

Oracle® Enterprise Performance Management System

Guia de Configuração de Segurança



Versão 11.2
F28799-23
Dezembro 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>.

Sumário

Acessibilidade da Documentação

Feedback sobre a Documentação

1 Sobre a Segurança do EPM System

Sobre o EPM System	1-1
Conhecimento Presumido	1-1
Componentes da Infraestrutura de Segurança	1-2
Autenticação do Usuário	1-2
Provisionamento (Autorização Baseada em Função)	1-6
Início do Shared Services Console	1-9

2 Habilitação para SSL dos Componentes do EPM System

Pressupostos	2-1
Origens de Informações	2-1
Referências de Local	2-2
Sobre os Produtos EPM System com Habilitação para SSL	2-2
Cenários de SSL Suportados	2-3
Certificados Necessários	2-4
Encerramento de SSL no Descarregador de SSL	2-5
Implantação Completa de SSL do EPM System	2-7
Arquitetura da Implantação	2-7
Pressupostos	2-8
Configuração do EPM System para SSL Completo	2-9
Redefinição das Configurações Comuns do EPM System	2-10
Opcional: Instalação de Certificado da CA Raiz para WebLogic Server	2-11
Instalação de Certificado no WebLogic Server	2-12
Configuração do WebLogic Server	2-13
Habilitação da Conexão do Servidor HFM com um Banco de Dados Oracle Ativado para SSL	2-15

Procedimentos do Oracle HTTP Server	2-21
Configuração de Componentes da Web do EPM System Implantados no WebLogic Server	2-25
Atualizar a Configuração do Domínio	2-26
Reinicialização de Servidores e do EPM System	2-28
Teste da Implantação	2-28
Configuração de Diretórios de Usuários Externos Habilitados para SSL	2-28
Encerramento de SSL no Servidor Web	2-29
SSL para Essbase 11.1.2.4	2-32
Instalação e Implantação de Componentes do Essbase	2-34
Uso de Certificados da CA de Terceiros Confiáveis para Essbase	2-35
Como Estabelecer uma Conexão SSL por Sessão	2-42
SSL para Essbase 21c	2-43
Instalação e Implantação de Componentes do Essbase	2-45
Uso de Certificados da CA de Terceiros Confiáveis para Essbase	2-46
Como Estabelecer uma Conexão SSL por Sessão	2-52

3 Habilitação do SSO com Agentes de Segurança

Métodos de SSO Suportados	3-1
Logon Único no Oracle Access Manager	3-4
OracleAS Single Sign-on	3-5
Teste da Implantação	3-7
Habilitação de OSSO para EPM System	3-7
Proteção de Produtos EPM System para SSO	3-11
SSO baseado em Cabeçalho com Produtos de Gerenciamento de Identidades	3-16
Configuração do EPM System para SSO baseado em Cabeçalho com o Oracle Identity Cloud Services	3-18
Pré-requisitos e URLs de Exemplo	3-18
Ativação da Autenticação Baseada em Cabeçalho para o EPM System	3-19
Adição do Gateway e do Aplicativo do EPM System ao Oracle Identity Cloud Services	3-19
Configuração do Gateway do Aplicativo	3-25
Configuração do Diretório de Usuário para Autorização	3-25
Habilitação do SSO no EPM System	3-25
Atualização de Configurações do EPM Workspace	3-25
SiteMinder SSO	3-26
Logon único Kerberos	3-29
Configuração do EPM System para SSO	3-43
Opções de Logon Único para Smart View	3-44

4 Configuração de Diretórios de Usuário

Diretórios de Usuário e Segurança do EPM System	4-1
Operações Relacionadas à Configuração do Diretório de Usuário	4-2
Oracle Identity Manager e EPM System	4-2
Informações do Active Directory	4-3
Configuração do OID, Active Directory e Outros Diretórios de Usuário baseados em LDAP	4-4
Configuração de Bancos de Dados Relacionais como Diretórios de Usuário	4-19
Como Testar Conexões do Diretório de Usuário	4-22
Edição de Configurações do Diretório de Usuário	4-22
Exclusão de Configurações do Diretório de Usuário	4-23
Gerenciamento da Ordem de Pesquisa do Diretório de Usuário	4-24
Configuração de Opções de Segurança	4-26
Nova Geração de Chaves de Criptografia	4-29
Uso de Caracteres Especiais	4-31

5 Uso do Módulo de Autenticação Personalizada

Visão Geral	5-1
Exemplos de Caso de Uso e Limitações	5-3
Pré-requisitos	5-3
Considerações de Codificação e Design	5-3
Implantação do Módulo de Autenticação Personalizado	5-9

6 Diretrizes de Segurança do EPM System

Implementação de SSL	6-1
Alteração da Senha de Administração	6-1
Nova Geração de Chaves de Criptografia	6-1
Alteração das Senhas de Banco de Dados	6-2
Proteção de Cookies	6-3
Redução do Tempo Limite do Token SSO	6-4
Revisão de Relatórios de Segurança	6-4
Personalização do Sistema de Autenticação para Autenticação Forte	6-4
Desabilitação dos Utilitários de Depuração do EPM Workspace	6-4
Alteração de Páginas de Erro do Servidor Web Padrão	6-5
Suporte para Software de Terceiros	6-5

A Código de Exemplo da Autenticação Personalizada

Código de Exemplo 1	A-1
Código de Exemplo 2	A-2

B Implementação de uma Classe de Logon Personalizada

Código de Exemplo de Classe de Logon Personalizada

B-1

Implantação de uma Classe de Logon Personalizada

B-4

C Migração de Usuários e Grupos entre Diretórios de Usuários

Visão Geral

C-1

Pré-requisitos

C-1

Procedimento de Migração

C-2

Atualizações Específicas de Produto

C-5

Acessibilidade da Documentação

Para obter mais informações sobre o compromisso da Oracle com a acessibilidade, visite o site do Programa de Acessibilidade da Oracle em <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Acesso ao Suporte Técnico da Oracle

Os clientes Oracle que adquiriram serviços de suporte têm acesso ao suporte eletrônico por meio do My Oracle Support. Para obter mais informações, visite <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> ou visite <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> caso tenha deficiência auditiva.

Feedback sobre a Documentação

Para fornecer feedback sobre esta documentação, clique no botão de feedback na parte inferior da página em qualquer tópico do Oracle Help Center. Você também pode enviar e-mail para epmdoc_ww@oracle.com.

1

Sobre a Segurança do EPM System

Consulte Também:

- [Sobre o EPM System](#)
- [Conhecimento Presumido](#)
- [Componentes da Infraestrutura de Segurança](#)
- [Autenticação do Usuário](#)
- [Provisionamento \(Autorização Baseada em Função\)](#)
- [Iniciando o Shared Services Console](#)

Sobre o EPM System

Os produtos Oracle Enterprise Performance Management System compõem o abrangente sistema enterprise-wide, que integra pacotes modulares de aplicativos de planejamento e gerenciamento financeiro com os mais completos recursos de business intelligence para geração de relatórios e análise. Os componentes principais dos produtos EPM System.

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

Para obter informações sobre os produtos e componentes em cada uma dessas famílias de produtos, consulte *A Instalação do Oracle Enterprise Performance Management System Começa Aqui*.

Conhecimento Presumido

Este guia destina-se aos administradores de sistema que configuram, protegem e gerenciam componentes do Oracle Enterprise Performance Management System. Ele considera os seguintes conhecimentos:

- Uma profunda compreensão da infraestrutura de segurança da sua organização, incluindo:
 - Servidores de diretório; por exemplo, Oracle Internet Directory, Sun Java System Directory Server e Microsoft Active Directory
 - Uso do Secure Socket Layer (SSL) para proteger canais de comunicação
 - Sistemas de Gerenciamento de Acesso, por exemplo, Oracle Access Manager, e SiteMinder
 - Infraestrutura de logon único (SSO); por exemplo, Kerberos
- Conhecimento dos conceitos de segurança do EPM System que são relevantes para sua organização

Componentes da Infraestrutura de Segurança

O Oracle Enterprise Performance Management System integra vários componentes de segurança para garantir segurança robusta dos aplicativos. Quando integrado a uma infraestrutura segura, o EPM System entrega um conjunto altamente seguro de aplicativos que garante a segurança de dados e acesso. Os componentes da infraestrutura que você pode usar para proteger o EPM System incluem:

- Um sistema de gerenciamento de acesso opcional; por exemplo, Oracle Access Manager para fornecer acesso SSO a componentes do EPM System
- Uso de uma infraestrutura SSO integrada, por exemplo, Kerberos.
É possível usar a autenticação Kerberos com o sistema de gerenciamento de acesso (SiteMinder) a fim de garantir que os usuários do Windows possam fazer logon de maneira transparente no SiteMinder e em componentes do EPM System.
- Uso do Secure Socket Layer (SSL) para proteger canais de comunicação entre componentes e clientes do EPM System

Autenticação do Usuário

A autenticação de usuário habilita a funcionalidade de logon único (SSO) nos componentes do Oracle Enterprise Performance Management System validando as informações de logon de cada usuário para determinar os usuários autenticados. A autenticação de usuário, com autorização específica do componente, concede ao usuário acesso aos componentes do EPM System. O processo de conceder autorização é chamado de provisionamento.

Componentes de Autenticação

As seções a seguir descrevem os componentes que oferecem suporte ao SSO:

- [Native Directory](#)
- [Diretórios de Usuários Externos](#)

Native Directory

Native Directory refere-se ao banco de dados relacional que o Oracle Hyperion Shared Services usa para dar suporte ao provisionamento e para armazenar dados pré-implantados, como contas de usuário padrão.

Funções do Native Directory:

- Manter e gerenciar as contas de usuário padrão do EPM System
- Armazenar todas as informações de provisionamento do EPM System (relacionamentos entre usuários, grupos e funções)

O Native Directory é acessado e gerenciado usando o Oracle Hyperion Shared Services Console. Consulte "Gerenciamento do Native Directory" no *Guia de Administração da Segurança de Usuário do Sistema Oracle Enterprise Performance Management*.

Diretórios de Usuários Externos

Os diretórios de usuários referem-se aos sistemas corporativos de gerenciamento de identidades e usuários que são compatíveis com os componentes do EPM System.

Os componentes do EPM System são suportados em vários diretórios de usuário, inclusive nos que têm base em LDAP, como o Oracle Internet Directory, Sun Java System Directory Server (denominado anteriormente Servidor de Diretórios SunONE) e Microsoft Active Directory. Os bancos de dados relacionais também são suportados como diretórios de usuário. Os diretórios de usuários, com exceção do Native Directory, são chamados de diretórios de usuários externos em todo este documento.

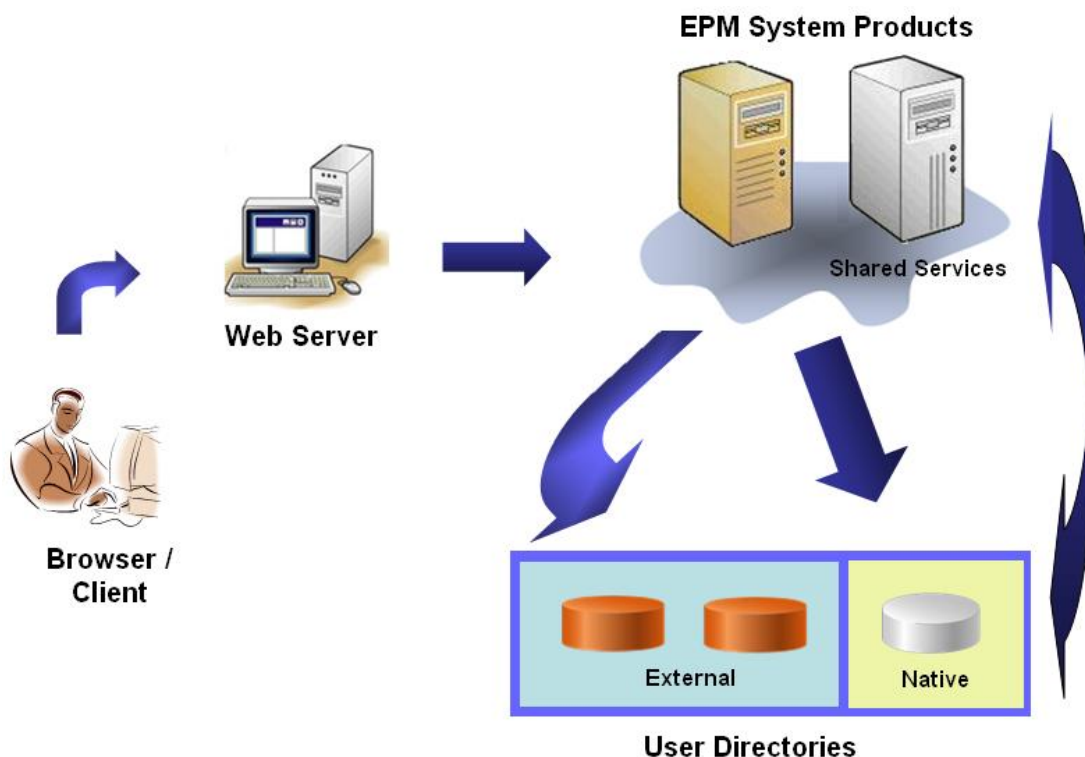
Para obter uma lista de diretórios de usuários suportados, consulte a *Matriz de Certificação do Oracle Enterprise Performance Management System* publicada na página [Configurações do Sistema Suportado do Oracle Fusion Middleware](#) do Oracle Technology Network (OTN).

No Shared Services Console, você pode configurar muitos diretórios de usuários externos como a origem para usuários e grupos do EPM System. Cada usuário do EPM System deve ter uma conta exclusiva em um diretório de usuários configurado. De modo geral, os usuários do EPM System são atribuídos a grupos para facilitar o provisionamento.

Logon Único Padrão do EPM System

O EPM System dá suporte ao SSO nos aplicativos Web do EPM System permitindo que usuários autenticados de um aplicativo naveguem ininterruptamente para outros aplicativos sem precisar inserir as credenciais novamente. O SSO é implementado pela integração de um ambiente de segurança comum que trata da autenticação do usuário e do provisionamento (autorização baseada em função) entre os componentes do EPM System.

O processo de SSO padrão é ilustrado na imagem a seguir.



1. Usando um navegador, os usuários acessam uma tela de logon do componente do EPM System e inserem um nome de usuário e uma senha.

O componente do EPM System consulta os diretórios de usuários configurados (incluindo o Native Directory) para verificar credenciais do usuário. Depois de encontrar a conta de usuário correspondente em um diretório de usuários, a pesquisa é encerrada e as informações do usuário são retornadas ao componente do EPM System.

O acesso será negado se nenhuma conta de usuário for encontrada em qualquer diretório de usuários configurado.

2. Usando as informações recuperadas do usuário, o componente do EPM System consulta o Native Directory para obter detalhes de provisionamento para o usuário.
3. O componente do EPM System verifica a Lista de Controle de Acesso (ACL) no componente para determinar os artefatos do aplicativo que o usuário pode acessar.

Mediante recebimento das informações de provisionamento do Native Directory, o componente do EPM System estará disponível para o usuário. Nesse ponto, o SSO é habilitado para todos os componentes do EPM System para os quais o usuário foi provisionado.

Logon Único em Sistemas de Gerenciamento de Acesso

Para proteger ainda mais os componentes do EPM System, você pode implementar um sistema de gerenciamento de acesso compatível, como Oracle Access Manager ou SiteMinder, que pode fornecer credenciais de usuário autenticado aos componentes do EPM System e controlar o acesso com base nos privilégios de acesso predefinidos.

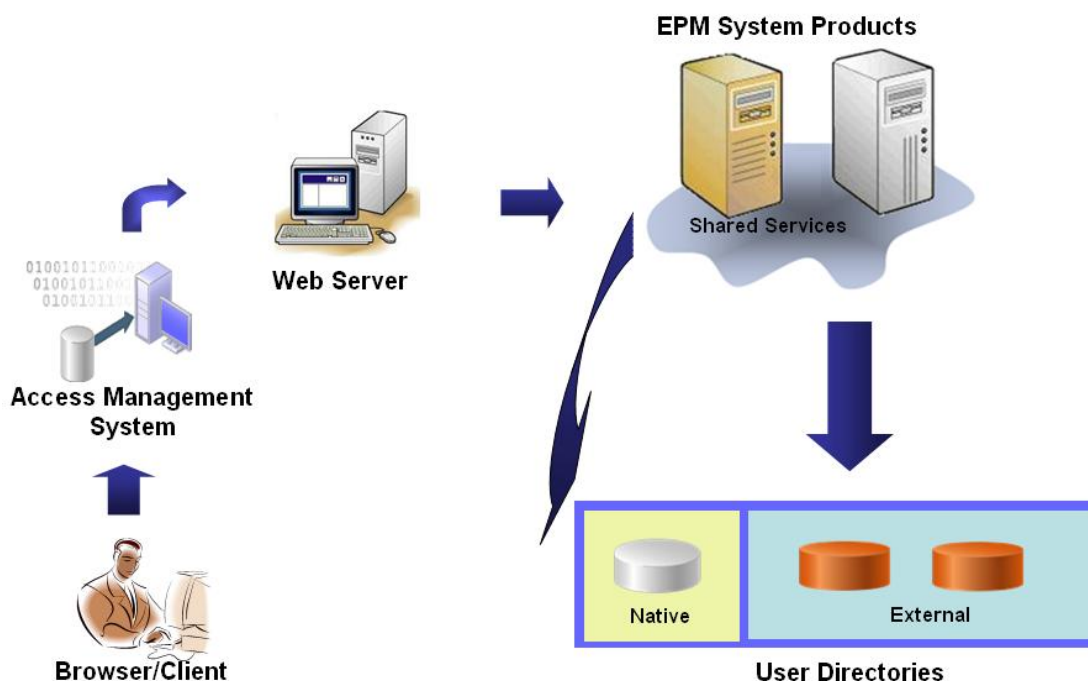
O SSO de agentes de segurança está disponível apenas para aplicativos Web do EPM System. Neste cenário, os componentes EPM System usam as informações sobre o usuário fornecidas pelo agente de segurança para determinar as permissões de acesso dos usuários. Para melhorar a segurança, a Oracle recomenda que o acesso direto aos servidores seja bloqueado por firewalls para que todas as solicitações sejam roteadas por meio de um portal SSO.

O SSO de sistemas de gerenciamento de acesso é suportado pela aceitação das credenciais do usuário autenticado por um mecanismo SSO aceitável. Consulte [Métodos de SSO Suportados](#). O sistema de gerenciamento de acesso autentica usuários e passa o nome de logon ao EPM System. O EPM System verifica o nome de logon nos diretórios de usuários configurados.

Consulte estes tópicos.

- [Logon Único no Oracle Access Manager](#)
- [OracleAS Single Sign-on](#)
- [SiteMinder SSO](#)
- [Logon Único Kerberos](#)

O conceito ilustrado:



1. Usando um navegador, os usuários solicitam acesso a recurso protegido por um sistema de gerenciamento de acesso, por exemplo, Oracle Access Manager, ou pelo SiteMinder.

 **Nota:**

Os componentes do EPM System são definidos como recursos protegidos pelo sistema de gerenciamento de acesso.

O sistema de gerenciamento de acesso intercepta a solicitação e apresenta uma tela de login. Os usuários inserem um nome de usuário e uma senha, que são validados em diretórios de usuários configurados no sistema de gerenciamento de acesso para verificar a autenticidade do usuário. Os componentes do EPM System também são configurados para funcionar com esses diretórios de usuários.

As informações sobre o usuário autenticado são passadas ao componente do EPM System, que aceita as informações como válidas.

O sistema de gerenciamento de acesso passa o nome de logon do usuário (valor de `Login Attribute`) ao componente do EPM System usando um mecanismo SSO aceitável. Consulte [Métodos de SSO Suportados](#).

2. Para verificar credenciais de usuário, o componente do EPM System tenta localizar o usuário em um diretório de usuários. Se uma conta de usuário correspondente for encontrada, as informações do usuário serão retornadas ao componente do EPM System. A segurança do EPM System define o token SSO que habilita o SSO nos componentes do EPM System.
3. Usando as informações recuperadas do usuário, o componente do EPM System consulta o Native Directory para obter detalhes de provisionamento para o usuário.

Após o recebimento das informações de provisionamento do usuário, o componente do EPM System estará disponível para o usuário. O SSO é habilitado em todos os componentes do EPM System nos quais o usuário é provisionado.

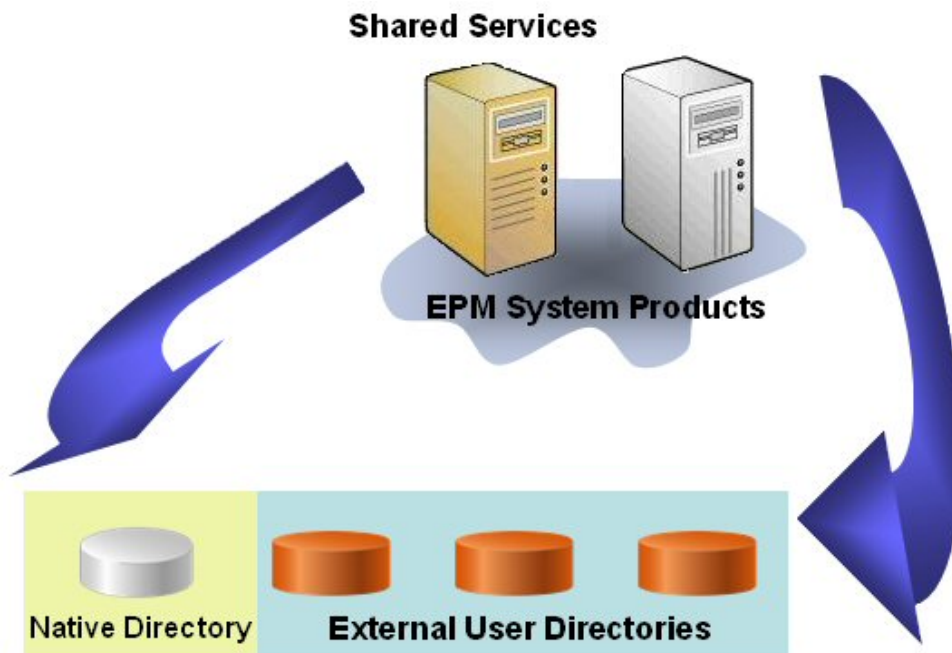
Provisionamento (Autorização Baseada em Função)

A segurança do Oracle Enterprise Performance Management System determina o acesso do usuário aos aplicativos usando o conceito de funções. As funções são permissões que determinam o acesso do usuário a funções de aplicativo. Alguns componentes do EPM System impõem as ACLs no nível do objeto para refinar ainda mais o acesso do usuário aos seus artefatos, como relatórios e membros.

Cada componente do EPM System possui várias funções predefinidas adequadas a várias necessidades de negócios. Cada aplicativo que pertence a um componente do EPM System herda essas funções. As funções predefinidas de aplicativos registrados no Oracle Hyperion Shared Services estão disponíveis no Oracle Hyperion Shared Services Console. Também é possível criar funções adicionais que agreguem as funções padrão para atender a requisitos específicos. Essas funções são usadas no provisionamento. O processo de conceder funções específicas pertencentes a aplicativos do EPM System e os seus recursos a usuários e grupos é denominado *provisionamento*.

O Native Directory e os diretórios de usuários configurados são origens de informações de usuários e grupos no processo de provisionamento. Você pode navegar e provisionar usuários e grupos de todos os diretórios de usuário configurados a partir do Shared Services Console. Também possível usar as funções agregadas específicas do aplicativo criadas no Native Directory no processo de provisionamento.

Uma visão geral ilustrada do processo de autorização:



1. Depois que um usuário é autenticado, o componente do EPM System consulta os diretórios de usuários para determinar os grupos do usuário.
2. O componente do EPM System usa as informações de usuário e do grupo para recuperar os dados de provisionamento do usuário no Shared Services. O componente usa esses dados para determinar quais recursos um usuário pode acessar.

As tarefas de provisionamento específicas do produto, como definir o controle de acesso específico do produto, são concluídas para cada produto. Estes dados são combinados com os dados de provisionamento para determinar o acesso do produto para os usuários.

O provisionamento com base na função dos produtos EPM System usa esses conceitos.

Funções

Uma função é uma construção (semelhante a uma lista de controle de acesso) que define as permissões de acesso concedidas a usuários e grupos para executar funções nos recursos do EPM System. Uma função é uma combinação de recursos ou tipos de recurso (o que os usuários podem acessar; por exemplo, um relatório) e ações que os usuários podem executar no recurso (por exemplo, exibir e editar).

O acesso aos recursos de aplicativo do EPM System é restrito. Os usuários podem acessá-los somente depois que uma função que fornece acesso completo é atribuída ao usuário ou grupo ao qual o usuário pertence. As restrições de acesso com base nas funções permitem que os administradores controlem e gerenciem acesso ao aplicativo.

Funções Globais

Funções globais, que são funções do Shared Services que abrangem diversos produtos, permitem que usuários realizem certas tarefas nos produtos EPM System. Por exemplo, o Administrador do Shared Services pode provisionar usuários para todos os aplicativos do EPM System.

Funções Predefinidas

As funções predefinidas são funções internas nos produtos EPM System. Não é possível excluí-las. Cada instância do aplicativo que pertence a um produto EPM System herda todas as funções predefinidas do produto. Essas funções, para cada aplicativo, são registradas no Shared Services quando você cria o aplicativo.

Funções Agregadas

As funções agregadas, também conhecidas como funções personalizadas, agregam várias funções predefinidas pertencentes a um aplicativo. Uma função agregada pode conter outras funções agregadas. Por exemplo, um Gerente de Provisionamento ou Administrador do Shared Services pode criar uma função agregada que combine as funções Planejador e Exibir Usuário de um aplicativo do Oracle Hyperion Planning. A agregação de funções pode simplificar a administração de aplicativos que tenham muitas funções granulares. As funções globais do Shared Services podem ser incluídas em funções agregadas. Não é possível criar uma função agregada que abarque aplicativos ou produtos.

Usuários

Os diretórios de usuários armazenam informações sobre os usuários que podem acessar os produtos do EPM System. Os processos de autenticação e de autorização utilizam as informações do usuário. Você pode criar e gerenciar os usuários do Native Directory somente no Shared Services Console.

Os usuários de todos os diretórios de usuário configurados estão visíveis no Shared Services Console. Esses usuários podem ser provisionados individualmente para conceder direitos de acesso nos aplicativos do EPM System registrados no Shared Services. A Oracle não recomenda o provisionamento de usuários individuais.

Administrador Padrão do EPM System

Uma conta de administrador, com o nome padrão de `admin`, é criada no Native Directory durante o processo de implantação. Essa é a conta mais poderosa do EPM System e deverá ser usada somente para configurar um Administrador do Sistema, que é o especialista da Tecnologia da Informação com a tarefa de gerenciar a segurança e o ambiente do EPM System.

O nome de usuário e a senha do Administrador do EPM System são definidos durante a implantação do Oracle Hyperion Foundation Services. Como essa conta não pode ser sujeitada a políticas de senha de conta corporativa, a Oracle recomenda que ela seja desativada após a criação de uma conta do Administrador de Sistema.

De modo geral, a conta do Administrador padrão do EPM System é usada para executar estas tarefas:

- Configure o diretório corporativo como um diretório de usuários externo. Consulte [Configuração de Diretórios de Usuário](#).
- Crie uma conta de Administrador de Sistema provisionando um especialista corporativo em Tecnologia da Informação com a função de Administrador do Shared Services. Consulte "Provisionamento de Usuários e Grupos" no *Guia de Administração da Segurança de Usuário do Sistema Oracle Enterprise Performance Management*.

Administrador do Sistema

O Administrador de Sistema normalmente é um especialista corporativo em Tecnologia da Informação que tem direitos de acesso de leitura, gravação e execução para todos os servidores envolvidos em uma implantação do EPM System.

De modo geral, o Administrador de Sistema executa estas tarefas:

- Desabilitar a conta do Administrador do EPM System padrão.
- Criar pelo menos um Administrador Funcional.
- Definir a configuração de segurança para o EPM System usando o Shared Services Console.
- Se desejar, configurar diretórios de usuários como um diretório de usuários externo.
- Monitorar o EPM System executando periodicamente a ferramenta Análise de Log.

As tarefas que os Administradores Funcionais executam são descritas neste guia.

Procedimentos para criar um Administrador Funcional:

- Configure o diretório corporativo como um diretório de usuários externo. Consulte [Configuração de Diretórios de Usuário](#).
- Provisione um usuário ou grupo com as funções necessárias para criar um Administrador Funcional. Consulte "Provisionamento de Usuários e Grupos" no *Guia de Administração da Segurança de Usuário do Sistema Oracle Enterprise Performance Management*.

O Administrador Funcional deve ser provisionado com estas funções:

- Função de Administrador do LCM do Shared Services
- Função de Administrador e Gerente de Provisionamento de cada componente do EPM System implantado

Administradores Funcionais

O Administrador Funcional é um usuário corporativo que é um especialista do EPM System. Normalmente, esse usuário é definido no diretório corporativo que é configurado no Shared Services como um diretório de usuários externos.

O Administrador Funcional executa tarefas de administração do EPM System, como criar outros Administradores Funcionais, configurar a administração delegada, criar e provisionar aplicativos e artefatos, e configurar a auditoria do EPM System. As tarefas que os Administradores Funcionais executam são descritas no *Guia de Administração da Segurança de Usuário do Sistema Oracle Enterprise Performance Management*.

Grupos

Grupos são recipientes de usuários ou outros grupos. Você pode criar e gerenciar grupos do Native Directory no Shared Services Console. Grupos de todos os diretórios configurados de usuários são exibidos no Shared Services Console. Você pode provisionar estes grupos para conceder permissões aos produtos EPM System registrados com o Shared Services.

Início do Shared Services Console

Você usa uma opção de menu em Oracle Hyperion Enterprise Performance Management Workspace para Acessar o Oracle Hyperion Shared Services Console.

Para iniciar o Shared Services Console:

1. Vá para:

`http://web_server_name:port_number/workspace`

No URL, `web_server_name` indica o nome do computador em que o servidor Web usado pelo Oracle Hyperion Foundation Services está sendo executado, e `port_number` indica a porta do servidor Web; por exemplo, `http://myWebserver:19000/workspace`.

Nota:

Se você estiver acessando o EPM Workspace em ambientes seguros, use `https` como protocolo (não `http`) e o número de porta do Servidor de Web seguro. Por exemplo, use um URL como este: `https://meuservidor:19043/workspace`.

2. Clique em **Iniciar Aplicativo**.

Nota:

Os bloqueadores de pop-up podem impedir a abertura do EPM Workspace.

3. Na tela **Log-on**, insira o seu nome e senha de usuário.

Inicialmente, o único usuário que pode acessar o Shared Services Console é o administrador do Oracle Enterprise Performance Management System cujo nome e senha de usuário foram especificados durante o processo de implantação.

4. Clique em **Logon**.
5. Selecione **Navegar, Administrar e Shared Services Console**.

2

Habilitação para SSL dos Componentes do EPM System

Consulte Também:

- [Pressupostos](#)
- [Origens de Informações](#)
- [Referências de Local](#)
- [Sobre Produtos EPM System com Habilitação para SSL](#)
- [Cenários de SSL Suportados](#)
- [Certificados Necessários](#)
- [Encerramento de SSL no Descarregador de SSL](#)
- [Implantação Completa de SSL do EPM System](#)
- [Encerramento de SSL no Servidor Web](#)
- [SSL para Essbase 11.1.2.4](#)
- [SSL para Essbase 21c](#)

Pressupostos

- Você determinou a topologia de implantação e identificou os links de comunicação a serem assegurados usando SSL.
- Você obteve os certificados necessários de uma Autoridade Certificadora (CA), uma CA conhecida ou a sua própria, ou criou certificados autoassinados. Consulte [Certificados Necessários](#).
- Você está familiarizado com os conceitos e procedimentos de SSL, como a importação de certificados.

Consulte [Origens de Informações](#) para obter uma lista de documentos de referência.

Origens de Informações

A habilitação para SSL do Oracle Enterprise Performance Management System exige que você prepare componentes, como o servidor de aplicativos, servidor Web, bancos de dados e diretórios de usuários para se comunicar usando o SSL. Este documento pressupõe que você esteja familiarizado com as tarefas envolvidas na habilitação para SSL desses componentes.

- **Oracle WebLogic Server:** Consulte "[Configuração de SSL](#)" no Guia de *Proteção do WebLogic Server*.
- **Oracle HTTP Server:** Consulte os seguintes tópicos no *Guia do Administrador do Oracle HTTP Server*:

- [Gerenciamento da Segurança](#)
- [Habilitação de SSL para Oracle HTTP Server](#)
- **Diretórios de Usuários:** Consulte a documentação do fornecedor do diretório de usuários. Links úteis:
 - **Oracle Internet Directory:** Consulte [Guia do Administrador do Oracle Internet Directory](#)
 - **Sun Java System Directory Server:** Consulte "[Segurança do Servidor de Diretórios](#)" no *Guia de Administração do Sun Java System Directory Server*
 - **Active Directory:** Consulte a documentação da Microsoft.
- **Bancos de Dados:** Consulte a documentação do fornecedor do banco de dados.

Referências de Local

Este documento refere-se aos seguintes locais de instalação e implantação:

- *MIDDLEWARE_HOME* refere-se ao local dos componentes de middleware, como o Oracle WebLogic Server e, como opção, um ou mais *EPM_ORACLE_HOME*. O *MIDDLEWARE_HOME* é definido durante a instalação do produto Oracle Enterprise Performance Management System. O diretório *MIDDLEWARE_HOME* padrão é Oracle/Middleware.
- *EPM_ORACLE_HOME* refere-se ao diretório de instalação que contém os arquivos necessários para dar suporte aos produtos EPM System. *EPM_ORACLE_HOME* reside em *MIDDLEWARE_HOME*. O *EPM_ORACLE_HOME* padrão é *MIDDLEWARE_HOME/EPMSys11R1*; por exemplo, Oracle/Middleware/EPMSys11R1.

Os produtos EPM System são instalados no diretório *EPM_ORACLE_HOME/products*; por exemplo, Oracle/Middleware/EPMSys11R1/products.

Além disso, durante a configuração do produto EPM System, alguns produtos implantam componentes em *MIDDLEWARE_HOME/user_projects/epmsys11R1*; por exemplo, Oracle/Middleware/user_projects/epmsys11R1.

- *EPM_ORACLE_INSTANCE* denota um local que é definido durante o processo de configuração onde alguns produtos implantam componentes. O local padrão de *EPM_ORACLE_INSTANCE* é *MIDDLEWARE_HOME/user_projects/epmsys11R1*; por exemplo, Oracle/Middleware/user_projects/epmsys11R1.

Sobre os Produtos EPM System com Habilitação para SSL

O processo de implantação do Oracle Enterprise Performance Management System implanta automaticamente os produtos do EPM System para trabalhar nos modos SSL e não SSL.

 **Nota:**

- O EPM System aceita SSL somente por HTTP e JDBC. Ele não aceita outros padrões, por exemplo, Thrift e ODBC, para comunicação segura.
- Para se proteger contra a vulnerabilidade Poodle (Padding Oracle On Downgraded Legacy Encryption), que é um ataque no protocolo SSL v3, você deve desabilitar o suporte ao SSL v3 em seus servidores e nos navegadores que são usados para acessar os componentes do EPM System. Veja a documentação do servidor e navegador para obter informações de como desativar o suporte ao SSLv3.
- Os servidores do EPM System poderão começar a falhar se você desativar o modo não SSL após a configuração do SSL.
Ative a replicação segura para todos os servidores do EPM System no domínio para que eles sejam iniciados quando o modo não SSL for desativado.

Ao especificar configurações comuns para o EPM System, você especifica se vai habilitar para SSL toda comunicação de servidor para servidor em sua implantação.

A seleção das configurações de SSL durante o processo de implantação não configura automaticamente seu ambiente do SSL. Isso apenas define um sinalizador no Oracle Hyperion Shared Services Registry para indicar que todos os componentes do EPM System que usam o Shared Services Registry devem usar o protocolo seguro (HTTPS) para comunicação entre servidores. Você deve concluir procedimentos adicionais para habilitar o SSL no seu ambiente. Esses procedimentos são discutidos neste documento.

 **Nota:**

A reimplantação de seus aplicativos apaga as configurações personalizadas do servidor de aplicativos e servidor Web que você especifica para habilitar o SSL.

 **Nota:**

No Enterprise Performance Management System Versão 11.2.x, SSL (Secure Sockets Layer) para MS SQL Server no RCU (Repository Creation Utility) é suportado.

Cenários de SSL Suportados

Os seguintes cenários de SSL são suportados:

- Encerramento do SSL no descarregador de SSL. Consulte [Encerramento de SSL no Descarregador de SSL](#).
- Implantação de SSL completa. Consulte [Implantação Completa de SSL do EPM System](#).

Certificados Necessários

A comunicação SSL usa certificados para estabelecer confiança entre componentes. A Oracle recomenda usar certificados de CAs de terceiros reconhecidas para habilitar para SSL o Oracle Enterprise Performance Management System em um ambiente de produção.

 **Nota:**

O EPM System dá suporte ao uso de certificados curinga, que podem proteger vários subdomínios com um certificado SSL. Usar um certificado curinga pode reduzir o tempo e o custo de gerenciamento.

Se estiver usando certificados curinga para criptografar a comunicação, você deve desabilitar a verificação de nome do host no Oracle WebLogic Server.

São necessários os seguintes certificados para cada servidor que hospeda componentes do EPM System:

- Um certificado da CA raiz

 **Nota:**

Você não precisa instalar um certificado da CA raiz no keystore Java se estiver usando certificados de uma CA de terceiros reconhecida cujo certificado raiz já está instalado no keystore Java.

