM System para inicio de sesión único basado en cabecera con Oracle Identity Cloud Services](#).

1. Registre EPM System como una aplicación empresarial en el producto de administración de identidad. Este paso permite al administrador de administración de identidad configurar la autenticación en la aplicación empresarial, incluidas las funciones soportadas, como la autenticación multifactor. Utilice el nombre de dominio totalmente cualificado (FQDN) de la puerta de enlace junto con `workspace/index.jsp` (por ejemplo, `https://gateway.server.example.com:443/workspace/index.jsp`) como la URL de la aplicación empresarial para EPM System. Configure la aplicación empresarial de EPM System para propagar una cabecera HTTP. Puede elegir cualquier nombre de cabecera no reservado como nombre de la cabecera HTTP. El valor de la cabecera debe ser la propiedad que identifique de forma única a los usuarios de EPM System.
2. Instale, configure y registre una puerta de enlace de aplicación para garantizar que la aplicación empresarial solo reenvíe solicitudes autenticadas a EPM System. Utilice los siguientes parámetros de configuración:
  - FQDN de servidor de puerta de enlace (por ejemplo, `gateway.server.example.com:443`) como punto de acceso.
  - FQDN de EPM System (por ejemplo, `epm.server.example.com:443`) como recurso al que deben reenviarse las solicitudes de HTTPS autenticadas.
3. Active el inicio de sesión único en EPM System para respetar las cabeceras HTTPS propagadas por la puerta de enlace de la aplicación. Para obtener más información, consulte [Establecimiento de las opciones de seguridad](#). Para activar el inicio de sesión único:
  - a. Acceda a Oracle Hyperion Shared Services Console como administrador del sistema. Consulte [Inicio de Shared Services Console](#).
  - b. Seleccione **Administración** y, a continuación, **Configurar directorios de usuario**.
  - c. Haga clic en **Opciones de seguridad**.
  - d. En la sección **Configuración de inicio de sesión único**:
    - i. Seleccione la casilla de verificación **Activar inicio de sesión único**.
    - ii. En la lista desplegable **Proveedor de inicio de sesión único o Agente de seguridad**, seleccione **Otros**.
    - iii. En la lista desplegable **Mecanismo de inicio de sesión único**, seleccione **Cabecera HTTP personalizada** y, a continuación, especifique el nombre de cabecera que el agente de seguridad pasa a EPM System.
  - e. Haga clic en **Aceptar**.
4. Actualice la configuración de la URL posterior al cierre de sesión de Oracle Hyperion Enterprise Performance Management Workspace con la de la página web que desea que vean los usuarios al cerrar la sesión en EPM System.

Para actualizar la configuración de URL tras el cierre de sesión en EPM Workspace:

- a. Acceda a EPM Workspace como administrador de sistema. Consulte [Acceso a EPM Workspace](#).
  - b. Seleccione **Navegar**, a continuación **Configuración de Workspace** y, por último, **Configuración de servidor**.
  - c. En **Configuración de servidor de Workspace**, cambie la **URL posterior al cierre de sesión** por la de la página web que desea que vean los usuarios al desconectarse de EPM System.
  - d. Haga clic en **Aceptar**.
5. Reinicie Oracle Hyperion Foundation Services y todos los servidores administrados de EPM System.

## Configuración de EPM System para el inicio de sesión único basado en cabecera con Oracle Identity Cloud Services

En este escenario, Oracle Identity Cloud Services autentica los usuarios de Oracle Enterprise Performance Management System y propaga las cabeceras HTTP necesarias para activar el inicio de sesión único.

Esta sección trata los pasos implicados en la configuración de EPM System para soportar el inicio de sesión único con Oracle Identity Cloud Services. Puede extrapolar estos pasos para soportar la autenticación basada en cabecera de EPM System con cualquier sistema de administración de identidad (por ejemplo, Azure AD) o un proveedor de infraestructura como servicio (IaaS) que soporte la autenticación basada en cabecera.

El flujo de trabajo conceptual es el siguiente:

- Una puerta de enlace de aplicación que actúa como proxy inverso protege los componentes de EPM System al restringir el acceso a la red no autenticado.
- La puerta de enlace de la aplicación intercepta las solicitudes HTTPS a componentes de EPM System y garantiza que el producto de administración de identidad autentique los usuarios antes de reenviar las solicitudes a componentes de EPM System.
- Mientras se reenvían las solicitudes a componentes de EPM System, la puerta de enlace de aplicación propaga la identidad de usuario autenticado al componente de EPM System a través de solicitudes de cabecera HTTP.

## Requisitos previos y direcciones URL de ejemplo

Para establecer un inicio de sesión único basado en cabecera con Oracle Identity Cloud Services:

- Oracle Enterprise Performance Management System totalmente configurado.
- Un host o contenedor con Oracle App Gateway totalmente configurado, que actúe como proxy inverso para proteger el EPM System al restringir el acceso no autorizado.  
Se debe configurar Oracle App Gateway para interceptar solicitudes HTTP para los componentes de EPM System y garantizar que los

usuarios se hayan autenticado con Oracle Identity Cloud Services antes de reenviar las solicitudes a EPM System. Aunque se reenvíen solicitudes a los componentes de EPM System, Oracle App Gateway debe propagar la identidad del usuario autenticado a través de las solicitudes de cabecera HTTP.

- Acceso de administrador de dominio a Oracle Identity Cloud Services.

Las siguientes URL de ejemplo se utilizan en esta discusión:

- URL de la base del nombre de dominio totalmente cualificado (FQDN) del servidor de Oracle Identity Cloud Services (proveedor de identidad):  
`https://identity.server.example.com:443/`
- FQDN del servidor de Oracle App Gateway (que aloja la puerta de enlace de aplicación):  
`https://gateway.server.example.com:443/`
- URL de aplicación empresarial para EPM System. Este es el FQDN del servidor de Oracle App Gateway agregado `workspace/index.jsp`:  
`https://gateway.server.example.com:443/workspace/index.jsp`

#### Note:

Oracle Identity Cloud Services y Oracle App Gateway se han configurado con soporte HTTPS. El soporte HTTPS para EPM System es opcional. En esta discusión se asume que EPM System se ha configurado con soporte HTTPS.

## Activación de la autenticación basada en cabecera para EPM System

Para activar la autenticación basada en cabecera para Oracle Enterprise Performance Management System siga los siguientes pasos:

- [Adición de aplicaciones y puertas de enlace del sistema EPM a Oracle Identity Cloud Services](#)
- [Configuración de la puerta de enlace de aplicación](#)
- [Configuración del directorio de usuario para autorización](#)
- [Habilitación del inicio de sesión único en EPM System](#)
- [Actualización de la configuración de EPM Workspace](#)

## Adición de aplicación y puerta de enlace de EPM System a Oracle Identity Cloud Services

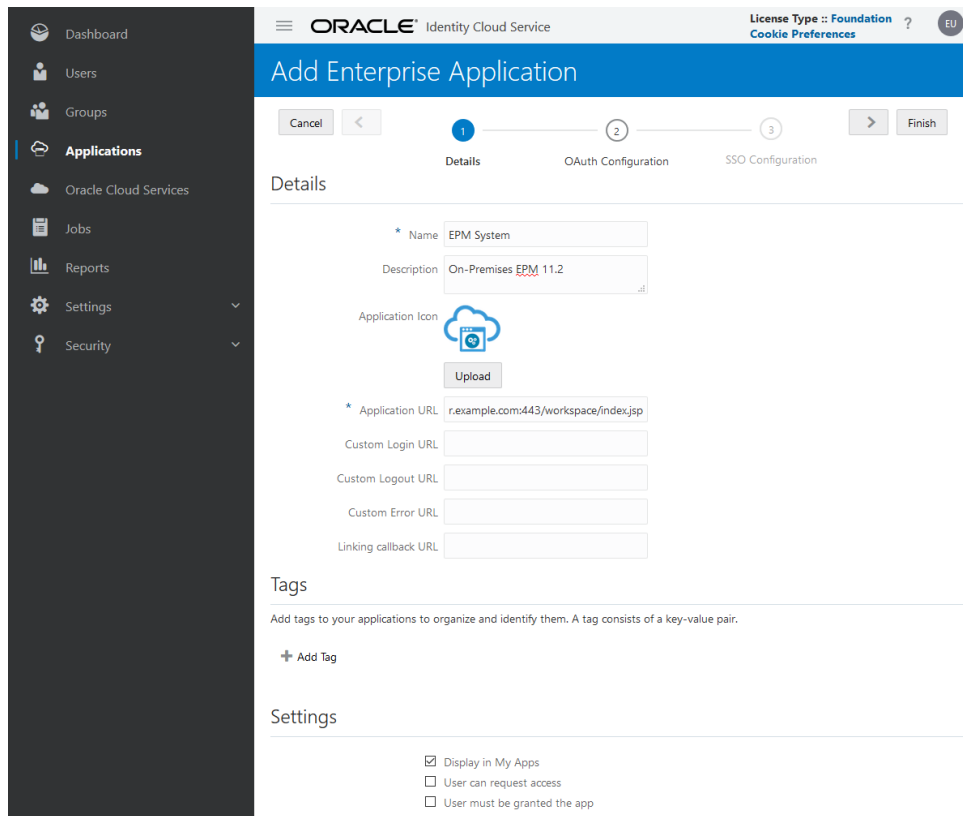
Para configurar una autenticación basada en cabecera, debe establecer Oracle Enterprise Performance Management System como aplicación empresarial.

### **Agregue EPM System como aplicación empresarial en la consola de Oracle Cloud Identity**

Para agregar EPM System como aplicación empresarial:

1. Acceda a la consola de Oracle Cloud Identity como administrador de dominio.
  - a. Mediante un explorador, vaya a `https://www.oracle.com/cloud/sign-in.html`.

- b. Introduzca su nombre de cuenta de Oracle Fusion Cloud EPM.
  - c. En la página de inicio de sesión de la cuenta de Oracle Fusion Cloud EPM, introduzca su nombre usuario y contraseña y, a continuación, haga clic en **Iniciar sesión**.
  - d. En el **Cajón de navegación**, haga clic en **Usuarios** y, a continuación, en **Identidad (principal)**.
  - e. Haga clic en **Consola de identidad**.
2. Agregue EPM System como aplicación empresarial.
- a. En el Cajón de navegación, haga clic en **Aplicaciones**.
  - b. Haga clic en **Agregar** y, a continuación, en **Aplicación empresarial**.



3. Agregue detalles de la aplicación:
- a. En **Nombre**, introduzca un nombre único para identificar la aplicación empresarial de EPM System.
  - b. Introduzca una descripción (opcional).
  - c. Si lo desea, cargue un icono de aplicación para EPM System. Haga clic en **Cargar** para seleccionar y cargar el icono.
  - d. En la **URL de aplicación**, introduzca la URL de inicio a la que la puerta de enlace debe redirigir los usuarios. Esta URL es el FQDN de Oracle App Gateway agregado a `workspace/index.jsp`, que es el contexto de la aplicación EPM System.

- e. En **Configuración**, seleccione **Mostrar en mis aplicaciones** para mostrar la aplicación empresarial EPM System en el separador **Configuración de inicio de sesión único** de la página **Mis aplicaciones** en la consola de Oracle Cloud Identity.
  - f. Haga clic en **Siguiente**.
4. Especifique los detalles de configuración del inicio de sesión único.
    - a. Haga clic en **Configuración de inicio de sesión único**.
    - b. Agregue un recurso para la aplicación empresarial.  
En **Configuración de inicio de sesión único**, amplíe **Recursos**.
      - i. Haga clic en **Agregar**.

The screenshot shows a dialog box titled "Add Resource" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Resource Name:** A text input field containing "EPM".
- Resource URL:** A text input field containing "/.\*".
- URL Query String:** An empty text input field.
- Regex:** A checkbox that is checked.
- Description:** An empty text area.

An "OK" button is located in the bottom right corner of the dialog.

- ii. Especifique un nombre de recurso único.
  - iii. En **Recurso de URL**, introduzca /.\*.
  - iv. Seleccione la casilla de verificación **Expresión regular**.
  - v. Haga clic en **Aceptar**.
  - vi. En **Configuración de inicio de sesión único**, amplíe **Recursos**.
- c. Agregue la política de autenticación.  
En **Configuración de inicio de sesión único**, amplíe **Política de autenticación**.
    - i. Seleccione las casillas de verificación **Permitir CORS** y **Requerir cookies seguras**.
    - ii. Haga clic en **Agregar** en **Recursos administrados** y defina **Token de acceso o Formulario** como el método de autenticación para el recurso de inicio de sesión único.

- iii. En **Recurso**, seleccione el recurso de inicio de sesión que haya agregado en el paso anterior.
  - iv. Amplíe **Cabeceras**.
  - v. Introduzca el nombre de la cabecera HTTP que se propagará a EPM System.  
El nombre de cabecera de autenticación por defecto es `HYPLOGIN`. Puede utilizar el nombre que desee.
  - vi. En **Valor**, seleccione la propiedad que identifique de forma exclusiva a los usuarios de EPM System.  
El valor de este campo debe coincidir con la identidad del usuario en EPM System. Por ejemplo, si la identidad del usuario en EPM System es el ID de correo electrónico, seleccione Correo electrónico de trabajo como valor.
  - vii. Haga clic en **Guardar**.
5. Haga clic en **Finalizar** para crear la aplicación empresarial.
  6. Haga clic en **Activar** para activar la aplicación.
  7. Registre una puerta de enlace de aplicación y configure el host y la aplicación para EPM System.
    - a. En el **Cajón de navegación**, haga clic en **Seguridad** y, a continuación, en **Puertas de enlace de aplicaciones**.
    - b. Haga clic en **Agregar**.
    - c. En **Detalles**, introduzca un nombre único para la puerta de enlace y una descripción opcional.
    - d. Haga clic en **Siguiente** para abrir la pantalla Hosts.
    - e. Agregue un host de App Gateway para EPM System.
      - i. En la pantalla Hosts, haga clic en **Agregar**.

- ii. En **Identificador de host**, introduzca EPMAAppGateway.
  - iii. En **Host**, introduzca el nombre de dominio totalmente cualificado del equipo que aloja el servidor de App Gateway. Por ejemplo, gateway.server.example.com.
  - iv. En **Puerto**, introduzca el puerto en el que el servidor de App Gateway responde a las solicitudes HTTPS.
  - v. Seleccione la casilla de verificación **SSL activado**.
  - vi. En **Propiedades adicionales**, introduzca lo siguiente:
    - Ubicación de certificado SSL
    - Clave de certificado SSL
    - Archivo de contraseña SSL (si es necesario)

Para obtener más información, consulte "[Registro de una puerta de enlace de aplicación](#)" en "Configuración de una puerta de enlace de aplicación" en *Administración de Oracle Identity Cloud Service*.
  - vii. Haga clic en **Guardar**.
  - viii. Haga clic en **Siguiente** para abrir la pantalla Aplicaciones.
- f. Agregue la aplicación empresarial EPM System a la puerta de enlace de aplicación.
- i. En **Aplicaciones**, haga clic en **Agregar**.
  - ii. En **Aplicación**, seleccione la aplicación empresarial EPM System que haya agregado anteriormente a la consola de Oracle Cloud Identity.

Assign an App to gate

\* Application

\* Select a Host

Policy default

\* Resource Prefix

\* Origin Server

Additional Properties

```
ssl_certificate /usr/local/epm.server.example.com.crt;
ssl_certificate_key /usr/local/epm.server.example.com.key;
ssl_password_file /usr/local/epm.server.example.com.password.txt;
```

Save

- iii. En **Seleccionar un host**, seleccione EPMAAppGateway (el host de EPM System que haya agregado a la puerta de enlace de aplicación).
  - iv. En **Prefijo de recurso**, introduzca / para reenviar todas las solicitudes al host de EPM System.
  - v. En **Servidor de origen**, introduzca el nombre de dominio totalmente cualificado del equipo que aloja Oracle Hyperion Enterprise Performance Management Workspace y el número de puerto que utiliza EPM Workspace.
  - vi. Haga clic en **Guardar**.
8. Registre el ID y secreto de cliente de la puerta de enlace de aplicación. Se necesitan estos valores para configurar la puerta de enlace de aplicación.
    - a. En el **Cajón de navegación**, haga clic en **Seguridad** y, a continuación, en **Puertas de enlace de aplicaciones**.
    - b. Haga clic en el nombre de la puerta de enlace que haya agregado para la aplicación empresarial EPM System.
    - c. Copie el ID de cliente (una cadena alfanumérica) en un editor de texto.
    - d. Haga clic en **Mostrar secreto** para mostrar el código secreto de cliente.
    - e. Copie el secreto de cliente (una cadena alfanumérica) en el editor de texto.
    - f. Guarde el archivo de texto.

 **Note:**

El servidor de App Gateway se debe reiniciar cada vez que se realiza una actualización de configuración en Oracle Identity Cloud Services. Para iniciar y para el servidor de App Gateway, consulte la sección sobre [inicio y parada de App Gateway](#).



## Configuración de la puerta de enlace de aplicación

Para obtener información detallada, consulte "[Configuración de una puerta de enlace de aplicación](#)" en *Administración de Oracle Identity Cloud Service*.

Necesitará el ID y el secreto de cliente que haya registrado en la sección anterior para configurar el servidor de la puerta de enlace de aplicación.

## Configuración del directorio de usuario para autorización

Algunos productos de administración de identidad como Oracle Identity Cloud Services y Microsoft Azure no se pueden configurar directamente como directorios de usuario en Oracle Enterprise Performance Management System. Puede configurar estos productos con Oracle Unified Directory o Oracle Virtual Directory y, a continuación, configurar este último como un directorio de usuario en EPM System. Para ver los pasos detallados de configuración de directorios de usuario, consulte [Configuración de directorios de usuario](#).

## Habilitación del inicio de sesión único en EPM System

Debe configurar las opciones de seguridad en Oracle Enterprise Performance Management System para activar el inicio de sesión único. Para obtener información detallada, consulte [Establecimiento de las opciones de seguridad](#).

Para activar el inicio de sesión único:

1. Acceda a Oracle Hyperion Shared Services Console como administrador del sistema. Consulte [Inicio de Shared Services Console](#).
2. Seleccione **Administración** y, a continuación, **Configurar directorios de usuario**.
3. Haga clic en **Opciones de seguridad**.
4. En la sección **Configuración de inicio de sesión único**:
  - a. Seleccione la casilla de verificación **Activar inicio de sesión único**.
  - b. En la lista desplegable **Proveedor de inicio de sesión único o Agente de seguridad**, seleccione **Otros**.
  - c. En la lista desplegable **Mecanismo de inicio de sesión único**, seleccione **Cabecera HTTP personalizada** y, a continuación, especifique el nombre de cabecera que el agente de seguridad pasa a EPM System (HYPLLOGIN o el nombre personalizado que haya especificado al agregar recursos en la aplicación empresarial en la consola de Oracle Cloud Identity).
5. Haga clic en **Aceptar**.

### Note:

Asegúrese de reiniciar todos los servicios de EPM System después de realizar cualquier cambio en la configuración de inicio de sesión único.

## Actualización de la configuración de EPM Workspace

1. Acceda a Oracle Hyperion Enterprise Performance Management Workspace como administrador del sistema. Consulte [Acceso a EPM Workspace](#).

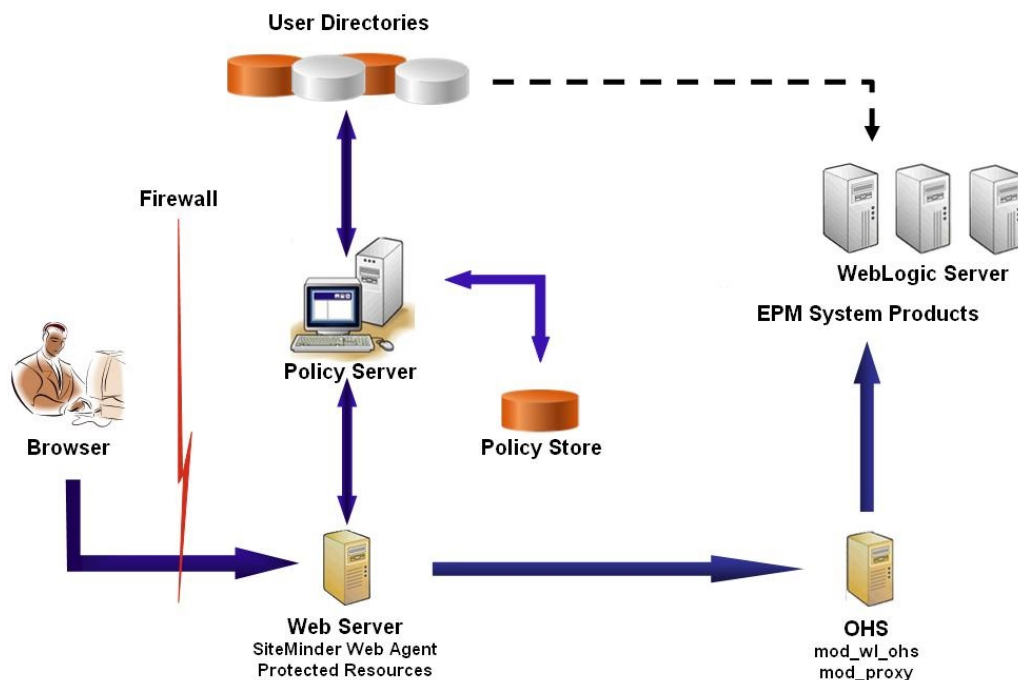
2. Seleccione **Navegar**, a continuación **Configuración de Workspace** y, por último, **Configuración de servidor**.
3. En **Configuración de servidor de Workspace**, cambie la **URL posterior al cierre de sesión** por la de la página web que desea que vean los usuarios al cerrar sesión en Oracle Enterprise Performance Management System.
4. Haga clic en **Aceptar**.
5. Reinicie Oracle Hyperion Foundation Services y todos los componentes de EPM System.

## Inicio de sesión único de SiteMinder

SiteMinder es una solución solo para web. Las aplicaciones de escritorio y sus complementos (por ejemplo, Microsoft Excel y el Diseñador de informes) no pueden usar la autenticación a través de SiteMinder. Sin embargo, Oracle Smart View for Office puede usar la autenticación de SiteMinder.

### Flujo de procesos

Descripción general ilustrada del inicio de sesión único activado para SiteMinder:



Proceso de inicio de sesión único de SiteMinder:

1. Los usuarios intentan acceder a un recurso de Oracle Enterprise Performance Management System con protección de SiteMinder. Usan una URL que los conecta al servidor web que aplica front-end al servidor de política de SiteMinder, por ejemplo, `http://WebAgent_Web_Server_Name:WebAgent_Web_ServerPort/interop/index.jsp`.
2. El servidor web redirige a los usuarios al servidor de políticas, que solicita a los usuarios las credenciales. Tras verificar las credenciales en los directorios de

usuario configurados, el servidor de políticas transfiere las credenciales al servidor web que aloja el agente web de SiteMinder.

3. El servidor web que aloja el agente web de SiteMinder redirige la solicitud a la instancia de Oracle HTTP Server que aplica front-end a EPM System. Oracle HTTP Server redirige a los usuarios a la aplicación solicitada desplegada en Oracle WebLogic Server.
4. El componente EPM System comprueba la información de aprovisionamiento y ofrece contenido. Para que este proceso funcione, los directorios de usuario que usa SiteMinder para autenticar al usuario se deben configurar como directorios de usuarios externos en EPM System. Estos directorios se deben configurar como de confianza.

### Consideraciones especiales

SiteMinder es una solución solo para web. Las aplicaciones de escritorio y sus complementos (por ejemplo, Microsoft Excel y el Diseñador de informes) no pueden usar la autenticación a través de SiteMinder. Sin embargo, Smart View puede usar la autenticación de SiteMinder.

### Requisitos

1. Una instalación de SiteMinder totalmente funcional que incluya los siguientes componentes:
  - Servidor de políticas de SiteMinder en los que se han definido las políticas y los objetos de agentes
  - Agente web de SiteMinder instalado en el servidor web que aplica front-end al servidor de políticas de SiteMinder
2. Un despliegue de EPM System totalmente funcional.  
Al configurar el servidor web para componentes de EPM System, EPM System Configurator configura `mod_wl_ohs.conf` en las solicitudes de proxy a WebLogic Server.

### Activación del agente web de SiteMinder

El agente web está instalado en un servidor web que intercepta las solicitudes para los recursos de EPM System. Los intentos realizados por usuarios no autenticados de acceder a recursos protegidos de EPM System fuerza al agente web a solicitar a los usuarios a las credenciales de inicio de sesión único. Cuando se autentifica un usuario, el servidor de directivas agrega el nombre de inicio de sesión del usuario autenticado, que se encuentra en la cabecera. Después, la solicitud HTTP se transfiere al servidor web de EPM System, que redirige las solicitudes. Los componentes de EPM System extraen de las cabeceras las credenciales de usuario autenticadas.

SiteMinder soporta el inicio de sesión único en los productos de EPM System que se ejecuten en plataformas de servidor web heterogéneas. Si los productos de EPM System utilizan diferentes servidores web, deberá asegurarse de que la cookie de SiteMinder se pueda transferir entre los servidores web del mismo dominio. Para ello, tendrá que especificar el dominio de aplicación de EPM System apropiado como valor de la propiedad `Cookiedomain` en el archivo `WebAgent.conf` de cada servidor web.

Consulte la sección sobre configuración de agentes web en *Netegrity SiteMinder Agent Guide* (Guía de Netegrity SiteMinder Agent).