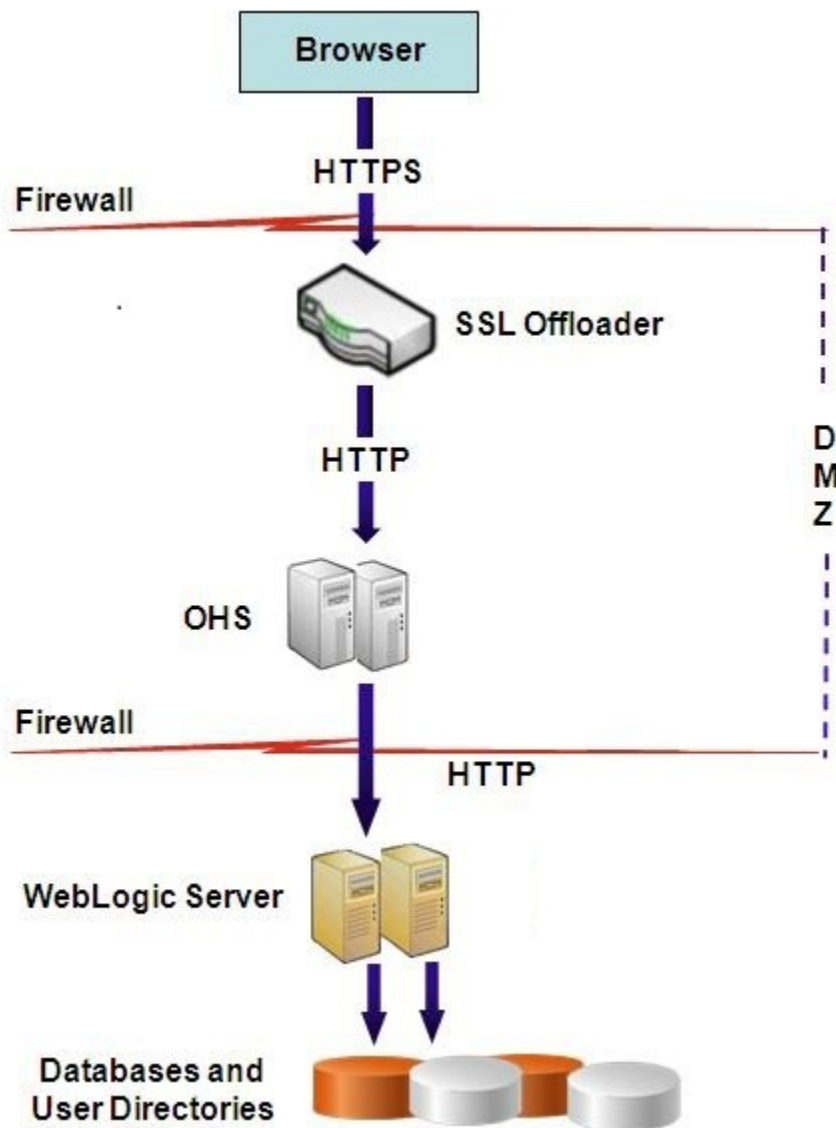
O Firefox e o Internet Explorer são pré-carregados com certificados de CAs de terceiros reconhecidas. Se estiver atuando como sua própria CA, você deverá importar seu certificado raiz de CA no keystore usado pelos clientes acessado de tais navegadores. Se estiver atuando como sua própria CA, os clientes da Web não poderão estabelecer um handshake SSL com o servidor se seu certificado raiz de CA não estiver disponível para o navegador do qual o cliente é acessado.

- Certificados assinados para cada Oracle HTTP Server em sua implantação
- Um certificado assinado para a máquina host do WebLogic Server. Servidores gerenciados nessa máquina também podem usar esse certificado
- Dois certificados para o descarregador/balancedor de carga SSL. Um desses certificados é para comunicação externa e o outro é para comunicação interna

Encerramento de SSL no Descarregador de SSL

Arquitetura da Implantação

Nesse cenário, o SSL é usado para proteger o link de comunicação entre os clientes do Oracle Enterprise Performance Management System (por exemplo, um navegador) e um Descarregador de SSL. O conceito ilustrado:



Pressupostos

Descarregador de SSL e Balanceador de Carga

Um descarregador de SSL totalmente configurado com um balanceador de carga deve estar presente no ambiente de implantação.

O balanceador de carga deve ser configurado para encaminhar todas as solicitações pelos hosts virtuais ao Oracle HTTP Servers.

Quando o SSL estiver sendo encerrado no Oracle HTTP Server (OHS) ou no balanceador de carga, você deverá:

- Definir cada Aplicativo Web Lógico para o host virtual não ssl do balanceador de carga ou do Oracle HTTP Server (por exemplo, `empinternal.myCompany.com:80`, onde 80 é a porta não SSL). Abra a tela Configuração e conclua estas etapas:
 1. Expanda a tarefa de configuração do **Hyperion Foundation**.
 2. Selecione **Configurar Endereço Lógico de Aplicativos Web**.
 3. Especifique o *Nome do host*, o número da porta não SSL e o número da porta SSL.
- Definir o URL externo para o host virtual habilitado para SSL do balanceador de carga ou do Oracle HTTP Server (por exemplo, `empexternal.myCompany.com:443`, onde 443 é a porta SSL). Abra a tela Configuração e conclua estas etapas:
 1. Expanda a tarefa de configuração do **Hyperion Foundation**.
 2. Selecione **Definir Configurações Comuns**.
 3. Selecione **Habilitar descarregamento de SSL** em Detalhes do URL Externo.
 4. Especifique o *Host do URL Externo* e a *Porta do URL Externo*.

 **Nota:**

A reimplantação de aplicativos web ou a reconfiguração do servidor web usando **configtool** substituirá as configurações do Aplicativo Web Lógico e URLs externos.

Hosts Virtuais

O SSL encerrado na configuração do descarregador de SSL usa dois aliases de servidor; por exemplo, `epm.myCompany.com` e `empinternal.myCompany.com`, no descarregador/balanceador de carga de SSL, um para comunicação externa entre o descarregador e os navegadores e o outro para comunicação interna entre os servidores do EPM System. Certifique-se de que os aliases de servidor apontem para o endereço IP da máquina e que eles possam ser resolvidos por meio de DNS.

Um certificado assinado para dar suporte à comunicação externa entre o descarregador e os navegadores (por meio de `epm.myCompany.com`) deve ser instalado no descarregador/balanceador de carga.

Configuração do EPM System

A implantação padrão dos componentes do EPM System dá suporte ao encerramento de SSL no descarregador de SSL. Não é necessária nenhuma ação adicional.

Durante a configuração do EPM System, certifique-se de que o endereço lógico para aplicativos Web apontem para o alias (por exemplo, `empinternal.myCompany.com`) que foi criado para comunicação interna. Consulte as seguintes origens de informação para instalar e configurar o EPM System:

- *Guia de Configuração e Instalação do Sistema Oracle Enterprise Performance Management*
- *A Instalação do Oracle Enterprise Performance Management System Começa Aqui*
- *Guia de Solução de Problemas de Instalação e Configuração do Oracle Enterprise Performance Management System*

Teste da Implantação

Após a conclusão do processo de implantação, verifique se tudo está funcionando conectando-se ao uRL seguro do Oracle Hyperion Enterprise Performance Management Workspace:

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

Por exemplo, `https://epm.myCompany.com:443/workspace/index.jsp`, onde 443 é a porta SSL.

Implantação Completa de SSL do EPM System

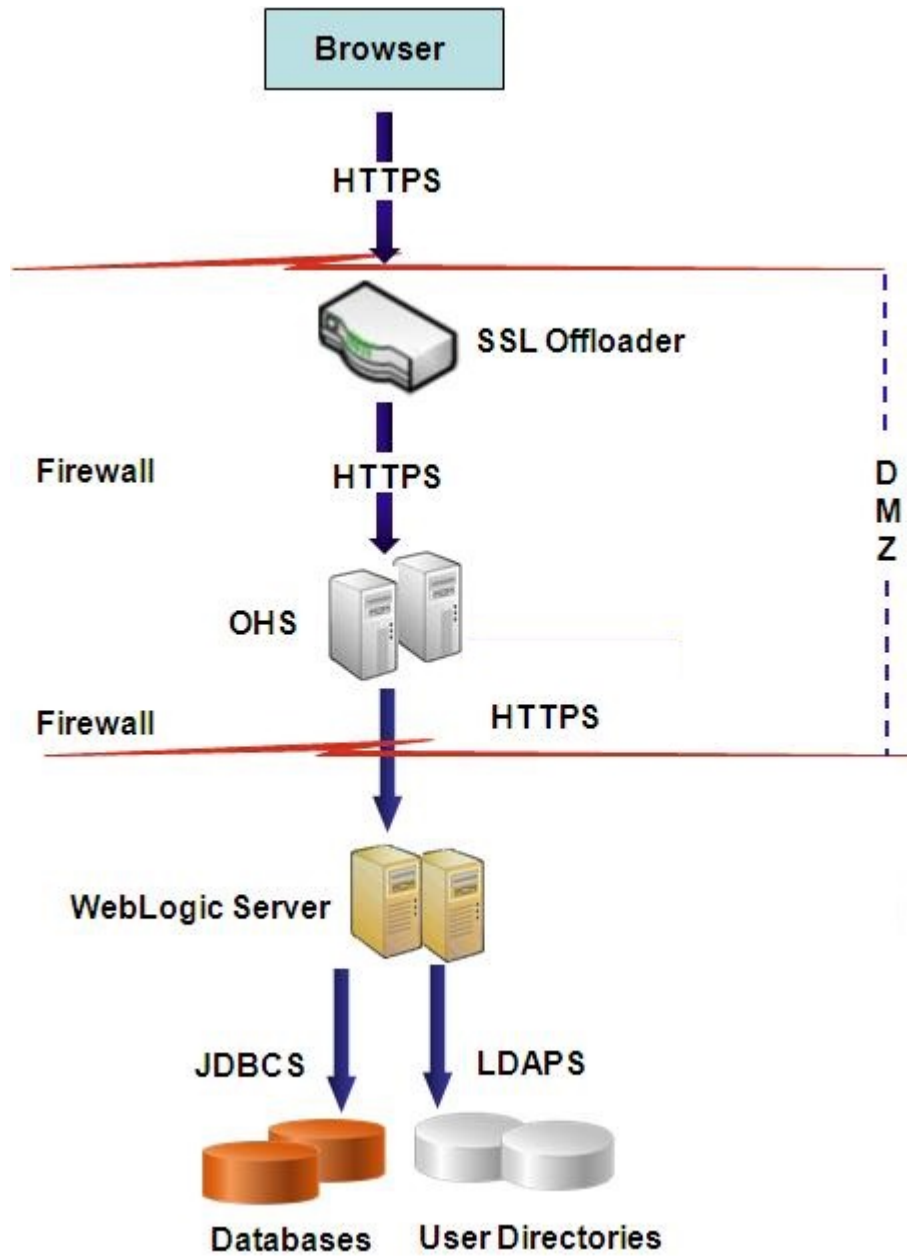
Consulte Também:

- [Arquitetura da Implantação](#)
- [Pressupostos](#)
- [Configuração do EPM System para SSL Completo](#)

Arquitetura da Implantação

No modo SSL completo, a comunicação entre todos os canais protegíveis é protegida usando SSL. Esse cenário de implantação do Oracle Enterprise Performance Management System é o mais seguro.

O conceito ilustrado:



Pressupostos

Banco de Dados

Os servidores e clientes de banco de dados são habilitados para SSL. Consulte a documentação do seu banco de dados para obter informações sobre habilitação para SSL do servidor e cliente de banco de dados.

EPM System

Os componentes do Oracle Enterprise Performance Management System, incluindo o Oracle WebLogic Server e o Oracle HTTP Server, são instalados e implantados. Além

disso, o ambiente do EPM System foi testado para garantir que tudo funcione no modo não SSL. Consulte as origens de informações a seguir:

- *Guia de Configuração e Instalação do Sistema Oracle Enterprise Performance Management*
- *A Instalação do Oracle Enterprise Performance Management System Começa Aqui*
- *Guia de Solução de Problemas de Instalação e Configuração do Oracle Enterprise Performance Management System*

Se você planeja habilitar para SSL as conexões de banco de dados, durante o processo de configuração, será preciso selecionar o link **Opções Avançadas** em cada tela de configuração de banco de dados e especificar as configurações necessárias, que incluem:

- Selecione **Usar conexão segura com o banco de dados (SSL)** e insira um URL de banco de dados seguro; por exemplo,

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCPS) (HOST=myDBhost)
(PORT=1529) (CONNECT_DATA=(SERVICE_NAME=myDBhost.myCompany.com)))
```
- **Keystore Confiável**
- **Senha do Keystore Confiável**

Consulte o *Guia de Configuração e Instalação do Sistema Oracle Enterprise Performance Management* para obter detalhes.

Descarregador de SSL e Balanceador de Carga

Uma descarregador de SSL totalmente configurado com um balanceador de carga deve estar presente no ambiente de implantação.

A configuração completa de SSL usa dois aliases de servidor, por exemplo, `epm.myCompany.com` e `empinternal.myCompany.com`, no descarregador de SSL. Um é para a comunicação externa entre o descarregador e os navegadores, e o outro é para a comunicação interna entre os servidores do EPM System. Certifique-se de que os aliases de servidor apontem para o endereço IP da máquina e que eles possam ser resolvidos por meio de DNS.

O balanceador de carga deve ser configurado para encaminhar todas as solicitações pelos hosts virtuais ao Oracle HTTP Servers.

Os dois certificados assinados – um para dar suporte à comunicação externa entre o descarregador e os navegadores (por meio de `epm.myCompany.com`), e o outro para dar suporte à comunicação interna (por meio de `empinternal.myCompany.com`) entre aplicativos – devem ser instalados no descarregador/balanceador de carga. A Oracle recomenda que esses certificados sejam associados aos aliases do servidor a fim de evitar a exposição dos nomes de servidor e aumentar a segurança.

Configuração do EPM System para SSL Completo

Consulte Também:

- [Redefinição das Configurações Comuns do EPM System](#)
- [Opcional: Instalação de Certificado da CA Raiz para WebLogic Server](#)
- [Instalação de Certificado no WebLogic Server](#)
- [Configuração do WebLogic Server](#)

- [Habilitação da Conexão do Servidor HFM com um Banco de Dados Oracle Ativado para SSL](#)
- [Procedimentos do Oracle HTTP Server](#)
- [Configuração de Componentes da Web do EPM System Implantados no WebLogic Server](#)
- [Atualizar a Configuração do Domínio](#)
- [Reinicialização de Servidores e do EPM System](#)
- [Teste da Implantação](#)
- [Configuração de Diretórios de Usuários Externos Habilitados para SSL](#)

Redefinição das Configurações Comuns do EPM System

Durante esse processo, selecione as configurações que forcem os componentes do Oracle Enterprise Performance Management System a usar a comunicação SSL.

Nota:

Se você estiver habilitando para SSL o servidor Web do Oracle Hyperion Financial Management: Antes de configurar o Financial Management, você deve tornar o cookie seguro editando o descritor por sessão do HFM WebApp no `weblogic.xml`.

1. Expanda o arquivo Web do Financial Management usando uma ferramenta como o 7 Zip. O local do `weblogic.xml` no arquivo é `EPM_ORACLE_HOME\products\FinancialManagement\AppServer\InstallableApps\HFMWebApplication.ear\HFMWeb.war\WEB-INF\weblogic.xml`.
2. Inclua a seguinte diretiva no descritor por sessão do HFM WebApp em `weblogic.xml`:

```
<cookie-secure>true</cookie-secure>
```
3. Salve `weblogic.xml`.
4. Clique em **Sim** quando 7 Zip consultar se você deseja atualizar o arquivo.

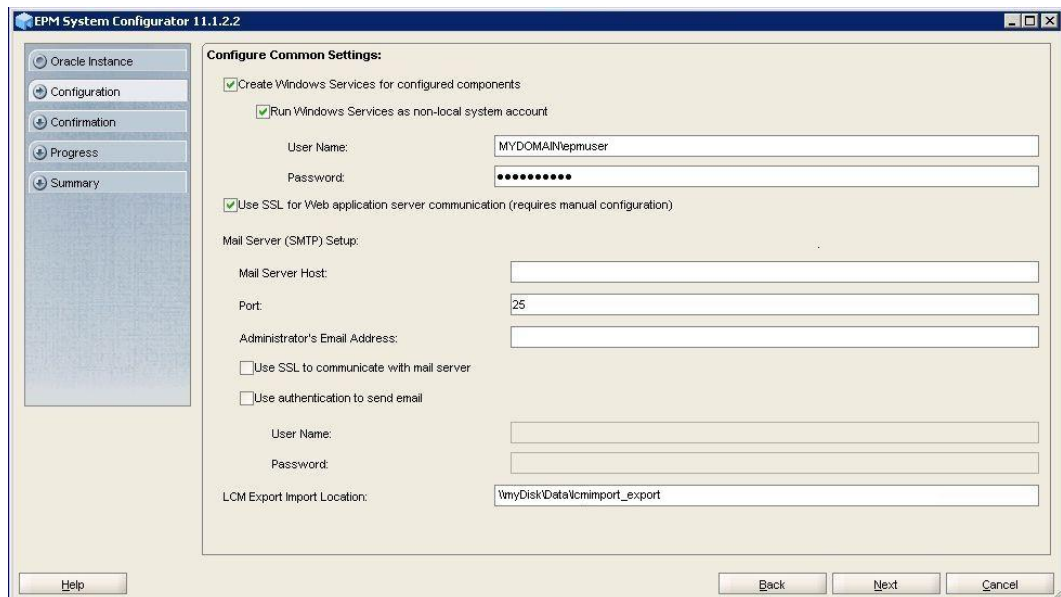
Para reconfigurar o EPM System para SSL:

1. Inicie o EPM System Configurator.
2. Em **Selecionar a Instância Oracle do EPM à qual a configuração será aplicada**, conclua estas etapas:
 - a. Em **Nome da instância Oracle do EPM**, insira o nome da instância que você usou ao configurar originalmente os componentes do EPM System.
 - b. Clique em **Próximo**.
3. Na tela Configuração, conclua estas etapas:
 - a. Desmarque **Desmarcar Todos**.
 - b. Expanda a tarefa de configuração de **Hyperion Foundation** e selecione **Configurar Definições Comuns**.

- c. Clique em **Próximo**.
4. Em **Configurar Definições Comuns**, conclua estas etapas:

▲ Cuidado:

Antes de selecionar as configurações para usar SSL de modo a se comunicar com o servidor de e-mail, certifique-se de que o servidor de e-mail seja configurado para SSL.



- a. Selecione **Usar SSL para comunicação do servidor de aplicativos Web Java (exige configuração manual)** para especificar que o EPM System deve usar SSL para comunicação.
 - b. **Opcional:** Insira informações em **Host do Servidor de E-mail** e **Porta**. Para dar suporte à comunicação SSL, é preciso especificar a porta segura usada pelo servidor de correio SMTP.
 - c. **Opcional:** Para dar suporte à comunicação SSL com o servidor de correio SMTP, selecione **Usar o SSL para comunicar-se com o servidor de e-mail**.
 - d. Selecione ou insira configurações nos campos restantes.
 - e. Clique em **Próximo**.
5. Clique em **Próximo** nas telas subsequentes do EPM System Configurator.
 6. Quando o processo de implantação é concluído, a tela Resumo é exibida. Clique em **Concluir**.

Opcional: Instalação de Certificado da CA Raiz para WebLogic Server

Os certificados raiz da maioria das CAs de terceiros reconhecidas já estão instalados no keystore da JVM. Conclua os procedimentos nesta seção se você não estiver usando

certificados de uma CA de terceiros reconhecida (não recomendado). O local do keystore padrão da JVM é `MIDDLEWARE_HOME/jdk/jre/lib/security/cacerts`.



Nota:

Execute este procedimento em cada servidor do Oracle Enterprise Performance Management System.

Para instalar o certificado da CA raiz:

1. Copie o certificado da CA raiz em um diretório local na máquina onde o Oracle WebLogic Server está instalado.
2. Em um console, altere o diretório para `MIDDLEWARE_HOME/jdk/jre/bin`.
3. Execute um comando `keytool`, como o seguinte, para instalar o certificado da CA raiz no keystore da JVM:

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

Por exemplo, você pode usar o comando a seguir para adicionar um certificado `CAcert.crt` armazenado no diretório atual no keystore da JVM com `Blister` como o alias de certificado no keystore. O `storepass example_pwd` é pressuposto.

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



Nota:

O comando e exemplo anteriores usam parte da sintaxe para importação de certificados usando `keytool`. Consulte a documentação de `keytool` para obter uma lista completa da sintaxe de importação.

Instalação de Certificado no WebLogic Server

A instalação padrão do Oracle WebLogic Server usa um certificado de demonstração para dar suporte ao SSL. A Oracle recomenda instalar o certificado de um terceiro reconhecido para fortalecer a segurança do seu ambiente.

Em cada máquina que hospeda o WebLogic Server, use uma ferramenta (por exemplo, `keytool`) de modo a criar um keystore personalizado para armazenar o certificado assinado de componentes da Web do WebLogic Server e Oracle Enterprise Performance Management System.

Para criar um keystore personalizado e importar o certificado:

1. Em um console, altere o diretório para `MIDDLEWARE_HOME/jdk/jre/bin`.

2. Execute o comando `keytool`, como o seguinte, para criar o keystore personalizado (identificado pela diretiva `-keystore` no comando) em um diretório 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:**

O nome comum (cn) que você define deve corresponder ao nome do servidor. Se você usar um nome de domínio totalmente qualificado (FQDN) como o cn, será preciso usar o FQDN ao implantar componentes da Web.

3. Gere uma solicitação 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. Obtenha um certificado assinado para a máquina do WebLogic Server.
5. Importe o certificado assinado no keystore:

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

Configuração do WebLogic Server

Depois de implantar componentes da Web do Oracle Enterprise Performance Management System, você deve configurá-los para comunicação de SSL.

Para configurar os componentes da Web para SSL:

1. Inicie o Oracle WebLogic Server executando `MIDDLEWARE_HOME/user_projects/domains/EPMSysstem/bin/startWebLogic.cmd`:
2. Inicie o Console de Administração do WebLogic Server acessando o seguinte URL:

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

Por exemplo, para acessar o console do WebLogic Server implantado na porta padrão em `myServer`, você deve usar `http://myServer:7001/console`.

3. Na tela de boas-vindas, informe o nome de usuário e a senha do administrador do WebLogic Server que você especificou no EPM System Configurator.
4. Em **Centro de Alterações**, clique em **Bloquear e Editar**.
5. No painel esquerdo do console, expanda **Ambiente** e selecione **Servidores**.
6. Na tela Resumo dos Servidores, clique no nome do servidor que deseja habilitar para SSL.

Por exemplo, para habilitar para SSL os componentes do Oracle Hyperion Foundation Services, trabalhe com o servidor do EPMServer0.

7. Desmarque **Escutar Porta Habilitada** para desativar a porta de escuta HTTP.
8. Certifique-se de que **Porta de Escuta SSL Habilitada** esteja selecionada.
9. Em **Porta de Escuta SSL**, informe a porta de escuta SSL onde esse servidor deve escutar solicitações.
10. Para especificar os keystores confiáveis e de identidade a serem usados, selecione **Keystores** para abrir a guia Keystores.
11. Clique em **Alterar**.
12. Selecione uma opção:
 - **Identidade e Confiança Personalizadas** se não estiver usando um certificado de servidor de uma CA de terceiros reconhecida
 - **Identidade Personalizada e Confiança Padrão Java** se estiver usando um certificado de servidor de uma CA de terceiros reconhecida
13. Clique em **Salvar**.
14. Em **Keystore de Identidade Personalizado**, insira o caminho do keystore onde o certificado assinado do WebLogic Server está instalado.
15. Em **Tipo de Keystore de Identidade Personalizado**, insira `jks`.
16. Em **Frase Secreta do Keystore de Identidade Personalizado e Confirmar Frase Secreta do Keystore de Identidade Personalizado**, informe a senha do keystore.
17. Se você selecionou **Identidade e Confiança Personalizadas** em **Keystores**:
 - Em **Keystore Confiável Personalizado**, informe o caminho do keystore personalizado onde o certificado raiz da CA que assinou o certificado do seu servidor está disponível.
 - Em **Tipo de Keystore Confiável Personalizado**, insira `jks`.
 - Em **Frase Secreta do Keystore Confiável Personalizado e Confirmar Frase Secreta do Keystore Confiável Personalizado**, informe a senha do keystore.
18. Clique em **Salvar**.
19. Especifique as configurações SSL:
 - Selecione **SSL**.
 - Em **Alias de Chave Privada**, informe o alias que você especificou ao importar o certificado assinado do WebLogic Server.
 - Em **Frase Secreta da Chave Privada e Confirmar Frase Secreta da Chave Privada**, informe a senha a ser usada para recuperar a chave privada.
 - Clique em **Salvar**.

 **Nota:**

Se estiver usando certificados SHA-2, você deverá selecionar a configuração **Usar SSL JSSE** para cada servidor gerenciado que é usado para dar suporte ao EPM System. Essa configuração está disponível na guia Avançado da página SSL. Você precisa reiniciar o WebLogic Server para ativar essa alteração.

20. Habilite a replicação segura para o servidor:
 - a. No painel esquerdo do console, expanda **Ambiente** e clique em **Clusters**.
 - b. Em Resumo dos Clusters, clique no nome do servidor, por exemplo `Foundation Services`, para o qual deseja habilitar a replicação segura.

A guia Configuração da tela Configurações para o servidor selecionado é exibida.
 - c. Clique em **Replicação** para abrir a guia Replicação.
 - d. Selecione **Replicação Segura Habilitada**. Talvez você precise clicar em **Bloquear e Editar** para poder selecionar essa opção.
 - e. Clique em **Salvar**.
21. Conclua da etapa 6 a 20 para cada servidor gerenciado que pertence a esse host.
22. Habilite a replicação segura de modo a fornecer canal para chamadas de replicação para o cluster.

Consulte o documento de metalink da Oracle 1319381.1 para obter detalhes.
 - No Console de Administração, expanda **Ambiente** e selecione **Clusters**.
 - Selecione **Replicação**.
 - Em **Replicação**, selecione (marque) **Replicação Segura Habilitada**.
 - Clique em **Salvar**.
23. Em **Centro de Alterações**, clique em **Ativar Alterações**.

Habilitação da Conexão do Servidor HFM com um Banco de Dados Oracle Ativado para SSL

A conexão de rede entre o DataSource HFM e o banco de dados Oracle pode ser criptografada usando SSL. Para isso funcionar, o Oracle Wallet deve estar configurado como descrito em [Documentação Oracle](#). O Listener TNS também deve estar configurado para fazer o listening de conexões criptografadas SSL em uma nova porta. Finalmente, os certificados apropriados precisam estar carregados no keystore e no armazenamento confiável dos servidores que hospedam o DataSource HFM. As instruções abaixo são provenientes de [Documentação do Banco de Dados Oracle](#).

Pré-requisitos

Certifique-se de que os seguintes pré-requisitos sejam atendidos antes de prosseguir com as etapas abaixo:

- Um servidor de banco de dados em funcionamento.

- Certifique-se de que nenhum firewall local ou de rede esteja bloqueando qualquer comunicação com o servidor na porta em que o listener TNS habilitado para SSL está em execução.

Nos exemplos abaixo, foi utilizada a versão Oracle 12c (12.1.0.2) em execução no MS Windows Server 2016. Essas instruções funcionarão igualmente bem em uma instalação Linux desde que os caminhos especificados para os arquivos wallet sejam caminhos do sistema de arquivos Linux e as substituições de variáveis de ambiente sejam alteradas adequadamente para o shell que está sendo usado no servidor de banco de dados. Essas mesmas instruções foram usadas com sucesso em instâncias de desenvolvimento e suporte 19c.

Os exemplos neste artigo usam certificados autoassinados, mas você também pode usar certificados de autoridade de certificação adequados, se preferir. Consulte [Documentação do Banco de Dados Oracle](#) para obter as etapas exatas a serem seguidas ao instalar um certificado emitido por uma autoridade de certificação.

Configuração do Bancos de Dados Oracle

Para configurar o Banco de Dados Oracle, siga as etapas abaixo:

1. Crie um novo wallet de login automática no servidor de banco de dados.

Nota:

Essas etapas são necessárias somente se um Oracle Wallet ainda não foi criado. As etapas a seguir não são necessárias se a ferramenta Oracle Wallet GUI for usada no servidor de banco de dados.

```
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
```

Você pode ignorar todas as mensagens que solicitem que você use - `auto_login_local` na linha de comando `orapki`. Se você se deparar com um erro de falha de autenticação SSL, consulte [ID do Doc. 2238096.1](#) para solucionar o problema.

Verifique também a permissão de segurança do arquivo `cwallet.sso` (no diretório do wallet) e certifique-se de que o usuário de serviço do listener Oracle possui permissão de leitura para esse arquivo. Sem a permissão de leitura, o handshake SSL falhará mais tarde. Essa situação ocorrerá se o banco de dados Oracle tiver sido instalado com o usuário Oracle sugerido o qual não possui permissão para efetuar logon. Se o banco de dados Oracle tiver sido instalado com o usuário Oracle, o Listener TNS deverá ser executado como um usuário diferente.

2. Crie um certificado autoassinado e carregue-o no wallet

```
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
```

A senha `password1` do exemplo acima deve corresponder à senha especificada na *Etapa 1*.

3. Exporte o certificado autoassinado criado recentemente

```
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 o arquivo de certificado Base64 exportado para o(s) servidor(es) HFM.

5. Configure o SQL*NET e os Listeners TNS:

- a.** Identifique uma porta não usada no servidor do banco de dados. O exemplo abaixo cria o novo listener na porta 1522. A porta típica usada por conexões SSL é 2484 e você pode usar qualquer porta disponível. Você precisa verificar se a porta que você quer usar está disponível no servidor de banco de dados antes de continuar e ajustar conforme necessário.
- b.** Atualize `SQLNET.ORA`. O elemento `DIRECTORY` da declaração `WALLET_LOCATION` deve apontar para o wallet criado na *Etapa 1* acima.

```
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.** Atualize `LISTENER.ORA` para definir um novo listener. Use a porta que foi identificada na *Etapa 5a* acima.

```
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. Crie uma nova entrada no TNSNAMES.ORA para a nova porta.

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

Você precisa especificar a mesma porta que foi identificada na *Etapa 5a* acima e usada na *Etapa 5c*.

- e. Reinicie o Listener TNS.

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

- f. Verifique se o novo listener TNS está funcionando

```
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)
```

Configuração do servidor HFM para usar conexões de banco de dados SSL

Adição do certificado do banco de dados ao armazenamento confiável no(s) servidor(es) HFM

As etapas seguintes devem ser realizadas em cada um dos servidores EPM em que a origem de dados do HFM é executada. A variável de ambiente `%MW_HOME%` usada abaixo é o local de instalação do Oracle Middleware. Esta variável de ambiente não é

criada por padrão durante a instalação do EPM e é usada aqui para mostrar o diretório pai da instalação do EPM.

O local da instalação do EPM é especificado pela variável de ambiente `EMP_ORACLE_HOME`. O exemplo abaixo coloca o keystore e o armazenamento confiável em um diretório colocalizado com a instalação do EPM. Os arquivos de keystore e armazenamento confiável podem estar localizados em qualquer lugar no sistema de arquivos do servidor HFM.

1. Crie um novo diretório em `%MW_HOME%` para armazenar o Java keystore e o armazenamento confiável PKCS12.
 - a. `cd %MW_HOME%`
 - b. `mkdir certs`
2. Copie o cacerts do arquivo do Java keystore a partir do JDK.
 - a. `cd %MW_HOME%\certs`
 - b. `copy %MW_HOME%\jdk1.8.0_181\jre\lib\security\cacerts testing_cacerts`
O motivo pelo qual você copia o keystore do JDK e o utiliza em lugar do keystore padrão do JDK é para que, se o JDK for atualizado e o JDK anterior for excluído, as chaves e certificados inseridos no keystore padrão não sejam perdidos.
3. Copie o certificado Base 64 para `%MW_HOME%\certs`.
4. Importe o certificado para o arquivo Java keystore `testing_cacerts`.
 - a. Por exemplo: `keytool -importcert -file bur00cbb-certificate.crt -keystore testing_cacerts -alias "myserver"`
 - i. Você precisará especificar a senha para o keystore.
 - ii. Você deve substituir "myserver" pelo domínio totalmente qualificado do servidor do banco de dados.
 - b. Quando você for perguntado se o certificado é confiável ou não, especifique **y**.
5. Crie o armazenamento confiável no formato PKCS12 a partir do arquivo Java keystore do JDK. Por exemplo,

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

Atualizando as conexões JDBC do HFM para usar SSL

1. Reconfigure a conexão JDBC do banco de dados HFM para usar SSL.
 - a. Inicie a ferramenta de Configuração do EPM.
 - i. Selecione os nós **Configurar Banco de Dados e Implantar no Servidor de Aplicativos** subordinados ao nó **Financial Management**.
 - ii. Clique em **Próximo**.
 - iii. Execute estas etapas para a conexão JDBC do HFM
 - i. Insira a porta SSL, o nome de serviço, o nome de usuário e a senha para a conexão nas colunas porta, nome de serviço, nome de usuário e senha.
 - ii. Clique em **(+)** para abrir as **opções de banco de dados Avançadas**.
 - iii. Marque a caixa de seleção **Usar conexões seguras**.
 - iv. Insira a localização do Java keystore criada na *Etapa 2*.

- v. Clique em **Aplicar**.
 - vi. Clique em (+) para abrir as **opções de banco de dados Avançadas**.
 - vii. Clique em **Editar e usar URL JDBC modificado**. Note que nenhuma alteração deve ser feita ao URL JDBC exibido.
 - viii. Clique em **Aplicar**.
 - ix. Clique em **Próximo**.
- b. Siga as etapas restantes para implantar o aplicativo HFM conforme descrito na documentação do EPM.
2. Abra uma janela de comando ou shell para atualizar manualmente o registro do EPM para que a conexão ODBC usada pelo DataSource possa ser habilitada para SSL.
Execute cada um dos comandos relacionados abaixo:

```
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
```

Nos exemplos acima, o caminho C:\Oracle\Middleware é o valor de %MW_HOME% nas etapas 1, 2 e 3.

A propriedade FINANCIAL_MANAGEMENT_PRODUCT/DATABASE_CONN/@ODBC_VALIDATESERVERCERTIFICATE só deve ser definida como falsa se um certificado autoassinado estiver sendo usado. O valor do FINANCIAL_MANAGEMENT_PRODUCT/DATABASE_CONN/@ODBC_TRUSTSTOREPASSWORD deve ser a senha do Java keystore original copiado na *Etapa 2*.

Atualize a entrada dos nomes TNS usados por HFM

Edite TNSNAMES.ORA para criar uma nova entrada e renomear a entrada antiga. O exemplo a seguir mostra um arquivo TNSNAMES.ORA atualizado no servidor HFM que possui as alterações necessárias aplicadas. Essas alterações acontecem por que o HFM procura e usa uma entrada de nomes TNS chamada HFMTNS. Essa entrada deve ter o protocolo e a porta altrados para que o XFMDDataSource funcione adequadamente.

```
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)
    )
  )
)

```

A entrada `HFMTNS` original foi renomeada para `HFMTNS_UNENC`. O novo `HFMTNS` foi criado copiando a entrada `HFMTNS_UNENC`, renomeando-a para `HFMTNS`. O protocolo foi então atualizado para `TCPS` e a porta foi alterada para `1522`. A porta especificada deve ser a mesma porta especificada no arquivo `TNS LISTENER.ORA`.

Procedimentos do Oracle HTTP Server

Criação de um Wallet e Instalação de Certificado para o Oracle HTTP Server

Um wallet padrão é instalado automaticamente com o Oracle HTTP Server. Você deve configurar um wallet real para cada Oracle HTTP Server em sua implantação.

Observação: A partir da versão 11.2.x, o Oracle Wallet Manager não será instalado com o Oracle HTTP Server. O Oracle Wallet Manager será instalado somente se você instalar o Oracle Database Client. Você deve usar o gerenciador de wallet disponível com o Database Client para criar o wallet e importar o certificado. Se você estiver configurando o Oracle HTTP Server para SSL, certifique-se de sempre instalar o Oracle Database Client de 64 bits como parte da instalação dos produtos do sistema EPM.

Para criar e instalar um certificado do Oracle HTTP Server:

1. Em cada máquina que hospeda o Oracle HTTP Server, inicie o Wallet Manager.

Selecione **Iniciar, Todos os Programas, Oracle-OHxxxxxx, Ferramentas Integradas de Gerenciamento** e, por fim, **Wallet Manager**.

xxxxxx é o número da instância do Oracle HTTP Server.
2. Crie um novo Wallet vazio.
 - a. No Oracle Wallet Manager, selecione **Wallet** e, em seguida, **Novo**.
 - b. Clique em **Sim** para criar um diretório de wallet padrão, ou em **Não** para criar o arquivo de Wallet em um local de sua escolha.
 - c. Em **Senha do Wallet** e **Confirmar Senha** na tela Novo Wallet, informe a senha que deseja usar.
 - d. Clique em **OK**.
 - e. Na caixa de diálogo de confirmação, clique em **Não**.
3. **Opcional:** Se você não estiver usando uma CA conhecida do Oracle HTTP Server, importe o certificado da CA raiz para o Wallet.
 - a. No Oracle Wallet Manager, clique com o botão direito do mouse em **Certificados Confiáveis** e selecione **Importar Certificado Confiável**.

Se nenhuma senha tiver sido especificada na linha de comando, esse comando solicitará que você informe e reinforme uma senha do wallet. Isso cria um wallet na localização especificada para `-wallet`.