 **Nota:**

Dado que Servicios compartidos de Oracle Hyperion utiliza autenticación básica para proteger su contenido, el servidor web que intercepta solicitudes para Servicios compartidos debería permitir autenticación básica para soportar el inicio de sesión único con SiteMinder.

Para configurar el agente web, ejecute el asistente de configuración de agente web de SiteMinder (al ejecutar `WEBAGENT_HOME/install_config_info/nete-wa-config`, por ejemplo, `C:\netegrity\webagent\install_config_info\nete-wa-config.exe` en Windows). El proceso de configuración crea un `WebAgent.conf` para el servidor web de SiteMinder.

Para activar el agente web de SiteMinder:

1. Mediante un editor de texto, abra `WebAgent.conf`. La ubicación de este archivo depende del servidor web que esté usando.
2. Establezca el valor de la propiedad `enableWebAgent` en `Yes`.  
`enableWebAgent="YES"`
3. Guarde y cierre el archivo de configuración del agente web.

### **Ejemplo 3-1 Configuración del servidor de directivas de SiteMinder**

Es preciso que un administrador de SiteMinder configure el servidor de directivas para habilitar el inicio de sesión único en los productos de EPM System.

El proceso de configuración consta de:

- Creación de un agente web de SiteMinder y adición de objetos de configuración adecuado para el servidor web de SiteMinder
- Creación de un dominio para cada recurso de EPM System que se deba proteger y agregando el agente web al dominio. Consulte [Recursos que proteger](#)
- En el dominio que se ha creado para los recursos de EPM System protegidos, cree dominios para recursos no protegidos. Consulte [Recursos que desproteger](#)
- Creación de una referencia de cabecera HTTP. La cabecera debe proporcionar el valor de `Login Attribute` a aplicaciones de EPM System. Consulte la sección sobre configuración de OID, Active Directory y otros directorios de usuarios basados en LDAP en *Guía de administración de seguridad de usuarios de Oracle Enterprise Performance Management System* para obtener una descripción breve de `Login Attribute`.
- Creación de reglas en los dominios con Get, Post y Put como acciones de agente web
- Creación de un atributo de respuesta con `hyplogin=<%userattr="SM_USERLOGINNAME"%>` como valor
- Creación de una política, asignación de acceso al directorio de usuario y adición de reglas que haya creado para EPM System a la lista de miembros actuales
- Establecimiento de respuestas para las reglas que haya creado para los componentes de EPM System

### Ejemplo 3-2 Configuración del servidor web de SiteMinder para reenviar solicitudes al servidor web de EPM System

Configure el servidor web que aloje el agente web de SiteMinder para reenviar solicitudes de usuarios autenticadores (que incluyan la cabecera que identifica al usuario) al servidor web de EPM System.

Para servidores web basados en Apache, utilice directivas similares a las siguientes para reenviar las solicitudes autenticadas:

```
ProxyPass / http://EPM_WEB_SERVER:EPM_WEB_SERVER_PORT/
ProxyPassReverse / http://EPM_WEB_SERVER:EPM_WEB_SERVER_PORT/
ProxyPreserveHost On
#If SiteMinder Web Server is using HTTPS but EPM Web Server is using HTTP
RequestHeader set WL-Proxy-SSL true
```

En esta directiva, reemplace *EPM\_WEB\_SERVER* y *EPM\_WEB\_SERVER\_PORT* por los valores reales de su entorno.

### Ejemplo 3-3 Habilitación de SiteMinder en EPM System

La integración con SiteMinder requiere que se habilite la autenticación de SiteMinder para los productos de EPM System. Consulte [Configuración de EPM System para inicio de sesión único](#).

## Inicio de sesión único en Kerberos

### Descripción general

Los productos de Oracle Enterprise Performance Management System soportan el inicio de sesión único en Kerberos si el servidor de aplicaciones que aloja los productos de EPM System está configurado para la autenticación con Kerberos.

Kerberos es un servicio de autenticación de confianza en el que cada cliente Kerberos confía en las identidades de otros clientes Kerberos (usuarios, servicios de red, etcétera) como válidas.

A continuación se muestra lo que ocurre cuando un usuario accede a un producto de EPM System:

1. Desde un equipo Windows, el usuario inicia sesión en un dominio Windows, que también es un dominio de Kerberos.
2. Con ayuda de un explorador configurado para utilizar Autenticación de Windows integrada, el usuario intenta iniciar sesión en los productos de EPM System que se ejecutan en el servidor de aplicaciones.
3. El servidor de aplicaciones (afirmación de identidad de negociación) intercepta la solicitud y obtiene el símbolo del mecanismo de negociación (SPNEGO) de la API de Simple and Protected Generic Security Services (GSSAPI) con el ticket de Kerberos desde la cabecera de autorización del explorador.
4. La afirmación valida la identidad del usuario incluida en el símbolo con respecto a su almacén de identidades con el fin de transferir información sobre el usuario al producto de EPM System. El producto EPM System valida el nombre de usuario con respecto a un Active Directory. El producto EPM System emite un símbolo de inicio de sesión único que soporta el inicio de sesión en todos los productos de EPM System.

### Limitaciones de compatibilidad

El inicio de sesión único de Kerberos es compatible con todos los productos de EPM System, a excepción de los siguientes:

- El inicio de sesión único de Kerberos no está soportado para clientes gruesos que no sean Oracle Smart View for Office.
- Smart View soporta la integración de Kerberos solo para proveedores de Oracle Essbase, Oracle Hyperion Planning y Oracle Hyperion Financial Management

### Suposiciones

En este documento, que contiene pasos de configuración de Kerberos de nivel de aplicación, se asume que se está familiarizado con la configuración de Kerberos en el nivel del sistema. Antes de iniciar estos procedimientos, confirme que se cumplen los requisitos para estas tareas.

En este documento se asume que está trabajando en un entorno de red activado para Kerberos totalmente funcional en el que los equipos de clientes de Windows estén configurados para autenticación de Kerberos.

- El Active Directory corporativo está configurado para autenticación Kerberos. Consulte [Documentación de Microsoft Windows Server](#).
- Los exploradores utilizados para acceder a productos de EPM System están configurados para negociación con tickets de Kerberos.
- Sincronización de tiempo con un sesgo de no más de cinco minutos entre KDC y los equipos del cliente. Consulte la sección sobre errores de autenticación causados por relojes no sincronizados en [http://technet.microsoft.com/en-us/library/cc780011\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc780011(WS.10).aspx).

### Inicio de sesión único en Kerberos con WebLogic Server

El inicio de sesión único en Kerberos con Oracle WebLogic Server utiliza un proveedor de aserción de identidades negociadas para negociar y descodificar símbolos de SPNEGO con el fin de permitir el inicio de sesión único con clientes de Microsoft. WebLogic Server descodifica los símbolos SPNEGO para obtener tickets de Kerberos, y valida y correlaciona el ticket con el usuario de una instancia de WebLogic Server. Puede usar el autenticador de Active Directory de WebLogic Server con la afirmación de identidad de negociación para configurar Active Directory como directorio de usuario para usuarios de WebLogic Server.

Cuando un explorador solicita acceso a un producto de EPM System, KDC emite un ticket de Kerberos al explorador, que crea un símbolo SPNEGO en el que se incluyen los tipos de símbolo GSS soportados. La afirmación de identidad de negociación descodifica el símbolo SPNEGO y utiliza instancias de GSSAPI para aceptar el contexto de seguridad. La identidad del usuario que inició la solicitud se correlaciona con un nombre de usuario y se pasa de vuelta a WebLogic Server. Adicionalmente, WebLogic Server determina los grupos a los que pertenece el usuario. En esta fase, se pone a disposición del usuario el producto de EPM System solicitado.



**Nota:**

Los usuarios deben usar un explorador que soporte el SPNEGO (por ejemplo, Internet Explorer o Firefox) para acceder a los productos de EPM System que se estén ejecutando en WebLogic Server.

Utilizando el ID de usuario derivado del proceso de autenticación, el proceso de autorización del producto de EPM System comprueba la existencia de datos de aprovisionamiento. El acceso al producto de EPM System se restringe según dichos datos.

### Procedimientos de WebLogic Server para soportar la autenticación de Kerberos

Un administrador debe realizar estas tareas para soportar la autenticación de Kerberos:

- Cree el dominio de WebLogic para EPM System. Consulte [Creación del dominio de WebLogic para EPM System](#).
- Cree un proveedor de autenticación. Consulte [Creación de un proveedor de autenticación de LDAP en WebLogic Server](#).
- Cree una afirmación de identidad de negociación. Consulte [Creación de una afirmación de identidad de negociación](#).
- Cree una identificación de Kerberos. Consulte [Creación de identificación de Kerberos para WebLogic Server](#).
- Actualice las opciones de JVM para Kerberos. Consulte [Actualización de opciones de JVM para Kerberos](#).
- Configure las políticas de autorización. Consulte [Configuración de políticas de autorización](#).
- Despliegue y use SSODiag para verificar que WebLogic Server soporta el inicio de sesión único de Kerberos para EPM System. Consulte [Uso de SSODiag para probar el entorno de Kerberos](#).

### Creación del dominio de WebLogic para EPM System

Por lo general, los componentes de EPM System se despliegan en el dominio de WebLogic de EPMSystem (la ubicación predeterminada es `MIDDLEWARE_HOME/user_projects/domains/EPMSystem`).

Para configurar el dominio de WebLogic de EPM System para la autenticación de Kerberos:

1. Instale los componentes de EPM System.
2. Despliegue solo Oracle Hyperion Foundation Services.  
Con el despliegue de Foundation Services se crea el dominio de WebLogic de EPM System predeterminado.
3. Inicie sesión en Consola de Servicios compartidos de Oracle Hyperion para verificar que el despliegue de Foundation Services se ha realizado correctamente. Consulte [Inicio de Shared Services Console](#).



### Creación del proveedor de autenticación de LDAP en WebLogic Server

Un administrador de WebLogic Server crea el proveedor de autenticación LDAP, que almacena la información de usuarios y grupos en un servidor LDAP externo. Los servidores compatibles con LDAP v2 o v3 funcionan con WebLogic Server. Consulte estas referencias:

- [Configuración de proveedores de autenticación de LDAP](#) en la guía *Oracle Fusion Middleware Securing Oracle WebLogic Server*.
- [Configurar proveedores de autenticación y afirmación de identidad](#) en la *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help*.

### Creación de una afirmación de identidad de negociación

El proveedor de afirmación de identidad de negociación permite el inicio de sesión único con clientes de Microsoft. Descodifica símbolos de SPNEGO para obtener símbolos de Kerberos, valida los símbolos de Kerberos y asigna los símbolos a los usuarios de WebLogic. El proveedor de afirmación de identidad de negociación, una implantación de la interfaz de proveedor de servicio de seguridad (SSPI) según la definición del marco de seguridad de WebLogic, proporciona la lógica necesaria para autenticar un cliente en función del símbolo SPNEGO del cliente.

- [Configuración de un proveedor de afirmación de identidad de negociación](#) en la guía *Oracle Fusion Middleware Securing Oracle WebLogic Server*.
- [Configurar proveedores de autenticación y afirmación de identidad](#) en la *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help*.

Al crear el proveedor de afirmación de identidad de negociación, establezca la opción Indicador de control de JAAS en `SUFFICIENT` para todos los autenticadores. Consulte la sección sobre establecimiento del indicador de control JAAS en la [Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help](#).

### Creación de identificación de Kerberos para WebLogic Server

En el equipo de controlador de dominios de Active Directory, cree objetos de usuario que representen a WebLogic Server y al servidor web de EPM System, y asígneles a los nombres principales de servicio (SPN) que representen su instancia de WebLogic Server y al servidor web en el dominio de Kerberos. Los clientes no encuentran un servicio que no tenga un SPN. Los SPN se almacenan en archivos de tabla e claves que se copian en el dominio de WebLogic Server para usarse en el proceso de inicio de sesión.

Consulte [Creación de identificación para WebLogic Server](#) en la guía *Oracle Fusion Middleware Securing Oracle WebLogic Server* para ver los procedimientos detallados.

Para crear la identificación de Kerberos para WebLogic Server:

1. En la máquina del controlador de dominios de Active Directory, cree una cuenta de usuario, por ejemplo, `epmHost`, para el equipo que aloja el dominio de WebLogic Server.



 **Nota:**

Cree la identificación como objeto de usuario, no como equipo. Utilice el nombre simple del equipo, por ejemplo, use `epmHost` si el host se denomina `epmHost.example.com`.

Registre la contraseña que usar al crear el objeto de usuario. Lo necesitará para crear SPN.

No seleccione ninguna opción de contraseña, especialmente la opción `User must change password at next logon`.

2. Modifique el objeto de usuario para cumplir con el protocolo Kerberos. La cuenta debe exigir la autenticación de Kerberos previa
  - En el separador **Cuenta**, seleccione el cifrado que usar.
  - Asegúrese de que no se haya seleccionado ninguna otra opción de cuenta (especialmente `Do not require Kerberos pre-authentication`).
  - Como la configuración del tipo de cifrado puede que haya dañado la contraseña del objeto, restablezca la contraseña a la que haya establecido al crear el objeto.
3. En el equipo que aloja el controlador de dominios de Active Directory, abra una ventana de símbolo del sistema y vaya al directorio donde estén instaladas las herramientas de soporte de Active Directory.
4. Cree y configure los SPN necesarios.
  - a. Use un comando similar al siguiente para verificar que los SPN estén asociados al objeto de usuario (`epmHost`) que ha creado en el paso 1 de este procedimiento.

```
setspn -L epmHost
```

- b. Con un comando como el siguiente, configure el SPN para WebLogic Server en Active Directory Domain Services (AD DS) y genere un archivo de tabla de claves que contenga la clave secreta compartida.

```
ktpass -princ HTTP/epmHost.example.com@EXAMPLE.COM -pass password -mapuser epmHost -out c:\epmHost.keytab
```

5. Cree un archivo de tabla de claves en el equipo que aloja la instancia de WebLogic Server.
  - a. Acceda a una línea de comandos.
  - b. Vaya a `MIDDLEWARE_HOME/jdk/bin`.
  - c. Ejecute un comando como el siguiente:
 

```
ktab -k keytab_filename -a epmHost@example.com
```
  - d. Cuando se le pida una contraseña, introduzca aquella que haya establecido al crear el usuario en el paso 1 de este procedimiento.
6. Copie el archivo de tabla de claves en el directorio de inicio del dominio de WebLogic, por ejemplo, en `C:\Oracle\Middleware\user_projects\domains\EPMSys`.

7. Verifique que la autenticación de Kerberos funciona correctamente.

```
kinit -k -t keytab-file account-name
```

En este comando, `account-name` indica el principal de Kerberos, por ejemplo, `HTTP/epmHost.example.com@EXAMPLE.COM`. La salida de este comando debe ser similar a la siguiente:

```
New ticket is stored in cache file C:\Documents and
Settings\Username\krb5cc_MachineB
```

### Actualización de opciones de JVM para Kerberos

Consulte [Uso de argumentos de inicio para la autenticación de Kerberos con WebLogic Server](#) y [Creación de un archivo de inicio de sesión de JAAS en Oracle Fusion Middleware Securing Oracle WebLogic Server 11g Release 1 \(10.3.1\)](#).

Si los servidores gestionados de EPM System se ejecutan como servicios de Windows, actualice el registro de Windows para establecer las opciones de inicio de JVM.

Para actualizar las opciones de inicio de JVM en el registro de Windows:

1. Abra el Editor del Registro de Windows.
2. Seleccione **Equipo, HKEY\_LOCAL\_MACHINE, Software, Hyperion Solutions, Foundationservices0** y, a continuación, **HyS9EPMServer\_epmsystem1**.
3. Cree los siguientes valores de cadena:

 **Nota:**

Los nombres que aparecen en la siguiente tabla son ejemplos.

**Tabla 3-3 Opciones de inicio de JVM para la autenticación de Kerberos**

| Nombre      | Tipo   | Datos                                                                                       |
|-------------|--------|---------------------------------------------------------------------------------------------|
| JVMOption44 | REG_SZ | -Djava.security.krb5.realm= <i>Active Directory Realm Name</i>                              |
| JVMOption45 | REG_SZ | -Djava.security.krb5.kdc= <i>Active Directory host name or IP address</i>                   |
| JVMOption46 | REG_SZ | -<br>Djava.security.auth.login.config= <i>location of Kerberos login configuration file</i> |
| JVMOption47 | REG_SZ | -<br>Djavax.security.auth.useSubjectCredsOnly= <i>false</i>                                 |

4. Actualice el valor de JVMOptionCount DWord para que refleje los valores de JVMOptions agregados (agregue 4 al valor decimal actual).

## Configuración de políticas de autorización

Consulte [Opciones para proteger la aplicación web y los recursos de EJB](#) en la guía *Oracle Fusion Middleware Securing Resources Using Roles and Policies for Oracle WebLogic Server* para obtener información sobre la configuración de las políticas de autorización para los usuarios de Active Directory que accedan a EPM System.

Para conocer los pasos de configuración de la política de ejemplo, consulte [Creación de políticas para SSODiag](#).

## Uso de SSODiag para probar el entorno de Kerberos

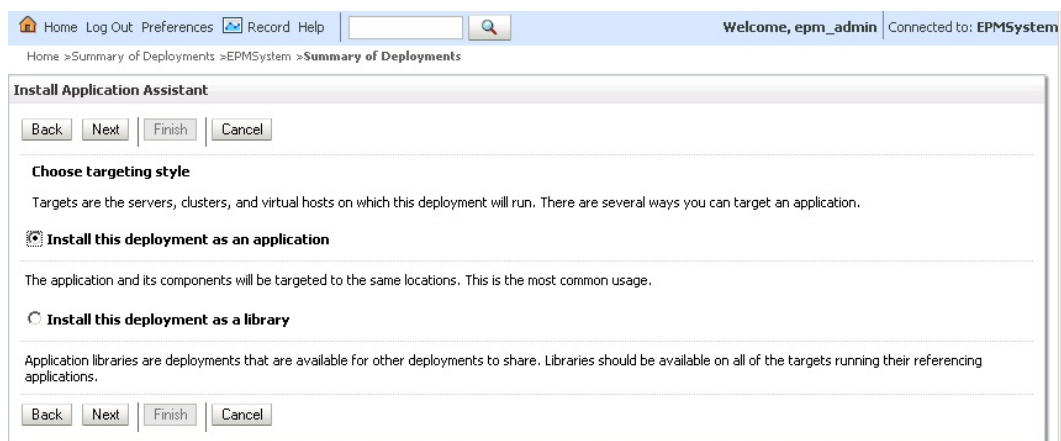
SSODiag es una aplicación web de diagnóstico que prueba si la instancia de WebLogic Server de su entorno de Kerberos está lista para soportar EPM System.

## Despliegue de SSODiag

Utilice las credenciales de administrador de WebLogic Server (el nombre de usuario predeterminado es `epm_admin`) que ha especificado al desplegar Foundation Services para desplegar SSODiag.

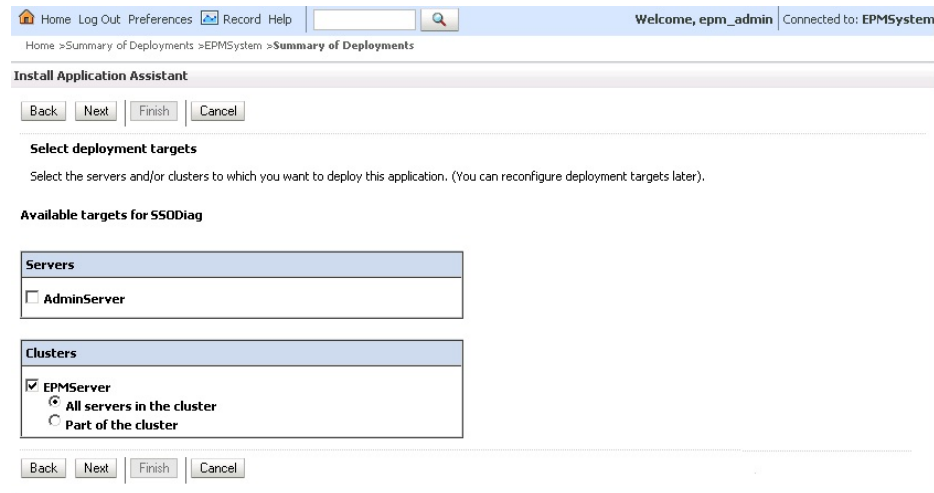
Para desplegar y configurar SSODiag:

1. Inicie sesión en la consola de administración de WebLogic Server para el dominio de EPM System.
2. En Centro de cambios, seleccione **Bloquear y editar**.
3. En **EPMSystem** en **Estructura de dominio**, haga clic en **Despliegues**.
4. En **Resumen de despliegues**, haga clic en **Instalar**.
5. En **Ruta**, seleccione `EPM_ORACLE_HOME/products/Foundation/AppServer/InstallableApps/common/SSODiag.war`.
6. Haga clic en **Siguiente**.
7. En **Seleccionar estilo de direccionamiento**, asegúrese de que se haya seleccionado **Instalar despliegue como aplicación** y, a continuación, haga clic en **Siguiente**.

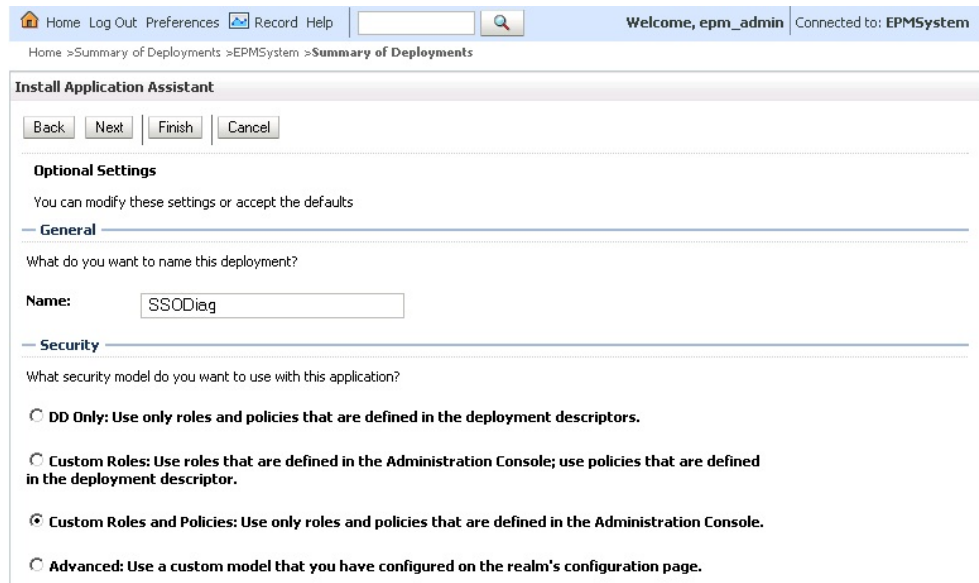


8. En **Seleccionar destinos de despliegue**, elija lo siguiente y, a continuación, haga clic en **Siguiente**.
  - **EPMServer**

- **Todos los servidores del cluster**



9. En **Configuración opcional**, seleccione **Roles y políticas personalizados**: **utilice solo roles y políticas definidos en la consola de administración** como modelo de seguridad.



10. Haga clic en **Siguiente**.
11. En la pantalla de revisión, seleccione **No, revisaré la configuración más tarde**.
12. Haga clic en **Finalizar**.
13. En Centro de cambios, seleccione **Activar cambios**.

### Configuración de Oracle HTTP Server para SSODiag

Actualice `mod_wl_ohs.conf` para configurar Oracle HTTP Server y reenviar las solicitudes de URL de SSODiag a la instancia de WebLogic Server.

Para configurar el reenvío de URL en Oracle HTTP Server:

1. Con un editor de texto, abra `EPM_ORACLE_INSTANCE/httpConfig/ohs/config/fmwconfig/components/OHS/ohs_component/mod_wl_ohs.conf`.
2. Agregue una definición de `LocationMatch` para `SSODiag`:

```
<LocationMatch /SSODiag/>
 SetHandler weblogic-handler
 WeblogicCluster myServer:28080
</LocationMatch>
```

En el ejemplo anterior, `myServer` indica que el equipo de host de Foundation Services y `28080` representa el puerto en el que Servicios compartidos de Oracle Hyperion escucha las solicitudes.

3. Guarde y cierre `mod_wl_ohs.conf`.
4. Reinicie Oracle HTTP Server.

### Creación de políticas para SSODiag

Cree una política en la consola de administración de WebLogic Server para proteger la siguiente URL de SSODiag.

```
http://OHS_HOST_NAME:PORT/SSODiag/krbssodiag
```

En este ejemplo, `OHS_HOST_NAME` indica el nombre del servidor que aloja Oracle HTTP Server y `PORT` indica el puerto donde Oracle HTTP Server escucha las solicitudes.

Para crear políticas para proteger SSODiag:

1. En el Centro de cambios, en la consola de administración de WebLogic Server para el dominio de EPM System, seleccione **Bloquear y editar**.
2. Seleccione **Despliegues, SSODiag, Seguridad, URLPatterns** y, a continuación, **Políticas**.
3. Cree los siguientes patrones de URL:
  - /
  - /index.jsp
4. Modifique cada patrón de URL que haya creado:
  - a. En la lista de patrones de URL de **Patrones de URL de aplicación web autónoma**, abra el patrón (/) que haya creado haciendo clic en él.
  - b. Seleccione **Agregar condiciones**.
  - c. En **Lista de predicados**, seleccione **Usuario**.
  - d. Seleccione **Siguiente**.
  - e. En **Nombre del argumento de usuario**, introduzca el usuario de Active Directory cuya cuenta se usa para acceder a un escritorio de cliente configurado para la autenticación de Kerberos, por ejemplo, `krbuser1` y seleccione **Agregar**. `krbuser1` es un usuario de Active Directory o de escritorio de Windows.
  - f. Seleccione **Finalizar**.
5. Seleccione **Guardar**.

## Uso de SSODiag para probar la configuración de WebLogic Server para la autenticación de Kerberos

Si la configuración de WebLogic Server para la autenticación de Kerberos funciona correctamente, en la página *Oracle Hyperion Kerberos SSO diagnostic Utility V 1.0* aparece el siguiente mensaje:

```
Retrieving Kerberos User principal name... Success.
Kerberos principal name retrieved... SOME_USER_NAME
```

### ▲ Atención:

No configure los componentes de EPM System para la autenticación de Kerberos si SSODiag no puede recuperar el nombre de principal de Kerberos.

Para probar la configuración de WebLogic Server para la autenticación de Kerberos:

1. Inicie Foundation Services y Oracle HTTP Server.
2. Con la consola de administración de WebLogic Server, inicie la aplicación web de SSODiag para atender todas las solicitudes.
3. Inicie sesión en un equipo de cliente configurado para la autenticación de Kerberos con credenciales de Active Directory válidas.
4. Con un explorador, conéctese a la siguiente URL de SSODiag:

```
http://OHS_HOST_NAME:PORT/SSODiag/krbssodiag
```

En este ejemplo, *OHS\_HOST\_NAME* indica el nombre del servidor que aloja Oracle HTTP Server y *PORT* indica el puerto donde Oracle HTTP Server escucha las solicitudes.

Si la autenticación de Kerberos funciona correctamente, SSODiag muestra la información siguiente:

```
Retrieving Kerberos User principal name... Success.
Kerberos principal name retrieved... SOME_USER_NAME
```

Si la autenticación de Kerberos no funciona correctamente, SSODiag muestra la información siguiente:

```
Retrieving Kerberos User principal name... failed.
```

## Cambio del modelo de seguridad

El modelo de seguridad predeterminado para las aplicaciones web protegidas por el dominio de seguridad es `DDonly`. Debe cambiar el modelo de seguridad a `CustomRolesAndPolicies`.

Para cambiar el modelo de seguridad:

1. Con un editor de texto, abra `MIDDLEWARE_HOME/user_projects/domains/EPMSystem/config/config.xml`.
2. Busque el elemento siguiente en el descriptor de despliegue de aplicaciones para cada componente de Foundation Services:

```
<security-dd-model>DDOnly</security-dd-model>
```

3. Cambie el modelo de seguridad como se detalla a continuación para cada componente:

```
<security-dd-model>CustomRolesAndPolicies</security-dd-model>
```

4. Guarde y cierre `config.xml`.

### Actualización de la configuración de seguridad de EPM System

Cambie la configuración de seguridad de EPM System para activar el inicio de sesión único de Kerberos.

Para configurar EPM System para la autenticación de Kerberos:

1. Inicie sesión en Consola de Servicios compartidos como administrador.
2. Agregue el dominio de Active Directory que esté configurado para la autenticación de Kerberos como directorio de usuario externo en Servicios compartidos. Consulte "Configuración de OID, Active Directory y otros directorios de usuarios basados en LDAP" en la *Guía de administración de seguridad de usuarios de Oracle Enterprise Performance Management System*.
3. Active el inicio de sesión único. Consulte [Configuración de OID, Active Directory y otros directorios de usuario basados en LDAP](#).  
En **Opciones de seguridad**, seleccione la configuración de la tabla que aparece a continuación para activar el inicio de sesión único de Kerberos.

**Tabla 3-4 Configuración para activar el inicio de sesión único de Kerberos**

| Campo                                        | Configuración necesaria                  |
|----------------------------------------------|------------------------------------------|
| Activar inicio de sesión único               | Seleccionadas                            |
| Agente o proveedor de inicio de sesión único | Otros                                    |
| Mecanismo de inicio de sesión único          | Obtener usuario remoto de solicitud HTTP |

4. Reinicie Foundation Services.

### Prueba del inicio de sesión único de Kerberos

Inicie sesión en Foundation Services para verificar que el inicio de sesión único de Kerberos funciona correctamente.

Para probar el inicio de sesión único de Kerberos:

1. Verifique que Foundation Services y Oracle HTTP Server se están ejecutando.
2. Inicie sesión en un equipo de cliente configurado para la autenticación de Kerberos con credenciales de Active Directory válidas.
3. Con un explorador, conéctese a la URL de Foundation Services.

## Configuración de los componentes de EPM System

Con EPM System Configurator, configure y despliegue otros componentes de EPM System en el dominio de WebLogic donde se despliegue Foundation Services.

## Configuración de servidores gestionados de EPM System para la autenticación de Kerberos

En entornos de Microsoft Windows, los servidores gestionados de EPM System se ejecutan como servicios de Windows. Debe modificar las opciones de JVM de inicio para cada servidor gestionado de WebLogic. Lista completada de servidores gestionados en modo de despliegue no compacto:

- AnalyticProviderServices0
- CalcMgr0
- ErpIntegrator0
- EssbaseAdminServer0
- FinancialReporting0
- HFMWeb0
- FoundationServices0
- HpsAlerter0
- HpsWebReports0
- Planning0
- Profitability0

Si las aplicaciones web de EPM System se despliegan en el modo de despliegue compacto, debe actualizar las opciones de JVM de inicio solo del servidor gestionado de `EPMSysTem0`. Si tiene varios servidores gestionados compactos, debe actualizar las opciones de JVM de inicio para todos los servidores gestionados.

Consulte [Uso de argumentos de inicio para la autenticación de Kerberos con WebLogic Server](#) en la guía *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

### Nota:

En el siguiente procedimiento se describe cómo establecer las opciones de JVM de inicio para el servidor gestionado de FoundationServices. Debe realizar esta tarea para cada servidor gestionado de WebLogic en el despliegue.

Para obtener procedimientos detallados para configurar opciones de JVM en los scripts de inicio de WebLogic Server, consulte [Actualización de opciones de JVM para Kerberos](#).

Para configurar opciones de JVM en los scripts de inicio de WebLogic Server



## Configuración de políticas de autorización

Configure las políticas de autorización para los usuarios de Active Directory que accederán a los componentes de EPM System que no sean Foundation Services. Consulte [Configuración de políticas de autorización](#) para obtener información sobre la configuración de las políticas de seguridad en la consola de administración de WebLogic.

## Cambio del modelo de seguridad predeterminado de los componentes de EPM System

El archivo de configuración de EPM System se edita para cambiar el modelo de seguridad predeterminado. En el caso de los despliegues de EPM System no compactos, debe cambiar el modelo de seguridad predeterminado de cada aplicación web de EPM System registrada en `config.xml`. Lista de aplicaciones web de EPM System:

- AIF
- APS
- CALC
- EAS
- FINANCIALREPORTING
- PLANNING
- PROFITABILITY
- SHARED SERVICES
- WORKSPACE

Para cambiar el modelo de seguridad:

1. Con un editor de texto, abra `MIDDLEWARE_HOME/user_projects/domains/EPMSystem/config/config.xml`
2. En la definición del despliegue de aplicaciones de cada componente de EPM System, establezca el valor de `<security-dd-model>` en `CustomRolesAndPolicies`, como se muestra en el siguiente ejemplo:

```
<app-deployment>
 <name>SHARED SERVICES#11.1.2.0</name>
 <target>EPMServer</target>
 <module-type>ear</module-type>
 <source-path>C:\Oracle\Middleware\EPMSystem11R1/products/Foundation/
AppServer/InstallableApps/common/interop.ear</source-path>
 <security-dd-model>CustomRolesAndPolicies</security-dd-model>
 <staging-mode>nostage</staging-mode>
</app-deployment>
```

3. Guarde y cierre `config.xml`.
4. Reinicie la instancia de WebLogic Server.

## Creación de políticas de protección de URL para los componentes de EPM System

Cree una política de protección de URL en la consola de administración de WebLogic Server para proteger cada URL de componente de EPM System. Consulte [Opciones para proteger las aplicaciones web y los recursos de EJB](#) en la guía *Oracle Fusion Middleware Securing Resources Using Roles and Policies for Oracle WebLogic Server* para obtener detalles.

Para crear políticas de protección de URL:

1. En el Centro de cambios, en la consola de administración de WebLogic Server para el dominio de EPM System, haga clic en **Bloquear y editar**.
2. Haga clic en **Despliegues**.
3. Expanda una aplicación empresarial de EPM System (por ejemplo, `PLANNING`) en el despliegue y, a continuación, haga clic en su aplicación web (por ejemplo, `HyperionPlanning`). Consulte [Cambio del modelo de seguridad predeterminado de los componentes de EPM System](#) para obtener una lista de los componentes de EPM System.

 **Nota:**

Algunas aplicaciones empresariales, por ejemplo Oracle Essbase Administration Services, incluyen varias aplicaciones web para las que se deben definir los patrones de URL.

4. Cree una política de ámbito de patrón de URL para la aplicación web.
  - AIF
  - APS
  - CALC
  - EAS
  - FINANCIALREPORTING
  - PLANNING
  - PROFITABILITY
  - SHAREDSEVICES
  - WORKSPACE
  - a. Haga clic en **Seguridad, Políticas** y, a continuación, **Nueva**.
  - b. En **Patrón de URL**, introduzca las URL protegidas y desprotegidas de los productos de EPM System. Consulte [Protección y desprotección de recursos de EPM System](#) para obtener más información.
  - c. Haga clic en **Aceptar**.
  - d. Haga clic en el patrón de URL que haya creado.
  - e. Haga clic en **Agregar condiciones**.
  - f. En **Lista de predicados**, seleccione una condición de política y, a continuación, haga clic en **Siguiente**. Oracle recomienda el uso de la condición `Group`, que otorga esta política de seguridad a todos los miembros de un grupo especificado.
  - g. Especifique los argumentos que pertenezcan al predicado que elija. Por ejemplo, si ha elegido `Group` en el paso anterior, debe realizar los siguientes pasos:
  - h. En **Nombre del argumento de grupo**, introduzca el nombre del grupo que contenga los usuarios que deben tener acceso a la aplicación web. El nombre

que introduzca debe coincidir exactamente con un nombre de grupo de Active Directory.

- Haga clic en **Agregar**.
  - Repita los pasos anteriores para agregar más grupos.
  - i. Haga clic en **Finalizar**.  
WebLogic Server muestra un mensaje de error si no encuentra el grupo en Active Directory. Debe corregir este error antes de continuar.
  - j. Seleccione **Guardar**.
5. Repita el paso 3 y el paso 4 de este procedimiento para el resto de componentes de EPM System de su despliegue.
  6. En el Centro de cambios, haga clic en **Configuración de liberación**.
  7. Reinicie WebLogic Server.

### Activación de la autenticación basada en el certificado del cliente en aplicaciones web

Inserte la definición de `login-config` en el archivo de configuración de los siguientes archivos de aplicaciones que se encuentran en `EPM_ORACLE_HOME/products/`.

- `Essbase/eas/server/AppServer/InstallableApps/Common/eas.ear`
- `FinancialDataQuality/AppServer/InstallableApps/aif.ear`
- `financialreporting/InstallableApps/HReports.ear`
- `Profitability/AppServer/InstallableApps/common/profitability.ear`

Para activar la autenticación basada en el certificado del cliente:

1. Detenga los componentes y procesos de EPM System.
2. Mediante 7 Zip, expanda un archivo web contenido en un archivo de empresa; por ejemplo, `EPM_ORACLE_HOME/products/Essbase/eas/server/AppServer/InstallableApps/Common/eas.ear/eas.war`.
3. Acceda a `WEB-INF`.
4. Modifique `web.xml` agregando la siguiente definición `login-config` inmediatamente antes del elemento `</webapp>`:

```
<login-config>
 <auth-method>CLIENT-CERT</auth-method>
</login-config>
```

5. Guarde `web.xml`.
6. Haga clic en **Sí** cuando 7 Zip consulte si desea actualizar el archivo.

### Actualización de la configuración de seguridad de EPM System

Configure la seguridad de EPM System para mantener el inicio de sesión único. Consulte [Configuración de EPM System para inicio de sesión único](#).

## Configuración de EPM System para inicio de sesión único

Los productos de Oracle Enterprise Performance Management System se deben configurar de forma que soporten al agente de seguridad para el inicio de sesión único. La configuración especificada en Servicios compartidos de Oracle Hyperion determina lo siguiente para todos los productos de EPM System:

- Si aceptar o no el inicio de sesión único desde un agente de seguridad
- El mecanismo de autenticación para aceptar el inicio de sesión único

En un entorno habilitado para el inicio de sesión único, el producto de EPM System al que el usuario accede primero analiza el mecanismo de inicio de sesión único para recuperar el ID de usuario autenticado contenido en él. El producto de EPM System comprueba el ID de usuario con los directorios de usuario configurados en Servicios compartidos para determinar que el usuario sea un usuario de EPM System válido. También envía un símbolo que habilita el inicio de sesión único en los productos de EPM System.

La configuración especificada en Shared Services habilita el inicio de sesión único y determina el mecanismo de autenticación para aceptar el inicio de sesión único en todos los productos de EPM System.

Para activar el inicio de sesión único desde una solución de gestión de identidades web:

1. Inicie Consola de Servicios compartidos de Oracle Hyperion como administrador de Servicios compartidos. Consulte [Inicio de Shared Services Console](#).
2. Seleccione **Administración** y, a continuación, **Configurar directorios de usuario**.
3. Compruebe que los directorios de usuario utilizados por la solución de gestión de identidades web se han configurado como directorios de usuario externos en Servicios compartidos.

Por ejemplo, para activar el inicio de sesión único de Kerberos, debe configurar Active Directory que está configurado para la autenticación de Kerberos como directorio de usuario externo.

Para obtener información sobre las instrucciones, consulte Configuración de directorios de usuario.

4. Seleccione **Opciones de seguridad**.
5. Seleccione **Mostrar opciones avanzadas**.
6. En **Configuración de inicio de sesión único**, en la pantalla Directorios de usuario definidos, realice las acciones siguientes:
  - a. Seleccione **Activar inicio de sesión único**.
  - b. En **Agente o proveedor de inicio de sesión único**, elija una solución de gestión de identidades web. Elija **Otro** si está configurando el inicio de sesión único con Kerberos.

El mecanismo de inicio de sesión único recomendado se seleccionará automáticamente. Consulte la siguiente tabla. Consulte también [Métodos de inicio de sesión único soportados](#).

 **Nota:**

Si no está utilizando el mecanismo de inicio de sesión único recomendado, debe elegir `Otro` en **Agente o proveedor de inicio de sesión único**. Por ejemplo, si desea utilizar un mecanismo distinto de la cabecera HTTP para SiteMinder, elija `Other` en **Agente o proveedor de inicio de sesión único** y, a continuación, escoja el mecanismo de inicio de sesión único que desee utilizar en **Mecanismo de inicio de sesión único**.

**Tabla 3-5 Mecanismos de inicio de sesión único preferidos para las soluciones de administración de identidades web**

Solución de administración de identidades web	Mecanismo de inicio de sesión único recomendado
Oracle Access Manager	Custom HTTP Header <sup>1</sup>
OSSO	Custom HTTP Header
SiteMinder	Custom HTTP Header
Kerberos	Obtener usuario remoto de solicitud HTTP

<sup>1</sup> El nombre de cabecera HTTP predeterminado es `HYPLOGIN`. Si va a utilizar una cabecera HTTP personalizada, reemplace el nombre.

- Haga clic en **Aceptar**.

## Opciones de inicio de sesión único para Smart View

Si bien Oracle Smart View for Office es un cliente grueso y no un explorador, se conecta a componentes de servidor usando HTTP y se comporta como un explorador desde una perspectiva del sistema. Smart View soporta todos los métodos de integración basados en web estándar que soportan las interfaces del explorador. Sin embargo, existen algunas limitaciones:

- Si se inicia Smart View desde una sesión de explorador existente que esté conectada a un componente de Oracle Enterprise Performance Management System, los usuarios deben volver a iniciar sesión en Smart View, porque no comparte la cookie de la sesión existente.
- Si está usando un formulario de inicio de sesión basado en HTML personalizado en lugar del formulario de inicio de sesión de Oracle Access Manager predeterminado, asegúrese de que el origen del formulario personalizado incluya la cadena `loginform`. Esto es necesario para permitir que funcione la integración de Smart View con Oracle Access Manager.

# 4

## Configuración de directorios de usuario

### Consulte también:

- [Directorios de usuarios y seguridad de EPM System](#)
- [Operaciones relacionadas con la configuración de directorios de usuario](#)
- [Oracle Identity Manager y EPM System](#)
- [Información sobre Active Directory](#)
- [Configuración de OID, Active Directory y otros directorios de usuario basados en LDAP](#)
- [Configuración de bases de datos relacionales como directorios de usuario](#)
- [Prueba de conexiones de directorios de usuario](#)
- [Edición de configuración de directorio de usuario](#)
- [Supresión de configuraciones de directorios de usuario](#)
- [Administración del orden de búsqueda de directorios de usuario](#)
- [Establecimiento de las opciones de seguridad](#)
- [Regeneración de claves de cifrado](#)
- [Utilización de caracteres especiales](#)

## Directorios de usuario y seguridad de EPM System

Los productos de Oracle Enterprise Performance Management System se admiten en un gran número de sistemas de administración de identidades y usuarios, denominados colectivamente como directorios de usuario. Entre estos se incluyen los directorios de usuario compatibles con LDAP (protocolo de acceso a directorios ligero), como Sun Java System Directory Server (anteriormente denominado SunONE Directory Server) y Active Directory. EPM System también admite bases de datos relacionales como directorio de usuario externo.

Normalmente, los productos de EPM System usan el directorio nativo y los directorios de usuario externos en el aprovisionamiento. Consulte la [Matriz de certificación de Oracle Enterprise Performance Management System](#) para obtener una lista de los directorios de usuario soportados.

Los productos de EPM System requieren una cuenta de directorio de usuario para todos los usuarios que acceden a los productos. Estos usuarios se pueden asignar a los grupos para facilitar el aprovisionamiento. Los usuarios y los grupos se pueden aprovisionar LCA de funciones y objetos de EPM System. Dada la sobrecarga administrativa, Oracle no recomienda el aprovisionamiento de usuarios individuales. Los usuarios y grupos de todos los directorios de usuario configurados se muestran en Oracle Hyperion Shared Services Console.

De manera predeterminada, EPM System Configurator configura el repositorio de Servicios compartidos como el directorio nativo que soporta los productos de EPM System. Los

gestores de directorios acceden al directorio nativo mediante Consola de Servicios compartidos y lo gestionan.

## Operaciones relacionadas con la configuración de directorios de usuario

Para soportar el inicio de sesión único y la autorización, los administradores del sistema deben configurar directorios de usuario externos. En Consola de Servicios compartidos de Oracle Hyperion, los administradores del sistema pueden realizar varias tareas relacionadas con la configuración y gestión de directorios de usuario. En estos temas se proporcionan instrucciones:

- Configuración de los directorios de usuario:
  - [Configuración de OID, Active Directory y otros directorios de usuario basados en LDAP](#)
  - [Configuración de bases de datos relacionales como directorios de usuario](#)
- [Prueba de conexiones de directorios de usuario](#)
- [Edición de configuración de directorio de usuario](#)
- [Supresión de configuraciones de directorios de usuario](#)
- [Administración del orden de búsqueda de directorios de usuario](#)
- [Establecimiento de las opciones de seguridad](#)

## Oracle Identity Manager y EPM System

Oracle Identity Manager es una solución de administración de funciones y usuarios que automatiza el proceso de adición, actualización y supresión de cuentas de usuario y derechos a nivel de atributo en los recursos de empresa. Oracle Identity Manager está disponible como producto independiente o como parte de Oracle Identity and Access Management Suite Plus.

Oracle Enterprise Performance Management System se integra con Oracle Identity Manager mediante roles de empresa que son grupos LDAP. Se puede asignar las funciones de los componentes de EPM System a las funciones de empresa. Los usuarios o grupos que se agreguen a las funciones de empresa de Oracle Identity Manager heredarán automáticamente las funciones asignadas de EPM System.

Por ejemplo, si tiene una aplicación de Oracle Hyperion Planning llamada *Planificación de presupuesto*. Para admitir esta aplicación, puede crear tres funciones de empresa (Usuario interactivo de Planificación de presupuesto, Usuario final de Planificación de presupuesto y Administrador de Planificación de presupuesto) en Oracle Identity Manager. Al aprovisionar los roles de EPM System, asegúrese de aprovisionar a los gestores de aprovisionamiento los roles de empresa desde Oracle Identity Manager con los roles necesarios de *Planificación de presupuesto* y otros componentes de EPM System incluido Servicios compartidos. Todos los usuarios y grupos asignados a las funciones de empresa de Oracle Identity Manager heredan las funciones de EPM System. Consulte la documentación de Oracle Identity Manager para obtener más información sobre el despliegue y la administración de Oracle Identity Manager.

Para integrar Oracle Identity Manager con EPM System, los administradores deben realizar estos pasos:

- Asegúrese de que los miembros (usuarios y grupos) de los roles de empresa de Oracle Identity Manager que se vayan a utilizar para el aprovisionamiento de EPM System están definidos en un directorio de usuario activado para LDAP, por ejemplo, OID o Active Directory.
- Configure el directorio de usuarios habilitado para LDAP en el que se han definido los miembros de las funciones de empresa como directorio de usuarios externo en EPM System. Consulte [Configuración de OID, Active Directory y otros directorios de usuario basados en LDAP](#).

## Información sobre Active Directory

En esta sección se explican algunos conceptos de Active Directory utilizados en este documento.

### Búsqueda DNS y búsqueda de nombre de host

Los administradores del sistema pueden configurar Active Directory de forma que Servicios compartidos de Oracle Hyperion pueda realizar una búsqueda de nombres de host estático o una búsqueda de DNS para identificar a Active Directory. La búsqueda de nombre de host estático no soporta el failover de Active Directory.

El empleo de la búsqueda DNS garantiza la alta disponibilidad de Active Directory en escenarios donde este se configura en varios controladores de dominio para garantizar precisamente eso, la alta disponibilidad. Cuando se configura para realizar una búsqueda DNS, Shared Services consulta al servidor DNS para identificar controladores de dominio registrados y conectar con el controlador con mayor peso. Si el controlador de dominio con el que se conecte Servicios compartidos falla, Servicios compartidos cambia de forma dinámica al siguiente controlador con mayor ponderación.

#### Nota:

La búsqueda DNS solo se puede configurar si hay disponible una configuración de Active Directory redundante que soporte el failover. Consulte la documentación de Microsoft para obtener más información.

### Catálogo global

Un catálogo global es un controlador de dominio que almacena una copia de todos los objetos de Active Directory de un bosque. Almacena una copia completa de todos los objetos en el directorio correspondiente a su dominio host y una copia parcial de todos los objetos correspondientes al resto de dominios del bosque, que se utilizan en operaciones de búsqueda de usuarios típicas. Consulte la documentación de Microsoft para obtener información sobre la configuración de un catálogo global.

Si su organización está utilizando un catálogo global, use uno de estos métodos para configurar Active Directory:

- Configure el servidor del catálogo global como directorio de usuario externo (recomendado).



- Configure cada dominio de Active Directory como directorio de usuario externo independiente.