4. Gere uma solicitação de assinatura de certificado (CSR) e adicione-a a seu wallet:

```
$ 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. Adicione o certificado raiz e intermediário ao keystore confiável

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

6. Use sua CA (Autoridade de Certificação) para assinar a CSR (Solicitação de Assinatura do Certificado). Para exportar a solicitação de certificado de um 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 a CSR assinada para o wallet:

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

8. Para exibir o conteúdo do wallet:

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

Habilitação para SSL do Oracle HTTP Server

Após reconfiguração do servidor Web em cada máquina que hospeda o Oracle HTTP Server, atualize o arquivo de configuração do Oracle HTTP Server substituindo o local do Wallet padrão pelo local do wallet que você criou.

Para configurar o Oracle HTTP Server para SSL:

1. Reconfigure o servidor Web em cada máquina host do Oracle HTTP Server em sua implantação.
2. Inicie o EPM System Configurator para a instância.
3. Na tela de seleção da tarefa de configuração, conclua estas etapas e clique em **Próximo**.
 - a. Desmarque a seleção de **Desmarcar Todos**.
 - b. Expanda o grupo de tarefas do **Hyperion Foundation** e selecione **Configurar Servidor Web**.
4. Em **Configurar Servidor Web**, clique em **Próximo**.

5. Em **Confirmação**, clique em **Próximo**.
6. Em **Resumo**, clique em **Concluir**.
7. Usando um editor de texto, abra `EPM_ORACLE_INSTANCE/httpConfig/ohs/config/fmwconfig/components/OHS/ohs_component/ssl.conf`.
8. Certifique-se de que a porta SSL que você está usando esteja listada em `OHS Listen port`, semelhante ao seguinte:

Se você estiver usando 19443 como a porta de comunicação SSL, suas entradas devem ser como se segue:

```
Listen 19443
```

9. Defina o valor do parâmetro `SSLSessionCache` como `none`.
10. Atualize as definições de configuração de cada Oracle HTTP Server em sua implantação.
 - a. Usando um editor de texto, abra `EPM_ORACLE_INSTANCE/httpConfig/ohs/config/fmwconfig/components/OHS/ohs_component/ssl.conf`.
 - b. Localize a diretiva `SSLWallet` e altere seu valor para que ele aponte para o wallet em que você instalou o certificado. Se você criou o wallet em `EPM_ORACLE_INSTANCEhttpConfig/ohs/config/OHS/ohs_component/keystores/epmsystem`, sua diretiva `SSLWallet` pode ser como se segue:

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

- c. Salve e feche `ssl.conf`.
11. Atualize `mod_wl_ohs.conf` em cada Oracle HTTP Server da implantação.
 - a. Usando um editor de texto, abra `EPM_ORACLE_INSTANCE/httpConfig//ohs/config/fmwconfig/components/OHS/ohs_component/mod_wl_ohs.conf`.
 - b. Certifique-se de que a diretiva `WLSSLWallet` aponte para o Oracle Wallet onde o certificado SSL está armazenado.

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

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

- c. Defina o valor da diretiva `SecureProxy` para `ON`.

`SecureProxy ON`
 - d. Certifique-se de que as definições `LocationMatch` para os componentes implantados do Oracle Enterprise Performance Management System sejam semelhantes ao exemplo de Oracle Hyperion Shared Services a seguir, que

supõe um cluster do Oracle WebLogic Server (em `myserver1` e `myserver2` usando a porta SSL 28443):

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

- e. Salve e feche `mod_wl_ohs.conf`.

Configuração de Componentes da Web do EPM System Implantados no WebLogic Server

Depois de implantar componentes da Web do Oracle Enterprise Performance Management System, você deve configurá-los para comunicação de SSL.

Para configurar os componentes da Web para SSL:

1. Inicie o Oracle WebLogic Server executando um arquivo armazenado em `EPM_ORACLE_INSTANCE/domains/EPMSystem/bin/startWebLogic.cmd`:
2. Inicie o Console de Administração do WebLogic Server acessando o seguinte URL:

`http://SERVER_NAME:Port/console`

Por exemplo, para acessar o console do WebLogic Server implantado na porta padrão em `myServer`, você deve usar `http://myServer:7001/console`.

3. Na tela de boas-vindas, insira o nome do usuário e a senha para acessar o EPMSystem. O nome do usuário e a senha são especificados no EPM System Configurator durante o processo de configuração.
4. Em **Centro de Alterações**, clique em **Bloquear e Editar**.
5. No painel esquerdo do console, expanda **Ambiente** e selecione **Servidores**.
6. Na tela Resumo dos Servidores, clique no nome do servidor que deseja habilitar para SSL.

Por exemplo, se você instalou os componentes do Oracle Hyperion Foundation Services, será possível habilitar para SSL estes servidores:

- CalcManager
- FoundationServices

7. Desmarque **Escutar Porta Habilitada** para desativar a porta de escuta HTTP.
8. Certifique-se de que **Porta de Escuta SSL Habilitada** esteja selecionada.
9. Em **Porta de Escuta SSL**, informe a porta de escuta SSL do WebLogic Server.
10. Especifique a identidade e os keystores de confiança a serem usados.
 - Selecione **Keystores** para abrir a guia Keystores.
 - Em **Keystores**, selecione uma opção:
 - a. Selecione **Keystores** para abrir a guia Keystores.

- b. Em **Keystores**, selecione uma opção:
 - **Identidade e Confiança Personalizadas** se não estiver usando um certificado de servidor de uma CA de terceiros reconhecida
 - **Identidade Personalizada e Confiança Padrão Java** se estiver usando um certificado de servidor de uma CA de terceiros reconhecida
 - c. Em **Keystore de Identidade Personalizado**, insira o caminho do keystore onde o certificado assinado do WebLogic Server está instalado.
 - d. Em **Tipo de Keystore de Identidade Personalizado**, insira `jks`.
 - e. Em **Frase Secreta do Keystore de Identidade Personalizado e Confirmar Frase Secreta do Keystore de Identidade Personalizado**, informe a senha do keystore.
 - f. Se você selecionou **Identidade e Confiança Personalizadas** em **Keystores**:
 - Em **Keystore Confiável Personalizado**, informe o caminho do keystore personalizado onde o certificado raiz da CA que assinou o certificado do seu servidor está disponível.
 - Em **Tipo de Keystore Confiável Personalizado**, insira `jks`.
 - Em **Frase Secreta do Keystore Confiável Personalizado e Confirmar Frase Secreta do Keystore Confiável Personalizado**, informe a senha do keystore.
 - g. Clique em **Salvar**.
11. Especifique as configurações do SSL.
- Selecione **SSL**.
 - Em **Alias de Chave Privada**, informe o alias que você especificou ao importar o certificado assinado do WebLogic Server.
 - Em **Frase Secreta da Chave Privada e Confirmar Frase Secreta da Chave Privada**, informe a senha a ser usada para recuperar a chave privada.
 - Apenas aplicativo Web do **Oracle Hyperion Provider Services**: Se estiver usando certificados curinga para criptografar a comunicação entre o WebLogic Server e outros componentes de servidor do EPM System, desative a verificação de nome de host para aplicativos Web do Provider Services.
 - Selecione **Avançado**.
 - Em **Verificação do Nome do Host**, selecione **Nenhum**.
 - Clique em **Salvar**.
12. Em **Centro de Alterações**, clique em **Ativar Alterações**.

Atualizar a Configuração do Domínio

Esse processo atualiza a configuração do domínio. Crie um backup completo da sua implantação antes de iniciar esse procedimento. A Oracle recomenda testar esse procedimento em uma implantação de teste antes de fazer alterações em uma implantação de produção.

Para atualizar a configuração do domínio:

1. Navegue até o diretório `MIDDLEWARE_HOME/oracle_common/bin` directory:
`cd MIDDLEWARE_HOME/oracle_common/bin`

2. Defina `ORACLE_HOME`, `WL_HOME` e `JAVA_HOME`.

```
set ORACLE_HOME= /Oracle/Middleware
set WL_HOME= /Oracle/Middleware/wlserver
set JAVA_HOME= /Oracle/Middleware/jdk
```
3. No Console do Web Logic, habilite a porta HTTP para o servidor de Administração.
4. Crie um keystore usando um comando semelhante ao seguinte:

```
libovdconfig.bat -host HOSTNAME -port 7001 -userName USERNAME -domainPath %MWH%\user_projects\domains\EPMSystem -createKeystore
```

Neste comando, substitua `HOSTNAME` e `USERNAME` pelo nome do host do WebLogic Server e pelo nome de usuário do Administrador, respectivamente. Certifique-se de que a saída relate a criação bem-sucedida do keystore OVD.

5. Exporte o certificado SSL do AdminServer.

 **Note:**

Essa etapa aplica-se somente ao LDAP Incorporado (Autenticador Padrão). Para outros LDAPS, o certificado deve ser exportado usando os comandos apropriados específicos do LDAP. O formato do arquivo do certificado deve ser **x.509 Codificado em Base 64**

- a. Usando o Internet Explorer, acesse o console de administração do Web Logic conectando-se a `https://HOSTNAME:7002/console`
 - b. Clique em **Exibir Certificado**, em **Detalhes** e selecione **Copiar para arquivo** para exportar o certificado SSL.
 - c. Salve o certificado como um arquivo de certificado **x.509 Codificado em Base 64** em um diretório local; por exemplo, `C:\certificate\slc17rby.cer`.
 - d. Transfira o certificado para o servidor.
6. Usando o keytool, importe o certificado para o keystore que você criou na etapa 4. Use comandos semelhantes aos seguintes (supondo que `JAVA_HOME` e o executável do keytool estejam no caminho):

```
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 exemplo:

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

 **Note:**

- A senha usada nesse comando deve corresponder à senha usada ao gerar o keystore na etapa 4.
- `CERTIFICATE_PATH` é o local e o nome do certificado
- Alias pode ser qualquer alias de sua escolha.

Na importação bem-sucedida do certificado, o keytool exibe a mensagem `Certificate was added to keystore.`

7. No Console do Web Logic, habilite a porta SSL para o Servidor de Administração além da porta HTTP.
8. Reinicie os Servidores Gerenciados e o Servidor de Administração do WebLogic.
9. Faça logon no Oracle Hyperion Enterprise Performance Management Workspace usando uma conexão segura para verificar se tudo está funcionando.

Reinicialização de Servidores e do EPM System

Reinicie todos os servidores na implantação e inicie o Oracle Enterprise Performance Management System em cada servidor.

Teste da Implantação

Após a conclusão da implantação do SSL, verifique se tudo está funcionando.

Para testar sua implantação:

1. Usando um navegador, acesse o URL seguro do Oracle Hyperion Enterprise Performance Management Workspace:

Se você usou `epm.myCompany.com` como o alias do servidor para comunicação externa e 4443 como a porta SSL, o URL do EPM Workspace será

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

2. Na tela de logon, insira o nome de usuário e a senha.
3. Clique em **Logon**.
4. Verifique se você pode acessar com segurança os componentes implantados do Oracle Enterprise Performance Management System.

Configuração de Diretórios de Usuários Externos Habilitados para SSL

Pressupostos

- Os diretórios de usuários externos que você pretende configurar no Oracle Hyperion Shared Services Console estão habilitados para SSL.
- Se você não usou um certificado de uma CA de terceiros reconhecida para habilitar para SSL o diretório de usuários, você terá uma cópia do certificado raiz da CA que assinou o certificado do servidor.

Importar o Certificado da CA Raiz

Se você não usou um certificado de uma CA de terceiros reconhecida para habilitar para SSL o diretório de usuários, será preciso importar o certificado raiz da CA que assinou o certificado de servidor nos seguintes keystores:



Nota:

Durante a implantação do aplicativo, o WebLogic adiciona a diretiva - `Djavax.net.ssl.trustStore` apontando para `DemoTrust.jks` em `setDomainEnv.sh` ou `setDomainEnv.cmd`. **Remova** `-Djavax.net.ssl.trustStore` de `setDomainEnv.sh` ou `setDomainEnv.cmd` se não estiver usando o certificado padrão do WebLogic.

Use uma ferramenta, como a `keytool`, para importar o certificado da CA raiz.

- Todos os servidores do Oracle Enterprise Performance Management System:

Keystore da JVM: `MIDDLEWARE_HOME/jdk/jre/lib/security/cacerts`

- O keystore usado pela JVM em cada máquina host do componente do EPM System. Por padrão, os componentes do EPM System usam o seguinte keystore:

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

Configurar Diretórios de Usuários Externos

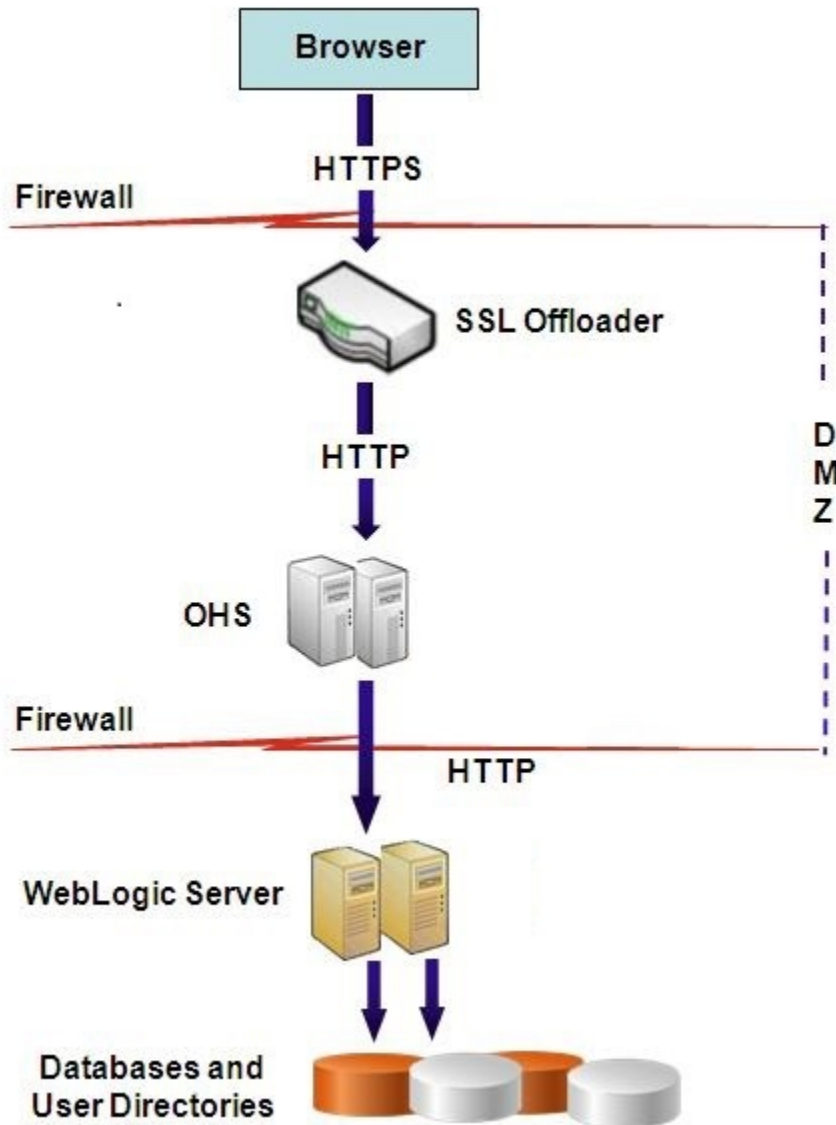
Você configura diretórios de usuários usando o Shared Services Console. Ao configurar diretórios de usuários, você deve selecionar a opção `Habilitado para SSL` que orienta a segurança do EPM System a usar o protocolo seguro para se comunicar com o diretório de usuários. É possível habilitar para SSL uma conexão entre a segurança do EPM System e os diretórios de usuários habilitados para LDAP; por exemplo, Oracle Internet Directory e Microsoft Active Directory.

Consulte o tópico sobre configuração de diretórios de usuários no *Guia de Administração da Segurança de Usuário do Sistema Oracle Enterprise Performance Management*.

Encerramento de SSL no Servidor Web

Arquitetura da Implantação

Nesse cenário, o SSL é usado para proteger o link de comunicação entre os clientes do Oracle Enterprise Performance Management System (por exemplo, um navegador) e o Oracle HTTP Server. O conceito ilustrado:



Pressupostos

Essa configuração usa dois aliases de servidor; por exemplo, `epm.myCompany.com` e `empinternal.myCompany.com`, no servidor Web, um para comunicação externa entre o servidor Web e os navegadores e o outro para comunicação interna entre os servidores do EPM System. Certifique-se de que os aliases de servidor apontem para o endereço IP da máquina e que eles possam ser resolvidos por meio de DNS.

Um certificado assinado para dar suporte à comunicação externa com navegadores (por exemplo, por meio de `epm.myCompany.com`) deve ser instalado no servidor Web (onde o host virtual que dá suporte à comunicação externa segura está definido). Esse host virtual deve encerrar o SSL e encaminhar as solicitações HTTP ao Oracle HTTP Server.

Quando o SSL estiver sendo encerrado no Oracle HTTP Server (OHS) ou no balanceador de carga, você deverá:

- Definir cada Aplicativo Web Lógico para o host virtual não ssl do balanceador de carga ou do Oracle HTTP Server (por exemplo, `empinternal.myCompany.com:80`, onde 80 é a porta não SSL). Abra a tela Configuração e conclua estas etapas:
 1. Expanda a tarefa de configuração do **Hyperion Foundation**.
 2. Selecione **Configurar Endereço Lógico de Aplicativos Web**.
 3. Especifique o *Nome do host*, o número da porta não SSL e o número da porta SSL.
- Definir o URL externo para o host virtual habilitado para SSL do balanceador de carga ou do Oracle HTTP Server (por exemplo, `empexternal.myCompany.com:443`, onde 443 é a porta SSL). Abra a tela Configuração e conclua estas etapas:
 1. Expanda a tarefa de configuração do **Hyperion Foundation**.
 2. Selecione **Definir Configurações Comuns**.
 3. Selecione **Habilitar descarregamento de SSL** em Detalhes do URL Externo.
 4. Especifique o *Host do URL Externo* e a *Porta do URL Externo*.

 **Nota:**

A reimplantação de aplicativos web ou a reconfiguração do servidor web usando **configtool** substituirá as configurações do Aplicativo Web Lógico e URLs externos.

Configuração do EPM System

A implantação padrão dos componentes do EPM System dá suporte ao encerramento de SSL no servidor Web. Não é necessária nenhuma ação adicional.

Durante a configuração do EPM System, certifique-se de que os aplicativos Web lógicos apontem para o host virtual (por exemplo, `empinternal.myCompany.com`) que foi criado para comunicação interna. Consulte as seguintes origens de informação para instalar e configurar o EPM System:

- *Guia de Configuração e Instalação do Sistema Oracle Enterprise Performance Management*
- *A Instalação do Oracle Enterprise Performance Management System Começa Aqui*

Teste da Implantação

Após a conclusão do processo de implantação, verifique se tudo está funcionando conectando-se ao uRL seguro do Oracle Hyperion Enterprise Performance Management Workspace:

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

Por exemplo, `https://epm.myCompany.com:443/workspace/index.jsp`, onde 443 é a porta SSL.

SSL para Essbase 11.1.2.4

Visão Geral

Esta seção explica os procedimentos para substituir os certificados padrão que são usados para proteger a comunicação entre uma instância do Oracle Essbase e componentes como o MaxL, Servidor do Oracle Essbase Administration Services, Servidor do Oracle Essbase Studio, Oracle Hyperion Provider Services, Oracle Hyperion Foundation Services, Oracle Hyperion Planning, Oracle Hyperion Financial Management e Oracle Hyperion Shared Services Registry.

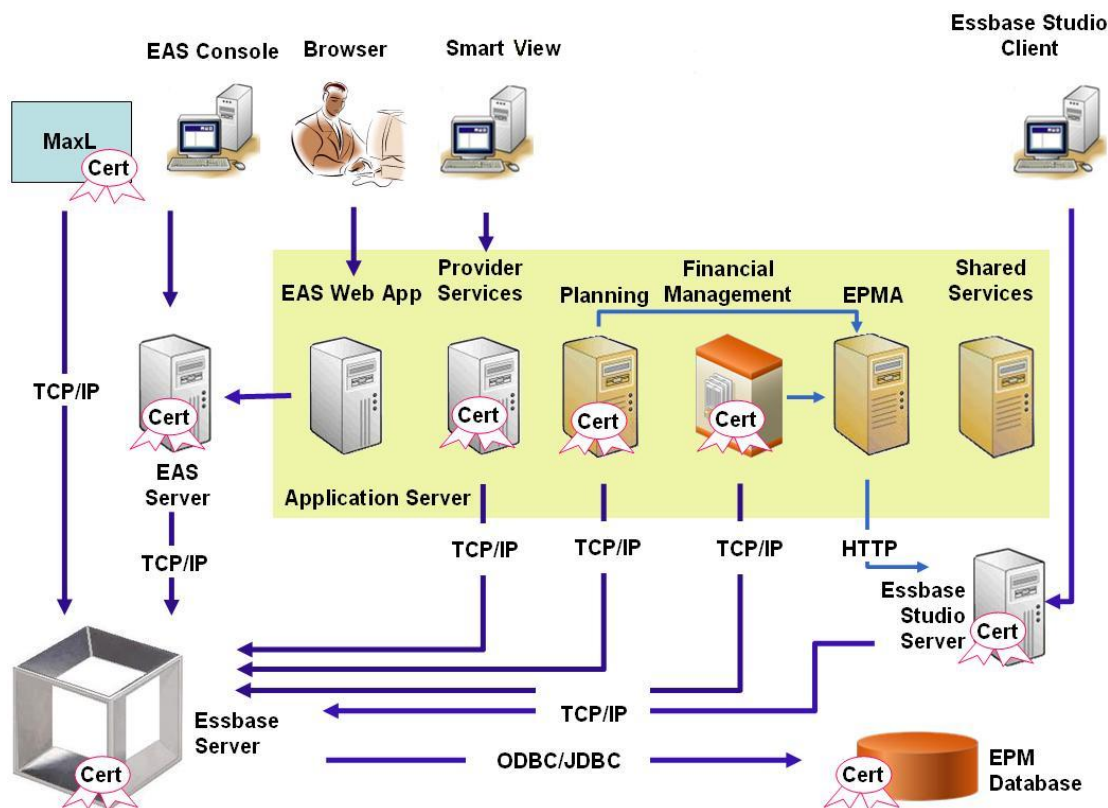
Implantação Padrão

O Essbase pode ser implantado para funcionar nos modos de SSL e não SSL. O Agente do Essbase escuta em uma porta não segura; ele também pode ser configurado para escutar em uma porta segura. Todas as conexões que acessam a porta segura são tratadas como conexões SSL. Se um cliente se conectar ao Agente do Essbase na porta não SSL, a conexão será tratada como uma conexão não SSL. Os componentes podem estabelecer conexões simultâneas não SSL e SSL com um Agente do Essbase.

Você não pode controlar o SSL por sessão especificando o protocolo seguro e a porta quando faz logon. Consulte [Como Estabelecer uma Conexão SSL por Sessão](#).

Se o SSL estiver habilitado, toda a comunicação em uma instância do Essbase será criptografada para garantir a segurança de dados.

As implantações padrão dos componentes do Essbase no modo seguro usam certificados autoassinados para habilitar a comunicação SSL, basicamente para fins de teste. A Oracle recomenda usar certificados de CAs de terceiros reconhecidas a fim de habilitar para SSL o Essbase em ambientes de produção.



Normalmente, um Oracle Wallet armazena o certificado que habilita a comunicação SSL com clientes que usam o Essbase RTC e um keystore Java armazena o certificado que habilita a comunicação SSL com componentes que utilizam JAPI para comunicação. Para estabelecer comunicação SSL, os clientes e ferramentas do Essbase armazenam o certificado raiz da CA que assinou os certificados do Servidor e Agente do Essbase. Consulte [Certificados Necessários e Respetivo Local](#).

Certificados Necessários e Respetivo Local

A Oracle recomenda o uso de certificados de CAs de terceiros reconhecidas de modo a habilitar para SSL o Essbase em um ambiente de produção. Você pode usar os certificados autoassinados padrão para teste.

Nota:

O Essbase dá suporte ao uso de certificados curinga, que podem proteger vários subdomínios com um certificado SSL. Usar um certificado curinga pode reduzir o tempo e o custo de gerenciamento.

Os certificados curinga não poderão ser usados se a verificação do nome do host for habilitada.

Exija os seguintes certificados:

- Um certificado da CA raiz.
Os componentes que usam o Essbase RTC para estabelecer uma conexão com o Essbase exigem que o certificado da CA raiz seja armazenado em um Oracle Wallet. Os

componentes que usam JAPI para estabelecer uma conexão exigem que o certificado da CA raiz seja armazenado em um keystore Java. Os certificados necessários e seus locais são indicados na tabela a seguir.

 **Nota:**

Talvez você não precise instalar um certificado da CA raiz se estiver usando certificados de uma CA de terceiros reconhecida cujo certificado raiz já está instalado no Oracle Wallet.

- Certificado assinado para o Servidor do Essbase e o Agente do Essbase.

Tabela 2-1 Certificados Necessários e Respetivos Locais

Componente ¹	Keystore	Certificado ²
MaxL	Oracle Wallet	Certificado da CA raiz
Servidor do Administration Services	Oracle Wallet	Certificado da CA raiz
Provider Services	Oracle Wallet	Certificado da CA raiz
Banco de Dados do Oracle Enterprise Performance Management System	Oracle Wallet	Certificado da CA raiz
Servidor do Essbase Studio Planning	Keystore Java <ul style="list-style-type: none"> • Oracle Wallet • Keystore Java 	Certificado da CA raiz Certificado da CA raiz
Financial Management Essbase (Servidor e Agente) ³	Keystore Java <ul style="list-style-type: none"> • Oracle Wallet • Keystore Java 	Certificado da CA raiz <ul style="list-style-type: none"> • Certificado da CA raiz • Certificado assinado para o Servidor e Agente do Essbase
Repositório do Oracle Hyperion Shared Services		

¹ Você precisa apenas de uma instância do keystore para dar suporte a vários componentes que usam um keystore semelhante.

² Vários componentes podem usar um certificado raiz instalado em um keystore.

³ Os certificados devem ser instalados no Oracle Wallet padrão e no keystore Java.

Instalação e Implantação de Componentes do Essbase

O processo de configuração permite que você selecione uma porta de agente segura (o padrão é 6423), que você pode alterar ao configurar o Oracle Essbase. Por padrão, o processo de implantação instala os certificados autoassinados necessários para criar uma implantação funcional segura para teste.

O EPM System Installer instala um Wallet Oracle e um certificado autoassinado em `ARBOR_PATH` na máquina que hospeda a instância do Essbase se o Oracle HTTP Server estiver instalado. Em implantações de único host, todos os componentes do Essbase compartilham esse certificado.

Uso de Certificados da CA de Terceiros Confiáveis para Essbase

Criação de Solicitações de Certificado e Obtenção de Certificados

Gere uma solicitação de certificado a fim de obter um certificado para o servidor que hospeda o Servidor do Oracle Essbase e Agente do Essbase. Uma solicitação de certificado contém informações criptografadas específicas ao seu Nome Distinto (DN). Você envia a solicitação de certificado para uma autoridade de autenticação a fim de obter um certificado SSL.

Você usa uma ferramenta como o keytool ou o Oracle Wallet Manager para criar uma solicitação de certificado. Para obter informações detalhadas sobre como criar uma solicitação de certificado, veja a documentação para a ferramenta que você está usando.