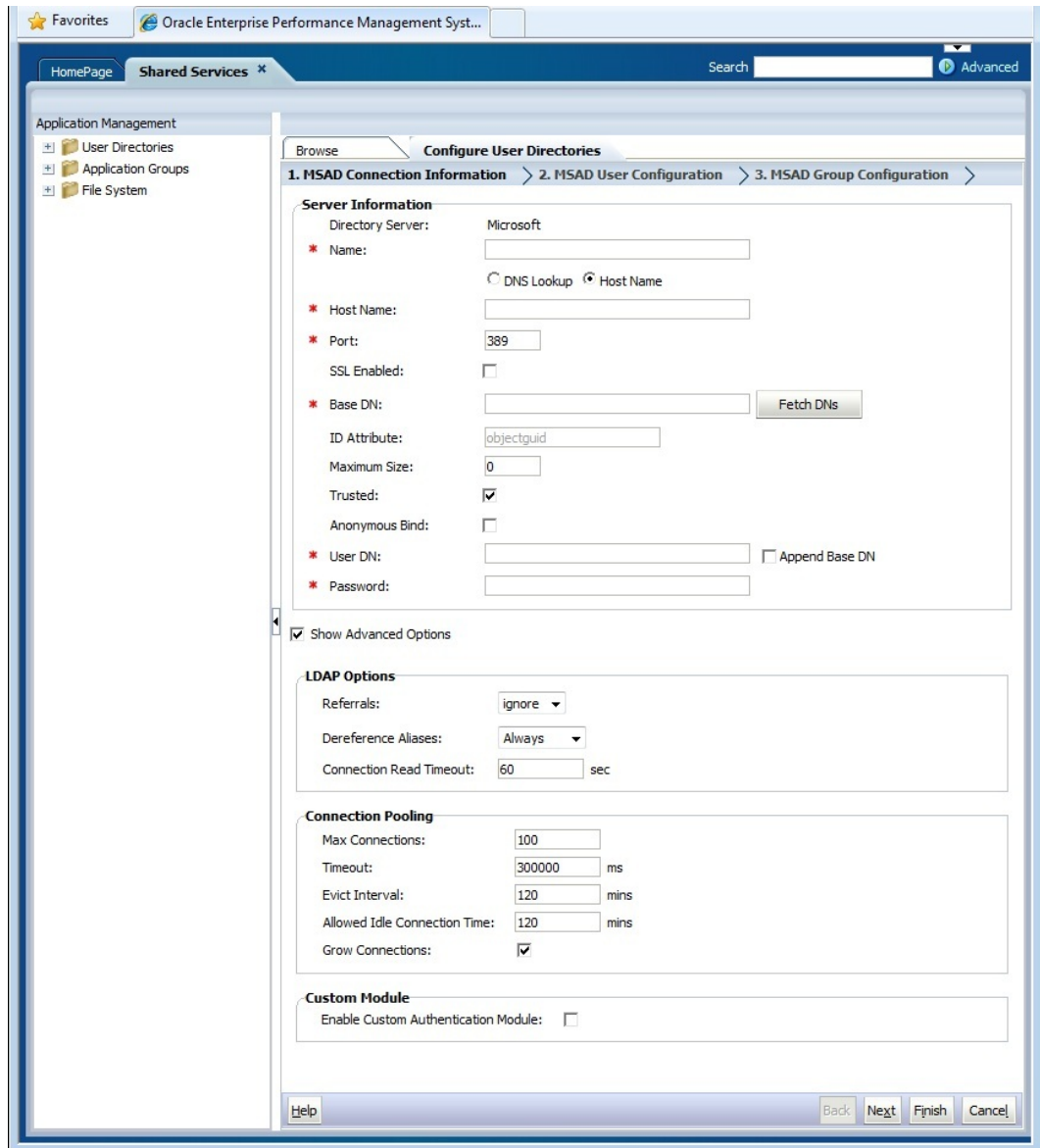
La configuración del catálogo global en lugar de dominios de Active Directory individuales permite a los productos de Oracle Enterprise Performance Management System acceder a grupos universales y locales dentro del bosque.

## Configuración de OID, Active Directory y otros directorios de usuario basados en LDAP

Los administradores del sistema utilizan los procedimientos descritos en esta sección para configurar cualquier directorio de usuario corporativo basado en LDAP, como OID, Sun Java System Directory Server, Oracle Virtual Directory, Active Directory, IBM Tivoli Directory Server o un directorio de usuario basado en LDAP que no aparezca en la pantalla de configuración.

Para configurar OID, Active Directory y otros directorios de usuario basados en LDAP:


1. Acceda a Oracle Hyperion Shared Services Console como administrador del sistema. Consulte [Inicio de Shared Services Console](#).
2. Seleccione **Administración** y, a continuación, **Configurar directorios de usuario**.  
Se abre la pestaña Configuración de proveedor. En esta pantalla se muestran todos los directorios de usuario configurados, incluido el directorio nativo.
3. Haga clic en **Nuevo**.
4. En **Tipo de directorio**, seleccione una opción:
  - **Lightweight Directory Access Protocol (LDAP)** para configurar un directorio de usuario basado en LDAP distinto de Active Directory. Seleccione esta opción para configurar Oracle Virtual Directory.
  - **Microsoft Active Directory (MSAD)** para configurar Active Directory.  
**Solo para Active Directory y Active Directory Application Mode (ADAM):** si desea utilizar un atributo de ID personalizado (un atributo que no sea `ObjectGUID`; por ejemplo, `sAMAccountName`) con Active Directory o ADAM, seleccione **Protocolo de acceso a directorios ligero (LDAP)** y configúrelo como tipo de directorio `Other`.
5. Haga clic en **Siguiente**.



6. Introduzca los parámetros necesarios.



**Tabla 4-1 Pantalla Información de conexión**

Etiqueta	Descripción
Servidor de directorios	<p>Seleccione un directorio de usuario. El valor <b>Atributo de ID</b> cambia al atributo de identidad constante recomendado para el producto seleccionado.</p> <p>Esta propiedad se selecciona automáticamente si elige Active Directory en el paso 4.</p> <p>Elija Otro en los siguientes escenarios:</p> <ul style="list-style-type: none"> <li>• Va a configurar un tipo de directorio de usuarios que no aparece en la lista; por ejemplo, Oracle Virtual Directory</li> <li>• Va a configurar un directorio de usuario activado para LDAP incluido en la lista (por ejemplo, OID), pero desea utilizar un atributo de ID personalizado.</li> <li>• Va a configurar Active Directory o ADAM para utilizar un atributo de ID personalizado.</li> </ul>
Nombre	<p><b>Ejemplo:</b> Oracle Internet Directory</p> <p>Nombre descriptivo para el directorio de usuario. Se utiliza para identificar un directorio de usuario específico si se configuran varios directorios de usuarios. El nombre no debe contener caracteres especiales distintos del espacio y el guión bajo.</p> <p><b>Ejemplo:</b> Corporate_OID</p>

 **Nota:**

Debido a que Oracle Virtual Directory proporciona una abstracción virtual de los directorios LDAP y de los repositorios de datos RDMBS en una vista de directorio, Oracle Enterprise Performance Management System lo considera un único directorio de usuario externo independientemente del número y tipo de directorios de usuario que soporte Oracle Virtual Directory.

**Tabla 4-1 (Continuación) Pantalla Información de conexión**

Etiqueta	Descripción
Búsqueda DNS	<p><b>Solo Active Directory:</b> seleccione esta opción para activar la búsqueda DNS. Consulte <a href="#">Búsqueda DNS y búsqueda de nombre de host</a>. Oracle recomienda configurar la búsqueda DNS como método para conectar a Active Directory en entornos de producción para evitar posibles fallos de conexión.</p>
	<div style="border-left: 2px solid #0070C0; border-right: 2px solid #0070C0; border-bottom: 2px solid #0070C0; padding: 10px;"> <p> <b>Nota:</b></p> <p>No seleccione esta opción si está configurando un catálogo global.</p> </div>
	<p>Al seleccionar esta opción aparecen los siguientes campos:</p> <ul style="list-style-type: none"> <li>• <b>Dominio:</b> nombre del dominio de un bosque de Active Directory. <b>Ejemplos:</b> <code>example.com</code> o <code>us.example.com</code></li> <li>• <b>Sitio de AD:</b> nombre del sitio de Active Directory; suele ser el nombre distintivo relativo al objeto de sitio almacenado en el contenedor de configuración de Active Directory. Normalmente, Sitio de AD identifica una ubicación geográfica, como puede ser una ciudad, estado, región o país. <b>Ejemplos:</b> <code>Santa Clara</code> o <code>US_West_region</code></li> <li>• <b>Servidor DNS:</b> nombre DNS del servidor que admite búsquedas de servidores DNS para controladores de dominio.</li> </ul>
Nombre de host	<p><b>Solo Active Directory:</b> seleccione esta opción para habilitar la búsqueda de nombre de host estático. Consulte <a href="#">Búsqueda DNS y búsqueda de nombre de host</a>.</p>
	<div style="border-left: 2px solid #0070C0; border-right: 2px solid #0070C0; border-bottom: 2px solid #0070C0; padding: 10px;"> <p> <b>Nota:</b></p> <p>Seleccione esta opción para configurar un catálogo global de Active Directory.</p> </div>

**Tabla 4-1 (Continuación) Pantalla Información de conexión**

Etiqueta	Descripción
Nombre de host	<p>Nombre DNS del servidor de directorios de usuario. Utilice el nombre de dominio completo si va a utilizar el directorio de usuario para admitir SSO desde SiteMinder. Oracle recomienda utilizar el nombre del host para establecer una conexión de Active Directory solo para pruebas.</p>
	<p> <b>Nota:</b></p> <p>Si está configurando un catálogo global de Active Directory, especifique el nombre de host del servidor de catálogo global. Consulte <a href="#">Catálogo global</a>.</p>
	<p><b>Ejemplo:</b> MyServer</p>
Puerto	<p>Número de puerto en el que se está ejecutando el directorio de usuario.</p>
	<p> <b>Nota:</b></p> <p>Si está configurando un catálogo global de Active Directory, especifique el puerto utilizado por el servidor de catálogo global (el valor predeterminado es 3268). Consulte <a href="#">Catálogo global</a>.</p>
	<p><b>Ejemplo:</b> 389</p>
SSL activado	<p>Casilla de verificación que habilita la comunicación segura con este directorio de usuario. El directorio de usuario debe configurarse para la comunicación segura.</p>
DN de base	<p>Nombre distintivo (DN) del nodo en el que debería comenzar la búsqueda de usuarios y grupos. Puede usar también el botón <b>Recuperar los DN</b> para mostrar los DN de base disponibles y seleccionar a continuación el DN de base adecuado de la lista.</p>
	<p> <b>Nota:</b></p> <p>Si está configurando un catálogo global, especifique el DN de base del bosque.</p>
	<p>Consulte <a href="#">Utilización de caracteres especiales</a> para ver las restricciones sobre el uso de caracteres especiales.</p> <p>Oracle recomienda la selección del DN más bajo que contenga todos los usuarios y grupos de productos de EPM System.</p> <p><b>Ejemplo:</b> dc=example,dc=com</p>

Tabla 4-1 (Continuación) Pantalla Información de conexión

Etiqueta	Descripción
Atributo de ID	<p>Este valor de atributo se puede modificar solamente si se selecciona <b>Otro</b> en <b>Tipo de directorio</b>. Este atributo debe ser un atributo común que exista en los objetos de usuario y de grupo en el servidor de directorios.</p> <p>El valor recomendado para este atributo se establece de forma automática para OID <code>orclguid</code>, SunONE (<code>nsuniqueid</code>), IBM Directory Server (<code>Ibm-entryUuid</code>), Novell eDirectory (<code>GUID</code>) y Active Directory (<code>ObjectGUID</code>).</p> <p><b>Ejemplo:</b> <code>orclguid</code></p> <p>Valor de atributo de ID, si lo establece manualmente después de seleccionar <b>Otro</b> en <b>Servidor de directorios</b>; por ejemplo, para configurar Oracle Virtual Directory, debe:</p> <ul style="list-style-type: none"> <li>• apuntar a un atributo único</li> <li>• no ser específico de la ubicación</li> <li>• no cambiar con el tiempo</li> </ul>
Tamaño máximo	<p>Número máximo de resultados que una búsqueda puede devolver. Si este valor es superior al admitido por la configuración del directorio de usuario, el valor del directorio de usuario reemplazará este valor.</p> <p>En el caso de los directorios de usuario distintos de Active Directory, deje este campo en blanco para recuperar todos los usuarios y grupos que se ajusten a los criterios de búsqueda.</p> <p>En el caso de Active Directory, establezca este valor en 0 para recuperar todos los usuarios y grupos que se ajusten a los criterios de búsqueda.</p> <p>Si está configurando Servicios compartidos de Oracle Hyperion en modo de administración delegada, establezca este valor en 0.</p>
De confianza	<p>Casilla de verificación para indicar que este proveedor es un origen de inicio de sesión único de confianza. Los símbolos de inicio de sesión único procedentes de orígenes de confianza no contienen la contraseña del usuario.</p>
Enlace anónimo	<p>Casilla de verificación para indicar que se puede enlazar Shared Services de manera anónima con el directorio de usuario para buscar usuarios y grupos. Sólo se puede usar si el directorio de usuario permite enlaces anónimos. Si esta opción no se ha seleccionado, debe especificar en el DN de usuario una cuenta con permisos de acceso suficientes para buscar el directorio donde se almacena la información de usuario. Oracle recomienda que no use el enlace anónimo.</p>

 **Nota:**

El enlace anónimo no está soportado para OID.

Tabla 4-1 (Continuación) Pantalla Información de conexión

Etiqueta	Descripción
DN de usuario	<p>Esta opción está deshabilitada si se ha seleccionado <b>Enlace anónimo</b>.</p> <p>El nombre distintivo del usuario que Shared Services debería usar para enlazar con el directorio de usuario. Este usuario debe tener privilegios de búsqueda en el atributo de RDN en el DN. Por ejemplo, en el DN: <code>cn=John Doe, ou=people, dc=myCompany, dc=com</code>, el usuario de enlace debe tener acceso de búsqueda para el atributo <code>cn</code>.</p> <p>Los caracteres especiales de DN de usuario se deben especificar utilizando caracteres de escape. Consulte <a href="#">Utilización de caracteres especiales</a> para ver las instrucciones.</p> <p><b>Ejemplo:</b> <code>cn=admin, dc=myCompany, dc=com</code></p>
Anexar DN de base	<p>La casilla de verificación para anexar el DN de base al DN de usuario. Si está usando la cuenta de gestor de directorios como el DN de usuario, no anexe el DN de base.</p> <p>Esta casilla de verificación está deshabilitada si se ha seleccionado la opción Enlace anónimo.</p>
Contraseña	<p>Contraseña del DN de usuario</p> <p>Este cuadro está deshabilitado si la opción Enlace anónimo está seleccionada.</p> <p><b>Ejemplo:</b> <code>UserDNpassword</code></p>
Mostrar opciones avanzadas	Casilla de verificación para mostrar opciones avanzadas.
Referencias	<p><b>Solo Active Directory:</b></p> <p>Si Active Directory está configurado para seguir las referencias, seleccione <code>follow</code> para seguir automáticamente las referencias LDAP. Seleccione <code>omitir</code> para no usar referencias.</p>
Alias de anulación de referencia	<p>Seleccione el método que las búsquedas de Shared Services deberían usar para anular la referencia a los alias en el directorio de usuario de manera que las búsquedas recuperen el objeto al que apunta el DN del alias. Seleccione:</p> <ul style="list-style-type: none"> <li>• <b>Siempre:</b> cancelar siempre las referencias a alias.</li> <li>• <b>Nunca:</b> no cancelar nunca las referencias a alias.</li> <li>• <b>Localizando:</b> cancelar las referencias a alias sólo durante la resolución de nombres.</li> <li>• <b>Buscando:</b> cancelar las referencias a alias sólo después de la resolución de nombres.</li> </ul>
Tiempo de espera de lectura de conexión	<p>Intervalo (segundos) después del cual el proveedor de LDAP interrumpirá el intento de lectura de LDAP si no obtiene una respuesta.</p> <p><b>Valor predeterminado:</b> 60 segundos</p>
Máximo de conexiones	<p>Conexiones máximas en la agrupación de conexiones. El valor predeterminado es 100 para directorios basados en LDAP, incluido Active Directory.</p> <p><b>Valor predeterminado:</b> 100</p>
Tiempo de espera	<p>Tiempo de espera para obtener una conexión de la agrupación. Se emite una excepción después de este periodo.</p> <p><b>Valor predeterminado:</b> 300.000 milisegundos (5 minutos)</p>

**Tabla 4-1 (Continuación) Pantalla Información de conexión**

Etiqueta	Descripción
Intervalo de expulsión	<b>Opcional:</b> intervalo tras el que ejecutar el proceso de expulsión para limpiar la agrupación. El proceso de expulsión elimina las conexiones inactivas que hayan superado el <code>Tiempo de conexión inactiva permitido</code> . <b>Valor predeterminado:</b> 120 minutos
Tiempo de conexión inactiva permitido	<b>Opcional:</b> El tiempo después del cual el proceso de expulsión elimina las conexiones inactivas en la agrupación. <b>Valor predeterminado:</b> 120 minutos
Ampliar conexiones	Esta opción indica si la agrupación de conexiones puede crecer más allá de <code>Máximo de conexiones</code> . Está seleccionada de manera predeterminada. Si no permite a la agrupación ampliarse, el sistema devuelve un error si alguna conexión no está disponible en el periodo establecido para <code>Tiempo de espera</code> .
Habilitar módulo de autenticación personalizado	Casilla de verificación para habilitar el uso de un módulo de autenticación personalizado para autenticar a usuarios definidos en este directorio de usuario. Debe introducir el nombre de clase de Java completo del módulo de autenticación en la pantalla Opciones de seguridad. Consulte <a href="#">Establecimiento de las opciones de seguridad</a> . La autenticación del módulo de autenticación personalizado es transparente para todo tipo de clientes y no requiere cambios de despliegue por su parte. Consulte la sección sobre el uso de un módulo de autenticación personalizado en <i>Guía de configuración de seguridad de Oracle Enterprise Performance Management System</i> .

7. Haga clic en **Siguiente**.

Shared Services usa las propiedades establecidas en la pantalla Configuración de usuarios para crear una URL de usuario que se usa para determinar el nodo en el que comienza la búsqueda de usuarios. El uso de esta URL acelera la búsqueda.

**▲ Atención:**

La URL de usuario no puede apuntar a ningún alias. Según la seguridad de EPM System, dicha URL debe apuntar a un usuario real.

Oracle recomienda que utilice el área Configurar automáticamente de la pantalla para recuperar la información solicitada.



The screenshot shows the 'Configure User Directories' wizard in the Oracle Fusion Middleware Administration console. The 'User Configuration' step is active, displaying the following fields and options:

- User Configuration:** A text box containing 'uid=HypUser' and an 'Auto Configure' button.
- User RDN:** A text box and an 'Edit User RDN' button.
- Login Attribute:** A text box.
- First Name Attribute:** A text box.
- Last Name Attribute:** A text box.
- Email Attribute:** A text box.
- Object Class:** A text box and an 'Add' button.

**Advanced Options:**

- Filter to Limit Users:** A text box containing 'MAccountName=a\*) (memberOf=CN=EPM\*)'.
- Resolve Custom Primary Groups:** A checked checkbox.

**Password Warning Notification:**

- Show warning if user password expires in:** A text box followed by 'days'.

Navigation buttons at the bottom include 'Help', 'Back', 'Next', 'Finish', and 'Cancel'.

 **Nota:**

Consulte [Utilización de caracteres especiales](#) para obtener una lista de caracteres especiales que se pueden usar en la configuración de usuario.

8. En **Autoconfigurar**, introduzca un identificador de usuario con el formato *attribute=identifier*, por ejemplo, `uid=jdoe`.



Los atributos del usuario se muestran en el área Configuración de usuarios.

Si está configurando OID, no puede configurar automáticamente el filtro de usuario, porque el DSE de raíz de OID no contiene entradas en el atributo de contextos de nombre. Consulte [Gestión de contextos de nombres](#) en la *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.


 **Nota:**

Puede introducir manualmente atributos de usuario necesarios en los cuadros de texto en el área Configuración de usuarios.

**Tabla 4-2 Pantalla Configuración de usuarios**

Etiqueta	Descripción <sup>1</sup>
RDN de usuario	<p>DN relativo del usuario. Cada componente de un DN se denomina "RDN" y representa una rama del árbol de directorios. El RDN de un usuario es, por lo general, el equivalente de <code>uid</code> o <code>cn</code>.</p> <p>Consulte <a href="#">Utilización de caracteres especiales</a> para ver las restricciones.</p> <p><b>Ejemplo:</b> <code>ou=People</code></p>
Atributo de inicio de sesión	<p>Atributo único (puede ser personalizado) que almacena el nombre de inicio de sesión del usuario. Los usuarios usan el valor de este atributo como nombre de usuario cuando inician sesión en los productos de EPM System.</p> <p>Los ID de usuario (valor de atributo de inicio de sesión) deben ser únicos en todos los directorios de usuario. Por ejemplo, puede utilizar <code>uid</code> y <code>sAMAccountName</code> respectivamente como atributo de inicio de sesión para las configuraciones de SunONE y Active Directory. Los valores de estos atributos deben ser únicos en todos los directorios de usuario, incluido el directorio nativo.</p> <div style="border: 1px solid #0070C0; padding: 10px; margin-top: 10px;"> <p> <b>Nota:</b></p> <p>Los ID de usuario no distinguen entre mayúsculas y minúsculas.</p> </div> <div style="border: 1px solid #0070C0; padding: 10px; margin-top: 10px;"> <p> <b>Nota:</b></p> <p>Si configura OID como directorio de usuario externo para productos de EPM System desplegados en Oracle Application Server en un entorno de Kerberos, deberá establecer esta propiedad en <code>userPrincipalName</code>.</p> </div> <p><b>Valor predeterminado</b></p> <ul style="list-style-type: none"> <li>• <b>Active Directory:</b> <code>cn</code></li> <li>• <b>Directorios LDAP distintos a Active Directory:</b> <code>uid</code></li> </ul>
Atributo de nombre	<p>Atributo que almacena el nombre del usuario</p> <p><b>Valor predeterminado:</b> <code>givenName</code></p>
Atributo de apellido	<p>Atributo que almacena el apellido del usuario</p> <p><b>Valor predeterminado:</b> <code>sn</code></p>
Atributo de correo electrónico	<p><b>Opcional:</b> atributo que almacena la dirección de correo electrónico del usuario</p> <p><b>Valor predeterminado:</b> <code>mail</code></p>

**Tabla 4-2 (Continuación) Pantalla Configuración de usuarios**

Etiqueta	Descripción <sup>1</sup>
Clase de objeto	<p>Clases de objeto del usuario (los atributos opcionales y obligatorios que se pueden asociar con el usuario). Shared Services utiliza las clases de objeto mostradas en esta pantalla en el filtro de búsqueda. Con estas clases de objeto, Shared Services debería encontrar todos los usuarios que deban ser aprovisionados.</p>
Filtrar para limitar usuarios	<div data-bbox="735 506 1458 751" style="border: 1px solid #0070C0; padding: 10px; margin-bottom: 10px;"> <p> <b>Nota:</b></p> <p>Si configura Active Directory o ADAM como tipo de directorio de usuario <code>Other</code> para utilizar un atributo de ID personalizado, debe establecer este valor en <code>user</code>.</p> </div> <p>Puede agregar clases de objetos manualmente si fuera necesario. Para agregar una clase de objeto, introduzca el nombre de la clase de objeto en el cuadro <b>Clase de objeto</b> y haga clic en <b>Agregar</b>.</p> <p>Para suprimir clases de objeto, seleccione la clase de objeto y haga clic en <b>Eliminar</b>.</p> <p><b>Valor predeterminado</b></p> <ul style="list-style-type: none"> <li>• <b>Active Directory:</b> <code>user</code></li> <li>• <b>Directorios LDAP distintos a Active Directory:</b> <code>person, organizationalPerson, inetorgperson</code></li> </ul> <p>Consulta LDAP que recupera sólo los usuarios que van a aprovisionarse con las funciones de producto de EPM System. Por ejemplo, la consulta LDAP (<code>uid=Hyp*</code>) recupera sólo los usuarios cuyos nombres comienzan con <code>Hyp</code>.</p> <p>La pantalla Configuración de usuarios valida el RDN de usuario y recomienda el uso de un filtro de usuario, si fuera necesario. El filtro de usuario limita el número de usuarios devueltos durante una consulta. Es especialmente importante si el nodo identificado por el RDN de usuario contiene muchos usuarios que tienen que aprovisionarse. Los filtros de usuario pueden diseñarse para excluir a los usuarios que no se van a aprovisionar, con lo que se mejora el rendimiento.</p>

**Tabla 4-2 (Continuación) Pantalla Configuración de usuarios**

Etiqueta	Descripción <sup>1</sup>
Atributo de búsqueda de usuario para RDN de varios atributos	<p><b>Solo directorios de usuarios habilitados para LDAP distintos a Active Directory:</b> establezca este valor solo si el servidor de directorios está configurado para utilizar un RDN de varios atributos. El valor definido debe ser uno de los atributos de RDN. El valor del atributo especificado debe ser único y el atributo debe admitir búsquedas. Por ejemplo, supongamos que se configura un servidor de directorios SunONE para combinar los atributos cn (cn=John Doe) y uid (uid=jDoe12345) para crear un RDN de varios atributos similar al siguiente:</p> <pre>cn=John Doe+uid=jDoe12345, ou=people, dc=myCompany, dc=com</pre> <p>En este caso, puede utilizar cn o uid si estos atributos cumplen las siguientes condiciones:</p> <ul style="list-style-type: none"> <li>• El atributo admite búsquedas por parte del usuario identificado en el campo DN de usuario de la pestaña Información de conexión.</li> <li>• El atributo necesita que establezca un valor único en el directorio de usuario.</li> </ul>
Resolver grupos principales personalizados	<p><b>Solo Active Directory:</b> la casilla de verificación indica si se identifican grupos primarios de usuarios para determinar roles vigentes. De forma predeterminada, esta casilla está activada. Oracle recomienda que no se cambie esta configuración.</p>
Mostrar advertencia si la contraseña de usuario caduca en:	<p><b>Solo Active Directory:</b> la casilla de verificación indica si mostrar o no un mensaje de advertencia si la contraseña del usuario de Active Directory caduca al cabo del número de días especificado.</p>

<sup>1</sup> La seguridad de EPM System puede utilizar valores predeterminados para algunos campos cuyo valor de configuración es opcional. Si no introduce valores en estos campos, se utilizarán los valores predeterminados en el tiempo de ejecución.

**9. Haga clic en Siguiente.**

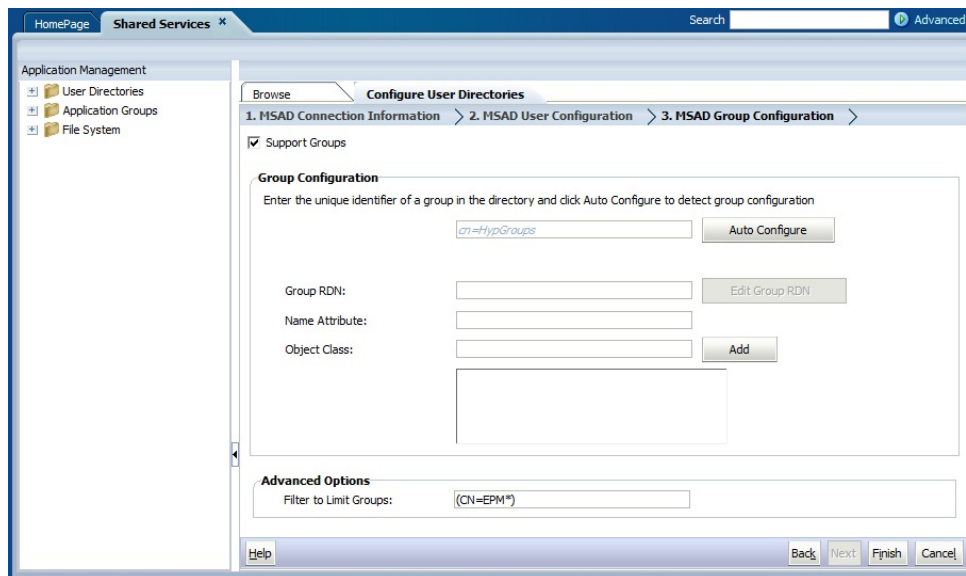
Se abre la pantalla Configuración de grupos. Shared Services usa las propiedades establecidas en esta pantalla para crear la URL de grupo que determina el nodo en el que empieza la búsqueda de grupos. El uso de esta URL acelera la búsqueda.

**▲ Atención:**

La URL de grupo no puede hacer referencia a un alias. La seguridad de EPM System necesita que la URL de grupo haga referencia a un grupo real. Si está configurando un Novell eDirectory que utiliza alias de grupo, los alias de grupo y las cuentas de grupo deben estar disponibles en la URL de grupo.

 **Nota:**

la introducción de datos en la pantalla Configuración de grupos es opcional. Si no introduce la configuración de URL de grupo, Shared Services busca dentro del DN de base para encontrar grupos, lo que puede afectar negativamente al rendimiento, especialmente si el directorio de usuario contiene muchos grupos.



10. Borre la selección de **Establecer soporte para grupos** si su organización no tiene pensado aprovisionar grupos, o si los usuarios no están categorizados en grupos en el directorio de usuarios. Al desactivar esta opción se deshabilitan los campos de esta pantalla.

Si está estableciendo compatibilidad para grupos, Oracle recomienda que utilice la función de configuración automática para recuperar la información necesaria.

Si está configurando OID como un directorio de usuario, no podrá usar la función de configuración automática porque el DSE de raíz de OID no contiene entradas en el atributo de contextos de nombre. Consulte [Gestión de contextos de nombres](#) en la *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

11. En el cuadro de texto **Autoconfigurar**, introduzca un identificador de grupo único y, a continuación, haga clic en **Ir**.

El identificador de grupo se debe expresar con el formato `attribute=identifier`, por ejemplo, `cn=western_region`.

Los atributos del grupo se muestran en el área Configuración de grupos.

 **Nota:**

Puede introducir manualmente los atributos de grupo necesarios en los cuadros de texto de configuración de grupos.

 **Atención:**

Si no está establecida la URL de grupo para directorios de usuario que contengan / (barra) o \ (barra invertida) en sus nombres de nodo, la búsqueda para usuarios y grupos fallará. Por ejemplo, cualquier operación para mostrar el usuario o grupo fallará si no se especifica la URL de grupo para un directorio de usuario en el que los usuarios y los grupos existan en un nodo, como `OU=child\ou,OU=parent/ou` u `OU=child/ou,OU=parent \ ou`.

**Tabla 4-3 Pantalla Configuración de grupos**

Etiqueta	Descripción <sup>1</sup>
RDN de grupo	<p>El DN relativo del grupo. Este valor, que corresponde a la ruta relativa al DN base, se utiliza como URL del grupo. Especifique un RDN de grupo que identifique el nodo de directorio de usuario más bajo en el que todos los grupos que está pensando en aprovisionar estén disponibles.</p> <p>Si utiliza un grupo principal de Active Directory para aprovisionamiento, asegúrese de que el grupo principal queda dentro del RDN del grupo. Shared Services no recupera el grupo principal si queda fuera del ámbito de la URL del grupo. El RDN de grupo repercute de forma significativa en el inicio de sesión y en el rendimiento de las búsquedas. Debido a que es el punto de inicio de todas las búsquedas de grupos, debe identificar el nodo más bajo posible en el que todos los grupos para los sistemas de EPM System estén disponibles. Para garantizar un rendimiento óptimo, el número de grupos presente en el RDN de grupo no debería exceder de 10.000. Si hay más grupos, utilice un filtro de grupo para recuperar sólo los grupos que desee aprovisionar.</p>


 **Nota:**

Shared Services muestra una advertencia si el número de grupos disponibles en la URL de grupo supera 10.000.

Consulte [Utilización de caracteres especiales](#) para conocer las restricciones.

**Ejemplo:** `ou=Groups`

**Tabla 4-3 (Continuación) Pantalla Configuración de grupos**

Etiqueta	Descripción <sup>1</sup>
Atributo de nombre	<p>El atributo que almacena el nombre del grupo.</p> <p><b>Valor predeterminado</b></p> <ul style="list-style-type: none"> <li>• <b>Directorios LDAP incluido Active Directory:</b>cn</li> <li>• <b>Directorio nativo:</b> cssDisplayNameDefault</li> </ul>
Clase de objeto	<p>Clases de objeto del grupo. Shared Services utiliza las clases de objeto mostradas en esta pantalla en el filtro de búsqueda. Con estas clases de objeto, Shared Services debería encontrar todos los grupos asociados con el usuario.</p> <div style="border: 1px solid #0070C0; padding: 10px; margin: 10px 0;"> <p> <b>Nota:</b></p> <p>Si configura Active Directory o ADAM como tipo de directorio de usuario <code>Other</code> para utilizar un atributo de ID personalizado, debe establecer este valor en <code>group?member</code>.</p> </div> <p>Puede agregar clases de objetos manualmente si fuera necesario. Para agregar una clase de objeto, introduzca el nombre de la clase de objeto en el cuadro de texto Clase de objeto y haga clic en <b>Agregar</b>.</p> <p>Para suprimir clases de objeto, seleccione la clase de objeto y haga clic en <b>Eliminar</b>.</p> <p><b>Valor predeterminado</b></p> <ul style="list-style-type: none"> <li>• <b>Active Directory:</b> group?member</li> <li>• <b>Directorios LDAP distintos a Active Directory:</b> groupofuniquenames?uniquemember, groupOfNames?member</li> <li>• <b>Directorio nativo:</b> groupofuniquenames?uniquemember, cssGroupExtend?cssIsActive</li> </ul>
Filtrar para limitar grupos	<p>Consulta LDAP que recupera los grupos que se tienen que aprovisionar con funciones de producto de EPM System solamente. Por ejemplo, la consulta LDAP <code>( (cn=Hyp*)(cn=Admin*))</code> recupera solo grupos cuyos nombres comienzan por <code>Hyp</code> o <code>Admin</code>.</p> <p>El filtro de grupo se usa para limitar el número de grupos devueltos durante una consulta. Es especialmente importante si el nodo identificado por el RDN de grupo contiene un gran número de grupos que tienen que aprovisionarse. Los filtros pueden diseñarse para excluir a los grupos que no se van a aprovisionar, con lo que se mejora el rendimiento.</p> <p>Si utiliza el grupo principal de Active Directory para aprovisionamiento, asegúrese de que todos los filtros de grupo que defina puedan recuperar el grupo principal contenido dentro del ámbito de la URL del grupo. Por ejemplo, el filtro <code>( (cn=Hyp*)(cn=Domain Users))</code> recupera grupos cuyos nombres empiezan por <code>Hyp</code> y el grupo principal llamado <code>Domain Users</code>.</p>

<sup>1</sup> La seguridad de EPM System puede utilizar valores predeterminados para algunos campos cuyo valor de configuración es opcional. Si no introduce valores en estos campos, se utilizarán los valores predeterminados en el tiempo de ejecución.

**12.** Haga clic en **Finalizar**.

Shared Services guarda la configuración y vuelve a la pantalla Directorios de usuario definidos, que ahora muestra el directorio de usuario que haya configurado.

**13.** Pruebe la configuración. Consulte [Prueba de conexiones de directorios de usuario](#).

**14.** Cambie la asignación del orden de búsqueda, en caso necesario. Consulte [Administración del orden de búsqueda de directorios de usuario](#) para obtener información.

**15.** En caso necesario, especifique las opciones de seguridad. Consulte [Establecimiento de las opciones de seguridad](#) para obtener información.

**16.** Reinicie Oracle Hyperion EPM Foundation Services y otros componentes de EPM System.

## Configuración de bases de datos relacionales como directorios de usuario

La información de usuarios y grupos procedente de las tablas del sistema de bases de datos relacionales de Oracle, SQL Server e IBM DB2 puede utilizarse para admitir el aprovisionamiento. Si no se puede obtener información de grupo del esquema de sistema de la base de datos, Servicios compartidos de Oracle Hyperion no soportará el aprovisionamiento de grupos desde el proveedor de bases de datos. Por ejemplo, Shared Services no puede extraer información de grupos desde versiones anteriores de IBM DB2, dado que la base de datos utiliza grupos definidos en el sistema operativo. Los gestores de aprovisionamiento pueden, no obstante, agregar estos usuarios a grupos en el directorio nativo y aprovisionar dichos grupos. Para obtener información sobre la plataforma soportada, consulte la página *Matriz de certificación de Oracle Enterprise Performance Management System* publicada en la página [Configuraciones soportadas del sistema de Oracle Fusion Middleware](#) de Oracle Technology Network (OTN).

 **Nota:**

Si utiliza una base de datos DB2, el nombre de usuario debe contener al menos ocho caracteres. Los nombres de usuario no deben exceder los 256 caracteres (bases de datos de Oracle y SQL Server) ni los 1.000 caracteres (DB2).

Configure Shared Services para que se conecte a la base de datos como administrador de ésta; por ejemplo, como usuario `SYSTEM` de Oracle, con el fin de recuperar la lista de usuarios y grupos.

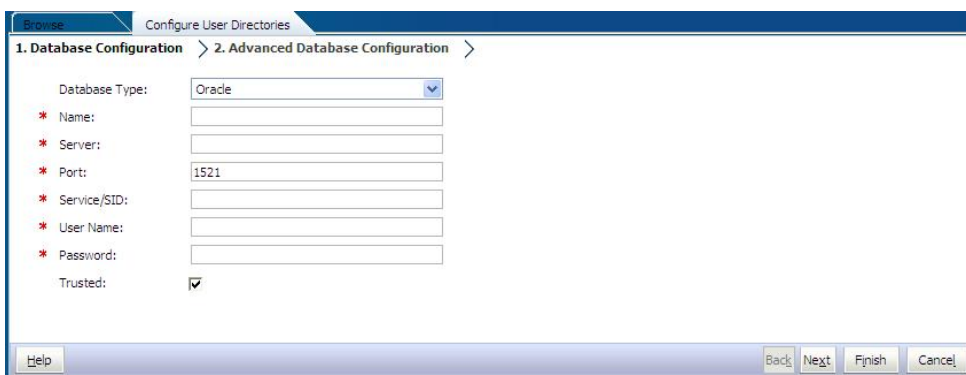
 **Nota:**

Shared Services recupera sólo usuarios de bases de datos activas para el aprovisionamiento. Las cuentas de usuarios de bases de datos inactivas o bloqueadas se omiten.



Para configurar proveedores de bases de datos:

1. Acceda a Oracle Hyperion Shared Services Console como administrador del sistema. Consulte [Inicio de Shared Services Console](#).
2. Seleccione **Administración** y, a continuación, **Configurar directorios de usuario**.
3. Haga clic en **Nuevo**.
4. En la pantalla **Tipo de directorio**, seleccione **Base de datos relacional (Oracle, DB2, SQL Server)**.
5. Haga clic en **Siguiente**.



6. En la pestaña Configuración de base de datos, introduzca los parámetros de configuración.

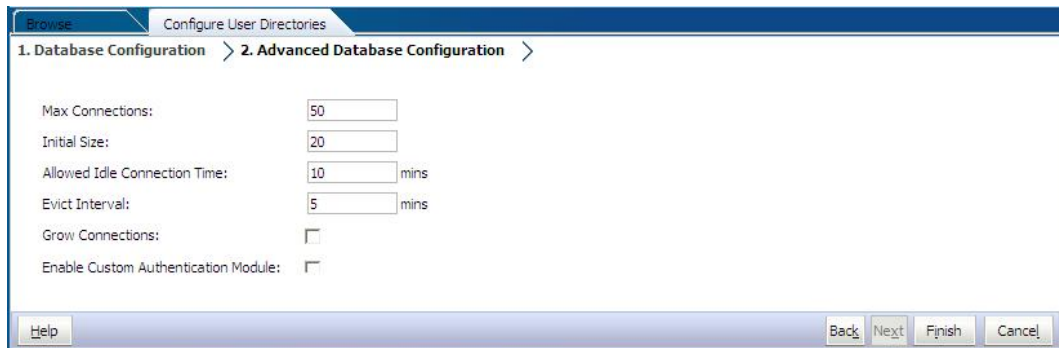
**Tabla 4-4 Separador Configuración de base de datos**

Etiqueta	Descripción
Tipo de base de datos	El proveedor de la base de datos relacional. Servicios compartidos solo soporta bases de datos Oracle y SQL Server como proveedores de bases de datos. <b>Ejemplo:</b> Oracle
Nombre	Nombre único de configuración para el proveedor de la base de datos. <b>Ejemplo:</b> Oracle_DB_FINANCE
Servidor	Nombre de DNS del equipo en que se está ejecutando el servidor de bases de datos. <b>Ejemplo:</b> myserver
Puerto	Número de puerto del servidor de base de datos. <b>Ejemplo:</b> 1521
Servicio/SID (sólo en Oracle)	Identificador del sistema (el valor predeterminado es orcl). <b>Ejemplo:</b> orcl
Base de datos (SQL Server y DB2 sólo)	Base de datos a la que debería conectarse Shared Services. <b>Ejemplo:</b> master

**Tabla 4-4 (Continuación) Separador Configuración de base de datos**

Etiqueta	Descripción
Nombre de usuario	Nombre de usuario que debería utilizar Shared Services para acceder a la base de datos. Este usuario de base de datos debe tener privilegios de acceso a las tablas de sistema de la base de datos. Oracle recomienda el uso de la cuenta <code>system</code> para bases de datos Oracle y el nombre de usuario del administrador de la base para las bases de datos SQL Server. <b>Ejemplo:</b> SYSTEM
Contraseña	Contraseña del usuario identificado en <b>Nombre de usuario</b> . <b>Ejemplo:</b> system_password
De confianza	Casilla de verificación que especifica que este proveedor es un origen de inicio de sesión único de confianza. Los símbolos de inicio de sesión único procedentes de orígenes de confianza no contienen la contraseña del usuario.

- Opcional:** Haga clic en **Siguiente** para configurar la agrupación de conexiones. Accederá a la pestaña Configuración de base de datos avanzada.



- En Configuración de base de datos avanzada, introduzca los parámetros de la agrupación de conexiones.

**Tabla 4-5 Pestaña Configuración de base de datos avanzada**

Etiqueta	Descripción
Máximo de conexiones	Número máximo de conexiones en la agrupación. El valor predeterminado es 50.
Tamaño inicial	Conexiones disponibles cuando se inicia la agrupación. El valor predeterminado es 20.
Tiempo de conexión inactiva permitido	<b>Opcional:</b> El tiempo después del cual el proceso de expulsión elimina las conexiones inactivas en la agrupación. El valor predeterminado es 10 minutos.

**Tabla 4-5 (Continuación) Pestaña Configuración de base de datos avanzada**

Etiqueta	Descripción
Intervalo de expulsión	<b>Opcional:</b> el intervalo de ejecución del proceso de expulsión encargado de limpiar la agrupación. Este proceso elimina las conexiones inactivas que hayan excedido el tiempo de conexión inactiva permitido. El valor predeterminado es cinco minutos.
Ampliar conexiones	Indica si la agrupación de conexiones puede ampliarse más allá de lo especificado en <i>Máximo de conexiones</i> . De forma predeterminada, esta opción está desactivada, lo que indica que la agrupación no puede ampliarse. Si no permite a la agrupación ampliarse, el sistema devuelve un error si alguna conexión no está disponible en el periodo establecido para <i>Tiempo de espera</i> .
Habilitar módulo de autenticación personalizado	Casilla de verificación para habilitar el uso de un módulo de autenticación personalizado para autenticar a usuarios definidos en este directorio de usuario. Debe introducir el nombre de clase de Java completo del módulo de autenticación en la pantalla <i>Opciones de seguridad</i> . Consulte <a href="#">Establecimiento de las opciones de seguridad</a> . La autenticación del módulo de autenticación personalizado es transparente para clientes de todo tipo. Consulte la sección sobre el uso de un módulo de autenticación personalizado en <i>Guía de configuración de seguridad de Oracle Enterprise Performance Management System</i> .

9. Haga clic en **Finalizar**.
10. Haga clic en **Aceptar** para volver a la pantalla Directorios de usuario definidos.
11. Pruebe la configuración del proveedor de bases de datos. Consulte [Prueba de conexiones de directorios de usuario](#).
12. Cambie la asignación del orden de búsqueda, en caso necesario. Consulte [Administración del orden de búsqueda de directorios de usuario](#) para obtener información.
13. Especifique la configuración de seguridad, en caso necesario. Consulte [Establecimiento de las opciones de seguridad](#).
14. Reinicie Oracle Hyperion Foundation Services y otros componentes de Oracle Enterprise Performance Management System.

## Prueba de conexiones de directorios de usuario

Una vez configurado un directorio de usuario, pruebe la conexión para asegurarse de que Servicios compartidos de Oracle Hyperion puede conectarse a él mediante la configuración actual.

Para probar una conexión de directorio de usuario:

1. Acceda a Oracle Hyperion Shared Services Console como administrador del sistema. Consulte [Inicio de Shared Services Console](#).
2. Seleccione **Administración** y, a continuación, **Configurar directorios de usuario**.

3. En la lista de directorios de usuario, seleccione una configuración de directorio de usuario externo para probar.
4. Haga clic en **Probar** y, a continuación, en **Aceptar**.

## Edición de configuración de directorio de usuario

Los administradores pueden modificar cualquier parámetro de una configuración de directorio de usuario, excepto el nombre. Oracle recomienda no editar los datos de configuración de directorios de usuario que se hayan empleado para aprovisionamiento.

### **Atención:**

La modificación de algunos parámetros como, por ejemplo, el `Atributo de ID`, en la configuración del directorio de usuario invalida los datos de aprovisionamiento. Extreme la precaución al modificar la configuración de un directorio de usuario que se haya aprovisionado.

Para editar la configuración de un directorio de usuario:

1. Acceda a Oracle Hyperion Shared Services Console como administrador del sistema. Consulte [Inicio de Shared Services Console](#).
2. Seleccione **Administración** y, a continuación, **Configurar directorios de usuario**.
3. Seleccione un directorio de usuario para editarlo.
4. Haga clic en **Editar**.
5. Modifique los parámetros de configuración.

### **Nota:**

No puede modificar el nombre de la configuración. Si está modificando la configuración de un directorio de usuario LDAP, puede elegir un servidor de directorios distinto u `Otro` (en el caso de directorios LDAP personalizados) en la lista de servidores de directorios. No se pueden editar los parámetros del directorio nativo.

Para obtener una explicación de los parámetros que puede editar, consulte las siguientes tablas:

- Active Directory y otros directorios de usuario basados en LDAP. Consulte las tablas en [Configuración de OID, Active Directory y otros directorios de usuario basados en LDAP](#).
  - Bases de datos: consulte la tabla en [Configuración de bases de datos relacionales como directorios de usuario](#)
6. Haga clic en **Aceptar** para guardar los cambios.

## Supresión de configuraciones de directorios de usuario

Los administradores del sistema pueden suprimir la configuración de los directorios de usuarios externos en cualquier momento. Al hacerlo se invalida toda la información de aprovisionamiento para los usuarios y los grupos derivada del directorio de usuario y se elimina el directorio del orden de búsqueda.

### **Sugerencia:**

Si no desea utilizar un directorio de usuario configurado utilizado para aprovisionamiento, elimínelo del orden de búsqueda de forma que no se busquen en él usuarios y grupos. De esta forma se mantiene la integridad de la información de aprovisionamiento y puede usar el directorio de usuario con posterioridad.

Para suprimir la configuración de un directorio de usuario:

1. Acceda a Oracle Hyperion Shared Services Console como administrador del sistema. Consulte [Inicio de Shared Services Console](#).
2. Seleccione **Administración** y, a continuación, **Configurar directorios de usuario**.
3. Seleccione un directorio.
4. Haga clic en **Suprimir**.
5. Haga clic en **Aceptar**.
6. Vuelva a hacer clic en **Aceptar**.
7. Reinicie Oracle Hyperion Foundation Services y otros componentes de Oracle Enterprise Performance Management System.

## Administración del orden de búsqueda de directorios de usuario

Cuando el administrador del sistema configura un directorio de usuario externo, Servicios compartidos de Oracle Hyperion agrega automáticamente el directorio de usuario al orden de búsqueda y lo asigna en la próxima secuencia de búsqueda disponible antes de la del directorio nativo. El orden de búsqueda se utiliza para recorrer los directorios de usuario configurados cuando Oracle Enterprise Performance Management System busca usuarios y grupos.

Los administradores del sistema pueden eliminar un directorio de usuario del orden de búsqueda, en cuyo caso Shared Services reasigna automáticamente el orden de búsqueda de los directorios restantes. Los directorios de usuario no incluidos en el orden de búsqueda no se utilizan para admitir la autenticación ni el aprovisionamiento.

 **Nota:**

Shared Services finaliza la búsqueda del usuario o grupo cuando encuentra la cuenta especificada. Oracle recomienda ubicar el directorio corporativo con el mayor número de usuarios de EPM System al principio del orden de búsqueda.

De forma predeterminada, el directorio nativo se establece como el último directorio en el orden de búsqueda. Los administradores pueden administrar el orden de búsqueda mediante una de las siguientes tareas:

- [Adición de un directorio de usuario al orden de búsqueda](#)
- [Cambio del orden de búsqueda](#)
- [Eliminación de la asignación de un orden de búsqueda](#)

### Adición de un directorio de usuario al orden de búsqueda

Los directorios de usuario recién configurados se agregan automáticamente al orden de búsqueda. Si ha eliminado un directorio de dicho orden pero desea volver a incluirlo, puede agregarlo al final.

Para agregar un directorio de usuario al orden de búsqueda:

1. Acceda a Oracle Hyperion Shared Services Console como administrador del sistema. Consulte [Inicio de Shared Services Console](#).
2. Seleccione **Administración** y, a continuación, **Configurar directorios de usuario**.
3. Seleccione un directorio de usuario desactivado que desee agregar al orden de clasificación.
4. Haga clic en **Incluir**.

Este botón sólo se encuentra disponible si selecciona un directorio de usuario que no se encuentre en el orden de búsqueda.

5. Haga clic en **Aceptar** para volver a la pantalla Directorios de usuario definidos.
6. Reinicie Oracle Hyperion EPM Foundation Services y otros componentes de EPM System.

### Eliminación de la asignación de un orden de búsqueda

La eliminación de un directorio de usuario del orden de búsqueda no implica la invalidación de la configuración de dicho directorio. Simplemente se elimina de la lista de directorios en los que se realiza la búsqueda para autenticar usuarios. Un directorio que no está incluido en el orden de búsqueda se establece con el estado *Desactivado*. Cuando un administrador elimina un directorio de usuario del orden de búsqueda, la secuencia de búsqueda asignada al resto de directorios se actualiza de forma automática.

 **Nota:**

El directorio nativo no se puede eliminar del orden de búsqueda.

Para eliminar un directorio de usuario del orden de búsqueda:

1. Acceda a Shared Services Console como administrador del sistema. Consulte [Inicio de Shared Services Console](#).
2. Seleccione **Administración** y, a continuación, **Configurar directorios de usuario**.
3. Seleccione un directorio para eliminarlo del orden de clasificación.
4. Haga clic en **Excluir**.
5. Haga clic en **Aceptar**.
6. Haga clic en **Aceptar** en la pantalla Resultado de configuración de directorio.
7. Reinicie EPM Foundation Services y otros componentes de EPM System.

### Cambio del orden de búsqueda

El orden de búsqueda predeterminado asignado a cada directorio de usuario se basa en la secuencia en la que se configuró el directorio. De forma predeterminada, el directorio nativo se establece como el último directorio en el orden de búsqueda.