Se você estiver usando o keytool, use um comando como o seguinte para criar uma solicitação 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
```

Obtenção e Instalação do Certificado da CA Raiz

O certificado da CA raiz verifica a validade do certificado que é usado para dar suporte ao SSL. Ele contém a chave pública em relação à qual a chave privada que foi usada para assinar o certificado é compatível para verificar o certificado. É possível obter o certificado da CA raiz da autoridade de certificação que assinou seus certificados SSL.

Instale o certificado raiz da CA que assinou o certificado do Servidor do Essbase em clientes que se conectam ao Servidor ou Agente do Essbase. Certifique-se de que o certificado raiz seja instalado no keystore apropriado para o cliente. Consulte [Certificados Necessários e Respeetivo Local](#) .



Nota:

Vários componentes podem usar um certificado de CA raiz instalado em uma máquina de servidor.

Oracle Wallet

Consulte a [Certificados Necessários e Respeetivo Local](#) para obter uma lista de componentes que exigem o certificado raiz da CA em um Oracle Wallet. Você pode criar um wallet ou instalar o certificado no wallet de demonstração onde o certificado autoassinado padrão está instalado.

Consulte a documentação do Oracle Wallet Manager para obter procedimentos detalhados a fim de criar wallets e importar o certificado da CA raiz.

Keystore Java

Consulte a [Certificados Necessários e Respeetivo Local](#) para obter uma lista de componentes que exigem o certificado da CA raiz em um keystore Java. Você pode

adicionar o certificado no keystore onde o certificado autoassinado padrão está instalado ou criar um keystore para armazenar o certificado.



Nota:

Os certificados da CA raiz de muitas CAs reconhecidas de terceiros já estão instalados no keystore Java.

Consulte a documentação da ferramenta que você está usando para obter instruções detalhadas. Se você estiver usando o keytool, use um comando, como o seguinte, para importar o certificado raiz:

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

Instalação de Certificados Assinados

Você instala os certificados SSL assinados no servidor que hospeda o Servidor do Essbase e o Agente do Essbase. Os componentes que usam o Essbase RTC (APIs C) para estabelecer uma conexão com o Servidor ou Agente do Essbase exigem que o certificado seja armazenado em um Oracle Wallet com o certificado da CA raiz. Os componentes que usam JAPI para estabelecer uma conexão com o Servidor ou Agente do Essbase exigem que o certificado da CA raiz e o certificado SSL assinado sejam armazenados em um keystore Java. Para ver os procedimentos detalhados, consulte estas origens de informações:

- Documentação do Oracle Wallet Manager
- Documentação ou ajuda on-line da ferramenta; por exemplo, keytool, que você usa para importar o certificado

Se você estiver usando o keytool, use um comando, como o seguinte, para importar o certificado:

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

Atualize Valores do Registro de Servidores Essbase

Windows

1. Em um prompt de comando, altere o diretório para `EPM_ORACLE_INSTANCE/epmsystem1/bin`.
2. Execute estes comandos para atualizar o Windows Registry:


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

Certifique-se de substituir <Object ID> pelo ID componente do Servidor Essbase, que está disponível no Relatório de Registro gerado depois que você conclui o processo de configuração do Servidor Essbase.

Linux

1. Em um console, altere o diretório para `EPM_ORACLE_INSTANCE/epmsystem1/bin`.
2. Execute estes comandos para atualizar o registro:

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

Certifique-se de substituir <Object ID> pelo ID componente do Servidor Essbase, que está disponível no Relatório de Registro gerado depois que você conclui o processo de configuração do Servidor Essbase.

Atualização das Configurações de SSL do Essbase

Você personaliza as configurações de SSL para Servidor e clientes do Essbase especificando o valor para o seguinte em `essbase.cfg`.

- Configuração para habilitar o modo seguro
- Configuração para habilitar o modo de limpeza
- Modo preferencial para comunicação com clientes (usado apenas pelos clientes)
- Porta segura
- Conjuntos de cifras
- Caminho do Oracle Wallet

Nota:

Em `essbase.cfg`, certifique-se de adicionar todos os parâmetros necessários ausentes, especialmente, `EnableSecureMode`, `AgentSecurePort` e defina os respectivos valores.

Para atualizar `essbase.cfg`:

1. Copie o Oracle Wallet com certificados para ServidorEssbase para `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin/wallet`. Este é o único local do Oracle Wallet aceitável para o Servidor Essbase.
2. Usando um editor de texto, abra `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin/essbase.cfg`.
3. Insira as configurações conforme a necessidade. As configurações padrão do Essbase estão implícitas. Se precisar alterar o comportamento padrão, adicione as configurações para o comportamento personalizado em `essbase.cfg`. Por exemplo, `EnableClearMode` é aplicado por padrão, pelo qual o Servidor do Essbase é habilitado para se comunicar pelo canal não criptografado. Para desativar a capacidade do Servidor do Essbase de se comunicar pelo canal não criptografado, você deve especificar `EnableClearMode FALSE` em `essbase.cfg`. Consulte a tabela a seguir.

Tabela 2-2 Configurações de SSL do Essbase

Configuração	Descrição ¹
EnableClearMode ²	Habilita a comunicação não criptografada entre os aplicativos do Essbase e o Agente do Essbase. Se essa propriedade for definida como FALSE, o Essbase não tratará das solicitação não SSL. Padrão: EnableClearMode TRUE Exemplo: EnableClearMode FALSE
EnableSecureMode	Habilita a comunicação criptografada por SSL entre os clientes do Essbase e o Agente do Essbase. Essa propriedade deve ser definida como TRUE para dar suporte ao SSL. Padrão: FALSE Exemplo: EnableSecureMode TRUE
SSLCipherSuites	Uma lista de conjuntos de cifras, em ordem de preferência, a serem usados na comunicação SSL. O Agente do Essbase usa um desses conjuntos de cifras para comunicação SSL. O primeiro conjunto de cifras na lista recebe a prioridade mais alta quando o agente escolhe um conjunto de cifras. Padrão: SSL_RSA_WITH_RC4_128_MD5 Exemplo: SSLCipherSuites SSL_RSA_WITH_AES_256_CBC_SHA256,SSL_RSA_WITH_AES_256_GCM_SHA384
APSRESOLVER	URL do Oracle Hyperion Provider Services. Se você estiver usando vários servidores do Provider Services, separe cada URL usando um ponto-e-vírgula. Exemplo: APSRESOLVER https:// exampleAPShost1:PORT/aps;https:// exampleAPShost2:PORT/aps
AgentSecurePort	A porta segura na qual o agente escuta. Padrão: 6423 Exemplo: AgentSecurePort 16001
WalletPath	Local do Oracle Wallet (menos de 1.024 caracteres) que armazena o certificado da CA raiz e o certificado assinado. Padrão: ARBORPATH/bin/wallet Exemplo: WalletPath/usr/local/wallet
ClientPreferredMode ³	O modo (Seguro ou Limpeza) para a sessão do cliente. Se essa propriedade for definida como Segura, o modo SSL será usado para todas as sessões. Se essa propriedade for definida como Limpar, o transporte será escolhido com base no fato de a solicitação de logon do cliente conter a palavra-chave de transporte seguro. Consulte Como Estabelecer uma Conexão SSL por Sessão . Padrão: CLEAR Exemplo: ClientPreferredMode SECURE

Tabela 2-2 (Cont.) Configurações de SSL do Essbase

Configuração	Descrição ¹
	¹ O valor padrão será imposto se estas propriedades não estiverem disponíveis em <code>essbase.cfg</code> .
	² O Essbase vai parar de funcionar se <code>EnableClearMode</code> e <code>EnableSecureMode</code> forem definidas como <code>FALSE</code> .
	³ Os clientes usam essa configuração para determinar se eles devem estabelecer uma conexão segura ou não segura com o Essbase.

4. Salve e feche `essbase.cfg`.

Atualização de Nós Essbase Distribuídos para SSL



Nota:

Esta seção se aplica apenas à implantação distribuída do Essbase

Certifique-se de que a pasta `Wallet` (por exemplo, `WalletPath/usr/local/wallet`) que contém o certificado de CA raiz e o certificado assinado esteja na localização exigida em cada nó distribuído.

1. Copie a pasta `Wallet` para essas localizações em cada nó distribuído:
 - `EPM_ORACLE_HOME/common/EssbaseRTC/11.1.2.0/bin`
 - `EPM_ORACLE_HOME/common/EssbaseRTC-64/11.1.2.0/bin`
2. Copie a pasta `Wallet` para essas localizações, se presentes, em cada nó distribuído:
 - `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` para estas localizações em cada nó distribuído:
 - `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` para estas localizações, se presentes, em cada nó distribuído:
 - `EPM_ORACLE_HOME/products/Essbase/EssbaseServer/bin`
 - `EPM_ORACLE_HOME/products/Essbase/EssbaseServer-32/bin`
 - `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin`
5. Copie a pasta `Wallet` para essas localizações de instalação cliente Essbase em cada nó distribuído:
 - `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` para estas localizações de instalação cliente Essbase em cada nó distribuído:

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

7. Adicione estas propriedades ao arquivo `essbase.properties`:

- `essbase.ssleverywhere=true`
- `olap.server.ssl.alwaysSecure=true`
- `APSRESOLVER=http[s]://host:httpsPort/aps`
Esteja certo de substituir este valor pelo URL apropriado.

É preciso atualizar o arquivo `essbase.properties` nestas localizações, se presentes, em cada nó distribuído:

- `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` para o diretório `EPM_ORACLE_HOME/products/Essbase/eas`, se disponível, em cada nó distribuído.

9. **Apenas Para Oracle Hyperion Planning:** Adicione estas três propriedades ao arquivo `essbase.properties`:

- `essbase.ssleverywhere=true`
- `olap.server.ssl.alwaysSecure=true`
- `APSRESOLVER=APS_URL`
Substitua `APS_URL` pelo URL do Provider Services. Se você estiver usando vários servidores do Provider Services, separe cada URL usando um ponto-e-vírgula. Por exemplo, `https://exampleAPShost1:PORT/aps;https://exampleAPShost2:PORT/aps`.

É preciso atualizar o arquivo `essbase.properties` nestas localizações em cada nó distribuído:

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

10. **Apenas Para Oracle Hyperion Financial Reporting:** Adicione estas três propriedades ao arquivo `EPM_ORACLE_HOME/products/financialreporting/bin/EssbaseJAPI/bin/essbase.properties`:

- `essbase.ssleverywhere=true`
- `olap.server.ssl.alwaysSecure=true`
- `APSRESOLVER=APS_URL`
Substitua `APS_URL` pelo URL do Provider Services. Se você estiver usando vários servidores do Provider Services, separe cada URL usando um ponto-e-vírgula. Por exemplo, `https://exampleAPShost1:PORT/aps;https://exampleAPShost2:PORT/aps`.

 **Nota:**

Em ambientes SSL completos, o Financial Reporting requer o Nome de Cluster do Essbase para estabelecer uma conexão. As conexões falharão se o nome do host for usado para conectar.

11. a. Defina as variáveis de ambiente:
 - **Windows:** Crie uma nova variável de sistema chamada `API_DISABLE_PEER_VERIFICATION` e defina seu valor para 1.
 - **Linux:** Adicione a diretiva `API_DISABLE_PEER_VERIFICATION=1` em `setCustomParamsPlanning.sh`.
- b. Adicione a diretiva `API_DISABLE_PEER_VERIFICATION=1` em `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin/setEssbaseenv.bat` Or `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin/setEssbaseenv.sh`.

Defina variáveis de ambiente:

Personalização das Propriedades de SSL para Clientes JAPI

Várias propriedades padrão são predefinidas para os componentes do Essbase que dependem da JAPI. As propriedades padrão podem ser substituídas, incluindo as propriedades em `essbase.properties`.

 **Nota:**

Somente algumas das propriedades de SSL identificadas na tabela a seguir são externalizadas em `essbase.properties`. Você deve adicionar as propriedades que não são externalizadas.

Para atualizar as propriedades SSL dos clientes JAPI:

1. Usando um editor de texto, abra `EPM_ORACLE_HOME/common/EssbaseJavaAPI/11.1.2.0/bin/essbase.properties`.
2. Atualize as propriedades conforme a necessidade. Consulte a tabela a seguir para ver uma descrição das propriedades personalizáveis do cliente JAPI. Se uma propriedade desejada não estiver incluída em `essbase.properties`, adicione-a.

Tabela 2-3 Propriedades SSL padrão para Clientes JAPI

Propriedade	Descrição
<code>olap.server.ssl.alwaysSecure</code>	Define o modo que os clientes devem ser usados em todas as instâncias do Essbase. Altere o valor dessa propriedade para <code>true</code> a fim impor o modo SSL. Padrão: <code>false</code>
<code>olap.server.ssl.securityHandler</code>	Nome do pacote para tratamento de protocolo. Você pode alterar esse valor para indicar outro manipulador. Padrão: <code>java.protocol.handler.pkgs</code>

Tabela 2-3 (Cont.) Propriedades SSL padrão para Clientes JAPI

Propriedade	Descrição
<code>olap.server.ssl.securityProvider</code>	A Oracle usa a implementação do protocolo SSL do Sun. Você pode alterar esse valor para indicar outro provedor. Padrão: <code>com.sun.net.ssl.internal.www.protocol</code>
<code>olap.server.ssl.supportedCiphers</code>	Uma lista de cifras adicionais separadas por vírgula a serem habilitadas para comunicação segura. É preciso especificar somente cifras que são aceitas pelo Essbase. Exemplo: <code>SSL_RSA_WITH_AES_256_CBC_SHA256,SSL_RSA_WITH_AES_256_GCM_SHA384</code>
<code>olap.server.ssl.trustManagerClass</code>	A classe <code>TrustManager</code> a ser usada para validar o certificado SSL verificando a assinatura e a data de expiração do certificado. Por padrão, essa propriedade não é definida para impor todas as confirmações de verificação. Para não impor confirmações de verificação, defina o valor desse parâmetro para <code>com.essbase.services.olap.security.EssDefaultTrustManager</code> , que é a classe <code>TrustManager</code> padrão que permite que todas as verificações de validação sejam bem-sucedidas. Para implementar um <code>TrustManager</code> personalizado, especifique um nome de classe totalmente qualificado da classe <code>TrustManager</code> que implementa a interface <code>javax.net.ssl.X509TrustManager</code> . Exemplo: <code>com.essbase.services.olap.security.EssDefaultTrustManager</code>

3. Salve e feche `essbase.properties`.
4. Reinicie todos os componentes do Essbase.

Como Estabelecer uma Conexão SSL por Sessão

Os componentes do Oracle Essbase, por exemplo, MaxL, podem controlar o SSL no nível de sessão conectando-se ao Agente do Essbase usando `secure` como a palavra-chave de transporte. Por exemplo, você pode estabelecer uma conexão segura entre o MaxL e o Agente do Essbase executando um dos seguintes comandos em um Console do MaxL:

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

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

O controle por sessão tem prioridade sobre as definições de configuração especificadas em `essbase.cfg`. Se nenhuma palavra-chave de transporte for especificada, os clientes do Essbase usarão o valor definido para `ClientPreferredMode` a fim de determinar se deve ser iniciada uma conexão segura com o Essbase. Se a configuração `ClientPreferredMode` não for definida para `secure`, a comunicação ocorrerá por um canal não seguro.

SSL para Essbase 21c

Visão Geral

Esta seção explica os procedimentos para substituir os certificados padrão usados para proteger a comunicação entre uma instância do Oracle Essbase e componentes como MaxL, Servidor do Oracle Essbase Administration Services, Oracle Hyperion Provider Services, Oracle Hyperion Foundation Services, Oracle Hyperion Planning, Oracle Hyperion Financial Management e Oracle Hyperion Shared Services Registry.

Nota:

O Essbase Administration Services (EAS) Lite não usa a porta do HTTP Server SSL (443, por exemplo) configurada com o EPM Configurator. O URL seguro no arquivo `easconsole.jnlp` é definido como a porta não-SSL (80) como padrão.

Solução alternativa: Substitua a porta não-SSL padrão no URL seguro identificado em `easconsole.jnlp` pelo URL seguro atualizado:

URL Seguro Padrão: `https://myserver:SECURE_PORT/easconsole/console.html`.
Por exemplo: `https://myserver:80/easconsole/console.html`

URL Seguro Atualizado: `https://myserver:SECURE_PORT/easconsole/console.html`. Por exemplo: `https://myserver:443/easconsole/console.html`

Veja o artigo do My Oracle Support (MOS) - [Doc ID 1926558.1 - Porta SSL Não Inclusa em easconsole.jnlp do Console Web do EAS](#) para mais informações.

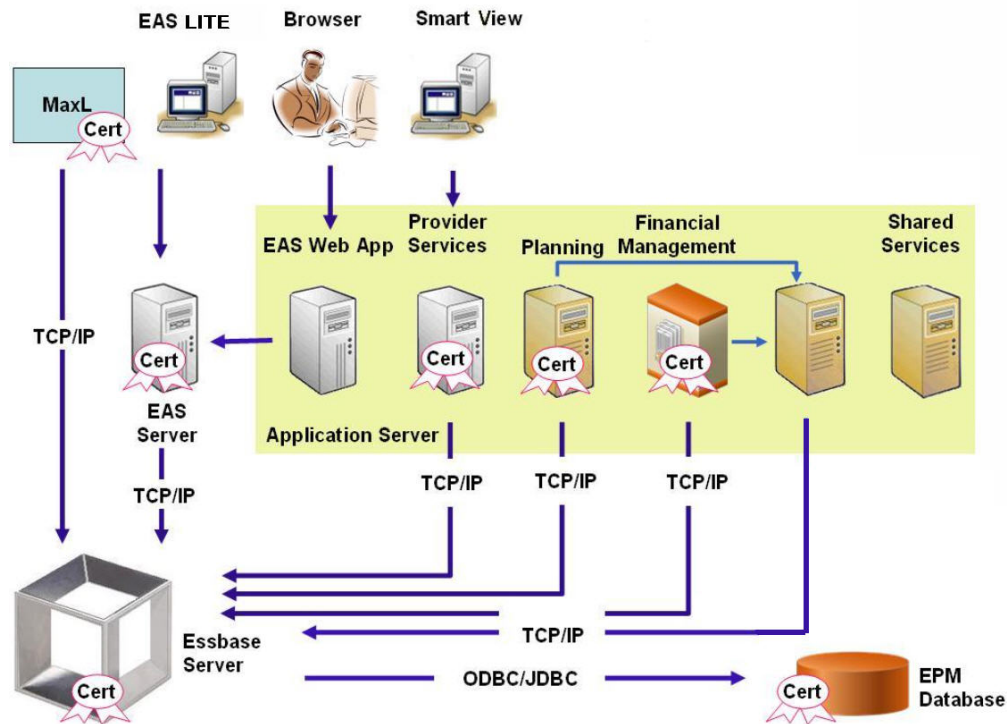
Implantação Padrão

O Essbase pode ser implantado para funcionar nos modos de SSL e não SSL. O Agente do Essbase escuta em uma porta não segura; ele também pode ser configurado para escutar em uma porta segura. Todas as conexões que acessam a porta segura são tratadas como conexões SSL. Se um cliente se conectar ao Agente do Essbase na porta não SSL, a conexão será tratada como uma conexão não SSL. Os componentes podem estabelecer conexões simultâneas não SSL e SSL com um Agente do Essbase.

Você não pode controlar o SSL por sessão especificando o protocolo seguro e a porta quando faz login. Consulte [Como Estabelecer uma Conexão SSL por Sessão](#).

Se o SSL estiver habilitado, toda a comunicação em uma instância do Essbase será criptografada para garantir a segurança de dados.

As implantações padrão dos componentes do Essbase no modo seguro usam certificados autoassinados para habilitar a comunicação SSL, basicamente para fins de teste. A Oracle recomenda usar certificados de CAs de terceiros reconhecidas a fim de habilitar para SSL o Essbase em ambientes de produção.



Normalmente, um Oracle Wallet armazena o certificado que habilita a comunicação SSL com clientes que usam o Essbase RTC e um keystore Java armazena o certificado que habilita a comunicação SSL com componentes que utilizam JAPI para comunicação. Para estabelecer comunicação SSL, os clientes e ferramentas do Essbase armazenam o certificado raiz da CA que assinou os certificados do Servidor e Agente do Essbase.

Certificados Necessários e Respetivo Local

A Oracle recomenda o uso de certificados de CAs de terceiros reconhecidas de modo a habilitar para SSL o Essbase em um ambiente de produção. Você pode usar os certificados autoassinados padrão para teste.

Nota:

O Essbase dá suporte ao uso de certificados curinga, que podem proteger vários subdomínios com um certificado SSL. Usar um certificado curinga pode reduzir o tempo e o custo de gerenciamento.

Os certificados curinga não poderão ser usados se a verificação do nome do host for habilitada.

Exija os seguintes certificados:

- Um certificado da CA raiz.
Os componentes que usam o Essbase RTC para estabelecer uma conexão com o Essbase exigem que o certificado da CA raiz seja armazenado em um Oracle Wallet. Os componentes que usam JAPI para estabelecer uma conexão exigem

que o certificado da CA raiz seja armazenado em um keystore Java. Os certificados necessários e seus locais são indicados na tabela a seguir.

 **Nota:**

Talvez você não precise instalar um certificado da CA raiz se estiver usando certificados de uma CA de terceiros reconhecida cujo certificado raiz já está instalado no Oracle Wallet.

- Certificado assinado para o Servidor do Essbase e o Agente do Essbase.

Tabela 2-4 Certificados Necessários e Respetivos Locais

Componente ¹	Keystore	Certificado ²
MaxL	Oracle Wallet	Certificado da CA raiz
Servidor do Administration Services	Oracle Wallet	Certificado da CA raiz
Provider Services	Oracle Wallet	Certificado da CA raiz
Banco de Dados do Oracle Enterprise Performance Management System	Oracle Wallet	Certificado da CA raiz
Planning	<ul style="list-style-type: none"> • Oracle Wallet • Keystore Java 	Certificado da CA raiz
Financial Management	Keystore Java	Certificado da CA raiz
Essbase (Servidor e Agente) ³	<ul style="list-style-type: none"> • Oracle Wallet • Keystore Java 	<ul style="list-style-type: none"> • Certificado da CA raiz • Certificado assinado para o Servidor e Agente do Essbase

Repositório do Oracle Hyperion Shared Services

¹ Você precisa apenas de uma instância do keystore para dar suporte a vários componentes que usam um keystore semelhante.

² Vários componentes podem usar um certificado raiz instalado em um keystore.

³ Os certificados devem ser instalados no Oracle Wallet padrão e no keystore Java.

Instalação e Implantação de Componentes do Essbase

O processo de configuração permite que você selecione uma porta de agente segura (o padrão é 6423), que você pode alterar ao configurar o Oracle Essbase. Por padrão, o processo de implantação instala os certificados autoassinados necessários para criar uma implantação funcional segura para teste.

O EPM System Installer instala um Wallet Oracle e um certificado autoassinado em `ARBOR_PATH` na máquina que hospeda a instância do Essbase se o Oracle HTTP Server estiver instalado. Em implantações de único host, todos os componentes do Essbase compartilham esse certificado.

Uso de Certificados da CA de Terceiros Confiáveis para Essbase

Criação de Solicitações de Certificado e Obtenção de Certificados

Gere uma solicitação de certificado a fim de obter um certificado para o servidor que hospeda o Servidor do Oracle Essbase e Agente do Essbase. Uma solicitação de certificado contém informações criptografadas específicas ao Nome Comum (CN=) do seu servidor. Você envia a solicitação de certificado para uma autoridade de autenticação a fim de obter um certificado SSL.

Você usa uma ferramenta como o keytool ou o Oracle Wallet Manager para criar uma solicitação de certificado. Para obter informações detalhadas sobre como criar uma solicitação de certificado, veja a documentação para a ferramenta que você está usando.

Exemplos usando keytool:

Crie uma Java Keystore (JKS) e gere uma chave privada:

```
keytool.exe -genkey -dname "cn=myserver, ou=EPM, o=Oracle, c=US"
-alias essbase_ssl -keypass password -keystore
C:\oracle\Middleware\EPMSysstem11R1\ssl\EPM.JKS -storepass password
-validity 365 -keyalg RSA -keysize 2048 -sigalg SHA256withRSA -noprompt
```

Gere uma solicitação de certificado:

```
keytool -certreq -alias essbase_ssl -file
C:\oracle\Middleware\EPMSysstem11R1\ssl\essbase_server.csr -keypass
password
-keystore C:\oracle\Middleware\EPMSysstem11R1\ssl\EPM.JKS -storepass
password
```

Exporte a sua chave privada (requer o utilitário openssl):

1. openssl.exe pkcs12 -in C:\oracle\Middleware\EPMSysstem11R1\ssl\EPM.JKS -passin pass:password -legacy -nocerts -out c:\Apache24\ssl\Apache24.key -passout pass:password
2. Assine a Solicitação de Certificado que você acabou de gerar usando a sua CA (Autoridade de Certificação) e cole-a no seguinte arquivo:
C:\oracle\Middleware\EPMSysstem11R1\ssl\essbase.cer.

Obtenção e Instalação do Certificado da CA Raiz

O certificado da CA raiz verifica a validade do certificado que é usado para dar suporte ao SSL. Ele contém a chave pública em relação à qual a chave privada que foi usada para assinar o certificado é compatível para verificar o certificado. É possível obter o certificado da CA raiz da autoridade de certificação que assinou seus certificados SSL.

Instale o certificado raiz da CA que assinou o certificado do Servidor do Essbase em clientes que se conectam ao Servidor ou Agente do Essbase. Certifique-se de que o certificado raiz seja instalado no keystore apropriado para o cliente. Consulte [Certificados Necessários e Respetivo Local](#) .

 **Nota:**

Vários componentes podem usar um certificado de CA raiz instalado em uma máquina de servidor.

Instalação de Certificados Assinados por CA

Para saber como Instalar Certificados Assinados por CA, veja os links a seguir:

- [Configuração de Conexão TLS do Weblogic para Essbase](#)
- [Atualização de Certificados TLS](#)

Atualize o arquivo `tls.properties` em

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

Em que:

```
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.
```

Execute o seguinte para atualizar o servidor do Essbase com os novos 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
```

Atualização das Configurações de SSL do Essbase

Você personaliza as configurações de SSL para Servidor e clientes do Essbase especificando o valor para o seguinte em `essbase.cfg`.

- Configuração para habilitar o modo seguro
- Configuração para habilitar o modo de limpeza
- Modo preferencial para comunicação com clientes (usado apenas pelos clientes)
- Porta segura
- Conjuntos de cifras
- Caminho do Oracle Wallet

 **Nota:**

Em `essbase.cfg`, certifique-se de adicionar todos os parâmetros necessários ausentes, especialmente, `EnableSecureMode`, `AgentSecurePort` e defina os respectivos valores.

Para atualizar `essbase.cfg` localizado em:

`ESSBASE_DOMAIN_HOME\config\fmwconfig\essconfig\essbase`

1. Insira as configurações conforme a necessidade. As configurações padrão do Essbase estão implícitas. Se precisar alterar o comportamento padrão, adicione as configurações para o comportamento personalizado em `essbase.cfg`. Por exemplo, `EnableClearMode` é aplicado por padrão, pelo qual o Servidor do Essbase é habilitado para se comunicar pelo canal não criptografado. Para desativar a capacidade do Servidor do Essbase de se comunicar pelo canal não criptografado, você deve especificar `EnableClearMode FALSE` em `essbase.cfg`. Consulte a tabela a seguir:

Tabela 2-5 Configurações de SSL do Essbase

Configuração	Descrição ¹
<code>EnableClearMode</code> ²	Habilita a comunicação não criptografada entre os aplicativos do Essbase e o Agente do Essbase. Se essa propriedade for definida como <code>FALSE</code> , o Essbase não tratará das solicitações não SSL. Padrão: <code>EnableClearMode TRUE</code> Exemplo: <code>EnableClearMode FALSE</code>
<code>EnableSecureMode</code>	Habilita a comunicação criptografada por SSL entre os clientes do Essbase e o Agente do Essbase. Essa propriedade deve ser definida como <code>TRUE</code> para dar suporte ao SSL. Padrão: <code>FALSE</code> Exemplo: <code>EnableSecureMode TRUE</code>
<code>SSLCipherSuites</code>	Uma lista de conjuntos de cifras, em ordem de preferência, a serem usados na comunicação SSL. O Agente do Essbase usa um desses conjuntos de cifras para comunicação SSL. O primeiro conjunto de cifras na lista recebe a prioridade mais alta quando o agente escolhe um conjunto de cifras. Padrão: <code>SSL_RSA_WITH_RC4_128_MD5</code> Exemplo: <code>SSLCipherSuites SSL_RSA_WITH_AES_256_CBC_SHA256,SSL_RSA_WITH_</code> <code>AES_256_GCM_SHA384</code>
<code>APRESOLVER</code>	URL do Oracle Hyperion Provider Services. Se você estiver usando vários servidores do Provider Services, separe cada URL usando um ponto-e-vírgula. Exemplo: <code>https://exampleAPShost1:PORT/</code> <code>essbase;https://exampleAPShost2:PORT/essbase</code>

Tabela 2-5 (Cont.) Configurações de SSL do Essbase

Configuração	Descrição ¹
AgentSecurePort	A porta segura na qual o agente escuta. Padrão: 6423 Exemplo: AgentSecurePort 16001
WalletPath	Local do Oracle Wallet (menos de 1.024 caracteres) que armazena o certificado da CA raiz e o certificado assinado. Padrão: ARBORPATH/bin/wallet Exemplo: WalletPath/usr/local/wallet
ClientPreferredMode ³	O modo (Seguro ou Limpeza) para a sessão do cliente. Se essa propriedade for definida como Segura, o modo SSL será usado para todas as sessões. Se essa propriedade for definida como Limpar, o transporte será escolhido com base no fato de a solicitação de logon do cliente conter a palavra-chave de transporte seguro. Consulte Como Estabelecer uma Conexão SSL por Sessão . Padrão: CLEAR Exemplo: ClientPreferredMode SECURE

- ¹ O valor padrão será imposto se estas propriedades não estiverem disponíveis em `essbase.cfg`.
- ² O Essbase vai parar de funcionar se `EnableClearMode` e `EnableSecureMode` forem definidas como `FALSE`.
- ³ Os clientes usam essa configuração para determinar se eles devem estabelecer uma conexão segura ou não segura com o Essbase.

2. Salve e feche `essbase.cfg`.

Atualização de Nós Essbase Distribuídos para SSL



Nota:

Esta seção se aplica apenas à implantação distribuída do Essbase

Certifique-se de que a pasta Wallet (por exemplo, `WalletPath/usr/local/wallet`) que contém o certificado de CA raiz e o certificado assinado esteja na localização exigida em cada nó distribuído.

1. Importe todos os novos certificados de CA usando ferramentas TLS.

Para mais informações, consulte os seguintes links:

- [Configuração de Conexão TLS do Weblogic para Essbase](#)
- [Atualização de Certificados TLS](#)

2. Acesse o local de origem: `ESSBASE_DOMAIN_HOME\config\fmwconfig\essconfig\essbase` e modifique as seguintes propriedades no arquivo `essbase.properties`:

- `essbase.ssleverywhere=true`
- `olap.server.ssl.alwaysSecure=true`

- `APSRESOLVER=APS_URL`
Substitua `APS_URL` pelo URL do Provider Services. Se você estiver usando vários servidores do Provider Services, separe cada URL usando um ponto-e-vírgula.

`https://exampleAPShost1:PORT/essbase;https://exampleAPShost2:PORT/essbase.`

3. Copie a pasta `Wallet`, a pasta `Walletssl`, o arquivo `essbase.cfg` e o arquivo `essbase.properties` para os seguintes caminhos de destino.

Tabela 2-6 Caminhos de Destino

Caminhos de Destino	Walle t	Walle tssl	essb ase.c fg	essbas e. properti es
<code>EPM_ORACLE_HOME\common\EssbaseRTC-21C\11.1.2.0\bin</code>	Sim	Sim	Sim	Sim
<code>EPM_ORACLE_HOME\common\EssbaseJavaAPI-21C\11.1.2.0\bin</code>	Sim	Sim	Sim	Sim
<code>ESSBASE_DOMAIN_HOME\config\fmwconfig\essconfig\aps</code>	Sim	Sim	Sim	Sim
<code>ESSBASE_DOMAIN_HOME\config\fmwconfig\essconfig\essbase</code>	Sim	Sim	Sim	Sim
<code>MIDDLEWARE_HOME\essbase\products\Essbase\template_files\essbase</code>	Sim	Sim	Sim	Sim
<code>MIDDLEWARE_HOME\essbase\products\Essbase\EssbaseServer\bin</code>	Sim	Sim	Sim	Sim
<code>MIDDLEWARE_HOME\essbase\products\Essbase\aps\bin</code>	Sim	Sim	Sim	Sim
<code>MIDDLEWARE_HOME\essbase\products\Essbase\ea s</code>	Sim	Sim	Sim	Sim
<code>MIDDLEWARE_HOME\essbase\common\EssbaseJavaA PI\bin</code>	Sim	Sim	Sim	Sim
Somente para Oracle Hyperion Financial Reporting <code>EPM_ORACLE_HOME/products/ financialreporting/bin/EssbaseJAPI/bin/</code> Observação: Em ambientes SSL completos, o Financial Reporting requer o Nome de Cluster do Essbase para estabelecer uma conexão. As conexões falharão se o nome do host for usado para conectar.	Sim	Sim	Sim	Sim
Somente para Oracle Hyperion Planning <code>EPM_ORACLE_HOME/products/Planning/config/ EPM_ORACLE_HOME/products/Planning/lib/</code>	Sim	Sim	Sim	Sim

4. Defina as variáveis de ambiente:

- **Windows:** Crie uma nova variável de sistema chamada `API_DISABLE_PEER_VERIFICATION` e defina seu valor para 1.
- **Linux:** Adicione a diretiva `API_DISABLE_PEER_VERIFICATION=1` em `setCustomParamsPlanning.sh`.

Personalização das Propriedades de SSL para Clientes JAPI

Várias propriedades padrão são predefinidas para os componentes do Essbase que dependem da JAPI. As propriedades padrão podem ser substituídas, incluindo as propriedades em `essbase.properties`.



Nota:

Somente algumas das propriedades de SSL identificadas na tabela a seguir são externalizadas em `essbase.properties`. Você deve adicionar as propriedades que não são externalizadas.

Para atualizar as propriedades SSL dos clientes JAPI:

1. Usando um editor de texto, abra `EPM_ORACLE_HOME/common/EssbaseJavaAPI-21C/11.2.0/bin/essbase.properties`.
2. Atualize as propriedades conforme a necessidade. Consulte a tabela a seguir para ver uma descrição das propriedades personalizáveis do cliente JAPI. Se uma propriedade desejada não estiver incluída em `essbase.properties`, adicione-a.

Tabela 2-7 Propriedades SSL padrão para Clientes JAPI

Propriedade	Descrição
<code>olap.server.ssl.alwaysSecure</code>	Define o modo que os clientes devem ser usados em todas as instâncias do Essbase. Altere o valor dessa propriedade para <code>true</code> a fim impor o modo SSL. Padrão: <code>false</code>
<code>olap.server.ssl.securityHandler</code>	Nome do pacote para tratamento de protocolo. Você pode alterar esse valor para indicar outro manipulador. Padrão: <code>java.protocol.handler.pkgs</code>
<code>olap.server.ssl.securityProvider</code>	A Oracle usa a implementação do protocolo SSL do Sun. Você pode alterar esse valor para indicar outro provedor. Padrão: <code>com.sun.net.ssl.internal.www.protocol</code>
<code>olap.server.ssl.supportedCiphers</code>	Uma lista de cifras adicionais separadas por vírgula a serem habilitadas para comunicação segura. É preciso especificar somente cifras que são aceitas pelo Essbase. Exemplo: <code>SSL_RSA_WITH_AES_256_CBC_SHA256,SSL_RSA_WITH_AES_256_GCM_SHA384</code>

Tabela 2-7 (Cont.) Propriedades SSL padrão para Clientes JAPI

Propriedade	Descrição
<code>olap.server.ssl.trustManagerClass</code>	<p>A classe <code>TrustManager</code> a ser usada para validar o certificado SSL verificando a assinatura e a data de expiração do certificado.</p> <p>Por padrão, essa propriedade não é definida para impor todas as confirmações de verificação.</p> <p>Para não impor confirmações de verificação, defina o valor desse parâmetro para <code>com.essbase.services.olap.security.EssDefaultTrustManager</code>, que é a classe <code>TrustManager</code> padrão que permite que todas verificações de validação sejam bem-sucedidas.</p> <p>Para implementar um <code>TrustManager</code> personalizado, especifique um nome de classe totalmente qualificado da classe <code>TrustManager</code> que implementa a interface <code>javax.net.ssl.X509TrustManager</code>.</p> <p>Exemplo:<code>com.essbase.services.olap.security.EssDefaultTrustManager</code></p>

3. Salve e feche `essbase.properties`.
4. Reinicie todos os componentes do Essbase.

Como Estabelecer uma Conexão SSL por Sessão

Os componentes do Oracle Essbase, por exemplo, MaxL, podem controlar o SSL no nível de sessão conectando-se ao Agente do Essbase usando `secure` como a palavra-chave de transporte. Por exemplo, você pode estabelecer uma conexão segura entre o MaxL e o Agente do Essbase executando um dos seguintes comandos em um Console do MaxL:

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

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

O controle por sessão tem prioridade sobre as definições de configuração especificadas em `essbase.cfg`. Se nenhuma palavra-chave de transporte for especificada, os clientes do Essbase usarão o valor definido para `ClientPreferredMode` a fim de determinar se deve ser iniciada uma conexão segura com o Essbase. Se a configuração `ClientPreferredMode` não for definida para `secure`, a comunicação ocorrerá por um canal não seguro.

3

Habilitação do SSO com Agentes de Segurança

Consulte Também:

- [Métodos de SSO Suportados](#)
- [Logon Único no Oracle Access Manager](#)
- [OracleAS Single Sign-on](#)
- [Proteção de Produtos EPM System para SSO](#)
- [SSO baseado em Cabeçalho com Produtos de Gerenciamento de Identidades](#)
- [Configuração do EPM System para SSO baseado em Cabeçalho com o Oracle Identity Cloud Services](#)
- [SiteMinder SSO](#)
- [Logon Único Kerberos](#)
- [Configuração do EPM System para SSO](#)
- [Opções de Logon Único para Smart View](#)

Métodos de SSO Suportados

O SSO requer que a solução de gerenciamento de identidade na Web passe o nome de logon dos usuários autenticados nos produtos Oracle Enterprise Performance Management System. É possível usar os seguintes métodos padrão do EPM System para integrar o EPM System a soluções SSO baseadas na Web personalizadas e comerciais.

- [Cabeçalho HTTP](#)
- [Classe de Logon Personalizada](#)
- [Cabeçalho de Autorização HTTP](#)
- [Obter Usuário Remoto de uma Solicitação HTTP](#)
- [Autenticação baseada em Cabeçalho com Produtos de Gerenciamento de Identidades](#)

▲ Cuidado:

Como uma medida de segurança, a Oracle recomenda implementar autenticação de certificado de cliente (SSL bidirecional) entre o servidor Web e o servidor de aplicativos se sua organização usar métodos que carreguem a identidade de usuário no cabeçalho para propagação de identidade.

Cabeçalho HTTP

Se você estiver usando o Oracle Single Sign-on (OSSO), SiteMinder ou Oracle Access Manager como a solução de gerenciamento de identidade na Web, a segurança do EPM System selecionará automaticamente o cabeçalho HTTP personalizado para passar o nome de logon dos usuários autenticados para os componentes do EPM System.

O nome de logon de um usuário do produto EPM System é determinado pelo `Login Attribute` especificado durante a configuração dos diretórios de usuários no Oracle Hyperion Shared Services. Consulte o tópico sobre configuração do OID, Active Directory e outros diretórios baseados em LDAP no *Guia de Administração da Segurança de Usuário do Sistema Oracle Enterprise Performance Management* para obter uma breve descrição de `Login Attribute`.

O cabeçalho HTTP deve conter o valor do atributo definido como o `Atributo de Logon`. Por exemplo, se `uid` for o valor do `Login Attribute`, o cabeçalho HTTP deverá carregar o valor do atributo `uid`.

Consulte a documentação da sua solução de gerenciamento de identidade na Web para obter informações detalhadas sobre a definição e emissão de cabeçalhos HTTP personalizados.

A segurança do EPM System analisa o cabeçalho HTTP e valida o nome de logon que ele carrega nos diretórios de usuários configurados no Shared Services.

Classe de Logon Personalizada

Quando um usuário faz logon, a solução de gerenciamento de identidade na Web autentica o usuário em um servidor de diretório e encapsula as credenciais do usuário autenticado em um mecanismo SSO para habilitar o SSO com sistemas downstream. Se a solução de gerenciamento de identidade na Web usar um mecanismo sem suporte dos produtos EPM System ou se o valor de `Login Attribute` não estiver disponível no mecanismo SSO, você poderá usar uma classe de logon personalizada para derivar e passar o valor de `Login Attribute` aos produtos EPM System.

Usar uma classe de logon personalizada permite que o EPM System integre-se aos agentes de segurança que usam autenticação baseada em certificado X509. Usar esse mecanismo de autenticação requer a implementação de APIs padrão do Shared Services para definir a interface de SSO entre os componentes do EPM System e a solução de gerenciamento de identidade na Web. A classe de logon personalizada deverá passar o valor do `Atributo de Logon` aos produtos EPM System. Consulte o tópico sobre configuração do OID, Active Directory e outros diretórios de usuários baseados em LDAP no *Guia de Administração da Segurança de Usuário do Sistema Oracle Enterprise Performance Management* para obter uma breve descrição de `Login Attribute`. Para obter um código de exemplo e as etapas de implementação, consulte [Implementação de uma Classe de Logon Personalizada](#).

Para usar uma classe de logon personalizada (o nome padrão é `com.hyperion.css.sso.agent.X509CertificateSecurityAgentImpl`), uma implementação da interface `com.hyperion.css.CSSSecurityAgentIF` deverá estar disponível no classpath. `CSSSecurityAgentIF` define o método `getter` para recuperar o nome de usuário e senha (opcional). Se a interface retornar uma senha nula, a autenticação de segurança tratará o provedor como confiável e verificará a existência do usuário nos provedores configurados. Se a interface retornar um valor não nulo

para a senha , o EPM System tentará autenticar a solicitação usando o nome de usuário e a senha retornados por esta implementação.

CSSSecurityAgentIF engloba dois métodos: `getUserName` e `getPassword`.

Método `getUserName`

Este método retorna o nome de usuário para autenticação.

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

O parâmetro `req` identifica a solicitação HTTP que carrega as informações usadas para determinar o nome de usuário. O parâmetro `res` não é utilizado (predefinido para compatibilidade com versões anteriores).

Método `getPassword`

Esse método retorna uma senha de texto não criptografado para autenticação. A recuperação da senha é opcional.

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

O parâmetro `req` identifica a solicitação HTTP que transmite as informações que são usadas para determinar a senha. O parâmetro `res` não é utilizado (predefinido para compatibilidade com versões anteriores).

Cabeçalho de Autorização HTTP

A segurança do EPM System dá suporte ao uso de um cabeçalho de autorização HTTP para passar valor de `Login Attribute` aos produtos EPM System das soluções de gerenciamento de identidade na Web. Os produtos EPM System analisam o cabeçalho da autorização para recuperar o nome de logon do usuário.

Obter Usuário Remoto de uma Solicitação HTTP

A segurança do EPM System dá suporte ao uso de uma solicitação HTTP para passar valor de `Login Attribute` aos produtos EPM System das soluções de gerenciamento de identidade na Web. Use esse método SSO se a solução de gerenciamento de identidade na Web passar uma solicitação HTTP contendo o valor de `Login Attribute`, que é definido usando a função `setRemoteUser`.

Autenticação baseada em Cabeçalho com Produtos de Gerenciamento de Identidades

O EPM System oferece suporte a qualquer produto de gerenciamento de identidades, como Oracle Identity Cloud Services, Microsoft Azure AD ou Okta, que permitem a autenticação baseada em cabeçalho. O fluxo de trabalho conceitual ocorre da seguinte forma:

- Um aplicativo do gateway funcionando como proxy reverso protege os componentes do EPM System restringindo o acesso não autenticado à rede.

- O aplicativo do gateway intercepta solicitações HTTP(S) para componentes do EPM System e assegura que o produto de gerenciamento de identidades autentique usuários antes de encaminhar solicitações para componentes do EPM System.
- Ao encaminhar solicitações para componentes do EPM System, o gateway do aplicativo propaga a identidade do usuário autenticado para o componente do EPM System por meio de solicitações de cabeçalho HTTP.

Para oferecer suporte a esse cenário de autenticação, o EPM System deve estar configurado para trabalhar com a identidade do usuário autenticado que é propagada por meio de solicitações de cabeçalho HTTP(S).

Logon Único no Oracle Access Manager

O Oracle Enterprise Performance Management System integra-se ao Oracle Access Manager aceitando um cabeçalho HTTP personalizado (nome padrão `HYPLOGIN`) que contém o valor de atributo do logon. O atributo de logon é definido quando você configura um diretório de usuários externo no Oracle Hyperion Shared Services. Consulte o tópico sobre configuração do OID, Active Directory e outros diretórios de usuários baseados em LDAP no *Guia de Administração da Segurança de Usuário do Sistema Oracle Enterprise Performance Management* para obter uma breve descrição de `Login Attribute`.

É possível usar qualquer nome de cabeçalho que forneça o valor do atributo de logon ao EPM System. Use o nome de cabeçalho ao configurar o Shared Services para SSO no Oracle Access Manager.

O EPM System usa o valor do atributo de logon para autenticar o usuário em um diretório de usuários configurado (nesse caso, o diretório de usuários no qual o Oracle Access Manager autentica usuários) e, em seguida, gerar um token SSO do EPM que habilita o SSO no EPM System. As informações de provisionamento do usuário são verificadas no Native Directory para autorizar o usuário aos recursos do EPM System.

Nota:

O console do Oracle Essbase Administration Services, que é um thick client, não dá suporte ao SSO no Oracle Access Manager.

As informações sobre como configurar o Oracle Access Manager e executar tarefas como configurar o cabeçalho HTTP e domínios de política estão disponíveis na documentação do Oracle Access Manager. Este guia supõe uma implantação funcional do Oracle Access Manager onde você concluiu as seguintes tarefas:

- Configurou os domínios de política necessários para componentes do EPM System
- Configurou um cabeçalho HTTP para passar o valor do atributo de logon ao EPM System
- Protegeu os recursos do EPM System listados em [Recursos a Serem Protegidos](#). As solicitações para acessar recursos protegidos são desafiadas pelo Oracle Access Manager.

- Cancelou a proteção de recursos do EPM System listados em [Recursos a Serem Desprotegidos](#). As solicitações para acessar recursos desprotegidos não são desafiadas pelo Oracle Access Manager.

Para configurar o EPM System para OSSO no Oracle Access Manager:

1. Adicione o diretório de usuários que o Oracle Access Manager usa para autenticar usuários como um diretório de usuários externo no EPM System. Consulte o tópico sobre configuração do OID, Active Directory e outros diretórios de usuários baseados em LDAP no *Guia de Administração da Segurança de Usuário do Sistema Oracle Enterprise Performance Management*.

 **Nota:**

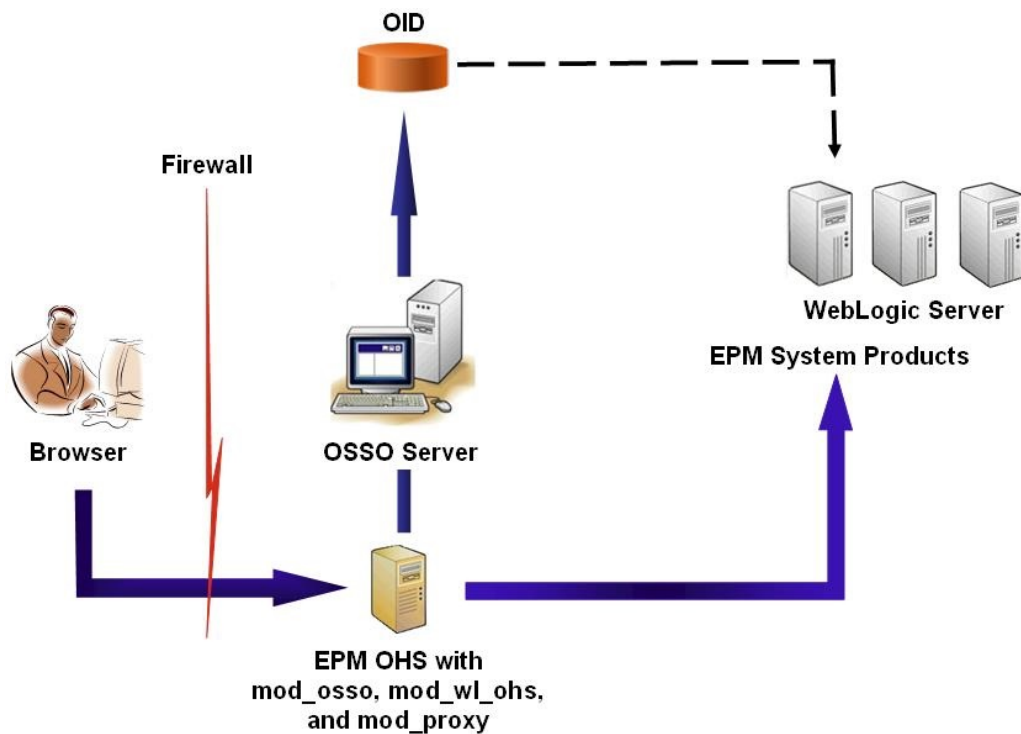
Certifique-se de que a caixa de seleção **Confiável** na tela Informações de Conexão esteja marcada para indicar que o diretório de usuários é uma origem de SSO confiável.

2. Configure o EPM System para SSO. Consulte [Configuração do EPM System para SSO](#).
Selecione Oracle Access Manager na lista **Provedor ou Agente SSO**. Se o cabeçalho HTTP no Oracle Access Manager usar um nome diferente de `HYPLOGIN`, informe o nome do cabeçalho personalizado na caixa de texto ao lado da lista **Mecanismo SSO**.
3. Oracle Data Relationship Management
 - a. Configure o Data Relationship Management para autenticação do Shared Services.
 - b. Habilite o SSO no Console do Data Relationship Management.
Consulte a documentação do Data Relationship Management para obter informações detalhadas.

OracleAS Single Sign-on

A solução OracleAS Single Sign-on (OSSO) fornece acesso SSO aos aplicativos Web usando o Oracle Internet Directory (OID) como o diretório de usuários. Os usuários usam um nome de usuário e senha definidos em um OID para fazer logon em produtos Oracle Enterprise Performance Management System.

Fluxo do Processo



O processo do OSSO:

1. Usando um URL do EPM System, por exemplo, `http://OSSO_OHS_Server_NAME:OSSO_OHS_Server_PORT/interop/index.jsp`, os usuários acessam um componente do EPM System que está definido como um aplicativo protegido pelo OSSO.
2. Como o URL está sob proteção do OSSO, `mod_osso`, implantado em Oracle HTTP Server, intercepta a solicitação. Usando `mod_osso`, o Oracle HTTP Server verifica se há um cookie válido. Se um cookie válido não estiver disponível na solicitação, o Oracle HTTP Server redirecionará os usuários para o Servidor do OSSO, que desafia os usuários quanto às credenciais, que ele autentica no OID.
3. O Servidor do OSSO cria o `obSSOCookie` e retorna o controle para o módulo `mod_osso` no Oracle HTTP Server, que define o `obSSOCookie` no navegador. Ele também redireciona a solicitação para o recurso do EPM System por meio de `mod_wl_ohs` (Oracle WebLogic Server). Antes de encaminhar a solicitação para um recurso do EPM System, o Oracle HTTP Server define o cabeçalho `Proxy-Remote-User`, que a segurança do EPM System usa para habilitar o SSO.
4. O componente do EPM System verifica se o usuário cuja identidade é recuperada no `Proxy-Remote-User` está presente no OID. Para que esse processo funcione, o OID que é configurado com o Servidor do OSSO deve ser configurado como um diretório de usuários externo no Oracle Hyperion Shared Services.

Pré-requisitos

1. Uma Infraestrutura do Oracle Application Server totalmente funcional.

Para estabelecer uma Infraestrutura do Oracle Application Server, instale e configure o Oracle Identity Management Infrastructure 10.1.4. Certifique-se de que o OSSO esteja habilitado. A instalação do Oracle Identity Management Infrastructure 10.1.4 inclui os componentes a seguir para dar suporte ao OSSO.

- Servidor do OSSO para Oracle 10g.
- Um OID, que o Servidor do OSSO usa para validar credenciais. Consulte os seguintes guias:
 - *Guia de Instalação do Oracle Fusion Middleware para o Oracle Identity Management*
 - *Guia do Administrador do Oracle Fusion Middleware para o Oracle Internet Directory*
- Oracle HTTP Server como um front-end para o Servidor do OSSO. Essa instalação inclui `mod_osso`, que permite a você definir aplicativos parceiros para o OSSO.

 **Nota:**

Essa instância do Oracle HTTP Server faz parte da infraestrutura do OSSO; ela não é usada diretamente para configurar o OSSO para componentes do EPM System.

Durante o processo de instalação, garanta que `mod_osso` seja registrado no Servidor do OSSO como um aplicativo parceiro.

2. Uma implantação do EPM System totalmente funcional.
Quando você configura o servidor Web para os componentes do EPM System, o EPM System Configurator configura `mod_wl_ohs.conf` no Oracle HTTP Server para fazer solicitações ao WebLogic Server.

Teste da Implantação

Após a conclusão da implantação do SSL, verifique se tudo está funcionando.

Para testar sua implantação:

1. Usando um navegador, acesse o URL seguro do Oracle Hyperion Enterprise Performance Management Workspace:

Se você usou `epm.myCompany.com` como o alias do servidor para comunicação externa e 4443 como a porta SSL, o URL do EPM Workspace será

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

2. Na tela de logon, insira o nome de usuário e a senha.
3. Clique em **Logon**.
4. Verifique se você pode acessar com segurança os componentes implantados do Oracle Enterprise Performance Management System.

Habilitação de OSSO para EPM System

Esta seção supõe que você tenha uma infraestrutura de OSSO totalmente configurada. Consulte o *Guia do Administrador do Oracle Application Server*.

Registro do Servidor Web do EPM System como um Aplicativo Parceiro

Você usa a ferramenta de registro de SSO do Oracle Identity Manager (`ssoreg.sh` ou `ssoreg.bat`) para registrar o servidor Web do Oracle Enterprise Performance Management System como um aplicativo parceiro no Oracle HTTP Server que atua como front-end para o Servidor do OSSO.

Execute esse procedimento no servidor que hospeda o Oracle HTTP Server que atua como front-end para o Servidor do OSSO. Esse processo gera e armazena um `osso.conf` ofuscado no local de sua escolha.

Para registrar o servidor Web do EPM System como um aplicativo parceiro:

1. Abra um console no servidor que hospeda o Oracle HTTP Server que atua como front-end do Servidor do OSSO e navegue para o diretório `ORACLE_HOME/sso/bin` do Oracle HTTP Server, por exemplo, para `C:\OraHome_1\sso\bin` (Windows).
2. Execute um comando semelhante para o seguinte com a opção `-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
```

Veja a seguir a explicação dos parâmetros usados nesse comando. Nessa descrição, o aplicativo parceiro refere-se ao Oracle HTTP Server que é usado como o servidor Web do EPM System.

- `-site_name` identifica o site do aplicativo parceiro; por exemplo, `epm.myCompany.com`.
- `-mod_osso_url` indica o URL do aplicativo parceiro, no formato `PROTOCOL://HOST_NAME:PORT`. Esse é o URL no qual o servidor Web do EPM System aceita solicitações de cliente de entrada; por exemplo, `http://epm.myCompany.com:19000`.
- `-config_mod_osso` identifica que o aplicativo parceiro usa `mod_osso`. Você deve incluir o parâmetro `config_mod_osso` para gerar `osso.conf`.
- `-update_mode` indica o modo de atualização. Use `CREATE`, o padrão, para gerar um novo registro.
- `-remote_midtier` especifica que o aplicativo parceiro `mod_osso` está em uma camada intermediária remota. Use essa opção quando o aplicativo parceiro está em um `ORACLE_HOME` diferente de onde está o Servidor do OSSO.
- `-virtualhost` indica que o URL do aplicativo parceiro é um host virtual. Não use esse parâmetro se você não estiver usando um host virtual. Se estiver registrando um URL de aplicativo parceiro associado a um host virtual, será preciso definir o host virtual em `httpd.conf`. Consulte [Opcional: Definição de Host Virtual](#).
- `-config_file` indica o caminho em que o arquivo `osso.conf` deve ser gerado.

Opcional: Definição de Host Virtual

Se você usou um URL de host virtual ao registrar o aplicativo parceiro, será preciso definir o host virtual atualizando `httpd.conf` no Oracle HTTP Server que é usado como o servidor Web do EPM System.

Para definir um host virtual:

1. Usando um editor de texto, abra `EPM_ORACLE_INSTANCE/httpConfig/ohs/config/OHS/ohs_component/httpd.conf`.
2. Adicione uma definição semelhante à seguinte. Essa definição supõe que o servidor Web está em execução no servidor virtual `epm.myCompany.com` na porta `epm.myCompany.com:19400`. Modifique as configurações para ajustá-las aos seus requisitos.

```
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>
```

Criação de `mod_osso.conf`

Crie `mod_osso.conf` no Oracle HTTP Server que serve de front-end ao servidor Web do EPM System.

Para criar `mod_osso.conf`:

1. Usando um editor de texto, crie um arquivo.
2. Copie o conteúdo a seguir no arquivo e modifique-o para seu ambiente.

```
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. Na definição `<IfModule mod_osso.c`, inclua definições de local semelhantes à que se segue para identificar cada recurso que você pretende proteger usando o OSSO.

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

4. Salve o arquivo como `mod_osso.conf`.

Realocação de `osso.conf`

O processo de registrar o servidor Web do EPM System como um aplicativo parceiro (consulte [Registro do Servidor Web do EPM System como um Aplicativo Parceiro](#)) cria um arquivo `osso.conf` ofuscado no local identificado pela diretiva `-config_file`.

Para realocar `osso.conf`:

1. Localize o `osso.conf` que foi criado quando você registrou o servidor Web do EPM System como um aplicativo parceiro (consulte [Registro do Servidor Web do EPM System como um Aplicativo Parceiro](#)).
2. Copie `osso.conf` no diretório (no Oracle HTTP Server que atua como front-end do Servidor do OSSO) identificado pela propriedade `OsoConfigFile` definida em `mod_osso.conf` (consulte [Criação de `mod_osso.conf`](#)).

Configuração do EPM System para OSSO

Configure o OID que é integrado à solução OSSO como um diretório de usuários externo no EPM System e habilite o SSO.

Para configurar o EPM System para OSSO:

1. Configure o OID que a solução OSSO usa como um diretório de usuários externo. Consulte o tópico sobre configuração do OID, Active Directory e outros diretórios de usuários baseados em LDAP no *Guia de Administração da Segurança de Usuário do Sistema Oracle Enterprise Performance Management*.
2. Habilite o SSO no EPM System. [Configuração do EPM System para SSO](#)

Nota:

Para configurar o OSSO como a solução de gerenciamento de identidade, você deve escolher `Other` em **Provedor ou Agente SSO**, `Custom HTTP Header` em **Mecanismo SSO** e inserir `Proxy-Remote-User` como o nome do cabeçalho HTTP personalizado.

3. Provisione pelo menos um usuário do OID como um administrador do Oracle Hyperion Shared Services.
4. Reinicie os produtos EPM System e aplicativos personalizados que usam os APIs de segurança do Shared Services.

Nota:

Certifique-se de que o OID configurado com o Shared Services esteja em execução antes de iniciar os produtos EPM System.

Opcional: Ativação das Mensagens de Depuração no Servidor do OSSO

Para registrar mensagens de depuração no servidor do OSSO, modifique `policy.properties`. As mensagens de depuração são gravadas em `ORACLE_HOME/sso/log/ssoServer.log`.

Para registrar mensagens de depuração:

1. Usando um editor de texto, abra `ORACLE_HOME/sso/conf/policy.properties`; por exemplo, `C:\OraHome_1\sso\conf\policy.properties`, no servidor do OSSO.
2. Defina o valor da propriedade `debugLevel` para `DEBUG`.

```
debugLevel = DEBUG
```

3. Salve e feche `policy.properties`.

Opcional: Ativação das Mensagens de Depuração para Recursos Protegidos

Para registrar mensagens de depuração do OSSO para recursos protegidos usando `mod_osso.conf`, modifique `httpd.conf` no servidor Web do EPM System. As mensagens de depuração são gravadas em `EPM_ORACLE_INSTANCE/httpConfig/ohs/diagnostics/logs/OHS/ohs_component/ohs_component.log`.

Para registrar mensagens de depuração para recursos protegidos:

1. Usando um editor de texto, abra `EPM_ORACLE_INSTANCE/httpConfig/ohs/config/OHS/ohs_component/httpd.conf`.
2. Defina o valor da propriedade `OraLogSeverity` para `TRACE`.

```
OraLogSeverity TRACE:32
```

3. Salve e feche `httpd.conf`.

Proteção de Produtos EPM System para SSO

Você deve proteger os recursos do Oracle Enterprise Performance Management System para que as solicitações SSO de usuários sejam redirecionadas para o agente de segurança (OAM, OSSO ou SiteMinder).

O Oracle HTTP Server usa `mod_osso` para redirecionar usuários para o servidor do OSSO. Os usuários serão redirecionados apenas se os URLs solicitados estiverem configurados em `mod_osso` para serem protegidos. Consulte [Gerenciamento da Segurança](#) no *Guia do Administrador do Oracle HTTP Server*.

Para obter informações sobre como proteger recursos no SSO SiteMinder, consulte a documentação do SiteMinder.

OAM Somente: Proibindo a Inclusão de Cabeçalhos Padrão em Respostas

Por padrão, o OAM adiciona dois cabeçalhos padrão – `Pragma: no-cache` e `Cache-Control: no-cache` – para proteger URLs. Como esses cabeçalhos estão em conflito com diretivas semelhantes de armazenamento em cache adicionadas pelo EPM System e por aplicativos da Web, os navegadores não podem armazenar em cache o conteúdo de URLs protegidos que estão prejudicando o desempenho.

Para obter informações detalhadas sobre como impedir que esses cabeçalhos do OAM sejam incluídos em respostas, consulte "Ajustando Agentes do OAM" na seção "[Ajuste de Desempenho do Oracle Access Management](#)" do *Guia do Administrador do Fusion Middleware para o Oracle Access Manager com o Oracle Security Token Service*.

Recursos a Serem Protegidos

A tabela a seguir lista os contextos que devem ser protegidos. A sintaxe para proteger um recurso (usando `interop` como um exemplo) para OSSO:

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

O parâmetro `allow from` especifica servidores a partir dos quais a proteção do contexto pode ser ignorada.

Para Oracle Hyperion Enterprise Performance Management Workspace e Oracle Hyperion Financial Reporting, você precisa definir apenas os parâmetros indicados no seguinte exemplo:

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

Tabela 3-1 Recursos do EPM System a serem Protegidos

Produto EPM System	Contexto a ser Protegido
Oracle Hyperion Shared Services	<ul style="list-style-type: none"> • /interop • /interop/.../*
EPM Workspace	<ul style="list-style-type: none"> • /workspace • /workspace/.../*
Financial Reporting	<ul style="list-style-type: none"> • /hr • /hr/.../*
Oracle Hyperion Planning	<ul style="list-style-type: none"> • /HyperionPlanning • /HyperionPlanning/.../*
Oracle Integrated Operational Planning	<ul style="list-style-type: none"> • /interlace • /interlace/.../*
Oracle Hyperion Financial Management	<ul style="list-style-type: none"> • /hfmadf • /hfmadfe/.../* • /hfmoofficeprovider • /hfmoofficeprovider/.../* • /hfmsmartviewprovider • /hfmsmartviewprovider/.../*
Oracle Hyperion Financial Reporting Web Studio	/frdesigner/**
Oracle Data Relationship Management	<ul style="list-style-type: none"> • /drm-web-client • /drm-web-client/.../*

Tabela 3-1 (Cont.) Recursos do EPM System a serem Protegidos

Produto EPM System	Contexto a ser Protegido
Oracle Essbase Administration Services	<ul style="list-style-type: none"> • /hbrlauncher • /hbrlauncher/.../*
Oracle Hyperion Financial Data Quality Management	<ul style="list-style-type: none"> • /HyperionFDM • /HyperionFDM/.../*
Oracle Hyperion Calculation Manager	<ul style="list-style-type: none"> • /calcmgr • /calcmgr/.../*
Oracle Hyperion Provider Services	<ul style="list-style-type: none"> • /aps • /aps/.../*
Oracle Hyperion Profitability and Cost Management	<ul style="list-style-type: none"> • /profitability • /profitability/.../*
Account Reconciliation Manager	<ul style="list-style-type: none"> • /arm • /arm/.../*
Oracle Hyperion Financial Close Management	<ul style="list-style-type: none"> • /fcc • /fcc/.../*
Oracle Hyperion Financial Data Quality Management, Enterprise Edition	<ul style="list-style-type: none"> • /aif • /aif/.../*
Oracle Hyperion Tax Governance Tax Operations	/tss /taxop
Oracle Hyperion Tax Provision Supplemental Data Manager	/taxprov <ul style="list-style-type: none"> • /sdm* • /sdm/** • /sdm/./** • /SDM-Datamodel-context-root/**
Oracle Essbase	<ul style="list-style-type: none"> • /essbase/.../* • /essbase/** • /essbase*

Recursos a Serem Desprotegidos

A tabela a seguir lista os contextos que devem ser desprotegidos. A sintaxe para desproteger um recurso (usando /interop/framework(.*) como um exemplo) para OSSO:

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

Tabela 3-2 Recursos para Desproteger o EPM System

Produto EPM System	Contextos a serem Desprotegidos
Shared Services	<ul style="list-style-type: none"> • /interop/framework • /interop/framework* • /interop/framework.* • /interop/framework/.../* • /interop/Audit • /interop/Audit* • /interop/Audit.* • /interop/Audit/.../* • /interop/taskflow • /interop/taskflow* • /interop/taskflow/.../* • /interop/WorkflowEngine • /interop/WorkflowEngine/* • /interop/WorkflowEngine/.../* • /interop/TaskReceiver • /framework/lcm/HSSMigration
EPM Workspace	<ul style="list-style-type: none"> • /epmstatic/.../* • /workspace/bpmstatic/.../* • /workspace/static/.../* • /workspace/cache/.../*
Planning	<ul style="list-style-type: none"> • /HyperionPlanning/Smartview • /HyperionPlanning/faces/PlanningCentral • /HyperionPlanning/servlet/ HspDataTransfer • /HyperionPlanning/servlet/HspLCMServlet • /HyperionPlanning/servlet/ HspADMServlet/.../* • /HyperionPlanning/servlet/ HspADMServlet/** • /HyperionPlanning/servlet/ HspADMServlet* • /HyperionPlanning/servlet/ HspAppManagerServlet/.../* • /HyperionPlanning/servlet/ HspAppManagerServlet/** • /HyperionPlanning/servlet/ HspAppManagerServlet*

Tabela 3-2 (Cont.) Recursos para Desproteger o EPM System

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

Tabela 3-2 (Cont.) Recursos para Desproteger o EPM System

Produto EPM System	Contextos a serem Desprotegidos
Integrated Operational Planning	<ul style="list-style-type: none"> • /interlace/services/ • /interlace/services/* • /interlace/services/* • /interlace/services/.../* • /interlace/anteros • /interlace/anteros/* • /interlace/anteros/* • /interlace/anteros/.../* • /interlace/interlace • /interlace/interlace/* • /interlace/interlace/* • /interlace/interlace/.../* • /interlace/WebHelp • /interlace/WebHelp/* • /interlace/WebHelp/* • /interlace/WebHelp/.../* • /interlace/html • /interlace/html/* • /interlace/html/* • /interlace/html/.../* • /interlace/email-book • /interlace/email-book/* • /interlace/email-book/* • /interlace/email-book/.../*
Gerenciamento de Custo e Lucratividade	<ul style="list-style-type: none"> • /profitability/cesagent • /profitability/lcm • /profitability/control • /profitability/ApplicationListener • /profitability/HPMApplicationListener
Oracle Essbase	<ul style="list-style-type: none"> • /essbase/agent/.../* • /essbase/jet/logout.html • /essbase/jet/.\.(js css gif jpe?g png)\$
FDMEE	<ul style="list-style-type: none"> • /aif/services/FDMRuleService • /aif/services/RuleService • /aif/LCMServlet

SSO baseado em Cabeçalho com Produtos de Gerenciamento de Identidades

Pré-requisitos

- Um Oracle Enterprise Performance Management System totalmente configurado. É necessário que o servidor de diretórios do produto de gerenciamento de identidades seja configurado no EPM System como diretório de usuário para autorizar usuários.

- Um produto de gerenciamento de identidades totalmente configurado (Microsoft Azure AD, Okta e assim por diante) que oferece suporte à autenticação baseada em cabeçalho.

Os processos genéricos a seguir fazem parte da configuração do EPM System para SSO baseado em cabeçalho com um produto de gerenciamento de identidades compatível. Como as etapas específicas variam em função do produto que você está usando, consulte os manuais referentes ao produto de gerenciamento de identidades para obter as etapas detalhadas.

Para obter as etapas detalhadas sobre como configurar a autenticação baseada em cabeçalho com o Oracle Identity Cloud Services, consulte [Configuração do EPM System para SSO baseado em Cabeçalho com o Oracle Identity Cloud Services](#).

1. Registre o EPM System como um aplicativo corporativo no produto de gerenciamento de identidades. Essa etapa permite que o administrador de gerenciamento de identidades configure a autenticação no aplicativo corporativo, incluindo recursos suportados, como autenticação multifatores.

Use o nome de domínio totalmente qualificado (FQDN, Fully-Qualified Domain Name) do gateway anexado com `workspace/index.jsp` (por exemplo, `https://gateway.server.example.com:443/workspace/index.jsp`) como o URL do aplicativo corporativo para EPM System.

Configure o aplicativo corporativo do EPM System para propagar um cabeçalho HTTP. Você pode escolher qualquer nome de cabeçalho não reservado como o nome do cabeçalho HTTP. O valor do cabeçalho deve ser a propriedade que identifica os usuários do EPM System de maneira exclusiva.

2. Instale, configure e registre um gateway de aplicativo para garantir que o aplicativo corporativo encaminhe somente solicitações autenticadas para o EPM System. Use as seguintes definições de configuração:
 - FQDN do servidor do gateway (por exemplo, `gateway.server.example.com:443`) como o ponto de acesso.
 - FQDN do EPM System (por exemplo, `epm.server.example.com:443`) como o recurso para o qual as solicitações HTTP(S) autenticadas devem ser encaminhadas.

3. Habilite o SSO no EPM System para honrar cabeçalhos HTTP(S) propagados pelo gateway do aplicativo. Para obter informações detalhadas, consulte [Configuração de Opções de Segurança](#).

Para habilitar o SSO:

- a. Acesse o Oracle Hyperion Shared Services Console como Administrador do Sistema. Consulte [Iniciando o Shared Services Console](#).
- b. Selecione **Administração** e **Configurar Diretórios de Usuário**.
- c. Clique em **Opções de Segurança**.
- d. Na seção **Configuração do Logon Único**:
 - i. Marque a caixa de seleção **Habilitar SSO**.
 - ii. Na lista drop-down **Provedor SSO ou Agente de Segurança**, selecione **Outro**.
 - iii. Na lista drop-down **Mecanismo SSO**, selecione **Cabeçalho HTTP Personalizado** e depois especifique o nome do cabeçalho que o agente de segurança passa para o EPM System.
- e. Clique em **OK**.

4. Atualize a configuração URL Pós-Logoff do Oracle Hyperion Enterprise Performance Management Workspace para a configuração da página Web que deseja que usuários vejam ao efetuarem logout no EPM System. Para atualizar a configuração URL Pós-Logoff no EPM Workspace:
 - a. Acesse o EPM Workspace como Administrador do Sistema. Consulte [Acesso ao EPM Workspace](#).
 - b. Selecione **Navegar, Configurações do Workspace** e depois **Configurações do Servidor**.
 - c. Em **Configurações do Servidor do Workspace**, altere o **URL Pós-Logoff** para o URL da página Web que você deseja que usuários vejam ao efetuarem logout no EPM System.
 - d. Clique em **OK**.
5. Reinicie o Oracle Hyperion Foundation Services e todos os servidores gerenciados do EPM System

Configuração do EPM System para SSO baseado em Cabeçalho com o Oracle Identity Cloud Services

Nesse cenário, o Oracle Identity Cloud Services autentica os usuários do Oracle Enterprise Performance Management System e propaga os cabeçalhos HTTP obrigatórios para habilitar o SSO.

Esta seção aborda as etapas envolvidas na instalação e configuração do EPM System para permitir SSO com o Oracle Identity Cloud Services. Você pode exceder essas etapas para oferecer suporte à autenticação baseada em cabeçalho do EPM System com qualquer sistema de gerenciamento de identidades (por exemplo, Azure AD) ou provedor de IaaS (Infrastructure as a Service) compatível com a autenticação baseada em cabeçalho.

O fluxo de trabalho conceitual ocorre da seguinte forma:

- Um aplicativo do gateway funcionando como proxy reverso protege os componentes do EPM System restringindo o acesso não autenticado à rede.
- O aplicativo do gateway intercepta solicitações HTTP(S) para componentes do EPM System e assegura que o produto de gerenciamento de identidades autentique usuários antes de encaminhar solicitações para componentes do EPM System.
- Ao encaminhar solicitações para componentes do EPM System, o gateway do aplicativo propaga a identidade do usuário autenticado para o componente do EPM System por meio de solicitações de cabeçalho HTTP.

Pré-requisitos e URLs de Exemplo

Para estabelecer um SSO baseado em cabeçalho com o Oracle Identity Cloud Services:

- Um Oracle Enterprise Performance Management System totalmente configurado.
- Um host ou um contêiner com um Gateway do Aplicativo Oracle totalmente configurado, que age como proxy reverso para proteger o EPM System, restringindo o acesso não autorizado.

É necessário que o Gateway do Aplicativo Oracle esteja configurado para interceptar solicitações HTTP para componentes do EPM System e assegurar que usuários sejam autenticados pelo Oracle Identity Cloud Services antes de encaminharem solicitações para o EPM System. Ao encaminhar solicitações para componentes do EPM System, o Gateway do Aplicativo Oracle deve propagar a identidade do usuário autenticado por meio de solicitações de Cabeçalho HTTP.

- Acesso de Administrador do Domínio ao Oracle Identity Cloud Services.

Os URLs de exemplo a seguir são usados nesta discussão:

- URL base do nome de domínio totalmente qualificado (FQDN, Fully Qualified Domain Name) do servidor (provedor de identidade) do Oracle Identity Cloud Services:
`https://identity.server.example.com:443/`
- FQDN do servidor do Gateway do Aplicativo Oracle (que hospeda o aplicativo do gateway):
`https://gateway.server.example.com:443/`
- URL do aplicativo corporativo para EPM System. Esse é o FQDN do servidor do Gateway do Aplicativo Oracle anexado com `workspace/index.jsp`:
`https://gateway.server.example.com:443/workspace/index.jsp`

Note:

O Oracle Identity Cloud Services e o Gateway do Aplicativo Oracle são configurados com suporte a HTTPS. O suporte a HTTPS para EPM System é opcional. Essa discussão pressupõe que o EPM System tenha sido configurado com suporte a HTTPS.

Ativação da Autenticação Baseada em Cabeçalho para o EPM System

A ativação da autenticação baseada em cabeçalho para o Oracle Enterprise Performance Management System abrange as seguintes etapas:

- [Adição do Gateway e do Aplicativo EPM System para Oracle Identity Cloud Services](#)
- [Configuração do Gateway do Aplicativo](#)
- [Configuração do Diretório de Usuário para Autorização](#)
- [Habilitação do SSO no EPM System](#)
- [Atualização de Configurações do EPM Workspace](#)

Adição do Gateway e do Aplicativo do EPM System ao Oracle Identity Cloud Services

Para configurar a autenticação baseada em cabeçalho, crie o Oracle Enterprise Performance Management System como um Aplicativo Corporativo.

Adicione o EPM System como Aplicativo Corporativo no Oracle Cloud Identity Console

Para adicionar o EPM System como um aplicativo corporativo:

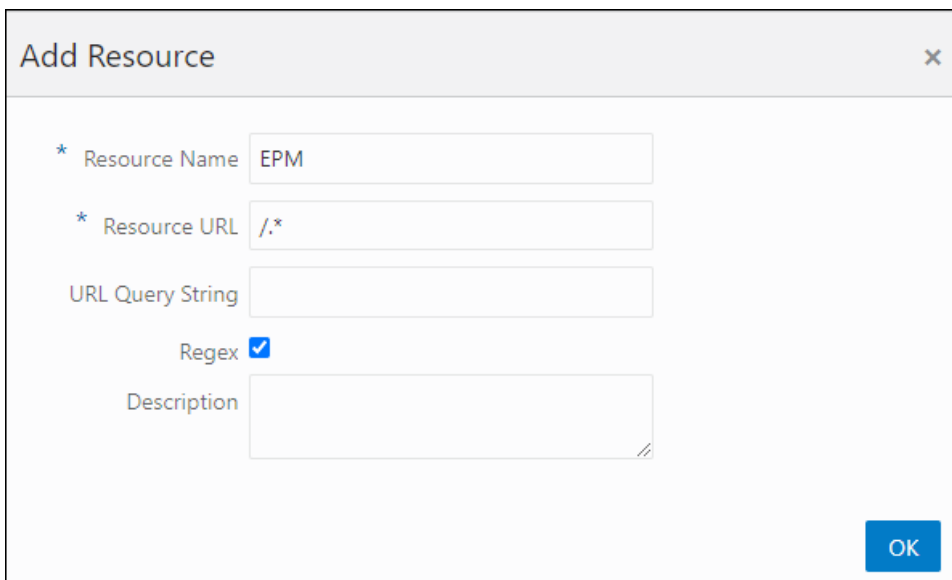
1. Acesse o Oracle Cloud Identity Console como Administrador do Domínio.
 - a. Usando um navegador, vá para <https://www.oracle.com/cloud/sign-in.html>.
 - b. Informe o Nome da Conta do Oracle Fusion Cloud EPM.
 - c. Na página Sign-in da Conta do Oracle Fusion Cloud EPM, insira o nome de usuário e senha e clique em **Efetuar Sign-in**.
 - d. Na **Gaveta de Navegação**, clique em **Usuários** e depois em **Identidade (Principal)**.
 - e. Clique em **Console de Identidade**.
2. Adicione o EPM System como um Aplicativo Corporativo.
 - a. Na Gaveta de navegação, clique em **Aplicativos**.
 - b. Clique em **Adicionar** e depois em **Aplicativo Corporativo**.

The screenshot shows the Oracle Identity Cloud Service console interface. On the left is a dark navigation sidebar with options like Dashboard, Users, Groups, Applications, Oracle Cloud Services, Jobs, Reports, Settings, and Security. The main content area is titled 'Add Enterprise Application' and features a blue header and a progress bar with three steps: 1. Details, 2. OAuth Configuration, and 3. SSO Configuration. The 'Details' step is currently active. The form contains several input fields: 'Name' (EPM System), 'Description' (On-Premises EPM 11.2), 'Application Icon' (with a cloud icon and an 'Upload' button), 'Application URL' (r.example.com:443/workspace/index.jsp), 'Custom Login URL', 'Custom Logout URL', 'Custom Error URL', and 'Linking callback URL'. Below the form are sections for 'Tags' and 'Settings'. The 'Settings' section includes three checkboxes: 'Display in My Apps' (checked), 'User can request access' (unchecked), and 'User must be granted the app' (unchecked).

3. Adicione os detalhes do aplicativo:
 - a. Em **Nome**, insira um nome exclusivo para identificar o aplicativo corporativo do EPM System.
 - b. Insira uma descrição opcional.
 - c. Opcionalmente, carregue um ícone de aplicativo para o EPM System. Clique em **Carregar** para selecionar e carregar o ícone.
 - d. Em **URL do Aplicativo**, informe o URL de inicialização para o qual o gateway deve redirecionar usuários. Esse URL é o FQDN do servidor do Gateway do

Aplicativo Oracle anexado com `workspace/index.jsp`, que é o contexto do aplicativo do EPM System.

- e. Em **Configurações**, selecione **Exibir em Meus Aplicativos** para exibir o aplicativo corporativo do EPM System na guia **Configuração SSO** da página **Meus Aplicativos** no Oracle Cloud Identity Console.
 - f. Clique em **Próximo**.
4. Especifique detalhes da Configuração de SSO.
- a. Clique em **Configuração de SSO**.
 - b. Adicione um recurso para o aplicativo corporativo. Em **Configuração de SSO**, expanda **Recursos**.
 - i. Clique em **Adicionar**.



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 controls:

- 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 with a small icon in the bottom right corner.
- OK**: A blue button located at the bottom right of the dialog.

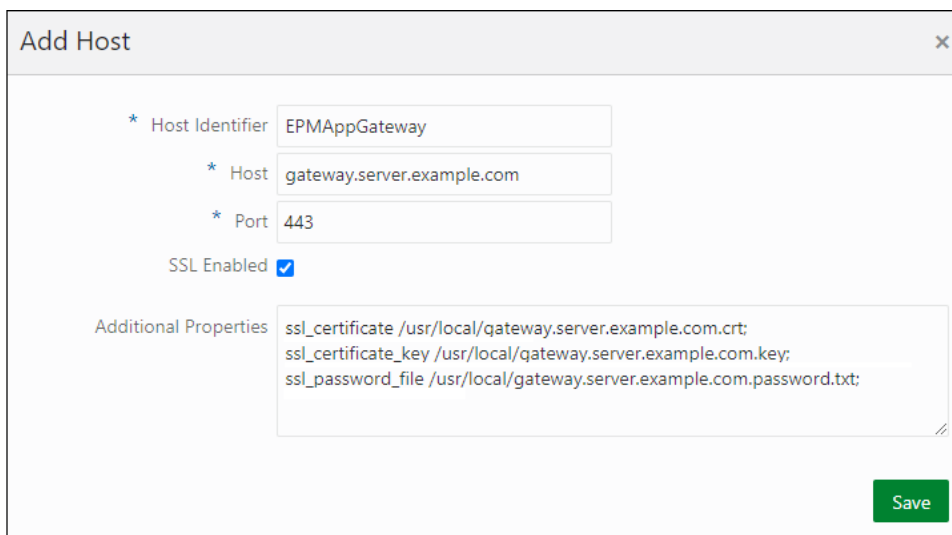
- ii. Especifique um nome de recurso exclusivo.
 - iii. Em **URL do Recurso**, informe `/*`.
 - iv. Marque a caixa de seleção **Regex**.
 - v. Clique em **OK**.
 - vi. Em **Configuração de SSO**, expanda **Recursos**.
- c. Adicione uma política de autenticação. Em **Configuração de SSO**, expanda **Política de Autenticação**.
- i. Marque as caixas de seleção **Permitir CORS** e **Exibir Cookies Seguros**.
 - ii. Clique em **Adicionar** em **Recursos Gerenciados** e defina **Formulário ou Token de Acesso** como o método de autenticação do recurso de SSO.

The screenshot shows a dialog box titled "Add Resource". It contains the following fields and options:

- Resource:** A search box containing "EPM".
- Authentication Method:** A dropdown menu showing "Form or Access Token".
- Authentication Method Overrides:** A plus sign (+) to add overrides.
- Headers:** A plus sign (+) to add headers.
- Header Configuration:** A table with two columns: "Name" and "Value".

Name	Value
HYPLOGIN	Work Email
- Buttons:** A blue "Add" button at the bottom right and a close "X" button at the top right.

- iii. Em **Recurso**, selecione o recurso de SSO que você adicionou na etapa anterior.
 - iv. Expanda **Cabeçalhos**.
 - v. Informe o nome do cabeçalho HTTP que será propagado para o EPM System.
O nome do cabeçalho de autenticação padrão é HYPLOGIN. É possível usar qualquer nome de sua preferência.
 - vi. Em **Valor**, selecione a propriedade que identifica os usuários do EPM System de maneira exclusiva.
O valor desse campo deve corresponder à identidade do usuário no EPM System. Por exemplo, se a identidade do usuário no EPM System for o ID do e-mail, selecione E-mail Comercial como o valor.
 - vii. Clique em **Salvar**.
5. Clique em **Finalizar** para criar o aplicativo corporativo.
 6. Clique em **Ativar** para habilitar o aplicativo corporativo.
 7. Registre um Gateway do Aplicativo e configure o host e o aplicativo para o EPM System.
 - a. Na **Gaveta de Navegação**, clique em **Segurança** e depois em **Gateways do Aplicativo**.
 - b. Clique em **Adicionar**.
 - c. Em **Detalhes**, informe um nome exclusivo para o gateway e uma descrição opcional.
 - d. Clique em **Próximo** para abrir a tela Hosts.
 - e. Adicione um host do Gateway do Aplicativo para o EPM System.
 - i. Na tela Hosts, clique em **Adicionar**.



Add Host

* Host Identifier: EPMAppGateway

* Host: gateway.server.example.com

* Port: 443

SSL Enabled

Additional Properties: ssl_certificate /usr/local/gateway.server.example.com.crt;
ssl_certificate_key /usr/local/gateway.server.example.com.key;
ssl_password_file /usr/local/gateway.server.example.com.password.txt;

Save

- ii. Em **Identificador do Host**, informe EPMAppGateway.
 - iii. Em **Host**, informe o nome do domínio totalmente qualificado do computador que hospeda o servidor do Gateway do Aplicativo; por exemplo, gateway.server.example.com.
 - iv. Em **Porta**, informe a porta em que o servidor do Gateway do Aplicativo responde a solicitações HTTPS.
 - v. Marque a caixa de seleção **Habilitado para SSL**.
 - vi. Em **Propriedades Adicionais**, informe o seguinte:
 - A localização do certificado SSL
 - A chave do certificado SSL
 - O arquivo de senhas SSL (se necessário)

Para obter informações detalhadas, consulte "[Registrar um Gateway do Aplicativo](#)" em "Configurar um Gateway do Aplicativo" em *Administrando o Oracle Identity Cloud Service*.
 - vii. Clique em **Salvar**.
 - viii. Clique em **Próximo** para abrir a tela Aplicativos.
- f. Adicione o aplicativo corporativo do EPM System ao Gateway do Aplicativo.
- i. Em **Aplicativos**, clique em **Adicionar**.
 - ii. Em **Aplicativo**, selecione o aplicativo corporativo do EPM System que você adicionou anteriormente ao Oracle Cloud Identity Console.