Para cambiar el orden de búsqueda:

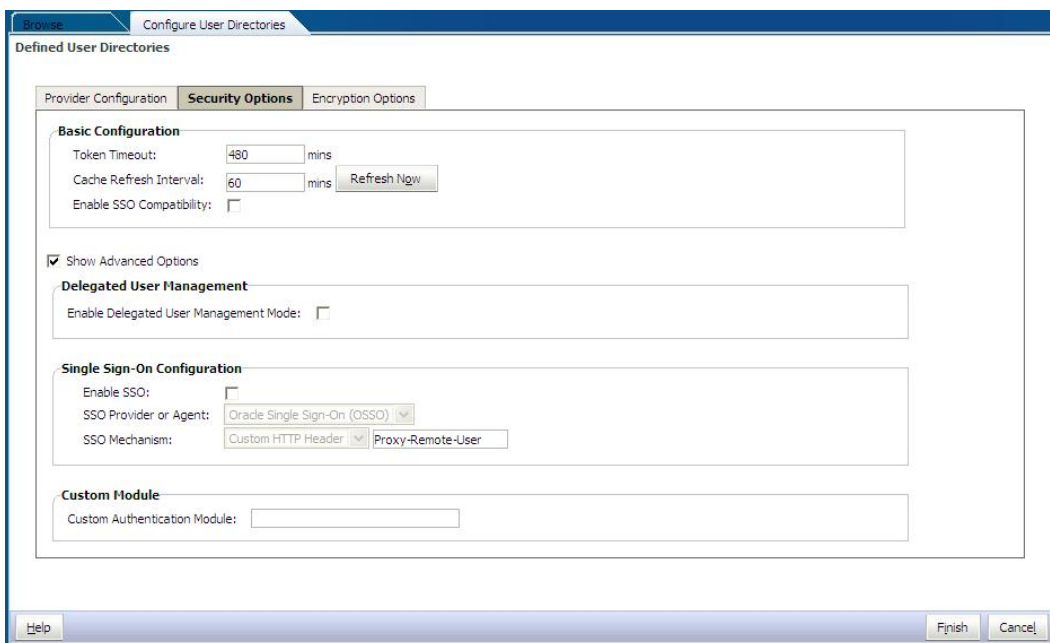
1. Acceda a Shared Services Console como administrador del sistema. Consulte [Inicio de Shared Services Console](#).
2. Seleccione **Administración** y, a continuación, **Configurar directorios de usuario**.
3. Seleccione un directorio cuyo orden de clasificación desee cambiar.
4. Haga clic en **Subir** o en **Bajar**.
5. Haga clic en **Aceptar**.
6. Reinicie Foundation Services, otros componentes de EPM System y las aplicaciones personalizadas que utilicen las API de seguridad de Shared Services.

## Establecimiento de las opciones de seguridad


Las opciones de seguridad comprenden los parámetros globales que se pueden aplicar a todos los directorios de usuario incluidos en el orden de búsqueda.

Para establecer las opciones de seguridad:

1. Acceda a Oracle Hyperion Shared Services Console como administrador del sistema. Consulte [Inicio de Shared Services Console](#).
2. Seleccione **Administración** y, a continuación, **Configurar directorios de usuario**.
3. Seleccione **Opciones de seguridad**.
4. En **Opciones de seguridad**, establezca los parámetros globales.



**Tabla 4-6 Opciones de seguridad para los directorios de usuario**


Parámetro	Descripción
Tiempo de espera de símbolo	Tiempo (en minutos) tras el cual el símbolo de inicio de sesión emitido por los productos de Oracle Enterprise Performance Management System o la solución de gestión de identidad web caduca. Los usuarios deberán iniciar sesión de nuevo después de este periodo. El tiempo de espera de símbolo se basa en el reloj del sistema del servidor. El valor predeterminado es 480 minutos.
	<p> <b>Nota:</b></p> <p>El parámetro de tiempo de espera del símbolo no corresponde con el tiempo de espera de sesión.</p>
Intervalo de refrescamiento de caché	Intervalo (en minutos) para refrescar la caché de Servicios compartidos de Oracle Hyperion de datos de relación entre grupos y usuarios. El valor predeterminado es de 60 minutos. Shared Services almacena en caché la información sobre los nuevos grupos de directorio de usuario externo y los nuevos usuarios agregados a los grupos existentes tras el siguiente refrescamiento de la caché. Los usuarios aprovisionados a través de un grupo de directorio de usuario externo recién creado no obtienen sus funciones aprovisionadas hasta que se refresca la caché.



**Tabla 4-6 (Continuación) Opciones de seguridad para los directorios de usuario**

Parámetro	Descripción
Refrescar ahora	Haga clic en este botón para iniciar manualmente el refrescamiento de la caché de Shared Services que contiene los datos de relación entre grupos y usuarios. Puede iniciar un refrescamiento de caché después de la creación de nuevos grupos en los directorios de usuario externos y su aprovisionamiento o después de la adición de nuevos usuarios a grupos existentes. La caché se refresca sólo después de que Shared Services realice una llamada utilizando los datos de la caché.
Activar compatibilidad con inicio de sesión único	Seleccione esta opción si el despliegue está integrado con Oracle Business Intelligence Enterprise Edition versión 11.1.1.5 o anterior.
Habilitar modo de administración de usuarios delegada	Opción que permite la administración de usuarios delegada de productos de EPM System para proporcionar compatibilidad con la administración distribuida de las actividades de aprovisionamiento. Consulte "Gestión de usuarios delegada" en la <i>Guía de administración de seguridad de usuarios de Oracle Enterprise Performance Management System</i> .
Activar inicio de sesión único	Opción que admite la compatibilidad con el sistema SSO de agentes de seguridad como Oracle Access Manager.
Agente o proveedor de inicio de sesión único	<p>Seleccione la solución de administración de identidades web de la que los productos de EPM System deben aceptar el inicio de sesión único. Seleccione <b>Otro</b> si su solución de gestión de identidades web, por ejemplo, Kerberos, no aparece en la lista. El nombre y el mecanismo de inicio de sesión único preferidos se seleccionarán automáticamente cuando escoja el proveedor de inicio de sesión único. Puede cambiar el nombre del mecanismo de inicio de sesión único (cabecera HTTP o clase de inicio de sesión personalizada) si así lo desea.</p> <p>Si selecciona <b>Otro</b> como agente o proveedor de inicio de sesión único, debe asegurarse de que se puede usar un mecanismo de inicio de sesión único compatible con EPM System. Consulte la sección sobre métodos de inicio de sesión soportados en <i>Guía de configuración de seguridad de Oracle Enterprise Performance Management System</i>.</p>

**Tabla 4-6 (Continuación) Opciones de seguridad para los directorios de usuario**

Parámetro	Descripción
Mecanismo de inicio de sesión único	<p>Método que la solución de administración de identidades web seleccionada utiliza para proporcionar el nombre de inicio de sesión de un usuario a los productos de EPM System. Si desea obtener una descripción de los métodos de inicio de sesión único soportados, consulte <i>Guía de configuración de seguridad de Oracle Enterprise Performance Management System</i>.</p> <ul style="list-style-type: none"> <li>• Cabecera HTTP personalizada: establece el nombre de la cabecera que el agente de seguridad pasa a EPM System.</li> <li>• Clase de inicio de sesión personalizada: especifica la clase Java personalizada que gestiona las solicitudes HTTP para la autenticación. Consulte la sección sobre la clase de inicio de sesión personalizada en <i>Guía de configuración de seguridad de Oracle Enterprise Performance Management System</i>.</li> </ul> <div style="border: 1px solid #0070C0; padding: 10px; margin: 10px 0;"> <p> <b>Nota:</b></p> <p>La clase de inicio de sesión personalizada no es lo mismo que la autenticación personalizada.</p> </div> <ul style="list-style-type: none"> <li>• Cabecera de autorización HTTP: mecanismo HTTP estándar.</li> <li>• Obtener usuario remoto de solicitud HTTP: seleccione esta opción si el agente de seguridad rellena el usuario remoto en la solicitud HTTP.</li> </ul>
Módulo de autenticación personalizado	<p>Nombre completo de clase Java del módulo de autenticación personalizado (por ejemplo, <code>com.mycompany.epm.CustomAuthenticationImpl</code>) que se debe utilizar para autenticar a los usuarios en todos los directorios de usuario para el módulo de autenticación personalizado.</p> <p>El módulo de autenticación se utiliza para un directorio de usuario sólo si se ha habilitado su uso (valor predeterminado) en la configuración de dicho directorio.</p> <p>Oracle Hyperion Foundation Services requiere que el archivo JAR de autenticación personalizado se denomine <code>CustomAuth.jar</code>. <code>CustomAuth.jar</code> debe estar disponible en <code>MIDDLEWARE_HOME\user_projects\domains\WEBLOGIC_DOMAIN\lib</code>, normalmente, <code>C:\Oracle\Middleware\user_projects\domains\EPMSys\lib</code>.</p> <p>En todas las instalaciones de cliente, <code>CustomAuth.jar</code> debe estar presente en <code>EPM_ORACLE_HOME/common\jlib\11.1.2.0</code>, normalmente, <code>C:\Oracle\Middleware\EPMSys11R1\common\jlib\11.1.2.0</code>.</p> <p>Puede utilizar cualquier estructura de paquete y nombre de clase en el archivo jar.</p> <p>Para obtener más información, la sección sobre el uso de un módulo de autenticación personalizado en <i>Guía de configuración de seguridad de Oracle Enterprise Performance Management System</i>.</p>

5. Haga clic en **Aceptar**.
6. Reinicie EPM Foundation Services y otros componentes de EPM System.

## Regeneración de claves de cifrado

Oracle Enterprise Performance Management System utiliza las siguientes claves para garantizar la seguridad:

- Clave de cifrado de símbolo de inicio de sesión único, que se utiliza para cifrar y descifrar los símbolos de inicio de sesión único de EPM System. Esta clave se almacena en Oracle Hyperion Shared Services Registry
- Clave de servicios de confianza, que utilizan los componentes de EPM System para verificar la autenticidad del servicio que solicita un símbolo de inicio de sesión único
- Clave de cifrado de configuración de proveedor, utilizada para cifrar la contraseña (contraseña DN de usuario para directorios de usuario habilitados para LDAP) que emplea la seguridad de EPM System para enlazar con un directorio de usuario externo configurado. Esta contraseña se establece cuando se configura un directorio de usuario externo.

Cambie estas claves periódicamente para aumentar la seguridad de EPM System. Servicios compartidos de Oracle Hyperion y el subsistema de seguridad de EPM System usa el cifrado AES con intensidad de claves de 128 bits.

### ▲ **Atención:**

Los flujos de tareas que usan Oracle Hyperion Financial Management y Oracle Hyperion Profitability and Cost Management se invalidan al volver a generar la clave de cifrado de inicio de sesión único. Después de volver a generar la clave, abra y guarde los flujos de tareas para volver a validarlos.

Para volver a generar la clave de cifrado de inicio de sesión único, de configuración del proveedor o de servicios de confianza:

1. Acceda a Oracle Hyperion Shared Services Console como administrador del sistema. Consulte [Inicio de Shared Services Console](#).
2. Seleccione **Administración** y, a continuación, **Configurar directorios de usuario**.
3. Seleccione **Opciones de cifrado**.
4. En **Opciones de cifrado**, seleccione la clave que desee volver a generar.

**Tabla 4-7 Opciones de cifrado de EPM System**

Opción	Descripción
Símbolo de inicio de sesión único	<p>Seleccione esta opción para volver a generar la clave de cifrado utilizada para cifrar y descifrar los símbolos de inicio de sesión único de EPM System.</p> <p>Seleccione uno de los siguientes botones si la opción <b>Activar compatibilidad con inicio de sesión único</b> está seleccionada en <b>Opciones de seguridad</b>:</p> <ul style="list-style-type: none"> <li>• <b>Generar nueva clave</b> para crear una nueva clave de cifrado de símbolo de inicio de sesión único</li> <li>• <b>Restablecer a valores predeterminados</b> para restaurar la clave de cifrado del símbolo de inicio de sesión único predeterminada</li> </ul>
Clave de servicios de confianza	<p>Seleccione esta opción para volver a generar la clave de autenticación de confianza, que utilizan los componentes de EPM System para verificar la autenticidad del servicio que solicita un símbolo de inicio de sesión único.</p>
Clave de configuración de proveedor	<p>Seleccione esta opción para volver a generar la clave utilizada para cifrar la contraseña (contraseña DN de usuario para directorios de usuario habilitados para LDAP) que emplea la seguridad de EPM System para enlazar con un directorio de usuario externo configurado. Esta contraseña se establece cuando se configura un directorio de usuario externo.</p>

 **Nota:**

Si vuelve a la clave de cifrado predeterminada, debe suprimir el archivo de almacén de claves existente (*EPM\_ORACLE\_HOME*/common/CSS/ssHandlerTK) de todos los equipos host de EPM System.

5. Haga clic en **Aceptar**.
6. Si elige generar una nueva clave de cifrado SSO, realice este paso.
  - a. Haga clic en **Descargar**.
  - b. Haga clic en **Aceptar** para guardar *ssHandlerTK*, el archivo de almacén de claves que soporta la nueva clave de cifrado de inicio de sesión único, en una carpeta del servidor que aloja Oracle Hyperion Foundation Services.
  - c. Copie *ssHandlerTK* en *EPM\_ORACLE\_HOME*/common/CSS en todos los equipos host de EPM System
7. Reinicie EPM Foundation Services y otros componentes de EPM System.

## Utilización de caracteres especiales

Active Directory y el resto de directorios de usuario basados en LDAP permiten la utilización de caracteres especiales en entidades como los nombres de dominio, nombres de usuario, roles y nombres de grupo. Puede que sea necesario aplicar un tratamiento especial a Oracle Hyperion Shared Services para que admita estos caracteres.

Normalmente, debe usar caracteres de escape cuando especifique caracteres especiales en los parámetros del directorio de usuario; por ejemplo, DN base y URL de grupo y de usuario. En la tabla siguiente, se muestran los caracteres especiales que se pueden utilizar en los nombres de usuario, de grupo, de URL de usuario, URL de grupo y en el valor de unidad operativa en el nombre distintivo del usuario.

**Tabla 4-8 Caracteres especiales soportados**

Carácter	Nombre o significado	Carácter	Nombre o significado
(	paréntesis de apertura	\$	dólar
)	paréntesis de cierre	+	signo más
"	comillas dobles	&	ampersand
'	comillas simples	\	barra invertida
,	coma	^	símbolo de intercalación
=	igual a	;	punto y coma
<	menor que	#	almohadilla
>	mayor que	@	arroba

 **Nota:**

No utilice / (barra oblicua) en los nombres de unidad de organización que se incluyan en el DN de base

- No se permiten caracteres especiales en el valor del atributo de usuario de inicio de sesión.
- El asterisco (\*) no está soportado en nombres de usuario, nombres de grupo, URL de usuario y de grupo, ni en el nombre de OU en el DN de usuario.
- No se admiten los valores de atributo que incluyan una combinación de caracteres especiales.
- El símbolo de ampersand (&) se puede utilizar sin carácter de escape. Para la configuración de Active Directory, se debe especificar & como `&amp;`.
- Los nombres de usuario y de grupo no pueden contener una barra diagonal (/) y una barra diagonal inversa (\) a la vez. Por ejemplo, no están soportados los nombres como `test/\user` y `new\test/user`.

**Tabla 4-9 Caracteres que no requieren carácter de escape**

Carácter	Nombre o significado	Carácter	Nombre o significado
(	paréntesis de apertura	'	comillas simples
)	paréntesis de cierre	^	símbolo de intercalación
\$	dólar	@	arroba
&	ampersand		



**Nota:**

& debe escribirse como &amp;.

Estos caracteres deben llevar carácter de escape si los utiliza en la configuración de directorios de usuario (nombres de usuario, nombres de grupo, URL de usuario y de grupo y DN de usuario).

**Tabla 4-10** Carácter de escape para caracteres especiales en los valores de configuración de directorios de usuario

Carácter especial	Carácter de escape	Valor de ejemplo	Ejemplo con carácter de escape
coma (,)	barra invertida (\)	ou=test,ou	ou=test\,ou
signo más (+)	barra invertida (\)	ou=test+ou	ou=test\+ou
igual a (=)	barra invertida (\)	ou=test=ou	ou=test\=ou
almohadilla (#)	barra invertida (\)	ou=test#ou	ou=test\#ou
punto y coma (;)	barra invertida (\)	ou=test;ou	ou=test\;ou
menor que (<)	barra invertida (\)	ou=test<ou	ou=test\<>ou
mayor que (>)	barra invertida (\)	ou=test>ou	ou=test\>ou
comillas (")	dos barras invertidas (\\)	ou=test"ou	ou=test\\"ou
barra invertida (\)	tres barras invertidas (\\)	ou=test\ou	ou=test\\\ou



**Nota:**

- En los DN de usuario, las comillas (") deben llevar carácter de escape con una barra invertida. Por ejemplo, `ou=test"ou` se debe especificar como `ou=test\"ou`.
- En los DN de usuario, la barra inversa (\) debe identificarse con una barra inversa. Por ejemplo, `ou=test\ou` se debe especificar como `ou=test\\ou`.



**Atención:**

Si no se ha especificado la URL de usuario, los usuarios creados en la raíz de RDN no deberán contener / (barra diagonal) ni \ (barra diagonal inversa). De la misma forma, estos caracteres no deberán utilizarse en los nombres de grupos creados en la raíz de RDN si no se ha especificado la URL de grupo. Por ejemplo, no están soportados los nombres de grupo como `OU=child\ou,OU=parent/ou` u `OU=child/ou,OU=parent\ou`. Este problema no se produce si se utiliza un atributo único como Atributo de ID en la configuración del directorio de usuario.

### Caracteres especiales en el directorio nativo

En el directorio nativo están soportados caracteres especiales en nombres de usuario y de grupo.

**Tabla 4-11 Caracteres especiales soportados: directorio nativo**

Carácter	Nombre o significado	Carácter	Nombre o significado
@	arroba	,	coma
#	almohadilla	=	igual a
\$	dólar	+	signo más
^	símbolo de intercalación	;	punto y coma
(	paréntesis de apertura	!	exclamación
)	paréntesis de cierre	%	porcentaje
'	comillas simples		

# 5

## Utilización de un módulo de autenticación personalizado

### Consulte también:

- [Descripción general](#)
- [Ejemplos y limitaciones de casos de uso](#)
- [Requisitos](#)
- [Consideraciones de codificación y diseño](#)
- [Despliegue del módulo de autenticación personalizado](#)

### Descripción general

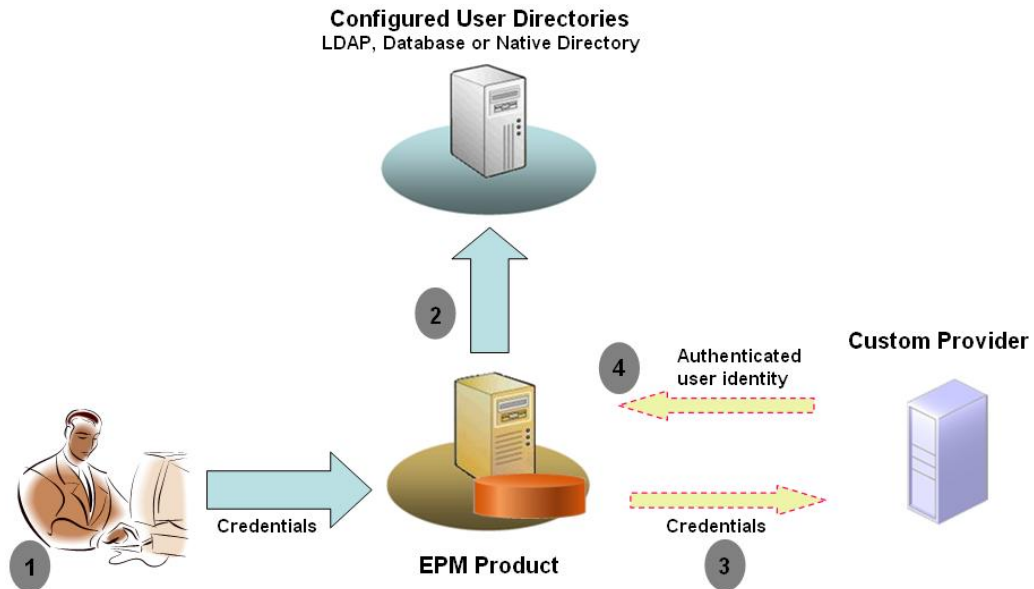
Un módulo de autenticación personalizado es un módulo Java que desarrollan los clientes e implantan para autenticar a los usuarios de Oracle Enterprise Performance Management System. Por normal general, los productos de EPM System utilizan una pantalla de inicio de sesión para capturar el nombre de usuario y la contraseña, empleados con el fin de autenticar a los usuarios. En lugar de usar la autenticación de EPM System, puede usar un módulo de autenticación personalizado para autenticar usuarios y transferir credenciales de usuario autenticadas a EPM System para un mayor procesamiento. Implantar un módulo de autenticación personalizado no implica la modificación de productos de EPM System.

Puede usar un módulo de autenticación personalizado tanto con clientes gruesos (por ejemplo, Oracle Smart View for Office y Oracle Essbase Studio) como con clientes finos (por ejemplo, Oracle Hyperion Enterprise Performance Management Workspace).

El módulo de autenticación personalizado utiliza la información que un usuario introduce para iniciar sesión en un producto de EPM System. Si está activado para un directorio de usuario, autentica los usuarios mediante el módulo de autenticación personalizado. Una vez autenticado correctamente el usuario, el módulo de autenticación personalizado devuelve el nombre de usuario a EPM System.

En la siguiente ilustración se muestra un escenario de autenticación personalizado de ejemplo:





Por ejemplo, puede usar la infraestructura de RSA SecurID como proveedor personalizado para garantizar una autenticación sólida transparente en EPM System. Una descripción general:

1. El usuario introduce las credenciales (normalmente, nombre de usuario y contraseña) para acceder a un producto de EPM System. Estas credenciales deberían identificar de forma única al usuario ante el proveedor que usa el módulo de autenticación personalizado. Por ejemplo, si está usando una infraestructura de RSA SecurID para autenticar usuarios, el usuario introduce un ID y un PIN de RSA (no un ID de usuario y una contraseña de EPM System).
2. Con el orden de búsqueda (consulte [Orden de búsqueda](#)), EPM System pasa de un directorio de usuario configurado a otro para buscar el usuario.
  - Si el directorio de usuario actual no está configurado para la autenticación personalizada, EPM System intenta buscar y autenticar al usuario mediante la autenticación de EPM System.
  - Si el directorio de usuario está configurado para la autenticación personalizada, EPM System delega el proceso de autenticación en el módulo personalizado.
3. Si EPM System delega la autenticación al módulo personalizado, el módulo de autenticación personalizado acepta las credenciales y usa su propia lógica para dirigir la autenticación del usuario a un proveedor personalizado, por ejemplo, la infraestructura de RSA SecurID.
4. El módulo de autenticación personalizado autentica al usuario en su proveedor, devuelve el nombre de usuario a EPM System o devuelve una excepción Java.

El nombre de usuario que devuelve el módulo de autenticación personalizado debe ser idéntico a un nombre de usuario en un directorio de usuario que permita la autenticación personalizada.

- Si el módulo de autenticación personalizado devuelve un nombre de usuario, EPM System busca al usuario en un directorio de usuario que permita la autenticación personalizada. En este momento, EPM System no busca los directorios de usuario que no estén configurados para la autenticación personalizada.

- Si el módulo de autenticación personalizado devuelve una excepción o devuelve un usuario nulo, EPM System sigue buscando el usuario en los demás directorios de usuarios en el orden de búsqueda que no esté activado para la autenticación personalizada. Si no se encuentra un usuario que coincida con las credenciales, EPM System muestra un error.

## Ejemplos y limitaciones de casos de uso

Entre los escenarios de implantación de autenticación personalizados se incluyen los siguientes:

- Adición de soporte para contraseña única
- Realización de la autenticación en una [Resource Access Control Facility \(RACF\)](#)
- Adición de un enlace Simple Authentication and Security Layer (SASL) a directorios de usuarios activados para LDAP en lugar de enlaces de LDAP simples

La autenticación con el mecanismo de solicitud/respuesta puede que no funcione correctamente si implanta un módulo de autenticación personalizado. Los mensajes personalizados emitidos por el módulo de autenticación personalizado no se propagan a los clientes. Los siguientes escenarios no son válidos porque los clientes, por ejemplo, Oracle Hyperion Enterprise Performance Management Workspace, sobrescriben el mensaje de error para mostrar un mensaje genérico:

- Dos PIN de RSA SecurID consecutivos
- Variante de contraseña con solicitudes, como introducir el primer, el último o el tercer carácter de la contraseña

## Requisitos

- Un archivo Java totalmente probado denominado `CustomAuth.jar`, que contiene bibliotecas de módulos de autenticación personalizados. `CustomAuth.jar` debe implantar la interfaz pública `CSSCustomAuthenticationIF`, definida en el paquete `com.hyperion.css` como parte de las API de Servicios compartidos de Oracle Hyperion estándar. Consulte [http://download.oracle.com/docs/cd/E12825\\_01/epm.111/epm\\_security\\_api\\_11111/client/com/hyperion/css/CSSCustomAuthenticationIF.html](http://download.oracle.com/docs/cd/E12825_01/epm.111/epm_security_api_11111/client/com/hyperion/css/CSSCustomAuthenticationIF.html).
- Acceso a Servicios compartidos como administrador de Servicios compartidos

## Consideraciones de codificación y diseño

### Orden de búsqueda

Además del directorio nativo, se pueden configurar varios directorios de usuario en Servicios compartidos de Oracle Hyperion. Se asigna una posición de orden de búsqueda predeterminada a todos los directorios de usuario configurados. Puede modificar el orden de búsqueda en Consola de Servicios compartidos de Oracle Hyperion. A excepción del directorio nativo, puede eliminar los directorios de usuario configurados del orden de búsqueda. Oracle Enterprise Performance Management System no usa los directorios de usuario que no estén incluidos en el orden de búsqueda. Consulte la *Guía de administración de seguridad de usuarios de Oracle Enterprise Performance Management System*.

El orden de búsqueda determina el orden en el que EPM System pasa de un directorio de usuario a otro para autenticar a los usuarios. Si al usuario se le autentifica en un directorio de

usuario, EPM System detiene la búsqueda y devuelve el usuario. EPM System deniega la autenticación y devuelve un error si el usuario no puede autenticarse en los directorios de usuario en el orden de búsqueda.

### Impacto de la autenticación personalizada en el orden de búsqueda

La autenticación personalizada afecta a la forma en que la seguridad de EPM System interpreta el orden de búsqueda.

Si el módulo de autenticación personalizado devuelve un nombre de usuario, EPM System solo busca al usuario en un directorio de usuario que permita la autenticación personalizada. En este momento, EPM System ignora los directorios de usuario que no estén configurados para la autenticación personalizada.

### Descripción del flujo de autenticación personalizada

Se usan los siguientes escenarios de caso de uso para explorar el flujo de autenticación personalizada:

- [Escenario de caso de uso 1](#)
- [Escenario de caso de uso 2](#)
- [Escenario de caso de uso 3](#)

#### Escenario de caso de uso 1

En la siguiente tabla se detallan la configuración de directorio de usuario de EPM System y el orden de búsqueda que se usa en este escenario. En este escenario se asume que el módulo de autenticación personalizado usa una infraestructura RSA para autenticar a los usuarios.

**Tabla 5-1 Configuración del escenario 1**

Tipo y nombre de directorio de usuario	Orden de búsqueda	Autenticación personalizada	Nombres de usuario de ejemplo	Contraseña <sup>1</sup>
Directorio nativo	1	Desactivada	test_user_1 test_user_2 test_user_3	password
Activado para LDAP SunONE_West	2	Desactivada	test_ldap1 test_ldap_2 test_user_3 test_ldap_4	ldappassword
Activado para LDAP SunONE_East	3	Activada	test_ldap1 test_ldap_2 test_user_3	ldappassword en SunONE y RSA PIN en el módulo personalizado

<sup>1</sup> Para hacerlo más sencillo, se asume que todos los usuarios usan la misma contraseña para el directorio de usuario.

Para iniciar el proceso de autenticación, un usuario introduzca un nombre de usuario y una contraseña en la pantalla de conexión de un producto EPM System. En este escenario, el módulo de autenticación personalizado realiza las siguientes acciones:

- Acepta un nombre de usuario y un PIN de RSA como credenciales de usuario
- Devuelve un nombre de usuario en formato `username@providername`, por ejemplo, `test_ldap_2@SunONE_East`, a la seguridad de EPM System

**Tabla 5-2 Interacción del usuario y resultados**

Nombre de usuario y contraseña	Resultado de autenticación	Directorio de usuario de conexión
test_user_1/password	Correcto	Directorio nativo
test_user_3/password	Correcto	Directorio nativo
test_user_3/ ldappassword	Correcto	SunONE_West (orden de búsqueda 2) <sup>1</sup>
test_user_3/RSA PIN	Correcto	SunONE_East (orden de búsqueda 3) <sup>2</sup>
test_ldap_2/ ldappassword	Correcto	SunONE_West (orden de búsqueda 2)
test_ldap_4/RSA PIN	Fallo EPM System muestra un error de autenticación. <sup>3</sup>	

<sup>1</sup> La autenticación personalizada no puede autenticar este usuario porque el usuario ha introducido las credenciales de EPM System. EPM System puede identificar solo este usuario en un directorio de usuario que no esté activado para autenticación personalizada. El usuario no está en el directorio nativo (número de orden de búsqueda 1), pero se identifica en SunONE West (número de orden de búsqueda 2).

<sup>2</sup> EPM System no encuentra este usuario en el directorio nativo (número de orden de búsqueda 1) o SunONE West (número de orden de búsqueda 2). El módulo de autenticación personalizado valida al usuario en un servidor de RSA y devuelve `test_user_3@SunONE_EAST` a EPM System. EPM System busca al usuario en SunONE East (número de orden de búsqueda 3), que es un directorio de usuario con la autenticación personalizada activa.

<sup>3</sup> Oracle recomienda que todos los usuarios autenticados por el módulo personalizado estén presentes en un directorio de usuario con autenticación personalizada activada incluida en el orden de búsqueda. Se produce un fallo de conexión si el nombre de usuario que devuelve el módulo de autenticación personalizado no está presente en un directorio de usuario con autenticación personalizada activada incluida en el orden de búsqueda.

## Escenario de caso de uso 2

En la siguiente tabla se detallan la configuración de directorio de usuario de EPM System y el orden de búsqueda que se usa en este escenario. En este escenario se asume que el módulo de autenticación personalizado usa una infraestructura RSA para autenticar a los usuarios.

En este escenario, el módulo de autenticación personalizado realiza las siguientes acciones:

- Acepta un nombre de usuario y un PIN de RSA como credenciales de usuario
- Devuelve un nombre de usuario, por ejemplo, `test_ldap_2`, a la seguridad de EPM System

**Tabla 5-3 Un orden de búsqueda de ejemplo**

Directorio de usuario	Orden de búsqueda	Autenticación personalizada	Nombres de usuario de ejemplo	Contraseña <sup>1</sup>
Directorio nativo	1	Desactivada	test_user_1 test_user_2 test_user_3	password
Activado para LDAP, por ejemplo, SunONE	2	Activada	test_ldap1 test_ldap2 test_user_3	ldappassword en SunONE y RSA PIN en el módulo personalizado

<sup>1</sup> Para hacerlo más sencillo, se asume que todos los usuarios usan la misma contraseña para el directorio de usuario.

Para iniciar el proceso de autenticación, un usuario introduce un nombre de usuario y una contraseña en la pantalla de inicio de sesión de un producto EPM System.

**Tabla 5-4 Interacción del usuario y resultados**

Nombre de usuario y contraseña	Resultado de inicio de sesión	Directorio de usuario de conexión
test_user_1/password	Correcto	Directorio nativo
test_user_3/password	Correcto	Directorio nativo
test_user_3/ldappassword	Fallo	SunONE <sup>1</sup>
test_user_3/RSA PIN	Correcto	SunONE <sup>2</sup>

- <sup>1</sup> La autenticación del usuario en el directorio nativo falla porque las contraseñas no coinciden. La autenticación del usuario mediante el módulo de autenticación personalizado falla porque la contraseña usada no es un PIN de RSA válido. EPM System no intenta autenticar a este usuario en SunONE (orden de búsqueda 2), porque la configuración de la autenticación personalizada sustituye a la autenticación de EPM System en este directorio.
- <sup>2</sup> La autenticación del usuario en el directorio nativo falla porque las contraseñas no coinciden. El módulo de autenticación personalizado autentica al usuario y devuelve el nombre de usuario test\_user\_3 a EPM System.

### Escenario de caso de uso 3

En la siguiente tabla se detallan la configuración de directorio de usuario de EPM System y el orden de búsqueda que se usa en este escenario. En este escenario se asume que el módulo de autenticación personalizado usa una infraestructura RSA para autenticar a los usuarios.

Para favorecer la claridad en esos escenarios, Oracle recomienda que su módulo de autenticación personalizado devuelva el nombre de usuario en formato username@providername, por ejemplo, test\_ldap\_4@SunONE.

**Tabla 5-5 Un orden de búsqueda de ejemplo**

Directorio de usuario	Orden de búsqueda	Autenticación personalizada	Nombres de usuario de ejemplo	Contraseña <sup>1</sup>
Directorio nativo	1	Activada	test_user_1 test_user_2 test_user_3	RSA_PIN
Activado para LDAP, por ejemplo, MSAD	2	Desactivada	test_ldap1 test_ldap4 test_user_3	ldappassword
Activado para LDAP, por ejemplo, SunONE	3	Activada	test_ldap1 test_ldap4 test_user_3	ldappassword en SunONE y RSA PIN en el módulo personalizado

<sup>1</sup> Para hacerlo más sencillo, se asume que todos los usuarios usan la misma contraseña para el directorio de usuario.

Para iniciar el proceso de autenticación, un usuario introduzca un nombre de usuario y una contraseña en la pantalla de conexión de un producto EPM System.

**Tabla 5-6 Interacción del usuario y resultados**

Nombre de usuario y contraseña	Resultado de autenticación	Directorio de usuario de conexión
test_user_1/password	Correcto	Directorio nativo
test_user_3/RSA_PIN	Correcto	Directorio nativo
test_user_3/ldappassword	Correcto	MSAD (orden de búsqueda 2)
test_ldap_4/ldappassword	Correcto	MSAD (orden de búsqueda 2)
test_ldap_4/RSA PIN	Correcto	SunONE (orden de búsqueda 3)

### Directorios de usuarios y módulo de autenticación personalizado

Para usar el módulo de autenticación personalizado, los directorios de usuarios que contienen información de usuarios y grupos de EPM System se pueden configurar de forma individual para delegar la autenticación al módulo personalizado.

Los usuarios de EPM System que estén autenticados mediante un módulo personalizado deben estar presentes en uno de los directorios de usuario incluidos en el módulo de búsqueda (consulte [Orden de búsqueda](#)). Asimismo, se debe configurar el directorio de usuario para delegar la autenticación al módulo personalizado.

La identidad del usuario en el proveedor personalizado (por ejemplo, 1357642 en la infraestructura SecurID de RSA) puede ser distinto del nombre de usuario del directorio de usuario (por ejemplo, jDoe en una instancia de Oracle Internet Directory) configurado en Servicios compartidos. Después de autenticar al usuario, el módulo de autenticación personalizado debe devolver el nombre de usuario jDoe a EPM System.

 **Nota:**

Como mejor práctica, Oracle recomienda que el nombre de usuario de los directorios de usuario configurados en EPM System sea idéntico a los disponibles en el directorio de usuario que usa el módulo de autenticación personalizado.

### Interfaz Java de `CSSCustomAuthenticationIF`

El módulo de autenticación personalizado debe usar la interfaz Java de `CSSCustomAuthenticationIF` para integrarse con el marco de seguridad de EPM System. Debe devolver una cadena de nombre de usuario si la autenticación personalizada es correcta o un mensaje de error si la autenticación personalizada no es correcta. Para que finalice el proceso de autenticación, el nombre de usuario que devuelve el módulo de autenticación personalizado debe estar presente en uno de los directorios de usuario incluidos en el orden de búsqueda de Servicios compartidos. El marco de seguridad de EPM System soporta el formato `username@providerName`.

 **Nota:**

Asegúrese de que el nombre de usuario que devuelve el módulo de autenticación personalizado no contengan un \* (asterisco), porque el marco de seguridad de EPM System lo interpreta como un carácter comodín al buscar usuarios.

Consulte [Código de ejemplo 1](#) para la firma de la interfaz de `CSSCustomAuthenticationIF`.

Su módulo de autenticación personalizado (puede ser un archivo de clase) se debe incluir en `CustomAuth.jar`. La estructura del paquete no es importante.

Para obtener información detallada sobre la interfaz de `CSSCustomAuthenticationIF`, consulte [Documentación de la API de seguridad](#).

El método `authenticate` de `CSSCustomAuthenticationIF` soporta la autenticación personalizada. El método `authenticate` acepta las credenciales (nombre de usuario y contraseña) que el usuario ha introducido al intentar acceder a EPM System como parámetros de entrada. Este método devuelve una cadena (nombre de usuario) si la autenticación personalizada es correcta. Devuelve una excepción `java.lang.Exception` si la autenticación no es correcta. El nombre de usuario que devuelve el método debería identificar de forma única un usuario en uno de los directorios de usuario incluidos en el orden de búsqueda de Servicios compartidos. El marco de seguridad de EPM System soporta el formato `username@providerName`.

 **Nota:**

Para inicializar recursos, por ejemplo, una agrupación de conexiones JDBC, utilice el constructor de clases. Al hacerlo, mejora el rendimiento al no cargar recursos para cada una de las autenticaciones.

## Despliegue del módulo de autenticación personalizado

Solo está soportado un módulo personalizado para un despliegue de Oracle Enterprise Performance Management System. Puede activar la autenticación personalizada para uno o más directorios de usuario en el orden de búsqueda.

El módulo de autenticación personalizado debe implantar la interfaz pública `CSSCustomAuthenticationIF`, definida en el paquete `com.hyperion.css`. En este documento se asume que cuenta con un módulo personalizado totalmente funcional que define la lógica para autenticar a los usuarios en el proveedor de usuarios que decida. Tras desarrollar y probar un módulo de autenticación personalizado, debe implantarlo en el entorno de EPM System.

### Descripción general de los pasos

En su código de autenticación personalizado no se debe usar `log4j` para el registro de errores. Si en el código que ha usado en una versión anterior se utiliza `log4j`, debe eliminarlo de este antes de usarlo con esta versión.

Para implantar el módulo de autenticación personalizado, realice los siguientes pasos:

- Detenga los productos de EPM System, incluidos Servicios compartidos de Oracle Hyperion y cualquier sistema que use API de Servicios compartidos.
- Copie el archivo Java del módulo de autenticación personalizado `CustomAuth.jar` en el despliegue:

- **WebLogic:** copie `CustomAuth.jar` a `MIDDLEWARE_HOME/user_projects/domains/WEBLOGIC_DOMAIN/lib`, normalmente, `C:/Oracle/Middleware/user_projects/domains/EPMSysstem/lib`.

Si está actualizando de la versión 11.1.2.0 o 11.1.2.1 con una implantación del módulo de autenticación personalizado, mueva `CustomAuth.jar` de `EPM_ORACLE_HOME/common/jlib/11.1.2.0` a `MIDDLEWARE_HOME/user_projects/domains/WEBLOGIC_DOMAIN/lib`.

- **Todos los despliegues de clientes:** copie `CustomAuth.jar` en todos los despliegues de clientes EPM System, en la siguiente ubicación:

`EPM_ORACLE_HOME/common/jlib/11.1.2.0`, normalmente, `Oracle/Middleware/common/jlib/11.1.2.0`. Asegúrese de que el archivo `CustomAuth.jar` esté siempre ubicado en el directorio `EPM_ORACLE_HOME/common/jlib/11.1.2.0`.

Para que todos los servidores y clientes funcionen con autenticación personalizada, el archivo `CustomAuth.jar` debe estar presente en las dos siguientes ubicaciones:

- \* `MIDDLEWARE_HOME/user_projects/domains/WEBLOGIC_DOMAIN/lib`
- \* `EPM_ORACLE_HOME/common/jlib/11.1.2.0`



- Actualice la configuración del directorio de usuario en Servicios compartidos. Consulte [Actualización de la configuración en Servicios compartidos](#).
- Inicie Shared Services, seguido por otros productos de EPM System.
- Pruebe su implementación. Consulte [Prueba de su despliegue](#).

### Actualización de la configuración en Servicios compartidos

De manera predeterminada, la autenticación personalizada se desactiva para todos los directorios de usuarios. Puede sobrescribir el comportamiento predeterminado para activar la autenticación personalizada para directorios de usuario externos específicos para el directorio nativo.

### Actualización de las configuraciones del directorio de usuario

Debe actualizar la configuración del directorio de usuario para la que esté activada la autenticación personalizada.

Para actualizar la configuración del directorio de usuario:

1. Inicie Oracle Hyperion Foundation Services.
2. Acceda a Oracle Hyperion Shared Services Console como administrador del sistema.
3. Seleccione **Administración** y, a continuación, **Configurar directorios de usuario**.
4. En la pantalla Directorios de usuario definidos, seleccione el directorio de usuario cuya autenticación personalizada desea cambiar.

 **Nota:**

EPM System utiliza sólo los directorios de usuario incluidos en el orden de búsqueda.

5. Haga clic en **Editar**.
6. Seleccione **Mostrar opciones avanzadas**.
7. En **Módulo de personalización**, seleccione **Módulo de autenticación** para activar el módulo personalizado para el directorio de usuario actual.
8. Haga clic en **Finalizar**.
9. Repita este procedimiento para actualizar la configuración de otros directorios de usuario en el orden de búsqueda.

### Actualización de opciones de seguridad

Asegúrese de que `CustomAuth.jar` esté disponible en `EPM_ORACLE_HOME/user_projects/domains/WEBLOGIC_DOMAIN/lib` antes de iniciar el siguiente procedimiento.

Para actualizar las opciones de seguridad:

1. Acceda a Shared Services Console como administrador del sistema.

2. Seleccione **Administración** y, a continuación, **Configurar directorios de usuario**.
3. Seleccione **Opciones de seguridad**.
4. Seleccione **Mostrar opciones avanzadas**.
5. En **Módulo de autenticación**, introduzca el nombre de clase de Java completo del módulo de autenticación personalizado que se debería usar para autenticar a los usuarios en todos los directorios de usuario para los que se haya seleccionado el módulo de autenticación personalizado. Por ejemplo,  
`com.mycompany.epm.CustomAuthenticationImpl.`
6. Haga clic en **Aceptar**.

### Prueba de su despliegue

Si el directorio nativo no está configurado para la autenticación personalizada, no utilice usuarios del mismo para probar la autenticación personalizada.



#### Nota:

Usted es el responsable de identificar y corregir los problemas del módulo de autenticación personalizado. Oracle asume que su módulo personalizado funciona a la perfección para asignar un usuario del directorio de usuario que usa el módulo personalizado a un usuario de un directorio de usuario con autenticación personalizada activada disponible en el orden de búsqueda de EPM System.

Para probar el despliegue, inicie sesión en EPM System con las credenciales de usuario del directorio de usuario, por ejemplo, una infraestructura de RSA SecurID, que use el módulo personalizado. Estas credenciales pueden ser distintas de las credenciales de EPM System.

Su implantación se considera que se ha realizado correctamente si los productos de EPM System le permiten acceder a sus recursos. Un error que indica que no se ha encontrado el usuario no siempre indica una implantación incorrecta. En esos casos, verifique que las credenciales que ha introducido estén presentes en el almacén de usuarios personalizado y que haya un usuario coincidente presente en uno de los directorios de usuario con la autenticación personalizada activada en el orden de búsqueda de EPM System.

Para probar la autenticación personalizada:

1. Asegúrese de que los productos de EPM System se estén ejecutando.
2. Acceda a un componente de EPM System, por ejemplo, Oracle Hyperion Enterprise Performance Management Workspace.
3. Inicie sesión como usuario definido en un directorio de usuario para el que esté activada la autenticación personalizada.
  - a. En **Nombre de usuario**, introduzca su identificador de usuario, por ejemplo, un ID de usuario de RSA.
  - b. En **Contraseña**, introduzca una contraseña, por ejemplo, un PIN de RSA.
  - c. Haga clic en **Inicio de sesión**.
4. Verifique que puede acceder a los recursos de los productos de EPM System.

# 6

## Pautas para establecer la seguridad de EPM System

### Consulte también:

- [Implantación de SSL](#)
- [Cambio de la contraseña de administración](#)
- [Regeneración de claves de cifrado](#)
- [Cambio de contraseñas de base de datos](#)
- [Cómo garantizar las cookies](#)
- [Reducción del tiempo de espera del símbolo de inicio de sesión único](#)
- [Revisión de informes de seguridad](#)
- [Personalización del sistema de autenticación para una autenticación compleja](#)
- [Desactivación de las utilidades de depuración de EPM Workspace](#)
- [Cambio de las páginas de error predeterminadas del servidor web](#)
- [Soporte del software de terceros](#)

### Implantación de SSL

SSL utiliza un sistema criptográfico que cifra datos. SSL crea una conexión segura entre un cliente y un servidor por la que los datos se pueden enviar de manera segura.

Para proteger su entorno de Oracle Enterprise Performance Management System, proteja todos los canales de comunicación que usen sus aplicaciones web y la conexiones de directorio de usuario mediante SSL. Consulte [Activación de SSL para componentes de EPM System](#).

Además, proteja todos los puertos de agente, por ejemplo, el puerto 6861, que es el puerto de agente de Oracle Hyperion Reporting and Analysis, mediante un cortafuegos. Los usuarios finales no necesitan acceder a los puertos de agente de EPM System.

### Cambio de la contraseña de administración

La cuenta de usuario de administración predeterminada de directorio nativo ofrece acceso a todas las funciones de Servicios compartidos de Oracle Hyperion. Esta contraseña se establece al desplegar Oracle Hyperion Foundation Services. Debe cambiar periódicamente la contraseña de esta cuenta.

Edite la cuenta de usuario *admin* para cambiar la contraseña. Consulte la sección sobre modificación de cuentas de usuario en *Guía de administración de seguridad de usuarios de Oracle Enterprise Performance Management System*.

## Regeneración de claves de cifrado

Utilice Consola de Servicios compartidos de Oracle Hyperion para volver a generar periódicamente lo siguiente:

- Símbolo de inicio de sesión único

### ▲ Atención:

Los flujos de tareas que usan Oracle Hyperion Financial Management y Oracle Hyperion Profitability and Cost Management se invalidan al generar un nuevo almacén de claves. Después de volver a generar el almacén, abra y guarde los flujos de tareas para revalidarlos.

- Clave de servicios de confianza
- Clave de configuración de proveedor

Consulte [Regeneración de claves de cifrado](#).

### ✎ Nota:

Servicios compartidos de Oracle Hyperion y el subsistema de seguridad de Oracle Enterprise Performance Management System usa el cifrado AES con intensidad de claves de 128 bits.

## Cambio de contraseñas de base de datos

Cambie periódicamente la contraseña de todas las bases de datos de productos de Oracle Enterprise Performance Management System. El procedimiento para cambiar la contraseña de la base de datos en Servicios compartidos de Oracle Hyperion Registry se detalla en esta sección.

Para obtener procedimientos detallados para cambiar una contraseña de base de datos de productos de EPM System, consulte la *Guía de configuración e instalación de Oracle Enterprise Performance Management System*.

Para cambiar las contraseñas de bases de datos de productos de EPM System en Shared Services Registry:

1. Mediante la consola de administración de la base de datos, cambie la contraseña del usuario cuya cuenta se utilizara para configurar la base de datos de productos de EPM System.
2. Detenga los productos (las aplicaciones web, los servicios y los procesos) de EPM System.
3. Mediante EPM System Configurator, vuelva a configurar la base de datos mediante uno de los procedimientos siguientes.

**Solo Servicios compartidos de Oracle Hyperion:**

 **Nota:**

En entornos distribuidos en los que los productos de EPM System se encuentran en equipos distintos al de Servicios compartidos, deberá realizar este procedimiento en todos los servidores.

- a. En las tareas de Foundation correspondientes a EPM System Configurator, seleccione **Configurar base de datos**.
- b. En la página “Configuración de la base de datos de registro y Shared Services”, seleccione **Conectar a una base de datos de Shared Services previamente configurada**.
- c. Especifique la contraseña nueva del usuario cuya cuenta se usará para configurar la base de datos de Servicios compartidos. No cambie ninguno de los valores de configuración restantes.
- d. Continúe con la configuración y haga clic en **Finalizar** cuando termine.

Productos de **EPM System distintos de Shared Services**:

 **Nota:**

Lleve a cabo estos pasos para los productos de EPM System desplegados en el servidor actual únicamente.

Consulte la *Guía de configuración e instalación de Oracle Enterprise Performance Management System* para obtener instrucciones detalladas.

4. Inicie los productos y servicios de EPM System.

## Cómo garantizar las cookies

La aplicación web de Oracle Enterprise Performance Management System establece una cookie para realizar un seguimiento de la sesión. Al hacerlo, sobre todo si se trata de una cookie de sesión, el servidor puede establecer el indicador seguro, que fuerza al explorador a enviar la cookie por un canal seguro. Con este comportamiento se reduce el riesgo de secuestro de sesión.

 **Nota:**

Garantice las cookies solo si los productos de EPM System se despliegan en un entorno activado para SSL.

Modifique el descriptor de sesión de Oracle WebLogic Server para asegurar las cookies de WebLogic Server. Establezca el valor del atributo `cookieSecure` en el elemento `session-param` como `true`. Consulte Protección de aplicaciones web en [Oracle Fusion Middleware Programming Security for Oracle WebLogic Server 11g](#).

## Reducción del tiempo de espera del símbolo de inicio de sesión único

El tiempo de espera de símbolo de inicio de sesión único predeterminado es 480 minutos. Convendría reducir este tiempo de espera, por ejemplo, a 60 minutos para minimizar la reutilización del símbolo en caso de quedar expuesto. Consulte "Establecimiento de las opciones de seguridad" en la *Guía de administración de seguridad de usuarios de Oracle Enterprise Performance Management System*.

## Revisión de informes de seguridad

El informe de seguridad contiene información de auditoría relacionada con las tareas de seguridad para las que está configurada la auditoría. Genere y revise este informe en Consola de Servicios compartidos de Oracle Hyperion de forma periódica, especialmente para identificar aquellos intentos de conexión con fallos en los productos de Oracle Enterprise Performance Management System y los cambios de aprovisionamiento. Seleccione **Vista de detalles** como opción de generación del informe a fin de agrupar los datos del informe en función de los atributos modificados y los nuevos valores de los atributos. Consulte la sección sobre generación de informes en *Guía de administración de seguridad de usuarios de Oracle Enterprise Performance Management System*.