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. Em **Selecione um Host**, selecione EPMAAppGateway (o host do EPM System que você adicionou ao Gateway do Aplicativo).
 - iv. Em **Prefixo do Recurso**, informe / para encaminhar todas as solicitações para o host do EPM System.
 - v. Em **Servidor de Origem**, informe o nome de domínio totalmente qualificado do computador que hospeda o Oracle Hyperion Enterprise Performance Management Workspace e o número da porta que o EPM Workspace usa.
 - vi. Clique em **Salvar**.
8. Registre o ID do Cliente e o Segredo do Gateway do Aplicativo. Esses valores são obrigatórios para configurar o Gateway do Aplicativo.
- a. Na **Gaveta de Navegação**, clique em **Segurança** e depois em **Gateways do Aplicativo**.
 - b. Clique no nome do Gateway que você adicionou ao aplicativo corporativo do EPM System.
 - c. Copie o ID do Cliente (uma string alfanumérica) em um editor de texto.
 - d. Clique em **Mostrar Segredo** para exibir o código secreto do cliente.
 - e. Copie o Segredo do Cliente (uma string alfanumérica) no editor de texto.
 - f. Salve o arquivo de texto.

 **Note:**

O servidor do Gateway do Aplicativo deve ser reiniciado sempre que uma atualização de configuração for realizada nos Oracle Identity Cloud Services. Para iniciar e parar o servidor do Gateway do Aplicativo, consulte [Iniciar e Parar o Gateway do Aplicativo](#).

Configuração do Gateway do Aplicativo

Para obter informações detalhadas, consulte "[Configurar um Gateway do Aplicativo](#)" em *Administrando o Oracle Identity Cloud Service*.

Você precisa do ID e o Segredo do Cliente que você registrou na seção anterior para configurar o Servidor do Gateway do Aplicativo.

Configuração do Diretório de Usuário para Autorização

Alguns produtos de gerenciamento de identidades, por exemplo, o Oracle Identity Cloud Services e o Microsoft Azure, não podem ser configurados diretamente como diretórios de usuário no Oracle Enterprise Performance Management System. Você pode configurar esses produtos com o Oracle Unified Directory ou o Oracle Virtual Directory e depois configurar o último como um diretório de usuário no EPM System. Para obter as etapas detalhadas sobre como configurar diretórios de usuário, consulte [Configuração de Diretórios de Usuário](#).

Habilitação do SSO no EPM System

Configure Opções de Segurança no Oracle Enterprise Performance Management System para habilitar o SSO. Para obter instruções detalhadas, consulte [Configuração de Opções de Segurança](#).

Para habilitar o SSO:

1. Acesse o Oracle Hyperion Shared Services Console como Administrador do Sistema. Consulte [Iniciando o Shared Services Console](#).
2. Selecione **Administração e Configurar Diretórios de Usuário**.
3. Clique em **Opções de Segurança**.
4. Na seção **Configuração do Logon Único**:
 - a. Marque a caixa de seleção **Habilitar SSO**.
 - b. Na lista drop-down **Provedor SSO ou Agente de Segurança**, selecione **Outro**.
 - c. Na lista drop-down **Mecanismo SSO**, selecione **Cabeçalho HTTP Personalizado** e depois especifique o nome do cabeçalho que o agente de segurança passa para o EPM System (`HYPLOGIN` ou o nome personalizado que você especificou ao adicionar o recurso para o aplicativo corporativo no Oracle Cloud Identity Console).
5. Clique em **OK**.

Note:

Confirme que você reiniciou todos os EPM System Services após qualquer alteração na configuração do SSO.

Atualização de Configurações do EPM Workspace

1. Acesse o Oracle Hyperion Enterprise Performance Management Workspace como um Administrador do Sistema. Consulte [Acesso ao EPM Workspace](#).

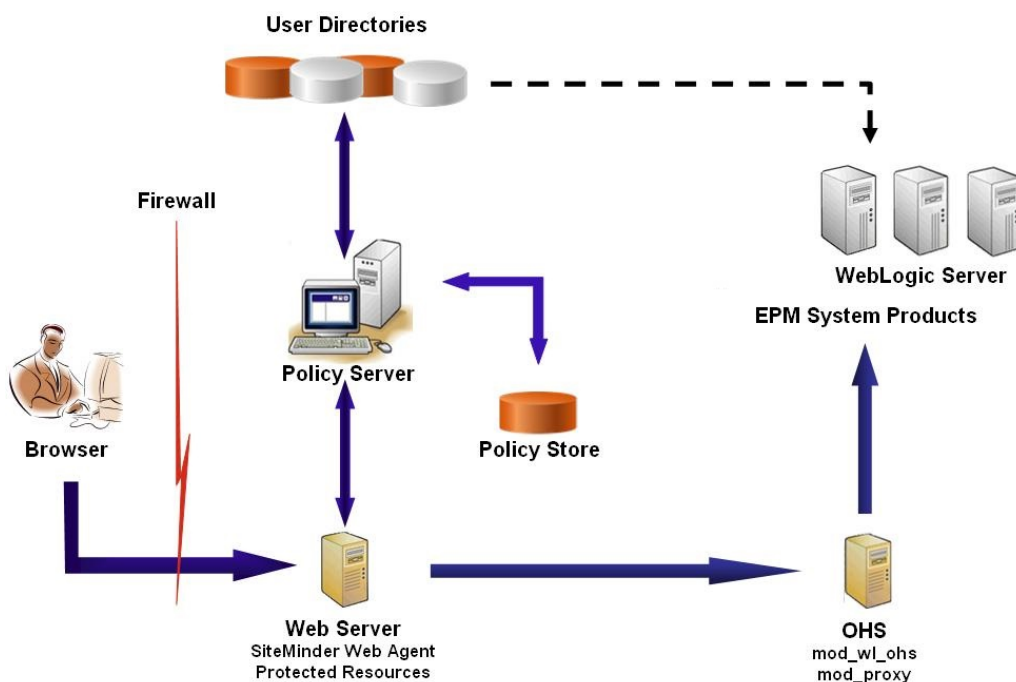
2. Selecione **Navegar, Configurações do Workspace** e depois **Configurações do Servidor**.
3. Em **Configurações do Servidor do Workspace**, altere o **URL Pós-Logout** para o URL da página Web que você deseja que usuários vejam ao efetuarem logout no Oracle Enterprise Performance Management System.
4. Clique em **OK**.
5. Reinicie o Oracle Hyperion Foundation Services e todos os componentes do EPM System.

SiteMinder SSO

O SiteMinder é uma solução somente para Web. Os aplicativos de área de trabalho e seus suplementos (por exemplo, Microsoft Excel e Report Designer) não podem usar a autenticação por meio do SiteMinder. No entanto, o Oracle Smart View para Office pode usar a autenticação do SiteMinder.

Fluxo do Processo

Visão geral ilustrada do SSO habilitado para o SiteMinder:



O processo do SSO do SiteMinder:

1. Os usuários tentam acessar um recurso do Oracle Enterprise Performance Management System protegido pelo SiteMinder. Eles usam um URL que os conecta ao servidor Web que atua como front-end do servidor de política do SiteMinder; por exemplo, `http://WebAgent_Web_Server_Name:WebAgent_Web_ServerPort/interop/index.jsp`.
2. O servidor Web redireciona os usuários para o servidor de política, que solicita aos usuários as credenciais. Após verificação das credenciais nos diretórios de

usuários configurados, o servidor de política passa as credenciais ao servidor Web que hospeda o Agente Web do SiteMinder.

3. O servidor Web que hospeda o Agente Web do SiteMinder redireciona a solicitação para o Oracle HTTP Server que atua como front-end do EPM System. O Oracle HTTP Server redireciona os usuários para o aplicativo solicitado implantado no Oracle WebLogic Server.
4. O componente do EPM System verifica as informações de provisionamento e serve-se de conteúdo. Para que esse processo funcione, os diretórios de usuários que o SiteMinder usa para autenticar usuários devem ser configurados como diretórios de usuários externos no EPM System. Esses diretórios devem ser configurados como confiáveis.

Considerações Especiais

O SiteMinder é uma solução somente para Web. Os aplicativos de área de trabalho e seus suplementos (por exemplo, Microsoft Excel e Report Designer) não podem usar a autenticação por meio do SiteMinder. No entanto, o Smart View pode usar a autenticação do SiteMinder.

Pré-requisitos

1. Uma instalação do SiteMinder totalmente funcional abrange os seguintes componentes:
 - O Servidor de Política do SiteMinder no qual as políticas e os objetos de agente são definidos
 - O Agente Web do SiteMinder instalado no servidor Web que atua como front-end do Servidor de Política do SiteMinder
2. Uma implantação do EPM System totalmente funcional.
Quando você configura o servidor Web para os componentes do EPM System, o EPM System Configurator configura `mod_wl_ohs.conf` para solicitações de proxy para o WebLogic Server.

Habilitação do Agente Web do SiteMinder

O agente Web é instalado em um servidor Web que intercepta solicitações para recursos do EPM System. As tentativas por usuários não autenticados de acessar recursos protegidos do EPM System forçam o agente Web a desafiar os usuários em relação às credenciais do SSO. Quando um usuário é autenticado, o servidor de política adiciona o nome de logon do usuário autenticado, que é carregado pelo cabeçalho. Subsequentemente, a solicitação HTTP é passada ao servidor Web do EPM System, que redireciona as solicitações. Os componentes do EPM System extraem as credenciais de usuário autenticado dos cabeçalhos.

O SiteMinder oferece suporte ao SSO para todos os produtos do EPM System executados em plataformas heterogêneas do servidor Web. Se os produtos EPM System usarem servidores Web diferentes, você deverá garantir que o cookie do SiteMinder possa ser passado para todos os servidores Web dentro do mesmo domínio. É possível fazer isso especificando o domínio de aplicativo apropriado do EPM System como o valor da propriedade `Cookiedomain` no arquivo `WebAgent.conf` de cada servidor Web.

Consulte o tópico sobre a configuração de agentes Web no *Guia de Agente do Netegrity SiteMinder*.

 **Nota:**

Tendo em vista que o Oracle Hyperion Shared Services usa a autenticação básica para proteger o seu conteúdo, o servidor Web que intercepta as solicitações para o Shared Services deve habilitar a autenticação básica para dar suporte ao SSO com SiteMinder.

Configure o Agente Web executando o assistente para Configuração do Agente Web do SiteMinder (executando `WEBAGENT_HOME/install_config_info/nete-wa-config`; por exemplo, `C:\netegrity\webagent\install_config_info\nete-wa-config.exe` no Windows). O processo de configuração cria um `WebAgent.conf` para o servidor Web do SiteMinder.

Para habilitar o Agente Web do SiteMinder:

1. Usando um editor de texto, abra `WebAgent.conf`. O local desse arquivo depende do servidor Web que você está usando.
2. Defina o valor da propriedade `enableWebAgent` para `Yes`.
`enableWebAgent="YES"`
3. Salve e feche o arquivo de configuração do agente Web.

Exemplo 3-1 Configuração do Servidor de Política do SiteMinder

Um administrador do SiteMinder deverá configurar o servidor de política para habilitar SSO para os produtos do EPM System.

O processo de configuração envolve:

- Criação de um Agente Web do SiteMinder e adição de objetos de configuração apropriados para o servidor Web do SiteMinder
- Criação de um realm para cada recurso do EPM System que deve ser protegido e adição do agente Web ao realm. Consulte [Recursos a Serem Protegidos](#)
- No realm que foi criado para recursos protegidos do EPM System, crie realms para recursos não protegidos. Consulte [Recursos a Serem Desprotegidos](#)
- Criação da referência do cabeçalho HTTP. O cabeçalho deve fornecer o valor de `Login Attribute` para aplicativos do EPM System. Consulte o tópico sobre configuração do OID, Active Directory e outros diretórios de usuários baseados em LDAP no *Guia de Administração da Segurança de Usuário do Sistema Oracle Enterprise Performance Management* para obter uma breve descrição de `Login Attribute`.
- Criação de regras nos realms com Get, Post e Put como ações do agente Web
- Criação de um atributo de resposta com `hyplogin=<%userattr="SM_USERLOGINNAME"%>` como o valor
- Criação de uma política, atribuindo acesso de diretório de usuários, e adição de regras que você criou para o EPM System à lista Membros Atuais
- Definição de respostas para as regras que você criou para componentes do EPM System

Exemplo 3-2 Configuração do Servidor Web do SiteMinder para Encaminhar Solicitações ao Servidor Web do EPM System

Configure o servidor Web que hospeda o agente Web do SiteMinder para encaminhar solicitações de usuários autenticados (contendo o cabeçalho que identifica o usuário) ao servidor Web do EPM System.

Para servidores Web baseados no Apache, use diretivas semelhantes às seguintes para encaminhar solicitações 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
```

Nessa diretiva, substitua *EPM_WEB_SERVER* e *EPM_WEB_SERVER_PORT* pelos valores reais do seu ambiente.

Exemplo 3-3 Habilitação do SiteMinder no EPM System

A integração com o SiteMinder requer que você habilite a autenticação do SiteMinder para os produtos do EPM System. Consulte [Configuração do EPM System para SSO](#).

Logon único Kerberos

Visão Geral

Os produtos Oracle Enterprise Performance Management System oferecerão suporte ao SSO Kerberos se o servidor de aplicativos que hospeda os produtos EPM System estiver configurado para autenticação Kerberos.

O Kerberos é um serviço de autenticação confiável onde cada cliente Kerberos confia na validade das identidades dos outros clientes Kerberos (usuários, serviços de rede etc.).

Veja a seguir o que acontece quando um usuário acessa um produto EPM System:

1. Em um computador Windows, o usuário faz logon em um domínio do Windows, que também é um realm Kerberos.
2. Usando um navegador configurado para usar o Integrated Windows Authentication, o usuário tenta fazer logon nos produtos do EPM System que estão sendo executados no servidor do aplicativo.
3. O servidor de aplicativos (Negotiate Identity Asserter) intercepta a solicitação e obtém o token do Mecanismo de Negociação (SPNEGO) da Simple and Protected Generic Security Services API (GSSAPI) com o tíquete Kerberos do cabeçalho de autorização do navegador.
4. A asserção valida a identidade do usuário incluída no token em seu armazenamento de identidades para passar informações sobre o usuário ao produto EPM System. O produto EPM System valida o nome do usuário em um Active Directory. O produto EPM System gera um token SSO que dá suporte ao SSO em todos os produtos EPM System.

Limitações de Suporte

O Kerberos SSO é suportado em todos os produtos EPM System, com as seguintes exceções:

- O SSO Kerberos não é permitido para thick clients, a não ser o Oracle Smart View para Office.
- O Smart View dá suporte à integração do Kerberos apenas para provedores do Oracle Essbase, Oracle Hyperion Planning e Oracle Hyperion Financial Management

Pressupostos

Este documento, que contém etapas de configuração do Kerberos no nível de configuração, supõe conhecimento da configuração do Kerberos no nível do sistema. Antes de iniciar estes procedimentos, confirme se os pré-requisitos para essas tarefas foram atendidos.

Este documento supõe que você esteja trabalhando em um ambiente de rede habilitado para Kerberos totalmente funcional, no qual as máquinas cliente do Windows são configuradas para autenticação Kerberos.

- O Active Directory corporativo é configurado para autenticação Kerberos. Consulte [Documentação do Microsoft Windows Server](#).
- Os navegadores usados para acessar os produtos EPM System são configurados para negociar usando tíquetes Kerberos.
- sincronização de tempo com uma distorção de no máximo cinco minutos entre as máquinas cliente e o KDC. Consulte "Erros de Autenticação são Causados por Relógios Não Sincronizados" em [http://technet.microsoft.com/en-us/library/cc780011\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc780011(WS.10).aspx).

SSO Kerberos com WebLogic Server

O SSO Kerberos no Oracle WebLogic Server utiliza o Negotiate Identity Asserter para negociar e decodificar tokens do SPNEGO de modo a habilitar o SSO com clientes Microsoft. O WebLogic Server decodifica os tokens SPNEGO para obter o tíquete Kerberos, bem como valida e mapeia o tíquete para um usuário do WebLogic Server. Você pode usar o Autenticador do WebLogic Server no Active Directory com o Negotiate Identity Asserter para configurar o Active Directory como o diretório para usuários do WebLogic Server.

Quando o navegador solicita acesso a um produto EPM System, o KDC emite um tíquete Kerberos para o navegador, que cria um token SPNEGO contendo os tipos de token GSS permitidos. O Negotiate Identity Asserter decodifica o token SPNEGO e utiliza o GSSAPIs para aceitar o contexto de segurança. A identidade do usuário que iniciou a solicitação é mapeada para um nome de usuário e encaminhada de volta para o WebLogic Server. Além disso, o WebLogic Server determina os grupos aos quais o usuário pertence. Nesse estágio, o produto solicitado do EPM System é disponibilizado para o usuário.

Nota:

Os usuários devem usar um navegador que aceite SPNEGO (por exemplo, Internet Explorer ou Firefox) para acessar os produtos EPM System executados no WebLogic Server.

Usando o ID do usuário derivado do processo de autenticação, o processo de autorização do produto do EPM System processa verificações dos dados de

provisionamento. O acesso ao produto EPM System é restrito com base nos dados de provisionamento.

Procedimentos do WebLogic Server para Suporte à Autenticação Kerberos

Um administrador deve concluir estas etapas para permitir a autenticação Kerberos:

- Crie o domínio do WebLogic para o EPM System. Consulte [Criação do Domínio do WebLogic para o EPM System](#).
- Crie um provedor de autenticação. Consulte [Criação de um Provedor de Autenticação LDAP no WebLogic Server](#).
- Crie um Negotiate Identity Asserter. Consulte [Criação de um Negotiate Identity Asserter](#).
- Crie uma identificação Kerberos. Consulte [Criação de Identificação Kerberos para o WebLogic Server](#).
- Atualize as opções de JVM para Kerberos. Consulte [Atualização das Opções de JVM para Kerberos](#).
- Configure políticas de autorização. Consulte [Configuração de Políticas de Autorização](#).
- Implante e use SSODiag para verificar se o WebLogic Server está pronto para dar suporte ao SSO Kerberos para o EPM System. Consulte [Uso de SSODiag para Testar o Ambiente Kerberos](#).

Criação do Domínio do WebLogic para o EPM System

De modo geral, os componentes do EPM System são implantados no domínio do WebLogic no EPMSystem (o local padrão é `MIDDLEWARE_HOME/user_projects/domains/EPMSystem`).

Para configurar o domínio do WebLogic no EPM System para autenticação Kerberos:

1. Instale os componentes do EPM System.
2. Implante apenas o Oracle Hyperion Foundation Services.
A implantação do Foundation Services cria o domínio do WebLogic padrão no EPM System.
3. Faça logon no Oracle Hyperion Shared Services Console para verificar se a implantação do Foundation Services foi bem-sucedida. Consulte [Iniciando o Shared Services Console](#).

Criação de um Provedor de Autenticação LDAP no WebLogic Server

Um administrador do WebLogic Server cria o provedor de autenticação LDAP, que armazena informações de usuário e grupo em um servidor LDAP externo. Os servidores LDAP compatíveis com LDAP v2 ou v3 funcionam com o WebLogic Server. Consulte estas referências:

- [Configuração de Provedores de Autenticação LDAP](#) no guia *Oracle Fusion Middleware Protegendo o Oracle WebLogic Server*.
- [Configurar Provedores de Asserção de Identidade e Autenticação](#) na *Ajuda On-line do Console de Administração do Oracle WebLogic Server no Oracle Fusion Middleware*.

Criação de um Negotiate Identity Asserter

O provedor Negotiate Identity Assertion permite SSO com clientes da Microsoft. Ele decodifica tokens SPNEGO para obter tokens Kerberos, valida os tokens Kerberos e mapeia os tokens para os usuários do WebLogic. O provedor Negotiate Identity Assertion, uma

implementação da Security Service Provider Interface (SSPI), conforme definido pela Estrutura de Segurança do WebLogic, fornece a lógica necessária para autenticar um cliente com base no token SPNEGO do cliente.

- [Configuração de um Provedor Negotiate Identity Assertion](#) no guia *Oracle Fusion Middleware Protegendo o Oracle WebLogic Server*.
- [Configurar Provedores de Asserção de Identidade e Autenticação](#) na *Ajuda On-line do Console de Administração do Oracle WebLogic Server no Oracle Fusion Middleware*.

Durante a criação do provedor Negotiate Identity Assertion, defina a opção JAAS Control Flag como `SUFFICIENT` para todos os autenticadores. Consulte "Definir JAAS control flag" na [Ajuda On-line do Console de Administração do Oracle WebLogic Server no Oracle Fusion Middleware](#).

Criação de Identificação Kerberos para o WebLogic Server

Na máquina do controlador de domínio do Active Directory, crie objetos de usuário que representem o servidor Web do WebLogic Server e do EPM System, e mapeie-os para os nomes da entidade de serviço (SPN) que representem seu WebLogic Server e servidor Web no realm Kerberos. Os clientes não podem localizar um serviço que não tenha um SPN. Você armazena SPNs em arquivos keytab que são copiados no domínio do WebLogic Server para serem usados no processo de logon.

Consulte [Criação de identificação para o WebLogic Server](#) no guia *Oracle Fusion Middleware Protegendo o Oracle WebLogic Server* para obter procedimentos detalhados.

Para criar a identificação Kerberos para o WebLogic Server:

1. Na máquina do controlador de domínio do Active Directory, crie uma conta de usuário, por exemplo, `epmHost`, para o computador que hospeda o domínio do WebLogic Server.

Nota:

Crie a identificação como um objeto de usuário, não como uma máquina.

Use o nome simples do computador; por exemplo, use `epmHost` se o host for chamado de `epmHost.example.com`.

Registre a senha usada durante a criação do objeto de usuário. Ela será necessária para criar SPNs.

Não selecione opções de senha, especialmente a opção `User must change password at next logon`.

2. Modifique o objeto de usuário para cumprir o protocolo Kerberos. A conta deve exigir pré-autenticação Kerberos.
 - Na guia **Conta**, selecione uma criptografia a ser usada.
 - Certifique-se de que nenhuma outra opção de conta (especialmente `Do not require Kerberos pre-authentication`) seja selecionada.
 - Uma vez que a definição do tipo de criptografia por ter corrompido a senha do objeto, redefina a senha para a senha definida durante a criação do objeto.

3. No computador que hospeda o controlador de domínio do Active Directory, abra uma janela do prompt de comando e navegue até o diretório em que as ferramentas de suporte do Active Directory estão instaladas.

4. Crie e configure os SPNs necessários.

- a. Use um comando semelhante ao seguinte para verificar se os SPNs estão associados ao objeto de usuário (`epmHost`) que você criou na Etapa 1 deste procedimento.

```
setspn -L epmHost
```

- b. Usando um comando como o seguinte, configure o SPN para o WebLogic Server no Active Directory Domain Services (AD DS) e gere um arquivo keytab que contenha a chave secreta compartilhada.

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

5. Crie um arquivo keytab no computador que hospeda o WebLogic Server.

- a. Abra um prompt de comando.
- b. Navegue para `MIDDLEWARE_HOME/jdk/bin`.
- c. Execute um comando como o seguinte:

```
ktab -k keytab_filename -a epmHost@example.com
```

- d. Quando a senha for solicitada, informe a senha definida durante a criação do usuário na etapa 1 deste procedimento.

6. Copie o arquivo keytab no diretório de inicialização no domínio do WebLogic; por exemplo, em `C:\Oracle\Middleware\user_projects\domains\EPMSys\`.

7. Verifique se a autenticação Kerberos está funcionando corretamente.

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

Neste comando, `account-name` indica a entidade de segurança Kerberos; por exemplo, `HTTP/epmHost.example.com@EXAMPLE.COM`. A saída deste comando deve ser semelhante à seguinte:

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

Atualização das Opções de JVM para Kerberos

Consulte [Uso de Argumentos de Inicialização para Autenticação Kerberos com WebLogic Server](#) e [Criação de um Arquivo de Logon JAAS](#) no *Oracle Fusion Middleware Protegendo o Oracle WebLogic Server 11g Versão 1 (10.3.1)*.

Se os servidores gerenciados do EPM System estiverem sendo executados como serviços do Windows, atualize o registro do Windows para definir as opções de inicialização da JVM.

Para atualizar as opções de inicialização da JVM no registro do Windows:

1. Abra o Editor de Registro do Windows.

2. Selecione **Meu Computador, HKEY_LOCAL_MACHINE, Software, Hyperion Solutions, FoundationServices0** e, finalmente, **HyS9EPMServer_epmsystem1**.
3. Crie os seguintes valores de string:

 **Nota:**

Os nomes listados na tabela a seguir são exemplos.

Tabela 3-3 Opções de Inicialização da JVM para Autenticação Kerberos

Nome	Tipo	Dados
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	- Djava.security.auth.login.config= <i>location of Kerberos login configuration file</i>
JVMOption47	REG_SZ	- Djavax.security.auth.useSubjectCredsOnly= false

4. Atualize o valor de JVMOptionCount DWord para refletir a JVMOptions adicionada (adicione 4 ao valor decimal atual).

Configuração de Políticas de Autorização

Consulte [Opções para Proteger Recursos EJB e Aplicativo Web](#) no guia *Oracle Fusion Middleware Protegendo Recursos Usando Funções e Políticas do Oracle WebLogic Server* para obter informações sobre configuração de políticas de autorização para os usuários do Active Directory que acessam o EPM System.

Para ver um exemplo de etapas de configuração de política, consulte [Criação de Políticas para SSODiag](#).

Uso de SSODiag para Testar o Ambiente Kerberos

SSODiag é um aplicativo Web de diagnostico que testa se o WebLogic Server em seu ambiente Kerberos está pronto para dar suporte ao EPM System.

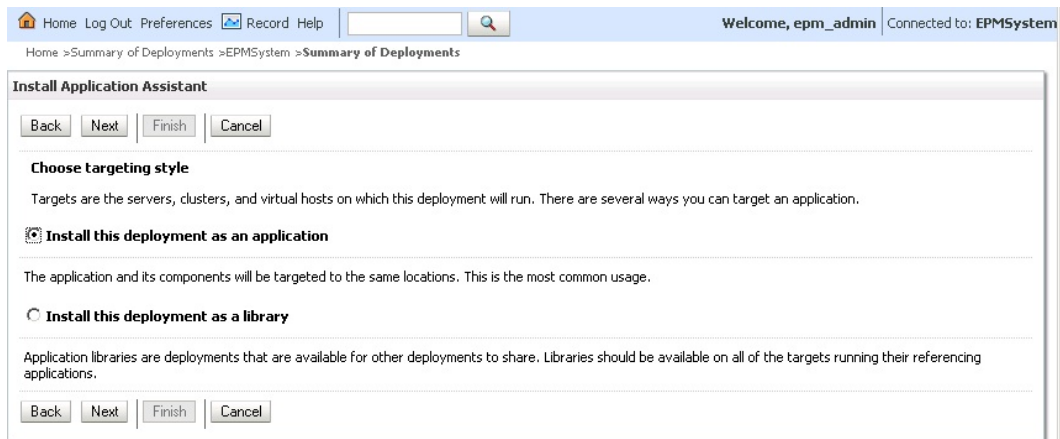
Implantação de SSODiag

Use as credenciais de administrador do WebLogic Server (o nome de usuário padrão é `epm_admin`) que você especificou durante a implantação de Foundation Services para implantar o SSODiag.

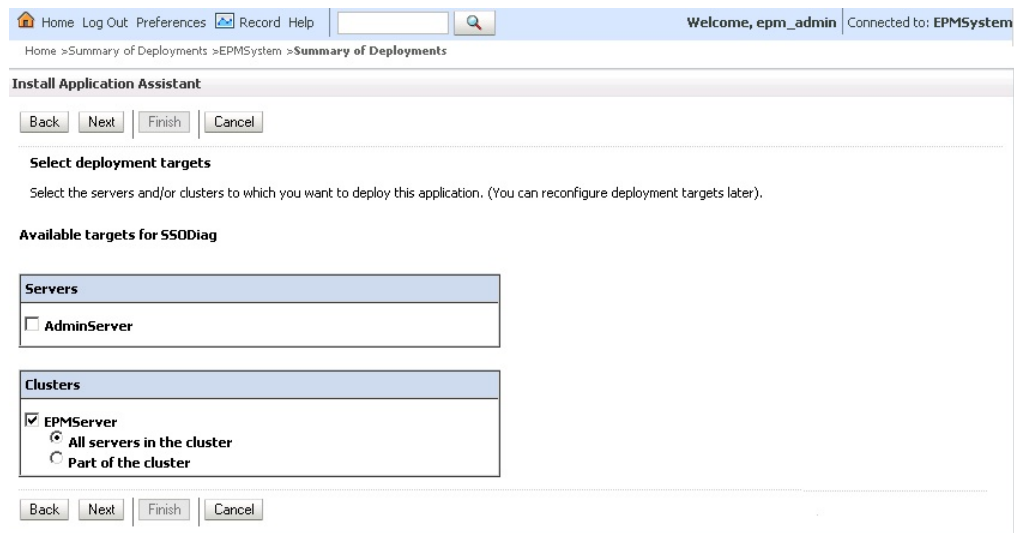
Para implantar e configurar o SSODiag:

1. Faça logon no Console de Administração do WebLogic Server para o domínio do EPM System.
2. Em Centro de Alterações, selecione **Bloquear & Editar**

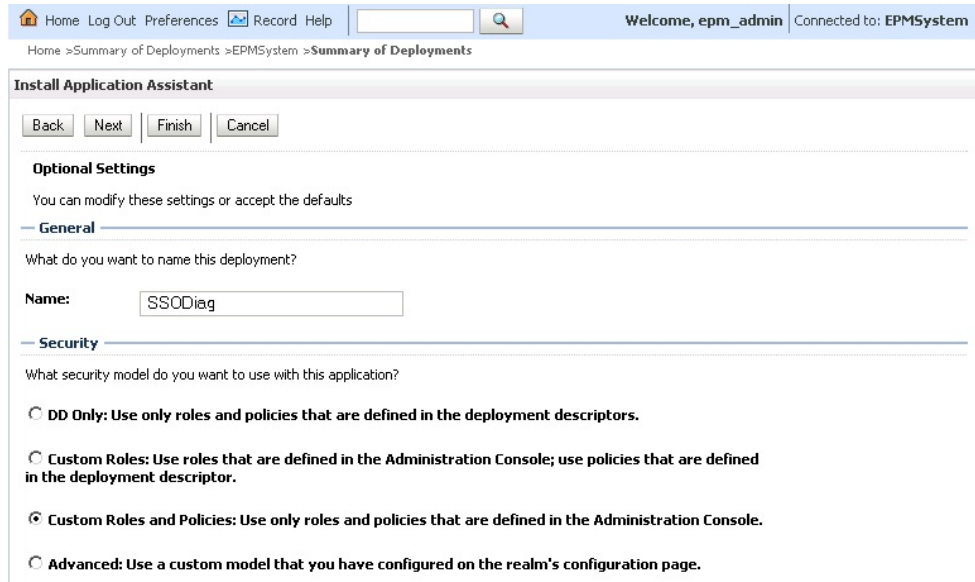
3. No **EPMSysystem**, em **Estrutura do Domínio**, clique em **Implantações**.
4. Em **Resumo de Implantações**, clique em **Instalar**.
5. Em **Caminho**, selecione `EPM_ORACLE_HOME/products/Foundation/AppServer/InstallableApps/common/SSODiag.war`.
6. Clique em **Próximo**.
7. Em **Escolher estilo do destino**, certifique-se de que **Instalar esta implantação como um aplicativo** esteja selecionada e clique em **Próximo**.



8. Em **Selecionar Destinos da Implantação**, selecione o seguinte e clique em **Próximo**.
 - **EPMServer**
 - **Todos os servidores no cluster**



9. Em **Configurações Opcionais**, selecione **Políticas e Funções Personalizadas: Usar apenas funções e Políticas que estão definidas no Console de Administração** como o modelo de segurança.



10. Clique em **Próximo**.
11. Na tela de revisão, selecione **Não, revisarei a configuração mais tarde**.
12. Clique em **Concluir**.
13. No Centro de Alterações, selecione **Ativar Alterações**.

Configuração do Oracle HTTP Server para SSODiag

Atualize `mod_wl_ohs.conf` de modo a configurar o Oracle HTTP Server para encaminhar as solicitações de URL do SSODiag ao WebLogic Server.

Para configurar o encaminhamento de URL no Oracle HTTP Server:

1. Usando um editor de texto, abra `EPM_ORACLE_INSTANCE/httpConfig/ohs/config/fmwconfig/components/OHS/ohs_component/mod_wl_ohs.conf`.
2. Adicione uma definição `LocationMatch` para SSODiag:

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

No exemplo anterior, `myServer` denota a máquina host de Foundation Services e `28080` representa a porta na qual o Oracle Hyperion Shared Services escuta as solicitações.

3. Salve e feche `mod_wl_ohs.conf`.
4. Reinicie o Oracle HTTP Server.

Criação de Políticas para SSODiag

Crie uma política no Console Administrativo do WebLogic Server para proteger o URL de SSODiag a seguir.

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

Neste exemplo, *OHS_HOST_NAME* indica o nome do servidor que hospeda o Oracle HTTP Server e *PORT* indica a porta em que o Oracle HTTP Server escuta as solicitações.

Para criar políticas a fim de proteger o SSODiag:

1. No Centro de Alterações do Console de Administração do WebLogic Server para o domínio do EPM System, selecione **Bloquear & Editar**.
2. Selecione **Implantações, SSODiag, Segurança, URLPatterns** e depois **Políticas**.
3. Crie os seguintes padrões de URL:
 - /
 - /index.jsp
4. Modifique cada padrão de URL que você criou:
 - a. Na lista de padrões de URL em **Padrões de URL de Aplicativo Web Autônomo**, abra o padrão (/) que você criou clicando nele.
 - b. Selecione **Adicionar Condições**.
 - c. Em **Lista de Predicados**, selecione **Usuário**.
 - d. Selecione **Próximo**.
 - e. Em **Nome de Argumento do Usuário**, insira o usuário do Active Directory cuja conta é usada para acessar uma área de trabalho do cliente configurada para autenticação Kerberos; por exemplo, `krbuser1`, e selecione **Adicionar**. `krbuser1` é um usuário de área de trabalho do Windows ou do Active Directory.
 - f. Selecione **Concluir**.
5. Selecione **Salvar**.

Uso do SSODiag para Testar a Configuração do WebLogic Server para Autenticação Kerberos

Se a configuração do WebLogic Server para autenticação Kerberos funcionar corretamente, a página *Utilitário de diagnóstico do SSO Kerberos do Oracle Hyperion V 1.0* exibirá a seguinte mensagem:

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

▲ Cuidado:

Não configure os componentes do EPM System para autenticação Kerberos se SSODiag não puder recuperar o nome da entidade de segurança Kerberos.

Para testar a configuração do WebLogic Server para autenticação Kerberos:

1. Inicie o Foundation Services e o Oracle HTTP Server.
2. Usando o Console de Administração do WebLogic Server, inicie o aplicativo Web SSODiag para atender a todas as solicitações.
3. Faça logon em uma máquina cliente configurada para autenticação Kerberos usando as credenciais válidas do Active Directory.
4. Usando um navegador, conecte-se ao seguinte URL do SSODiag:

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

Neste exemplo, *OHS_HOST_NAME* indica o nome do servidor que hospeda o Oracle HTTP Server e *PORT* indica a porta em que o Oracle HTTP Server escuta as solicitações.

Se a autenticação Kerberos funcionar corretamente, SSODiag exibirá as seguintes informações:

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

Se a autenticação Kerberos não funcionar corretamente, SSODiag exibirá as seguintes informações:

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

Alteração do Modelo de Segurança

O modelo de segurança padrão para aplicativos Web protegidos pelo realm de segurança é *DDOnly*. Você deve alterar o modelo de segurança para *CustomRolesAndPolicies*.

Para alterar o modelo de segurança:

1. Usando um editor de texto, abra *MIDDLEWARE_HOME/user_projects/domains/EPMSysstem/config/config.xml*.
2. Localize o seguinte elemento no descritor da implantação de aplicativo para cada componente do Foundation Services:

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

3. Altere o modelo de segurança como se segue para cada componente:

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

4. Salve e feche *config.xml*.

Atualização da Configuração de Segurança do EPM System

Altere a configuração de segurança do EPM System para habilitar o SSO Kerberos.

Para configurar o EPM System para autenticação Kerberos:

1. Faça logon no Shared Services Console como administrador.
2. Adicione o domínio do Active Directory que está configurado para autenticação Kerberos como um diretório de usuários externo no Shared Services. Consulte "Configuração do OID e Outros Diretórios de Usuários Baseados em LDAP" no *Guia de Administração da Segurança de Usuário do Sistema Oracle Enterprise Performance Management*.
3. Habilitar SSO Consulte [Configuração de OID, Active Directory e Outros Diretórios de Usuário com Base em LDAP](#).
Em **Opções de Segurança**, selecione as configurações na tabela a seguir para ativar o SSO Kerberos.

Tabela 3-4 Configurações para Habilitar o SSO Kerberos

Campo	Configuração Necessária
Habilitar SSO	Selecionado
Provedor ou Agente SSO	Outro
Mecanismo SSO	Obter Usuário Remoto de uma Solicitação HTTP

4. Reinicie o Foundation Services.

Teste do SSO Kerberos

Faça logon no Foundation Services para verificar se o SSO Kerberos está funcionando corretamente.

Para testar o SSO Kerberos:

1. Verifique se o Foundation Services e o Oracle HTTP Server estão em execução.
2. Faça logon em uma máquina cliente configurada para autenticação Kerberos usando as credenciais válidas do Active Directory.
3. Usando um navegador, conecte-se ao URL do Foundation Services.

Configuração dos Componentes do EPM System

Usando o EPM System Configurator, configure e implante outros componentes do EPM System no domínio do WebLogic onde o Foundation Services está implantado.

Configuração dos Servidores Gerenciados do EPM System para Autenticação Kerberos

Nos ambientes do Microsoft Windows, os servidores gerenciados do EPM System são executados como serviços do Windows. É preciso modificar as opções de inicialização da JVM para cada servidor gerenciado do WebLogic. Uma lista abrangente de servidores gerenciados no modo de implantação não compacta:

- AnalyticProviderServices0
- CalcMgr0
- ErpIntegrator0
- EssbaseAdminServer0
- FinancialReporting0
- HFMWeb0
- FoundationServices0

- HpsAlerter0
- HpsWebReports0
- Planning0
- Profitability0

Se os aplicativos Web do EPM System forem implantados no modo de implantação compacto, você precisará atualizar as opções de inicialização da JVM apenas do servidor gerenciado do `EPMSystem0`. Se você tiver vários servidores gerenciados compactos, será preciso atualizar as opções de inicialização da JVM para todos os servidores gerenciados.

Consulte [Uso de Argumentos de Inicialização para Autenticação Kerberos com WebLogic Server](#) no guia *Oracle Fusion Middleware Protegendo o Oracle WebLogic Server*.

 **Nota:**

O procedimento a seguir descreve como definir as opções de inicialização da JVM para o servidor gerenciado do Foundation Services. Você deve realizar essa tarefa para cada servidor gerenciado do WebLogic na implantação.

Para ver procedimentos detalhados de como configurar opções da JVM nos scripts de inicialização do WebLogic Server, consulte [Atualização das Opções de JVM para Kerberos](#).

Para configurar as opções da JVM nos scripts de inicialização do WebLogic Server

Configuração de Políticas de Autorização

Configure as políticas de autorização para usuários do Active Directory que acessarão os componentes do EPM System com exceção do Foundation Services. Consulte [Configuração de Políticas de Autorização](#) para obter informações sobre como configurar políticas de segurança no Console de Administração do WebLogic.

Alteração do Modelo de Segurança Padrão dos Componentes do EPM System

Você edita o arquivo de configuração do EPM System para alterar o modelo de segurança padrão. Para implantações do EPM System não compactas, você deve alterar o modelo de segurança padrão para cada aplicativo Web do EPM System registrado no `config.xml`. Uma lista de aplicativos Web do EPM System:

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

- WORKSPACE

Para alterar o modelo de segurança:

1. Usando um editor de texto, abra `MIDDLEWARE_HOME/user_projects/domains/EPMSystem/config/config.xml`
2. Na definição da implantação de aplicativo para cada componente do EPM System, defina o valor de `<security-dd-model>` como `CustomRolesAndPolicies`, como mostrado no seguinte exemplo:

```
<app-deployment>
  <name>SHAREDSERVICES#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. Salve e feche `config.xml`.
4. Reinicie o WebLogic Server.

Criação de Políticas de Proteção de URL para Componentes do EPM System

Crie uma política de proteção de URL no Console Administrativo do WebLogic Server para proteger cada URL de componente do EPM System. Consulte [Opções para Proteger Recursos EJB e Aplicativos Web](#) no guia *Oracle Fusion Middleware Protegendo Recursos Usando Funções e Políticas do Oracle WebLogic Server* para obter detalhes.

Para criar políticas de proteção de URL:

1. No Centro de Alterações do Console de Administração do WebLogic Server para o domínio do EPM System, clique em **Bloquear & Editar**.
2. Clique em **Implantações**.
3. Expanda um aplicativo corporativo do EPM System (por exemplo, `PLANNING`) em sua implantação e clique no respectivo aplicativo Web (por exemplo, `HyperionPlanning`). Consulte [Alteração do Modelo de Segurança Padrão dos Componentes do EPM System](#) para obter uma lista de componentes do EPM System.

 **Nota:**

Alguns aplicativos corporativos, por exemplo, o Oracle Essbase Administration Services, incluem vários aplicativos Web para os quais os padrões de URL devem ser definidos.

4. Crie uma política com escopo no Padrão de URL para o aplicativo Web.
 - AIF
 - APS
 - CALC
 - EAS

- FINANCIALREPORTING
 - PLANNING
 - PROFITABILITY
 - SHARED SERVICES
 - WORKSPACE
- a. Clique em **Segurança, Políticas** e em **Novo**.
 - b. No **Padrão de URL**, informe os URLs protegidos e desprotegidos para produtos do EPM System. Consulte [Proteção e Desproteção de Recursos do EPM System](#) para obter mais detalhes.
 - c. Clique em **OK**.
 - d. Clique no padrão de URL que você criou.
 - e. Clique em **Adicionar Condições**.
 - f. Na **Lista de Predicados**, selecione uma condição de política e clique em **Próximo**.
A Oracle recomenda usar a condição `Group`, que concede essa política de segurança a todos os membros de um grupo especificado.
 - g. Especifique os argumentos que pertence ao predicado escolhido. Por exemplo, se você escolher `Group` na etapa anterior, você deve concluir as seguintes etapas:
 - h. Em **Nome do Argumento do Grupo**, insira o nome do grupo que contém os usuários que devem ter permissão para acessar o aplicativo Web. O nome que você insere deve corresponder exatamente a um nome de grupo do Active Directory.
 - Clique em **Adicionar**.
 - Repita as etapas anteriores para adicionar mais grupos.
 - i. Clique em **Concluir**.
O WebLogic Server exibirá uma mensagem de erro se ele não puder localizar o grupo no Active Directory. É preciso resolver esse erro antes de continuar.
 - j. Selecione **Salvar**.
 5. Repita as Etapas 3 e 4 deste procedimento para os outros componentes do EPM System na sua implantação.
 6. No Centro de Alterações, clique em **Configuração da Versão**.
 7. Reinicie o WebLogic Server.

Habilitar a Autenticação Baseada no Certificado do Cliente em Aplicativos Web

Insira a definição `login-config` no arquivo de configuração dos arquivos de aplicativo a seguir localizados em `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 habilitar a autenticação baseada no certificado do cliente:

1. Interrompa os componentes e processos do EPM System.
2. Usando o 7 Zip, expanda o arquivo compactado da Web contido no arquivo compactado corporativo; por exemplo, `EPM_ORACLE_HOME/products/Esbase/eas/server/AppServer/InstallableApps/Common/eas.ear/eas.war`.
3. Navegue para WEB-INF.
4. Modifique `web.xml` adicionando a seguinte definição `login_config` justamente antes do elemento `</webapp>`:

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

5. Salve `web.xml`.
6. Clique em **Sim** quando 7 Zip consultar se você deseja atualizar o arquivo.

Atualização da Configuração de Segurança do EPM System

Configure a segurança do EPM System para respeitar o SSO. Consulte [Configuração do EPM System para SSO](#).

Configuração do EPM System para SSO

Os produtos Oracle Enterprise Performance Management System devem ser configurados para dar suporte ao agente de segurança de SSO. A configuração especificada no Oracle Hyperion Shared Services determina o seguinte para todos os produtos EPM System:

- Se aceitar o SSO de um agente de segurança
- O mecanismo de autenticação para aceitar o SSO

Em um ambiente habilitado para SSO, o produto EPM System que é primeiramente acessado pelo usuário analisa o mecanismo SSO para recuperar o ID do usuário autenticado contido nele. O produto EPM System verifica o ID do usuário em relação aos diretórios de usuários configurados no Shared Services para determinar se o usuário é um usuário válido do EPM System. Ele também emite um token que habilita o SSO em todos os produtos EPM System.

A configuração especificada no Shared Services habilita o SSO e determina o mecanismo de autenticação para aceitar o SSO em todos os produtos do EPM System.

Para habilitar o SSO em uma solução de gerenciamento de identidade na Web:

1. Inicie o Oracle Hyperion Shared Services Console como um Administrador do Shared Services. Consulte [Iniciando o Shared Services Console](#).
2. Selecione **Administração e Configurar Diretórios de Usuário**.
3. Verifique se os diretórios de usuários usados pela solução de gerenciamento da identidade na Web estão configurados como diretórios de usuários externos no Shared Services.

Por exemplo, para ativar o SSO Kerberos, é preciso configurar o Active Directory que está configurado para autenticação Kerberos como um diretório de usuários externo.

Para obter instruções, consulte [Configuração de Diretórios de Usuário](#).

4. Selecione **Opções de Segurança**.

5. Selecione **Mostrar Opções Avançadas**.
6. Na **Configuração de Logon Único** na tela dos Diretório Definidos pelo Usuário, execute os procedimentos a seguir:
 - a. Selecione **Habilitar SSO**.
 - b. No **Provedor ou Agente SSO**, selecione uma solução de gerenciamento de identidade na Web. Escolha **Outro** se estiver configurando o SSO com Kerberos.

O mecanismo SSO recomendado é selecionado automaticamente. Consulte a tabela a seguir. Consulte também [Métodos de SSO Suportados](#).

 **Nota:**

Se você não estiver usando o mecanismo SSO recomendado, deverá escolher **Outro** no **Provedor ou Agente SSO**. Por exemplo, para usar um mecanismo diferente de Cabeçalho HTTP para o SiteMinder, escolha **Outro** em **Provedor ou Agente SSO** e selecione o Mecanismo SSO que deseja usar em **Mecanismo SSO**.

Tabela 3-5 Mecanismos SSO de Preferência para Soluções de Gerenciamento de Identidade na Web

Solução de Gerenciamento de Identidade na Web	Mecanismo SSO Recomendado
Oracle Access Manager	Custom HTTP Header ¹
OSSO	Custom HTTP Header
SiteMinder	Custom HTTP Header
Kerberos	Get Remote User from HTTP Request

¹ O nome Cabeçalho HTTP padrão é HYPLOGIN. Se você estiver usando um Cabeçalho HTTP personalizado, substitua o nome.

7. Clique em **OK**.

Opções de Logon Único para Smart View

Embora o Oracle Smart View para Office seja um thick client e não um navegador, ele se conecta aos componentes de servidor usando HTTP e se comporta como um navegador de uma perspectiva de sistema. O Smart View dá suporte a todos os métodos de integração padrão baseados na Web que são permitidos pelas interfaces de navegador. No entanto, existem algumas limitações:

- Se o Smart View for iniciado de uma sessão de navegador existente que está conectada a um componente do Oracle Enterprise Performance Management System, os usuários deverão entrar novamente no Smart View, pois ele não compartilha o cookie da sessão existente.
- Se você estiver usando um formulário de logon baseado em HTML personalizado em vez do formulário de logon padrão do Oracle Access Manager, certifique-se de que a origem do formulário personalizado inclua a string `loginform`. Isso é

necessário para permitir que a integração do Smart View ao Oracle Access Manager funcione.

4

Configuração de Diretórios de Usuário

Consulte Também:

- [Diretórios de Usuário e Segurança do EPM System](#)
- [Operações Relacionadas à Configuração do Diretório de Usuário](#)
- [Oracle Identity Manager e EPM System](#)
- [Informações do Active Directory](#)
- [Configuração de OID, Active Directory e Outros Diretórios de Usuário com Base em LDAP](#)
- [Configuração de Bancos de Dados Relacionais como Diretórios de Usuário](#)
- [Como Testar Conexões do Diretório de Usuário](#)
- [Edição de Configurações do Diretório de Usuário](#)
- [Exclusão de Configurações do Diretório de Usuário](#)
- [Gerenciamento da Ordem de Pesquisa do Diretório de Usuário](#)
- [Configuração de Opções de Segurança](#)
- [Nova Geração de Chaves de Criptografia](#)
- [Uso de Caracteres Especiais](#)

Diretórios de Usuário e Segurança do EPM System

Os produtos do Oracle Enterprise Performance Management System podem ser usados em vários sistemas de gerenciamento de usuários e identidades, conhecidos como diretórios de usuário. Eles incluem diretórios de usuários habilitados para Lightweight Directory Access Protocol (LDAP), como o Sun Java System Directory Server (anteriormente denominado SunONE Directory Server) e o Active Directory. O EPM System também oferece suporte como diretório de usuário externo.

Em geral, os produtos EPM System usam o Native Directory e diretórios de usuários externos no provisionamento. Consulte [Matriz de Certificação do Oracle Enterprise Performance Management System](#) para obter uma lista de diretórios de usuários compatíveis.

Os produtos do EPM System exigem uma conta de diretório de usuário para cada usuário que acessar os produtos. Esses usuários podem ser atribuídos a grupos para facilitar o provisionamento. Os usuários e grupos podem ser provisionados com funções do EPM System e ACLs de objeto. Devido à carga administrativa, a Oracle não recomenda provisionar usuários individualmente. Os usuários e grupos de todos os diretórios de usuários configurados podem ser vistos através do Oracle Hyperion Shared Services Console.

Por padrão, o EPM System Configurator configura o repositório do Shared Services como o Native Directory para dar suporte aos produtos EPM System. Gerentes de Diretório acessam e gerenciam o Native Directory usando o Shared Services Console.

Operações Relacionadas à Configuração do Diretório de Usuário

Para obter suporte e autorização para SSO, os Administradores devem configurar diretórios de usuários externos. No Oracle Hyperion Shared Services Console, os Administradores do Sistema podem executar várias tarefas relacionadas à configuração e ao gerenciamento de diretórios de usuários. Estes tópicos fornecem instruções:

- Configuração de diretórios do usuário:
 - [Configuração de OID, Active Directory e Outros Diretórios de Usuário com Base em LDAP](#)
 - [Configuração de Bancos de Dados Relacionais como Diretórios de Usuário](#)
- [Como Testar Conexões do Diretório de Usuário](#)
- [Edição de Configurações do Diretório de Usuário](#)
- [Exclusão de Configurações do Diretório de Usuário](#)
- [Gerenciamento da Ordem de Pesquisa do Diretório de Usuário](#)
- [Configuração de Opções de Segurança](#)

Oracle Identity Manager e EPM System

O Oracle Identity Manager é uma solução de administração de função e usuário que automatiza o processo de adição, atualização e exclusão de contas de usuário e de autorizações no nível de atributo nos recursos corporativos. O Oracle Identity Manager está disponível como um produto independente ou como parte do Oracle Identity and Access Management Suite Plus.

O Oracle Enterprise Performance Management System integra-se ao Oracle Identity Manager usando funções corporativas, que são grupos do LDAP. Funções de componentes do EPM System podem ser designadas a funções corporativas. Usuários ou grupos adicionados às funções corporativas do Oracle Identity Manager herdam automaticamente as funções designadas herdadas do EPM System.

Por exemplo, considere que você tenha um aplicativo do Oracle Hyperion Planning nomeado *Budget Planning*. Para suportar esse aplicativo, você pode criar três funções corporativas: Usuário Interativo do Budget Planning, Usuário Final do Budget Planning e Administrador do Budget Planning, no Oracle Identity Manager. Ao provisionar funções do EPM System, verifique se os Gerentes de Provisionamento provisionam as funções corporativas do Oracle Identity Manager com as funções necessárias do *Budget Planning* e outros componentes do EPM System, incluindo o Shared Services. Todos os usuários e grupos designados às funções corporativas no Oracle Identity Manager herdam as funções do EPM System. Consulte a documentação do Oracle Identity Manager para obter informações sobre a implantação e gerenciamento do Oracle Identity Manager.

Para integrar o Oracle Identity Manager com o EPM System, os Administradores devem executar estas etapas:

- Verifique se os membros (usuários e grupos) de funções corporativas do Oracle Identity Manager usados para provisionamento do EPM System estão definidos

em um diretório de usuários habilitados para LDAP; por exemplo, OID ou Active Directory.

- Configure o diretório de usuário ativado para LDAP em que os membros das funções corporativas estejam definidos como um diretório de usuário externo no EPM System. Consulte [Configuração de OID, Active Directory e Outros Diretórios de Usuário com Base em LDAP](#).

Informações do Active Directory

Esta seção explica conceitos do Microsoft Active Directory usados neste documento.

Pesquisa de DNS e Pesquisa de Nome de Host

Os Administradores do Sistema podem configurar o Active Directory de modo que o Oracle Hyperion Shared Services possa executar uma pesquisa estática de nome de host ou de DNS para identificar o Active Directory. A pesquisa estática de nome de host não oferece suporte ao failover do Active Directory.

A utilização da pesquisa DNS garante a alta disponibilidade do Active Directory em cenários em que o Active Directory está configurado em vários controladores de domínio para garantir a alta disponibilidade. Quando configurado para realizar uma pesquisa DNS, o Shared Services consulta o servidor DNS para identificar os controladores de domínio registrados e conecta-se ao controlador de domínio com maior peso. Se o controlador de domínio ao qual o Shared Services está conectado falhar, o Shared Services mudará dinamicamente para o próximo controlador de domínio disponível com maior peso.



Nota:

A pesquisa DNS só poderá ser configurada se uma configuração redundante do Active Directory com suporte a failover estiver disponível. Consulte a documentação da Microsoft para obter informações.

Catálogo Global

Um catálogo global é um controlador de domínio que armazena uma cópia de todos os objetos do Active Directory em uma floresta. Ele armazena uma cópia completa de todos os objetos do diretório do seu domínio host e uma cópia parcial de todos os objetos dos outros domínios na floresta, as quais são usadas em operações típicas de pesquisa de usuário. Consulte a documentação da Microsoft para obter informações sobre como configurar um catálogo global.

Se a organização estiver usando um catálogo global, use um dos seguintes métodos para configurar o Active Directory:

- Configurar o servidor do catálogo global como diretório de usuário externo (recomendado)
- Configurar cada domínio do Active Directory como um diretório de usuário externo separado.

A configuração do catálogo global, em vez de domínios individuais do Active Directory, permite que os produtos Oracle Enterprise Performance Management System acessem grupos locais e universais dentro da floresta.

Configuração do OID, Active Directory e Outros Diretórios de Usuário baseados em LDAP

Os Administradores do Sistema usam os procedimentos desta seção para configurar diretórios de usuários corporativos baseados em LDAP, como OID, Sun Java System Directory Server, Oracle Virtual Directory, Active Directory, IBM Tivoli Directory Server ou um diretório de usuário com base em LDAP que não esteja listado na tela de configuração.

Para configurar o OID, Active Directory e outros diretórios de usuário baseados em LDAP:

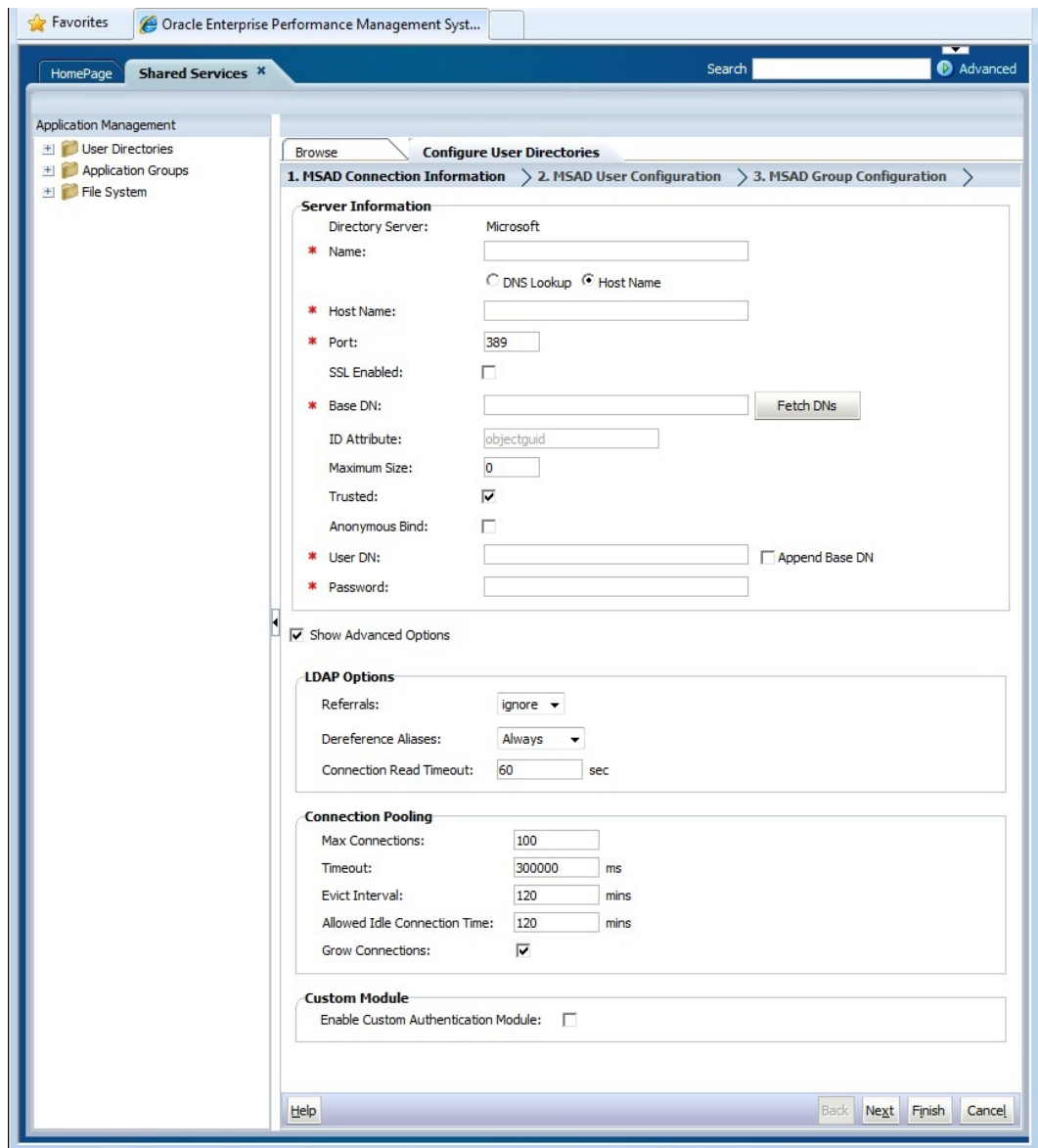
1. Acesse o Oracle Hyperion Shared Services Console como Administrador do Sistema. Consulte [Iniciando o Shared Services Console](#).
2. Selecione **Administração** e **Configurar Diretórios de Usuário**.

A tab Configuração do Provedor é aberta. Essa tela relaciona todos os diretórios configurados do usuário, inclusive o Native Directory.

3. Clique em **Novo**.
4. Em **Tipo de Diretório**, selecione uma opção:
 - **Lightweight Directory Access Protocol (LDAP)** para configurar um diretório de usuário baseado em LDAP diferente do Active Directory. Selecione esta opção para configurar o Oracle Virtual Directory.
 - **Microsoft Active Directory (MSAD)** para configurar o Active Directory.

Somente **Active Directory e ADAM (Active Directory Application Mode)**: se você deseja usar um atributo de ID personalizado (um atributo diferente de ObjectGUID; por exemplo sAMAccountName com o Active Directory or ADAM, select **Lightweight Directory Access Protocol (LDAP)**, e configure-o como tipo de diretório *Outros*.

5. Clique em **Próximo**.



6. Insira os parâmetros necessários.

Tabela 4-1 Tela de Informações de Conexão





Rótulo	Descrição
Servidor de Diretórios	<p>Selecione um diretório de usuário. O valor Atributo de ID é alterado para o atributo de identidade exclusiva de constante recomendado do produto selecionado.</p> <p>Essa propriedade será selecionada automaticamente se você escolher Active Directory na etapa 4.</p> <p>Selecione <code>Outros</code> nos seguintes cenários:</p> <ul style="list-style-type: none"> • Você está configurando um tipo de diretório de usuários não listado; por exemplo, o Oracle Virtual Directory • Você está configurando um diretório de usuário ativado para LDAP (por exemplo, OID), mas quer usar um Atributo de ID personalizado. • Você está configurando o Active Directory ou ADAM para usar um Atributo de ID personalizado.
	<p> Nota:</p> <p>Como o Oracle Virtual Directory oferece uma abstração virtualizada de diretórios LDAP e de repositórios de dados do RDMBS em uma exibição de diretório, o Oracle Enterprise Performance Management System o considera um único diretório de usuário externo, independentemente do número e do tipo de diretório de usuário permitidos pelo Oracle Virtual Directory.</p>
Nome	<p>Exemplo: Oracle Internet Directory</p> <p>Um nome descritivo do diretório de usuário. Usado para identificar um diretório de usuário específico se vários diretórios de usuário estiverem configurados. O nome não deve conter caracteres especiais diferentes de espaço e sublinhado.</p> <p>Exemplo: Corporate_OID</p>

Tabela 4-1 (Cont.) Tela de Informações de Conexão

Rótulo	Descrição
Pesquisa DNS	<p>Somente Active Directory: Selecione essa opção para habilitar a pesquisa DNS. Consulte Pesquisa de DNS e Pesquisa de Nome de Host. A Oracle recomenda configurar a pesquisa DNS como o método para conexão ao Active Directory em ambientes de produção para evitar falhas de conexão.</p> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> Nota:</p> <p>Não selecione essa opção se você estiver configurando um catálogo global.</p> </div> <p>Quando você seleciona esta opção, os seguintes campos são exibidos:</p> <ul style="list-style-type: none"> • Domínio: O nome de domínio de uma floresta do Active Directory. Exemplos: <code>example.com</code> ou <code>us.example.com</code> • Site do AD: o nome do site do Active Directory, em geral o nome distinto relativo do objeto do site armazenado no recipiente de configuração do Active Directory. Normalmente, o Site do AD identifica um local geográfico como uma cidade, um estado, uma região ou um país. Exemplos: <code>Santa Clara</code> ou <code>US_West_region</code> • Servidor DNS: nome do DNS do servidor que suportar pesquisa do servidor DNS para controladores de domínio.
Nome do Host	<p>Somente Active Directory: Selecione essa opção para habilitar a pesquisa de nome de host estático. Consulte Pesquisa de DNS e Pesquisa de Nome de Host.</p> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> Nota:</p> <p>Selecione essa opção se estiver configurando um catálogo global do Active Directory.</p> </div>
Nome do Host	<p>Nome DNS do servidor de diretório do usuário. Use o nome de domínio totalmente qualificado se o diretório do usuário tiver que ser usado para suportar SSO do SiteMinder. A Oracle recomenda o uso do nome do host para estabelecer uma conexão do Active Directory para testes.</p> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> Nota:</p> <p>Se você estiver configurando um catálogo global do Active Directory, especifique o nome do host do servidor do catálogo global. Consulte Catálogo Global.</p> </div>

Exemplo: MyServer

Tabela 4-1 (Cont.) Tela de Informações de Conexão



Rótulo	Descrição
Porta	<p>O número da porta em que o diretório de usuário está em execução.</p> <div style="border: 1px solid #0070C0; padding: 10px; margin-top: 10px;"> <p> Nota:</p> <p>Se você estiver configurando um catálogo global do Active Directory, especifique a porta usada pelo servidor de catálogo global (o padrão é 3268). Consulte Catálogo Global.</p> </div> <p>Exemplo: 389</p>
Habilitado para SSL	A caixa de seleção que permite a comunicação segura com o diretório do usuário. O diretório do usuário deve ser configurado para a comunicação segura.
DN de Base	<p>O nome distinto (DN) do nó em que a pesquisa de-usuários e grupos deve começar. Você pode usar o botão Buscar DNs para listar os DNs de base disponíveis e, em seguida, selecione o DN de base apropriado na lista.</p> <div style="border: 1px solid #0070C0; padding: 10px; margin-top: 10px;"> <p> Nota:</p> <p>Se você estiver configurando um catálogo global, especifique o DN de base da floresta.</p> </div> <p>Consulte Uso de Caracteres Especiais para ver as restrições sobre o uso de caracteres especiais.</p> <p>A Oracle recomenda que você selecione o menor DN que contenha todos os usuários e grupos do produto EPM System.</p> <p>Exemplo: dc=example,dc=com</p>
Atributo de ID	<p>Este valor de atributo pode ser modificado apenas se Outro for selecionado em Tipo de Diretório. Esse atributo deve ser um atributo comum que existe em objetos de usuários e grupos no servidor de diretórios.</p> <p>O valor recomendado desse atributo é definido automaticamente para OID (orclguid), SunONE (nsuniqueid), IBM Directory Server (Ibm-entryUuid), Novell eDirectory (GUID) e Active Directory (ObjectGUID).</p> <p>Exemplo: orclguid</p> <p>O valor do atributo ID, se você defini-lo manualmente depois de escolher Outro no Servidor de Diretório; por exemplo, para configurar um Oracle Virtual Directory, você deve:</p> <ul style="list-style-type: none"> • Apontar para um atributo exclusivo • Não ser específico ao local • Não alterar com o tempo

Tabela 4-1 (Cont.) Tela de Informações de Conexão


Rótulo	Descrição
Tamanho Máximo	<p>O número máximo de resultados que uma pesquisa pode retornar. Se esse valor for maior que o aceito pelas configurações do diretório de usuário, o valor do diretório de usuário substituirá esse valor.</p> <p>Para diretórios de usuário que não sejam Active Directory, deixe esse campo em branco para recuperar todos os usuários e grupos que atendam aos critérios de pesquisa.</p> <p>No Active Directory, defina esse valor como 0 para recuperar todos os usuários e grupos que atendam aos critérios de pesquisa.</p> <p>Se você estiver configurando o Oracle Hyperion Shared Services no modo Administração Delegada, defina esse valor como 0.</p>
Confiável	<p>A caixa de seleção para indicar que esse provedor é uma origem SSO confiável. Os tokens SSO de origens confiáveis não contêm a senha do usuário.</p>
Associação Anônima	<p>A caixa de seleção para indicar que o Shared Services pode se associar de forma anônima ao diretório de usuário para pesquisar usuários e grupos. Pode ser usada apenas se o diretório de usuário permitir associações anônimas. Se essa opção não estiver selecionada, você deverá especificar no DN do Usuário uma conta com permissões de acesso suficientes para pesquisar o diretório em que as informações do usuário estão armazenadas.</p> <p>A Oracle recomenda que você não use associação anônima.</p>
<div style="border: 1px solid #0070C0; padding: 5px; background-color: #E6F2FF;">  Nota: A associação anônima não é aceita no OID. </div>	
DN de Usuário	<p>Essa opção estará desmarcada se Ligação Anônima estiver selecionada.</p> <p>O nome distinto do usuário que o Shared Services deve usar para se associar ao diretório de usuário. Este usuário deverá ter o privilégios de pesquisa no atributo RDN no DN. No dn, por exemplo: <code>cn=John Doe, ou=people, dc=myCompany, dc=com</code>, o usuário da associação deve ter acesso ao atributo <code>cn</code>.</p> <p>Caracteres especiais no DN de Usuário devem ser especificados usando caracteres de escape. Consulte Uso de Caracteres Especiais para ver as restrições.</p> <p>Exemplo: <code>cn=admin, dc=myCompany, dc=com</code></p>
Incluir DN de Base	<p>A caixa de seleção para incluir o DN de base para o DN de Usuário. Se você estiver usando o Gerente de Diretórios como o DN de Usuário, não inclua o DN de Base.</p> <p>Essa caixa de seleção estará desmarcada se a opção Associação Anônima estiver selecionada.</p>

Tabela 4-1 (Cont.) Tela de Informações de Conexão

Rótulo	Descrição
Senha	Senha do DN de Usuário Essa caixa estará desmarcada se a opção Associação Anônima estiver selecionada. Exemplo: UserDNpassword
Mostrar Opções Avançadas	A caixa de seleção para exibir opções avançadas.
Referências	Somente Active Directory : Se o Active Directory estiver configurado para seguir referências, selecione <code>follow</code> para seguir automaticamente as referências do LDAP. Selecione <code>ignorar</code> para não usar as referências.
Alias de Referência	Selecione o método que as pesquisas do Shared Services devem usar para cancelar aliases no diretório de usuários, de modo que as pesquisas recuperem o objeto para o qual o DN do alias aponta. Selecione: <ul style="list-style-type: none"> • Sempre: sempre cancela os aliases. • Nunca: nunca cancela os aliases. • Localizar: cancela os aliases apenas durante a resolução de nomes. • Pesquisa: cancela os aliases apenas após a resolução de nomes.
Tempo Limite de Leitura da Conexão	Intervalo (segundos) após o qual o provedor LDAP aborta a tentativa de leitura caso ele não obtenha uma resposta. Padrão: 60 segundos
Máx. de Conexões	Máximo de conexões no pool de conexões. O padrão é 100 para diretórios com base em LDAP, incluindo o Active Directory. Padrão: 100
Tempo Limite	Tempo limite para obter uma conexão do pool. Uma exceção é lançada depois desse período. Padrão: 300000 milissegundos (5 minutos)
Intervalo de Remoção	Opcional: o intervalo para executar o processo de remoção para limpar o pool. O processo de remoção remove conexões inativas que excederam o Tempo de Conexão Inativo Permitido. Padrão: 120 minutos
Tempo de Conexão Inativo Permitido	Opcional: O tempo após o qual o processo de remoção remove as conexões inativas do pool. Padrão: 120 minutos
Ampliar Conexões	Essa opção indica se o pool de conexões pode crescer além do Máx. de Conexões. Selecionado por padrão. Se você não permitir que o pool de conexão cresça, o sistema retornará um erro se uma conexão não estiver disponível dentro do tempo disponível definido como Tempo Limite.

Tabela 4-1 (Cont.) Tela de Informações de Conexão

Rótulo	Descrição
Ativar Módulo de Autenticação Personalizada	A caixa de seleção para ativar o uso de um módulo de autenticação personalizado para autenticar usuários definidos nesse diretório de usuário. É necessário também inserir o nome da classe de Java totalmente qualificado do módulo de autenticação na tela Opções de Segurança. Consulte Configuração de Opções de Segurança . A autenticação do módulo de autenticação personalizado é transparente aos clientes finos e espessos e não requer alterações de disponibilização do cliente. Consulte o tópico sobre como usar um módulo de autenticação personalizado no <i>Guia de Configuração de Segurança do Oracle Enterprise Performance Management System</i> .

7. Clique em **Próximo**.

O Shared Services usa as propriedades definidas na tela Configuração do Usuário para criar um URL de usuário que será usado para determinar o nó em que a pesquisa por usuários começará. O uso dessa URL acelera a pesquisa.

 **Cuidado:**

O URL de usuário não deve apontar para um alias. A segurança do EPM System requer que o URL do usuário aponte para um usuário real.

A Oracle recomenda que você use a área Configuração Automática da tela para recuperar as informações necessárias.

The screenshot shows the Oracle Identity Management console with the 'Configure User Directories' wizard. The 'User Configuration' step is active, displaying fields for User RDN, Login Attribute, First Name Attribute, Last Name Attribute, Email Attribute, and Object Class. The 'Advanced Options' section includes a filter to limit users and a checkbox for resolving custom primary groups. The 'Password Warning Notification' section has a checkbox for showing warnings.

 **Nota:**

Consulte [Uso de Caracteres Especiais](#) para obter uma lista de caracteres especiais que podem ser usados na configuração do usuário.

8. Em **Configuração Automática**, insira um identificador de usuário exclusivo usando o formato *attribute=identifier*; por exemplo, *uid=jdoe*.

Os atributos do usuário são exibidos na área Configuração de Usuário.

Se você estiver configurando o OID, não será possível configurar automaticamente o filtro de usuário, pois o DSE raiz do OID não contém entradas do atributo Contextos de Nomenclatura. Consulte [Gerenciamento de Contextos de Nomenclatura](#) no *Guia do Administrador do Oracle Fusion Middleware para o Oracle Internet Directory*.

 **Nota:**

Você pode inserir manualmente os atributos do usuário necessários nas caixas de texto na área Configuração do Usuário.