## Personalización del sistema de autenticación para una autenticación compleja

Puede usar un módulo de autenticación personalizada para añadir una autenticación fuerte a EPM System. Por ejemplo, puede usar la autenticación de dos factores de RSA SecurID en un modo de respuesta de no verificación. El módulo de autenticación personalizado es transparente para clientes finos y gruesos y no necesita cambios de despliegue en el cliente. Consulte [Utilización de un módulo de autenticación personalizado](#).

## Desactivación de las utilidades de depuración de EPM Workspace

- Para la solución de problemas, Oracle Hyperion Enterprise Performance Management Workspace incluye archivos JavaScript sin comprimir. Por motivos de seguridad, debe eliminar los archivos JavaScript sin comprimir del entorno de producción:
  - Cree una copia de seguridad del directorio `EPM_ORACLE_HOME/common/epmstatic/wspace/js/`.
  - Excepto en el caso del archivo `DIRECTORY_NAME.js`, suprima los archivos `.js` de cada subdirectorio de `EPM_ORACLE_HOME/common/epmstatic/wspace/js/`.Cada subdirectorio contiene un archivo `.js` que lleva el nombre del directorio. Por ejemplo, `EPM_ORACLE_HOME/common/epmstatic/wspace/js/com/`

`hyperion/bpm/web/common` contiene `Common.js`. Elimine todos los archivos `.js` a excepción del que lleva el nombre del directorio, en este caso; `Common.js`.

- EPM Workspace proporciona algunas utilidades de depuración y aplicaciones de prueba, a las que se puede acceder si se despliega EPM Workspace en el modo de depuración. Por motivos de seguridad, los administradores deben desactivar la depuración del cliente en EPM Workspace.

Para desactivar el modo de depuración:

1. Inicie una sesión en EPM Workspace como administrador.
2. Seleccione **Navegar, Administrar** y, a continuación, **Configuración del servidor de Workspace**.
3. En **ClientDebugEnabled** en Configuración del servidor de Workspace, seleccione **No**.
4. Haga clic en **Aceptar**.

## Cambio de las páginas de error predeterminadas del servidor web

Cuando los servidores de aplicaciones no estén disponibles para aceptar solicitudes, el complemento de servidor web para el servidor de aplicaciones de backend (por ejemplo, el complemento de Oracle HTTP Server para Oracle WebLogic Server) devuelve una página de error predeterminada que muestra la información sobre la compilación del complemento. Los servidores web muestran la página de error predeterminada también en otras ocasiones. Los atacantes pueden utilizar esta información para descubrir vulnerabilidades en los sitios web públicos.

Personalice las páginas de error (del complemento del servidor de aplicaciones web y del servidor web) para que no contengan información acerca de los componentes del sistema de producción, por ejemplo, la versión del servidor, el tipo de servidor, la fecha de compilación del complemento y el tipo de complemento. Consulte la documentación del proveedor del servidor de aplicaciones y del servidor web para obtener más información.

## Soporte del software de terceros

Oracle reconoce y da soporte a las afirmaciones de compatibilidad con versiones anteriores ofrecidas por proveedores terceros. Por lo tanto, en los productos en los que los proveedores afirman que existe compatibilidad con versiones anteriores, se podrán usar las versiones de mantenimiento y Service Pack posteriores. Si se identifica una incompatibilidad, Oracle especificará una versión del parche en el que debería desplegarse el producto (y eliminar la versión incompatible de la matriz admitida) u ofrecerá una versión de mantenimiento o arreglo de servicio para el producto de Oracle.

**Actualizaciones de servidor:** La compatibilidad con actualizaciones para componentes de servidor de terceros está determinada por la política de versiones de mantenimiento subsiguiente. Normalmente, Oracle soporta la actualización de componentes de servidor de terceros a la siguiente versión de mantenimiento del Service Pack de la versión soportada en ese momento. Las actualizaciones a la siguiente versión principal no están soportadas.

**Actualizaciones de cliente:** Oracle soporta las actualizaciones automáticas para componentes de cliente, incluidas las actualizaciones a la siguiente versión principal de

componentes de cliente de terceros. Por ejemplo, puede actualizar la versión de JRE de explorador a la versión de JRE actualmente soportada.



# A

## Código de muestra de autenticación personalizado

### Código de ejemplo 1



#### Nota:

En su código de autenticación personalizado no se debe usar log4j para el registro de errores. Si en el código de autenticación personalizado que ha usado en una versión anterior ha utilizado log4j, debe eliminarlo de este antes de usarlo con esta versión.

El siguiente fragmento de código es una implantación vacía del módulo personalizado:

```
package com.hyperion.css.custom;

import java.util.Map;
import com.hyperion.css.CSSCustomAuthenticationIF;

public class CustomAuthenticationImpl implements CSSCustomAuthenticationIF {
 public String authenticate(Map context,String userName,
 String password) throws Exception{
 try{
 //Custom code to find and authenticate the user goes here.
 //The code should do the following:
 //if authentication succeeds:
 //set authenticationSuccessFlag = true
 //return authenticatedUserName
 // if authentication fails:
 //log an authentication failure
 //throw authentication exception
 }
 catch (Exception e){
 //Custom code to handle authentication exception goes here
 //Create a new exception, set the root cause
 //Set any custom error message
 //Return the exception to the caller
 }
 return authenticatedUserName;
 }
}
```

Parámetros de entrada:

- Contexto: mapa que contiene un par de clave-valor de la información de configuración regional
- Nombre de usuario: identificador que identifica de forma única al usuario en el directorio de usuario donde el módulo personalizado autentifica al usuario. El usuario introduce el valor de este parámetro al iniciar sesión en un componente de Oracle Enterprise Performance Management System.
- Contraseña: la contraseña establecida para el usuario en el directorio de usuario donde el módulo personalizado autentifica al usuario. El usuario introduce el valor de este parámetro al iniciar sesión en un componente de EPM System.

## Código de ejemplo 2

En el siguiente código de ejemplo se muestra la autenticación personalizada de los usuarios que usan el nombre de usuario y la contraseña incluidos en un archivo sin formato. Debe inicializar las listas de usuarios y contraseñas de este constructor de clase para que funcione la autenticación personalizada.

```
package com.hyperion.css.security;

import java.util.Map;
import java.util.HashMap;
import com.hyperion.css.CSSCustomAuthenticationIF;
import java.io.*;

public class CSSCustomAuthenticationImpl implements
CSSCustomAuthenticationIF{
 static final String DATA_FILE = "datafile.txt";

 /**
 * authenticate method includes the core implementation of the
 * Custom Authentication Mechanism. If custom authentication is
 * enabled for the provider, authentication operations
 * are delegated to this method. Upon successful authentication,
 * this method returns a valid user name, using which EPM System
 * retrieves the user from a custom authentication enabled provider.
 * User name can be returned in the format username@providerName,
 * where providerName indicates the name of the underlying provider
 * where the user is available. authenticate method can use other
 * private methods to access various core components of the
 * custom authentication module.

 * @param context
 * @param userName
 * @param password
 * @return
 * @throws Exception
 */

 Map users = null;

 public CSSCustomAuthenticationImpl(){
```

```

users = new HashMap();
InputStream is = null;
BufferedReader br = null;
String line;
String[] userDetails = null;
String userKey = null;
try{
 is = CSSCustomAuthenticationImpl.class.getResourceAsStream(DATA_FILE);
 br = new BufferedReader(new InputStreamReader(is));
 while(null != (line = br.readLine())){
 userDetails = line.split(":");
 if(userDetails != null && userDetails.length==3){
 userKey = userDetails[0]+ ":" + userDetails[1];
 users.put(userKey, userDetails[2]);
 }
 }
}
catch(Exception e){
 // log a message
}
finally{
 try{
 if(br != null) br.close();
 if(is != null) is.close();
 }
 catch(IOException ioe){
 ioe.printStackTrace();
 }
}
}

/* Use this authenticate method snippet to return username from a flat file
*/

public String authenticate(Map context, String userName, String password)
throws Exception{
 //userName : user input for the userName
 //password : user input for password
 //context : Map, can be used to additional information required by
 // the custom authentication module.

 String authenticatedUserKey = userName + ":" + password;

 if(users.get(authenticatedUserKey)!=null)
 return (String)users.get(authenticatedUserKey);
 else throw new Exception("Invalid User Credentials");
}

/* Refer to this authenticate method snippet to return username in
 username@providername format */

public String authenticate(Map context, String userName, String password)
throws Exception{

 //userName : user input for userName

```

```

//password : user input for password
//context : Map can be used to additional information required by
// the custom authentication module.

//Your code should uniquely identify the user in a custom provider
and in a configured
//user directory in Shared Services. EPM Security expects you to
append the provider
//name to the user name. Provider name must be identical to the name
of a custom
//authentication-enabled user directory specified in Shared Services.

//If invalid arguments, return null or throw exception with
appropriate message
//set authenticationSuccessFlag = false

String authenticatedUserKey = userName + ":" + password;
if(users.get(authenticatedUserKey)!=null)
 String userNameStr = (new StringBuffer()
 .append((String)users.get(authenticatedUserKey)
)
 .append("@").append(PROVIDER_NAME).toString(
);
 return userNameStr;
else throw new Exception("Invalid User Credentials");
 }
}

```

## Archivo de datos para código de ejemplo 2

Asegúrese de que el archivo de datos se denomine `datafile.txt`, que es el nombre que se usa en el código de ejemplo y que se incluye en el archivo Java que ha creado.

Utilice lo siguiente como contenido del archivo sin formato que se usa como directorio de usuario personalizado para soportar el módulo de autenticación personalizado implantado por el código de ejemplo 2 (consulte [Código de ejemplo 2.](#))

```

xyz:password:admin
test1:password:test1@LDAP1
test1:password:test1
test1@LDAP1:password:test1@LDAP1
test1@1:password:test1
user1:Password2:user1@SunONE1
user1_1:Password2:user1
user3:Password3:user3
DS_User1:Password123:DS_User1@MSAD1
DS_User1:Password123:DS_User1
DS_User1@1:Password123:DS_User1

```

Utilice lo siguiente como contenido del archivo sin formato que se usa como directorio de usuario personalizado si tiene previsto devolver el nombre de usuario con formato *username@providername*:

```
xyz:password:admin
test1:password:test1
test1@1:password:test1
user1_1:Password2:user1
user3:Password3:user3
DS1_1G100U_User61_1:Password123:DS1_1G100U_User61
DS1_1G100U_User61_1@1:Password123:DS1_1G100U_User61
TUser:password:TUser
```

# B

## Implantación de una clase de inicio de sesión personalizada

Oracle Enterprise Performance Management System proporciona `com.hyperion.css.sso.agent.X509CertificateSecurityAgentImpl` para extraer la identidad de usuario (DN) de los certificados x509.

Si debe obtener la identidad de usuario de un atributo en el certificado que no sea DN, debe desarrollar e implantar una clase de conexión personalizada similar a `com.hyperion.css.sso.agent.X509CertificateSecurityAgentImpl`, como se describe en este apéndice.

### Código de ejemplo de clase de inicio de sesión personalizada

En este ejemplo de código se muestra la implantación de `com.hyperion.css.sso.agent.X509CertificateSecurityAgentImpl` predeterminado. Por lo general, debe personalizar el método `parseCertificate(String sCertificate)` de esta implementación para obtener el nombre de usuario de un atributo de certificado que no sea DN:

```
package com.hyperion.css.sso.agent;

import java.io.ByteArrayInputStream;
import java.io.UnsupportedEncodingException;
import java.security.Principal;
import java.security.cert.CertificateException;
import java.security.cert.CertificateFactory;
import java.security.cert.X509Certificate;
import com.hyperion.css.CSSSecurityAgentIF;
import com.hyperion.css.common.configuration.*;

import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;

/**
 * X509CertificateAuthImpl implements the CSSSecurityAgentIF interface It
 * accepts
 * the X509 certificate of the authenticated user from the Web Server via a
 * header, parses the certificate, extracts the DN of the User and
 * authenticates the user.
 */
public class X509CertificateSecurityAgentImpl implements CSSSecurityAgentIF
{
 static final String IDENTITY_ATTR = "CN";
 String g_userDN = null;
 String g_userName = null;
 String hostAddress = null;
 /**
```

```

 * Returns the User name (login name) of the authenticated user,
 * for example demouser. See CSS API documentation for more
information
 */
 public String getUsername(HttpServletRequest req,
 HttpServletResponse res)
 throws Exception
 {
 hostAddress = req.getServerName();
 String certStr = getCertificate(req);

 String sCert = prepareCertificate(certStr);

 /* Authenticate with a CN */
 parseCertificate(sCert);

 /* Authenticate if the Login Attribute is a DN */
 if (g_userName == null)
 {
 throw new Exception("User name not found");
 }
 return g_userName;
 }

 /**
 * Passing null since this is a trusted Security agent
authentication
 * See Security API documentation for more information on
CSSSecurityAgentIF
 */
 public String getPassword(HttpServletRequest req,
 HttpServletResponse res)
 throws Exception
 {
 return null;
 }

 /**
 * Get the Certificate sent by the Web Server in the HYPLOGIN
header.
 * If you pass a different header name from the Web server, change
the
 * name in the method.
 */
 private String getCertificate(HttpServletRequest request)
 {
 String cStr = (String)request
 .getHeader(CSSConfigurationDefaults.HTTP_HEADER_HYPLOGI
N);
 return cStr;
 }

 /**
 * The certificate sent by the Web server is a String.
 * Put a "\n" in place of whitespace so that the X509Certificate

```

```

 * java API can parse the certificate.
 */
private String prepareCertificate(String gString)
{
 String str1 = null;
 String str2 = null;

 str1 = gString.replace("-----BEGIN CERTIFICATE-----", "");
 str2 = str1.replace("-----END CERTIFICATE-----", "");
 String certStrWithNL = "-----BEGIN CERTIFICATE-----"
 + str2.replace(" ", "\n") + "-----END CERTIFICATE-----";
 return certStrWithNL;
}

/**
 * Parse the certificate
 * 1. Create X509Certificate using the certificateFactory
 * 2. Get the Principal object from the certificate
 * 3. Set the g_userDN to a certificate attribute value (DN in this
sample)
 * 4. Parse the attribute (DN in this sample) to get a unique username
 */
private void parseCertificate(String sCertificate) throws Exception
{
 X509Certificate cert = null;
 String userID = null;
 try
 {
 X509Certificate clientCert = (X509Certificate)CertificateFactory
 .getInstance("X.509")
 .generateCertificate(
 new
 ByteArrayInputStream(sCertificate
 .getBytes("UTF-8")));

 if (clientCert != null)
 {
 Principal princDN = clientCert.getSubjectDN();
 String dnStr = princDN.getName();
 g_userDN = dnStr;
 int idx = dnStr.indexOf(",");
 userID = dnStr.substring(3, idx);
 g_userName = userID;
 }
 }
 catch (CertificateException ce)
 {
 throw ce;
 }
 catch (UnsupportedEncodingException uee)
 {
 throw uee;
 }
}

```



```
 } //end of getUsernameFromCert
} // end of class
```

## Despliegue de una clase de inicio de sesión personalizada

Para implantar la clase de lógica personalizada, realice los siguientes pasos:

1. Cree y pruebe la clase de inicio de sesión personalizada. Asegúrese de que en su código no hay ninguna referencia a `log4j`. Consulte [Código de ejemplo de clase de inicio de sesión personalizada](#).

Puede usar cualquier nombre para su clase personalizada.

2. Empaquete la clase de inicio personalizada en `CustomAuth.jar`
3. Copie `CustomAuth.jar` en el despliegue:

- **WebLogic:** Copie `CustomAuth.jar` en `MIDDLEWARE_HOME/user_projects/domains/WEBLOGIC_DOMAIN/lib`, normalmente, `Oracle/Middleware/user_projects/domains/EPMSysstem/lib`.

### Nota:

Si está actualizando de la versión 11.1.2.0 o 11.1.2.1 con una implantación de la clase de lógica personalizada, mueva `CustomAuth.jar` de `EPM_ORACLE_HOME/common/jlib/11.1.2.0` a `MIDDLEWARE_HOME/user_projects/domains/WEBLOGIC_DOMAIN/lib`.

- **Despliegues de clientes:** copie `CustomAuth.jar` en todos los despliegues de clientes de Oracle Enterprise Performance Management System, a la siguiente ubicación:

`EPM_ORACLE_HOME/common/jlib/11.1.2.0`, normalmente, `Oracle/Middleware/common/jlib/11.1.2.0`

Oracle recomienda que active la autenticación de certificado de cliente si está usando una clase de lógica personalizada.

# C

## Migración de usuarios y grupos de un directorio de usuario a otro

### Descripción general

Muchos escenarios pueden hacer que las identidades de los usuarios y grupos de los usuarios de Oracle Enterprise Performance Management System aprovisionados se queden obsoletas. No se puede acceder a los componentes de EPM System si la información de aprovisionamiento que tienen disponibles está obsoleta. Entre los escenarios que pueden crear datos de aprovisionamiento obsoletos se incluyen:

- Retirar un directorio de usuario: las organizaciones pueden retirar un directorio de usuario tras mover a los usuarios a otro.
- Actualizar la versión: la actualización de la versión del directorio de usuario puede implicar cambios en el nombre del equipo host o en los entornos del sistema operativo que la necesitan.
- Cambiar de proveedor: las organizaciones pueden dejar de usar un directorio de usuario y pasar a usar uno de otro proveedor. Por ejemplo, una organización puede reemplazar su Oracle Internet Directory por un SunONE Directory Server.

#### Nota:

- En este apéndice, el directorio de usuario que está dejando de usar se conoce como directorio de usuario *de origen*, mientras que el directorio de usuario al que se mueven las cuentas de usuario se conoce como directorio de usuario *de destino*.
- Este procedimiento de migración no soporta la migración de cuentas de usuario de un directorio de usuario de origen a un directorio de usuario de destino, sino solo su asociación en aplicaciones de EPM. Los usuarios se deben crear manualmente en el directorio de usuario de destino. Este proceso se puede aplicar a los usuarios de cualquier directorio de usuario de origen, incluido el directorio nativo.

Si un directorio de usuario de origen configurado con Hyperion Shared Services tenía grupos, excepto grupos de directorios nativos, esos grupos también se deben crear en el directorio de usuario de destino.

### Requisitos

- Los usuarios y grupos de Oracle Enterprise Performance Management System cuyos datos de aprovisionamiento se estén migrando en directorios de usuario deben estar disponibles en el directorio de usuario de destino.

Las relaciones de grupos que existan en el directorio de usuario de origen se deben mantener en el directorio de usuario de destino.

- Los nombres de usuarios de EPM System deben ser idénticos en los directorios de usuarios de origen y de destino.

## Procedimiento de migración

### Exportar datos del directorio nativo

Siga estos pasos en el entorno de origen:

Utilice Oracle Hyperion Enterprise Performance Management System Lifecycle Management para exportar solo los siguientes artefactos de Shared Services desde el directorio nativo:

- Grupos del directorio nativo
- Roles asignados
- Listas de delegación

Lifecycle Management crea archivos de exportación, normalmente en `EPM_ORACLE_INSTANCE/import_export/USER_NAME/EXPORT_DIR/resource/` Native Directory, donde `USER_NAME` es la identidad del usuario, por ejemplo, `admin`, quién ha realizado la operación de exportación y `EXPORT_DIR` es el nombre del directorio de exportación. Normalmente, se crean estos archivos:

- `Groups.csv`
- `Assigned Roles.csv`
- `Delegated Lists.csv`
- `Assigned Roles/PROD_NAME.csv` para cada aplicación desplegada, donde `PROD_NAME` es el nombre de un componente de Oracle Enterprise Performance Management System, por ejemplo, `Servicios compartidos`.

#### Nota:

- Consulte la *Guía de administración del ciclo de vida de Oracle Enterprise Performance Management System* para obtener instrucciones detalladas sobre la exportación de datos con Lifecycle Management.
- Asegúrese de que el archivo `Users.csv` no se ha exportado.

Tras exportar los artefactos, verifique que el informe de estado de migración muestra el estado de la última operación de exportación como `Completed`.

Para exportar los datos del directorio nativo:

1. En el panel de visualización de Consola de Servicios compartidos de Oracle Hyperion, en el grupo de aplicaciones de **Foundation**, seleccione la aplicación **Servicios compartidos**.
2. Para migrar, seleccione solo los artefactos necesarios en la lista siguiente:

- Grupos del directorio nativo
  - Roles asignados
  - Listas de delegación
3. Haga clic en **Exportar**.
  4. Introduzca un nombre para el archivo de exportación. El valor predeterminado es `admin DATE`, por ejemplo, `admin 13-03-18`.
  5. Haga clic en **Exportar**.

### Importar datos del directorio nativo

Siga estos pasos en el entorno de destino:

1. Cree manualmente:
  - a. Los usuarios del directorio de usuario externo, de la misma forma que el directorio de usuario de origen.
  - b. Los grupos del directorio de usuario externo, de la misma forma que el directorio de usuario de origen, excepto los grupos de directorios nativos.
2. Configure el directorio de usuario de destino.  
Agregue el directorio de usuario de destino como directorio de usuario externo en EPM System si ha movido las cuentas de usuario del directorio de usuario de origen a otro directorio de usuario distinto. Por ejemplo, si ha movido las cuentas de usuario de Oracle Internet Directory a SunONE Directory Server, agregue SunONE Directory Server como directorio de usuario externo. Consulte "Capítulo 3, Configuración de directorios de usuario" en la *Guía de administración de seguridad de usuarios de Oracle Enterprise Performance Management System*.

#### Nota:

Asegúrese de que el directorio de usuario de destino contiene cuentas y grupos de usuarios para todos los usuarios de EPM System cuyos datos se estén migrando del directorio de usuario de origen.

Si ha movido los usuarios a un directorio de usuario que ya se ha definido como directorio de usuario externo, verifique que las cuentas de usuarios estén visibles para Servicios compartidos de Oracle Hyperion. Puede realizar esto buscando los usuarios de Consola de Servicios compartidos. Consulte "Búsqueda de usuarios, grupos, roles y listas de delegación" en la *Guía de administración de seguridad de usuarios de Oracle Enterprise Performance Management System*.

Al configurar el directorio de usuario de destino como directorio de usuario externo, verifique que la propiedad Atributo de inicio de sesión apunta al atributo cuyo valor se hubiera usado originalmente como nombre de usuario en el directorio de usuario de origen. Consulte [Requisitos](#).

3. Mueva el directorio de usuario de destino a la parte superior del orden de búsqueda.

 **Nota:**

Si el nombre del directorio de usuario de destino es idéntico al nombre del directorio de origen, debe suprimir el directorio de usuario de origen en la configuración de EPM System.

Servicios compartidos asigna una prioridad de orden de búsqueda inferior a un directorio de usuario recién agregado en comparación con el orden de búsqueda asignado a los directorios existentes. Cambie el orden de búsqueda para que el directorio de usuario de destino tenga una prioridad de orden de búsqueda superior al directorio de usuario de origen. Este orden permite a Servicios compartidos detectar a los usuarios del directorio de usuario de destino antes de buscar el origen. Consulte "Gestión del orden de búsqueda de directorios de usuario" en la *Guía de administración de seguridad de usuarios de Oracle Enterprise Performance Management System*.

4. Reinicie Oracle Hyperion Foundation Services y otros componentes de EPM System para aplicar los cambios que haya realizado.
5. Importar datos del directorio nativo (exportados del entorno de origen): Ejecute Lifecycle Management con la opción `create/update` para importar los datos que haya exportado anteriormente (como se muestra a continuación) del directorio nativo.
  - `Groups.csv`
  - `Assigned Roles.csv`
  - `Delegated Lists.csv`

 **Nota:**

- Consulte la *Guía de administración del ciclo de vida de Oracle Enterprise Performance Management System* para obtener instrucciones detalladas sobre la importación de datos con Lifecycle Management.
- Asegúrese de que el archivo `Users.csv` no se ha importado.

Tras importar los datos, verifique que el informe de estado de migración muestra el estado de la última operación de importación como `Completed`.

Para importar los datos del directorio nativo:

- a. En el panel de visualización de Consola de Servicios compartidos, expanda **Sistema de archivos**.
- b. Seleccione la ubicación del sistema de archivos de los archivos de importación.
- c. Seleccione el tipo de artefactos para los que desea importar la información de aprovisionamiento.
- d. Haga clic en **Importar**.

- e. Haga clic en **Aceptar**.

## Actualizaciones de producto

### ▲ **Atención:**

Oracle recomienda que se realice una copia de seguridad de los datos de usuarios y grupos en el directorio que usa el componente Oracle Enterprise Performance Management System antes de iniciar las actualizaciones específicas de productos. Tras actualizar la información en el repositorio de productos local, puede revertir a los datos de grupos y usuarios anteriores del repositorio de productos local solo de las copias de seguridad.

### **Planning**

Oracle Hyperion Planning almacena información sobre usuarios y grupos aprovisionados en el repositorio de Planning. Si una identidad de usuario del directorio nativo ha cambiado como resultado de la migración de usuarios y grupos en directorios de usuarios, debe sincronizar la información del repositorio de Planning con el directorio nativo mediante la selección de Migrar usuarios/grupos. Este botón está disponible en Planning al asignar el acceso a los formularios de datos, miembros y listas de tareas.

### **Financial Management**

Oracle Hyperion Financial Management registra información acerca de los usuarios y grupos aprovisionados para acceder a objetos de un repositorio de Financial Management local. Si la información de usuarios y grupos de Native Directory ha cambiado como resultado de la migración de usuarios y grupos en directorios de usuarios, debe sincronizar la información del repositorio de Financial Management con la del directorio nativo.