Tabela 4-2 Tela de Configuração de Usuário

Rótulo	Descrição ¹
RDN do Usuário	<p>O DN Relativo do usuário. Cada componente de um DN é chamado de um RDN e representa uma ramificação da árvore de diretórios. O RDN de um usuário é geralmente o equivalente do <code>uid</code> ou <code>cn</code>.</p> <p>Consulte Uso de Caracteres Especiais para ver as restrições.</p> <p>Exemplo: <code>ou=People</code></p>
Atributo de Logon	<p>Um atributo exclusivo (pode ser um atributo personalizado) que armazena o nome de logon do usuário. Os usuários usam o valor desse atributo como o nome do usuário ao fazer logon nos produtos do EPM System.</p> <p>Os IDs do Usuário (valor do Atributo de Logon) devem ser exclusivos em todos os diretórios de usuário. Por exemplo, você pode usar <code>uid</code> e <code>sAMAccountName</code>, respectivamente, como o Atributo de Logon para suas configurações do SunONE e do Active Directory. Os valores desses atributos devem ser exclusivos em todos os diretórios do usuário, incluindo o Native Directory.</p>
	<p> Nota:</p> <p>Os IDs do Usuário não fazem distinção entre maiúsculas e minúsculas.</p>
	<p> Nota:</p> <p>Se você estiver configurando o OID como um diretório de usuário externo para produtos EPM System implantados no Oracle Application Server em um ambiente Kerberos, será preciso definir essa propriedade como <code>userPrincipalName</code>.</p>
	<p>Padrão</p> <ul style="list-style-type: none"> • Active Directory: <code>cn</code> • Diretórios LDAP além do Active Directory: <code>uid</code>
Atributo do Primeiro Nome	<p>O atributo que armazena o nome do usuário</p> <p>Padrão: <code>givenName</code></p>
Atributo de Sobrenome	<p>O atributo que armazena o sobrenome do usuário</p> <p>Padrão: <code>sn</code></p>
Atributo de E-mail	<p>Opcional: o atributo que armazena o endereço de e-mail do usuário</p> <p>Padrão: <code>mail</code></p>

Tabela 4-2 (Cont.) Tela de Configuração de Usuário


Rótulo	Descrição ¹
Classe de Objeto	<p>As classes de objeto do usuário (os atributos obrigatórios e opcionais que podem ser associados ao usuário). O Shared Services usa as classes de objeto desta tela no filtro de pesquisa. Usando essas classes de objeto, o Shared Services deve localizar todos os usuários que devem ser provisionados.</p> <div style="border: 1px solid #0070C0; padding: 10px; margin: 10px 0;"> <p> Nota:</p> <p>Caso o Active Directory ou ADAM esteja sendo configurado como diretório de usuário tipo <code>Outros</code> para usar um atributo de ID personalizado, você deverá definir esse valor como <code>user</code>.</p> </div> <p>Você pode adicionar manualmente classes de objeto, se necessário. Para adicionar uma classe de objeto, digite o nome da classe de objeto na caixa Classe de Objeto e clique em Adicionar.</p> <p>Para excluir classes de objeto, selecione a classe de objeto e clique em Remover.</p> <p>Padrão</p> <ul style="list-style-type: none"> • Active Directory: <code>usuário</code> • Diretórios LDAP além do Active Directory: <code>person</code>, <code>organizationalPerson</code>, <code>inetorgperson</code>
Filtrar para Limitar Usuários	<p>Uma consulta de LDAP que recupera apenas os usuários que devem ser provisionados com funções de produtos do EPM System. Por exemplo, a consulta de LDAP (<code>uid=Hyp*</code>) recupera apenas usuários cujos nomes começam com <code>Hyp</code>.</p> <p>A tela Configuração de Usuário valida o RDN do Usuário e recomenda o uso de um filtro de usuários, se for necessário.</p> <p>O filtro de usuários limita o número de usuários retornados durante uma consulta. Será especialmente importante se o nó identificado pelo RDN do usuário contiver vários usuários que não precisam ser provisionados. Os filtros de usuários podem ser projetados para excluir os usuários que não devem ser provisionados, melhorando, assim, o desempenho.</p>

Tabela 4-2 (Cont.) Tela de Configuração de Usuário

Rótulo	Descrição ¹
Atributo de Pesquisa do Usuário para o RDN de Vários Atributos	<p>Diretórios de usuário habilitados para LDAP além do Active Directory somente: defina este valor somente se o servidor de diretórios estiver configurado para usar um RDN de vários atributos. O valor definido deve ser um dos os atributos de RDN. O valor do atributo especificado deve ser exclusivo e o atributo deve ser pesquisável.</p> <p>Por exemplo, suponha que a um servidor de diretório SunONE está configurado para combinar os atributos <code>cn</code> (<code>cn=John Doe</code>) e <code>uid</code> (<code>uid=jDoe12345</code>) para criar um RDN de vários atributos similar ao seguinte:</p> <pre>cn=John Doe+uid=jDoe12345, ou=people, dc=myCompany, dc=com</pre> <p>Nesse caso, você pode usar <code>cn</code> ou <code>uid</code>, caso esses atributos atendam às seguintes condições:</p> <ul style="list-style-type: none"> • O atributo é pesquisável pelo usuário identificado DN de Usuário arquivado na guia Informações. • O atributo exige que você defina um valor único no diretório do usuário.
Resolver Grupos Primários Personalizados	<p>Somente Active Directory: a caixa de seleção que indica se devem ou não ser identificados grupos primários de usuários para determinar funções efetivas. Esta caixa de seleção é marcada por padrão. A Oracle recomenda que você não altere esta definição.</p>
Exibe aviso de que a senha do usuário expira em:	<p>Apenas Active Directory: a caixa de seleção que indica se deve ou não ser exibida uma mensagem caso a senha do usuário do Active Directory expire dentro de um número determinado de dias.</p>

¹ A segurança do EPM System pode usar valores padrão para alguns campos para os quais o valor de configuração é opcional. Se você não inserir valores em tais campos, valores padrão serão usados durante o run-time.

9. Clique em **Próximo**.

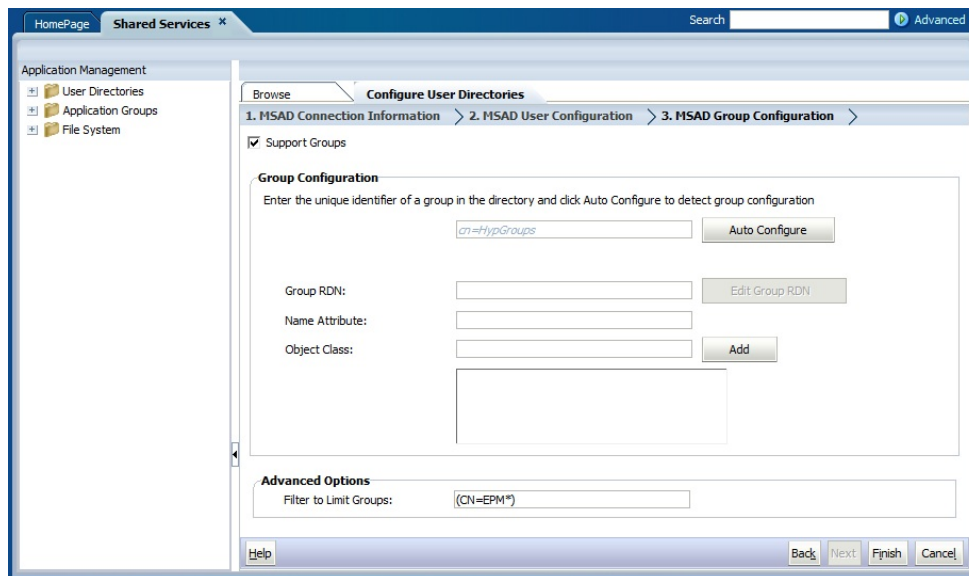
A tela Configuração de Grupo é exibida. O Shared Services usa as propriedades definidas nesta tela para criar a URL do grupo que determina o nó em que começa a pesquisa de grupos. O uso dessa URL acelera a pesquisa.

Cuidado:

A URL do Grupo não deve apontar para um alias. A segurança do EPM System exige que a URL do grupo aponte para um grupo real. Se você estiver configurando um Novell eDirectory que usa aliases de grupos, esses aliases e as contas dos grupos devem estar disponíveis dentro da URL do grupo.

 **Nota:**

A entrada de dados na tela Configuração de Grupo é opcional. Se você não inserir as configurações de URL do grupo, o Shared Services pesquisará no DN de Base para localizar grupos, o que pode afetar de forma negativa o desempenho, especialmente se o diretório de usuário contiver vários grupos.



10. Desmarque **Supportar Grupos** se sua organização não pretende provisionar grupos ou se os usuários não estiverem categorizados em grupos no diretório de usuário. A desmarcação dessa opção desativa os campos nesta tela.

Se você estiver aceitando grupos, a Oracle recomenda usar o recurso de configuração automática para recuperar as informações necessárias.

Se estiver configurando o OID como um diretório de usuário, você não poderá usar o recurso de configuração automática, pois o DSE raiz do OID não contém entradas do atributo Contextos de Nomenclatura. Consulte [Gerenciamento de Contextos de Nomenclatura](#) no *Guia do Administrador do Oracle Fusion Middleware para Oracle Internet Directory*.

11. Na caixa de texto **Configuração Automática**, digite um identificador de grupo exclusivo e clique em **Ir**.

O identificador de grupo deve ser expressado no formato `attribute=identifier`; por exemplo `cn=western_region`.

Os atributos do grupo são exibidos na área Configuração de Grupo.

 **Nota:**

Você pode inserir os atributos de grupo necessários nas caixas de texto Configuração de Grupo.

▲ Cuidado:

Se o URL de grupo não estiver definido para diretórios do usuário que contenham / (barra) ou \ (barra invertida) em seus nomes de nós, a pesquisa de usuários e grupos falhará. Por exemplo, qualquer operação para listar o usuário ou grupo falhará se o URL de grupo não estiver especificado para um diretório de usuário no qual os usuários e grupos existem em um nó, como `OU=child\ou,OU=parent/ou` ou `OU=child/ou,OU=parent \ ou`.

Tabela 4-3 Tela de Configuração de Grupo



Rótulo	Descrição ¹
RDN do Grupo	<p>O Relative DN do grupo. Este valor, que se refere ao caminho para o Base DN, é usado como o URL do grupo. Especifique um RDN do Grupo que identifica o menor nó do diretório de usuário no qual todos os grupos que você planeja provisionar estão disponíveis.</p> <p>Se você usar um grupo primário do Active Directory para provisionamento, verifique se o grupo primário se encaixa no Grupo RDN. O Shared Services não recupera o grupo primário se ele estiver fora do escopo do URL do grupo.</p> <p>O RDN do Grupo tem um impacto significativo no logon e no desempenho da pesquisa. Como ele é o ponto inicial de todas as pesquisas do grupo, você deve identificar o menor nó possível no qual todos os grupos de produtos EPM System estão disponíveis. Para garantir desempenho ideal, o número de grupos presentes dentro do RDN do Grupo não deve exceder 10.000. Se mais grupos estiverem presentes, use um filtro de grupos para recuperar apenas os grupos que você deseja provisionar.</p> <div style="border: 1px solid #0070C0; padding: 10px; margin-top: 10px;"> <p> Nota:</p> <p>O Shared Services exibirá um aviso se o número de grupos disponíveis dentro do URL de Grupo exceder 10.000.</p> </div> <p>Consulte Uso de Caracteres Especiais para ver as restrições.</p> <p>Exemplo: <code>ou=Groups</code></p>
Atributo do Nome	<p>O atributo que armazena o nome do grupo</p> <p>Padrão</p> <ul style="list-style-type: none"> • Diretórios LDAP incluindo Active Directory: <code>cn</code> • Native Directory: <code>cssDisplayNameDefault</code>

Tabela 4-3 (Cont.) Tela de Configuração de Grupo

Rótulo	Descrição ¹
Classe do objeto	<p>As classes de objeto do grupo. O Shared Services usa as classes de objeto desta tela no filtro de pesquisa. Usando essas classes de objeto, o Shared Services deve localizar todos os grupos associados ao usuário.</p> <div style="border: 1px solid #0070C0; padding: 10px; margin: 10px 0;"> <p> Nota:</p> <p>Caso o Active Directory ou ADAM esteja sendo configurado como diretório de usuário tipo <code>Outros</code> para usar um atributo de ID personalizado, você deverá definir esse valor como <code>group?member</code>.</p> </div> <p>Você pode adicionar manualmente classes de objeto, se necessário. Para adicionar uma classe de objeto, insira o nome da classe de objeto na caixa de texto Classe de objeto e clique em Adicionar.</p> <p>Para excluir classes de objeto, selecione a classe de objeto e clique em Remover.</p> <p>Padrão</p> <ul style="list-style-type: none"> Active Directory: <code>group?member</code> Diretórios LDAP além do Active Directory: <code>groupofuniquenames?uniquemember, groupOfNames?member</code> Native Directory: <code>groupofuniquenames?uniquemember, cssGroupExtend?cssIsActive</code>
Filtrar para Limitar Grupos	<p>Uma consulta de LDAP que recupera apenas os grupos que devem ser provisionados com funções de produtos do EPM System. Por exemplo, a consulta de LDAP (<code> (cn=Hyp*) (cn=Admin*)</code>) recupera apenas grupos cujos nomes começam com <code>Hyp</code> ou <code>Admin</code>.</p> <p>O filtro de grupos, usado para limitar o número de grupos retornados durante uma consulta, será especialmente importante se o nó identificado pelo RDN do Grupo contiver vários grupos que não precisam ser provisionados. Os filtros podem ser projetados para excluir os grupos que não devem ser provisionados, aprimorando o desempenho.</p> <p>Se você usar o grupo primário do Active Directory para provisionamento, verifique se cada filtro de grupo definido pode recuperar o grupo primário contido no escopo do URL do grupo. Por exemplo, o filtro (<code> (cn=Hyp*) (cn=Domain Users)</code>) recupera grupos com nomes que começam com <code>Hyp</code> e o grupo primário chamado <code>Domain Users</code>.</p>

¹ A segurança do EPM System pode usar valores padrão para alguns campos para os quais o valor de configuração é opcional. Se você não inserir valores em tais campos, valores padrão serão usados durante o run-time.

12. Clique em **Concluir**.

O Shared Services salva a configuração e retorna à tela Diretórios de Usuário Definidos, que lista agora o diretório de usuário configurado por você.

13. Teste a configuração. Consulte [Como Testar Conexões do Diretório de Usuário](#).
14. Se for necessário, altere a atribuição da ordem de pesquisa. Consulte [Gerenciamento da Ordem de Pesquisa do Diretório de Usuário](#) para obter detalhes.
15. Se for necessário, especifique as opções de segurança. Consulte [Configuração de Opções de Segurança](#) para obter detalhes.
16. Reinicie o Oracle Hyperion Foundation Services e outros componentes do EPM System

Configuração de Bancos de Dados Relacionais como Diretórios de Usuário

As informações de usuários e grupos nas tabelas de sistema dos bancos de dados relacionais Oracle, SQL Server e IBM DB2 podem ser usadas para realizar o provisionamento. Se não for possível derivar as informações de grupo do esquema de sistema do banco de dados, o Oracle Hyperion Shared Services não permitirá o provisionamento de grupos desse provedor de banco de dados. Por exemplo, o Shared Services não pode extrair informações de grupos de versões mais antigas do IBM DB2 porque o banco de dados utiliza grupos definidos no sistema operacional. No entanto, os gerentes de provisionamento podem adicionar esses usuários a grupos no Native Directory e provisionar esses grupos. Para obter informações sobre plataformas permitidas, consulte a *Matriz de Certificação do Oracle Enterprise Performance Management System* publicada na página [Configurações do Sistema Suportado do Oracle Fusion Middleware](#) do Oracle Technology Network (OTN).

Nota:

Caso você esteja usando um banco de dados DB2, o nome de usuário deverá conter pelo menos 8 caracteres. Os nomes de usuário não devem exceder 256 caracteres (bancos de dados Oracle e SQL Server) e 1000 caracteres (DB2).

É necessário configurar o Shared Services para se conectar ao banco de dados como administrador de banco de dados; por exemplo, o usuário `SYSTEM` do Oracle, para recuperar a lista de usuários e de grupos.

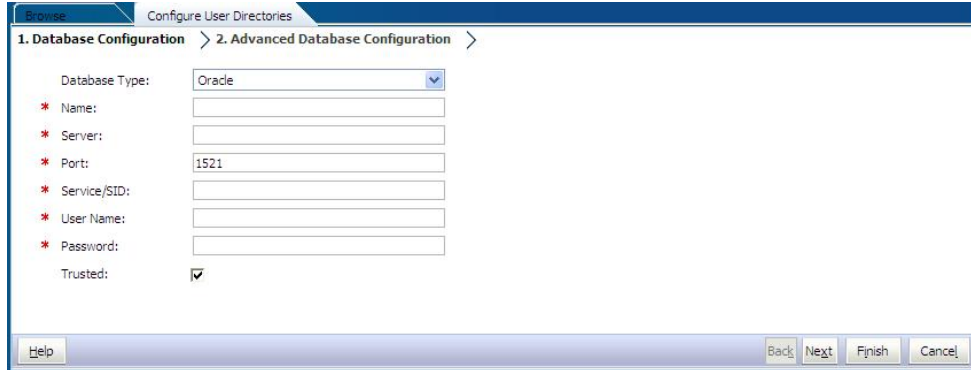
Nota:

O Shared Services recupera somente usuários de bancos de dados ativos para provisionamento. As contas de usuário de banco de dados inativas e bloqueadas são ignoradas.

Para configurar provedores de banco de dados:

1. Acesse o Oracle Hyperion Shared Services Console como Administrador do Sistema. Consulte [Iniciando o Shared Services Console](#).
2. Selecione **Administração** e **Configurar Diretórios de Usuário**.

3. Clique em **Novo**.
4. Na tela **Tipo de Diretório**, selecione **Banco de Dados Relacional (Oracle, DB2, SQL Server)**.
5. Clique em **Próximo**.



6. Na guia Configuração de Banco de Dados, digite os parâmetros de configuração

Tabela 4-4 Guia Configuração do Banco de Dados

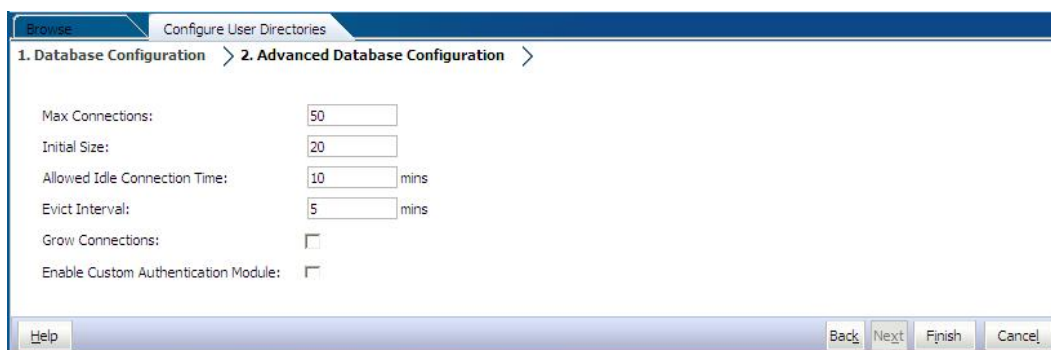
Rótulo	Descrição
Tipo de Banco de Dados	Provedor de banco de dados relacional. O Shared Services oferece suporte somente aos bancos de dados Oracle e SQL Server como provedores de banco de dados. Exemplo: Oracle
Nome	Um nome exclusivo de configuração para o provedor de banco de dados. Exemplo: Oracle_DB_FINANCE
Servidor	O nome do DNS do computador em que o servidor de banco dados está sendo executado. Exemplo: myserver
Porta	Número da porta do servidor de banco de dados Exemplo: 1521
Serviço/SID (Somente Oracle)	O identificador de sistema (o padrão é orcl). Exemplo: orcl
Banco de Dados (somente SQL Server e DB2)	Banco de dados ao qual o Shared Services deve se conectar Exemplo: master
Nome do Usuário	O nome de usuário que o Shared Services deve usar para acessar o banco de dados. Esse usuário de banco de dados deverá ter privilégios de acesso às tabelas do sistema de banco de dados. A Oracle recomenda usar a conta <code>system</code> com bancos de dados Oracle e o nome de usuário do administrador com os bancos de dados SQL Server. Exemplo: SYSTEM
Senha	Senha do usuário identificado no Nome do Usuário . Exemplo: system_password

Tabela 4-4 (Cont.) Guia Configuração do Banco de Dados

Rótulo	Descrição
Confiável	A caixa de verificação que especifica que o provedor é uma origem SSO confiável. Os tokens SSO de origens confiáveis não contêm a senha do usuário.

7. **Opcional:** Clique em **Avançar** para configurar o pool de conexão.

A guia de Configuração Avançada de Banco de Dados é aberta.



8. Em Configuração Avançada de Banco de Dados, digite os parâmetros do pool de conexões.

Tabela 4-5 Guia Configuração Avançada de Banco de Dados

Rótulo	Descrição
Máx. de Conexões	Máximo de conexões no pool. O padrão é 50.
Tamanho Inicial	Conexões disponíveis quando o pool é inicializado. O Padrão é 20.
Tempo de Conexão Inativo Permitido	Opcional: O tempo após o qual o processo de remoção remove as conexões inativas do pool. O padrão é 10 minutos.
Intervalo de Remoção	Opcional: o intervalo de execução do processo de remoção para limpeza do pool. A Remoção retira as conexões inativas que tenham excedido o Tempo de Conexão Inativo Permitido. O padrão é 60 minutos.
Ampliar Conexões	Indica se o pool de conexão pode crescer além de Máx. de Conexões. Por padrão, essa opção aparece esmaecida, indicando que o pool não pode crescer. Se você não permitir que o pool de conexão cresça, o sistema retornará um erro se uma conexão não estiver disponível dentro do tempo disponível definido como Tempo Limite.

Tabela 4-5 (Cont.) Guia Configuração Avançada de Banco de Dados

Rótulo	Descrição
Ativar Módulo de Autenticação Personalizada	A caixa de seleção para ativar o uso de um módulo de autenticação personalizado para autenticar usuários definidos nesse diretório de usuário. É necessário também inserir o nome da classe de Java totalmente qualificado do módulo de autenticação na tela Opções de Segurança. Consulte Configuração de Opções de Segurança . A autenticação do módulo de autenticação personalizado é transparente aos thin clients e thick clients. Consulte o tópico sobre como usar um módulo de autenticação personalizado no <i>Guia de Configuração de Segurança do Oracle Enterprise Performance Management System</i> .

9. Clique em **Concluir**.
10. Clique em **OK** para voltar à tela Diretórios de Usuário Definidos.
11. Teste a configuração do provedor de banco de dados. Consulte [Como Testar Conexões do Diretório de Usuário](#).
12. Altere a atribuição da ordem de pesquisa, se necessário. Consulte [Gerenciamento da Ordem de Pesquisa do Diretório de Usuário](#) para obter detalhes.
13. Especifique as configurações de segurança, se necessário. Consulte [Configuração de Opções de Segurança](#).
14. Reinicie o Oracle Hyperion Foundation Services e outros componentes do Oracle Enterprise Performance Management System.

Como Testar Conexões do Diretório de Usuário

Após configurar o diretório de usuário, teste a conexão para verificar se o Oracle Hyperion Shared Services consegue se conectar ao diretório de usuário usando as configurações atuais.

Para testar a conexão do diretório de usuário:

1. Acesse o Oracle Hyperion Shared Services Console como Administrador do Sistema. Consulte [Iniciando o Shared Services Console](#).
2. Selecione **Administração** e **Configurar Diretórios de Usuário**.
3. Na lista de diretórios de usuários, selecione uma configuração de diretório externo de usuários para testar.
4. Clique em **Testar** e em **OK**.

Edição de Configurações do Diretório de Usuário

Os administradores podem modificar qualquer parâmetro, exceto o nome, de uma configuração do diretório de usuário. A Oracle recomenda não editar os dados de configuração dos diretórios de usuários que foram usados para provisionamento.

 **Cuidado:**

A edição de algumas configurações, por exemplo, o `Atributo de ID` da configuração do diretório de usuário invalida os dados de provisionamento. Tenha muito cuidado ao modificar as configurações de um diretório de usuário que tenha sido provisionado.

Para editar uma configuração de diretório de usuário:

1. Acesse o Oracle Hyperion Shared Services Console como Administrador do Sistema. Consulte [Iniciando o Shared Services Console](#).
2. Selecione **Administração e Configurar Diretórios de Usuário**.
3. Selecione um diretório de usuários para edição.
4. Clique em **Editar**.
5. Modifique as definições de configuração.

 **Nota:**

Não é possível modificar o nome da configuração. Se você estiver modificando uma configuração de diretório de usuários LDAP, poderá escolher um servidor de diretório diferente ou `Outros` (para diretóriosLDAP personalizados) na lista Directory Server. Você não pode editar os parâmetros do Native Directory.

Para obter uma explicação sobre os parâmetros que podem ser editados, consulte as seguintes tabelas:

- Active Directory e outros diretórios de usuário baseados em LDAP. Consulte as tabelas em [Configuração de OID, Active Directory e Outros Diretórios de Usuário com Base em LDAP](#).
 - Bancos de dados: Consulte a tabela em [Configuração de Bancos de Dados Relacionais como Diretórios de Usuário](#)
6. Clique em **OK** para salvar as alterações.

Exclusão de Configurações do Diretório de Usuário

Os Administradores do Sistema podem excluir uma configuração de diretório de usuários externos a qualquer momento. A exclusão de uma configuração invalida todas as informações de provisionamento dos usuários e grupos derivados do diretório de usuário e remove o diretório da ordem de pesquisa.



Dica:

Se você não quiser usar um diretório de usuários configurado que foi usado no provisionamento, remova-o da ordem de pesquisa para que ele não seja pesquisado por usuários e grupos. Esse procedimento mantém a integridade da informações de provisionamento e habilita você a usar o diretório de usuários posteriormente.

Para excluir uma configuração do diretório de usuário:

1. Acesse o Oracle Hyperion Shared Services Console como Administrador do Sistema. Consulte [Iniciando o Shared Services Console](#).
2. Selecione **Administração e Configurar Diretórios de Usuário**.
3. Selecione um diretório.
4. Clique em **Excluir**.
5. Clique em **OK**.
6. Clique em **OK** novamente.
7. Reinicie o Oracle Hyperion Foundation Services e outros componentes do Oracle Enterprise Performance Management System.

Gerenciamento da Ordem de Pesquisa do Diretório de Usuário

Quando um Administrador do Sistema configura um diretório de usuários externos, o Oracle Hyperion Shared Services adiciona automaticamente o diretório de usuários à ordem da pesquisa e o atribui à próxima sequência de pesquisa disponível precedendo a do Native Directory. A ordem de pesquisa é usada para navegar sequencialmente pelos diretórios de usuários configurados quando o Oracle Enterprise Performance Management System pesquisa usuários e grupos.

Os Administradores do Sistema podem remover um diretório de usuários da ordem de pesquisa. Nesse caso, o Shared Services reatribui automaticamente a ordem de pesquisa dos diretórios restantes. Os diretórios de usuário que não fizerem parte da ordem de pesquisa não serão usados para permitir a autenticação e o provisionamento.



Nota:

O Shared Services interrompe a pesquisa do usuário ou grupo quando encontra a conta especificada. A Oracle recomenda que o diretório corporativo que contém a maior parte dos usuários do EPM System seja colocado no alto da ordem de pesquisa.

Por padrão, o Native Directory é configurado como o último diretório na ordem de pesquisa. Os administradores pode executar estas tarefas para gerenciar a ordem de pesquisa:

- [Adição de um Diretório de Usuário à Ordem de Pesquisa](#)
- [Alteração da Ordem de Pesquisa](#)
- [Remoção de uma Atribuição da Ordem de Pesquisa](#)

Adição de um Diretório de Usuário à Ordem de Pesquisa

Um diretório de usuário recém configurado é adicionado automaticamente à ordem de pesquisa. Se você remover um diretório da ordem de pesquisa, poderá adicioná-lo ao fim da ordem de pesquisa.

Para adicionar um diretório de usuário à ordem de pesquisa:

1. Acesse o Oracle Hyperion Shared Services Console como Administrador do Sistema. Consulte [Iniciando o Shared Services Console](#).
2. Selecione **Administração** e **Configurar Diretórios de Usuário**.
3. Selecione um diretório de usuários desativado a ser adicionado à ordem de pesquisa.
4. Clique em **Incluir**.
Este botão estará disponível somente se você tiver selecionado um diretório de usuário que não esteja na ordem de pesquisa.
5. Clique em **OK** para voltar à tela Diretórios de Usuário Definidos.
6. Reinicie o Oracle Hyperion Foundation Services e outros componentes do EPM System

Remoção de uma Atribuição da Ordem de Pesquisa

A remoção de um diretório de usuário da ordem de pesquisa não invalida a configuração do diretório. Ela remove o diretório de usuário da lista de diretórios pesquisados na autenticação de usuários. Um diretório não incluído na ordem de pesquisa é definido com o status *Desativado*. Quando um administrador remove um diretório de usuário da ordem de pesquisa, a sequência de pesquisa atribuída aos outros diretórios de pesquisa é automaticamente atualizada.



Nota:

O Native Directory não pode ser removido da ordem da pesquisa.

Para remover um diretório de usuário da ordem de pesquisa:

1. Acesse o Shared Services Console como Administrador do Sistema. Consulte [Iniciando o Shared Services Console](#).
2. Selecione **Administração** e **Configurar Diretórios de Usuário**.
3. Selecione um diretório a ser removido da ordem de pesquisa.
4. Clique em **Excluir**.
5. Clique em **OK**.
6. Clique em **OK** na tela de resultado da configuração do diretório
7. Reinicie o Foundation Services e outros componentes do EPM System

Alteração da Ordem de Pesquisa

A ordem de pesquisa padrão atribuída a cada diretório de usuário é baseada na sequência em que o diretório foi configurado. Por padrão, o Native Directory é configurado como o último diretório na ordem de pesquisa.

Para alterar a ordem de pesquisa:

1. Acesse o Shared Services Console como Administrador do Sistema. Consulte [Iniciando o Shared Services Console](#).
2. Selecione **Administração** e **Configurar Diretórios de Usuário**.
3. Selecione um diretório cuja ordem de pesquisa você deseja alterar.
4. Clique em **Move Up** ou **Move Down**.
5. Clique em **OK**.
6. Reinicie o Foundation Services, outros componentes do EPM System e aplicativos personalizados que usam os APIs de Segurança do Shared Services .

Configuração de Opções de Segurança

As opções de segurança compreendem os parâmetros globais aplicáveis a todos os diretórios de usuário incluídos na ordem de pesquisa.

Para configurar as opções de segurança:

1. Acesse o Oracle Hyperion Shared Services Console como Administrador do Sistema. Consulte [Iniciando o Shared Services Console](#).
2. Selecione **Administração** e **Configurar Diretórios de Usuário**.
3. Selecione **Opções de Segurança**.
4. Em **Opções de Segurança**, configure os parâmetros globais.

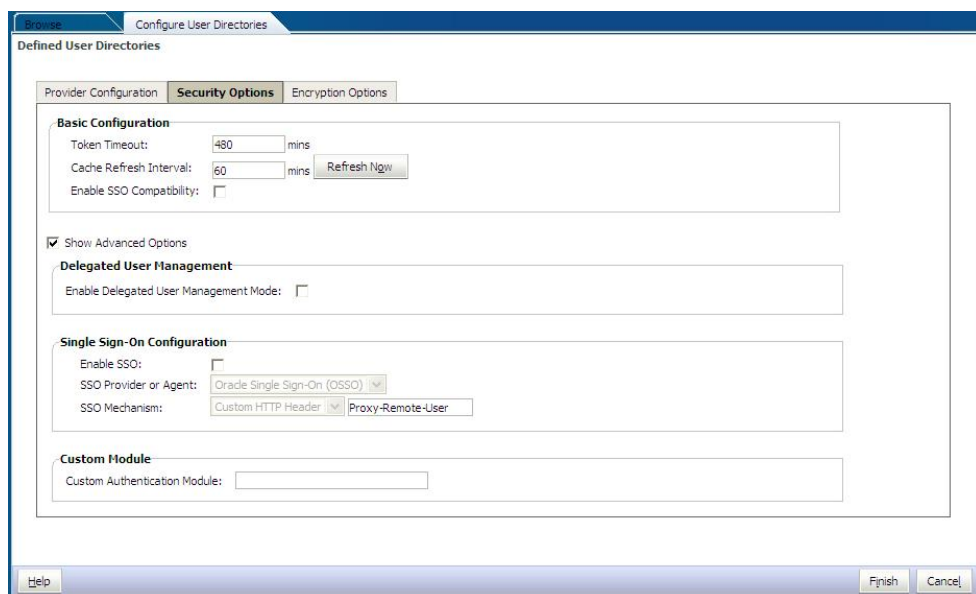


Tabela 4-6 Opções de Segurança para Diretórios de Usuário


Parâmetro	Descrição
Tempo Limite de Token	Tempo (em minutos) após o qual o token SSO emitido pelos produtos Oracle Enterprise Performance Management System ou a solução de gerenciamento de identidade da Web expira. Os usuários deverão fazer logon novamente após este período. O tempo limite de token é definido com base no relógio do sistema do servidor. O padrão é 480 minutos.
	<div style="border: 1px solid #0070C0; padding: 10px; background-color: #E6F2FF;"> <p> Nota:</p> <p>O tempo limite de token não é igual ao tempo limite da sessão.</p> </div>
Intervalo de Atualização de Cache	Intervalo (em minutos) para atualização do cache do Oracle Hyperion Shared Services de grupos para dados de relacionamento de usuários. O padrão é 60 minutos. As informações do cache do Shared Services sobre novos grupos de diretórios do usuário externo e novos usuários adicionados para os grupos existentes serão obtidas apenas após a próxima atualização do cache. Usuários provisionados através de um grupo de diretórios de usuário externo recém-criado não obtêm suas funções provisionadas até que o cache seja atualizado.
Atualizar Agora	Clique neste botão para inicializar manualmente a atualização do cache do Shared Services que contém grupos para dados de relacionamento de usuários. Pode ser necessário inicializar uma atualização de cache após a criação de novos grupos nos diretório de usuário externo e provisioná-los ou, posteriormente, adicionar novos usuários a grupos existentes. O cache é atualizado somente após o Shared Services realizar uma chamada que use os dados no cache.
Habilitar Compatibilidade do SSO	Selecione esta opção se sua implantação estiver integrada com o Oracle Business Intelligence Enterprise Edition Versão 11.1.1.5 ou anterior.
Habilitar Modo de Gerenciamento de Usuário Delegado	Opção que habilita o gerenciamento de usuário delegado dos produtos do EPM System para oferecer suporte ao gerenciamento distribuído das atividades de provisionamento. Consulte "Gerenciamento de Usuário Delegado" no <i>Guia de Administração da Segurança de Usuário do Sistema Oracle Enterprise Performance Management</i> .
Habilitar SSO	Opção que habilita o suporte de agentes de segurança para SSO como Oracle Access Manager

Tabela 4-6 (Cont.) Opções de Segurança para Diretórios de Usuário


Parâmetro	Descrição
Provedor ou Agente SSO	<p>Selecione a solução de gerenciamento de identidade na Web na qual os produtos do EPM System devem aceitar o SSO. Selecione Outros se a solução de gerenciamento de identidade na Web, por exemplo, Kerberos, não estiver listada. O mecanismo e o método SSO preferenciais são selecionados automaticamente quando você seleciona o provedor SSO. É possível alterar o nome do mecanismo SSO (cabeçalho HTTP ou a classe de log-in personalizada), se necessário.</p> <p>Se você selecionar Outro como o provedor ou agente de SSO, deverá garantir que ele seja compatível com um mecanismo de SSO suportado pelo EPM System. Consulte o tópico sobre os métodos de SSO permitidos no <i>Guia de Configuração de Segurança do Oracle Enterprise Performance Management System</i>.</p>
Mecanismo SSO	<p>Método usado pela solução de gerenciamento de identidades na Web selecionada para fornecer o nome de logon do usuário para os produtos do EPM System. Para obter uma descrição dos métodos de SSO aceitáveis, consulte o tópico sobre os métodos de SSO permitidos no <i>Guia de Configuração de Segurança do Oracle Enterprise Performance Management System</i>.</p> <ul style="list-style-type: none"> • Cabeçalho HTTP Personalizado: defina o nome do cabeçalho que o agente de segurança transmite ao EPM System. • Classe de Log-in Personalizada: especifique a classe Java personalizada que lida com as solicitações HTTP para autenticação. Consulte o tópico sobre a classe de logon personalizada no <i>Guia de Configuração de Segurança do Oracle Enterprise Performance Management System</i>. <div style="border: 1px solid #0070C0; padding: 5px; margin: 10px 0;"> <p> Nota:</p> <p>A Classe de Log-in Personalizado não é a mesma que a autenticação personalizada.</p> </div> <ul style="list-style-type: none"> • Cabeçalho de Autorização HTTP: esse é o mecanismo HTTP padrão. • Get Remote User from HTTP Request: Selecione esta opção se o agente de segurança preencher o usuário remoto na solicitação de HTTP.

Tabela 4-6 (Cont.) Opções de Segurança para Diretórios de Usuário

Parâmetro	Descrição
Módulo de Autenticação Personalizado	<p>O nome completo da classe Java do módulo de autenticação personalizado (por exemplo, <code>com.mycompany.epm.CustomAuthenticationImpl</code>) que deve ser usado para autenticar usuários em todos os diretórios de usuário para os quais o módulo de autenticação personalizado está selecionado.</p> <p>O módulo de autenticação será usado em um diretório de usuário somente se a configuração de diretório tiver seu uso habilitado (padrão).</p> <p>O Oracle Hyperion Foundation Services requer que o arquivo JAR de autenticação personalizada seja nomeado como <code>CustomAuth.jar</code>. <code>CustomAuth.jar</code> deve estar disponível em <code>MIDDLEWARE_HOME\user_projects\domains\WEBLOGIC_DOMAIN\lib</code>, normalmente, <code>C:\Oracle\Middleware\user_projects\domains\EPMSys\lib</code>.</p> <p>Em todas as instalações do cliente, <code>CustomAuth.jar</code> deve estar presente em <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>Você pode usar qualquer estrutura de pacote e nome de classe no arquivo JAR.</p> <p>Para obter mais informações, consulte o tópico sobre como usar um módulo de autenticação personalizado no <i>Guia de Configuração de Segurança do Oracle Enterprise Performance Management System</i>.</p>

5. Clique em **OK**.
6. Reinicie o Foundation Services e outros componentes do EPM System

Nova Geração de Chaves de Criptografia

O Oracle Enterprise Performance Management System usa as seguintes chaves para garantir segurança:

- Chave de criptografia Single Sign On Token, usada para criptografar e descriptografar tokens SSO do EPM System. Esta chave está armazenada no Oracle Hyperion Shared Services Registry
- Chave Serviço Confiável, usada em componentes do EPM System para verificar a autenticidade do serviço que está solicitando um token SSO
- Chave de criptografia Provider Configuration, usada para criptografar a senha (usuário DN, senha para diretórios de usuários habilitados para LDAP) que a segurança do EPM System usa para se vincular a um diretório de usuários externos configurado. A senha é definida durante a configuração de um diretório de usuários externos.

Altere essas chaves periodicamente, para fortalecer a segurança do EPM System. O Oracle Hyperion Shared Services e o subsistema de segurança do EPM System usam criptografia AES com restrição de chave de 128 bits.

▲ Cuidado:

Os fluxos de tarefas usados pelo Oracle Hyperion Financial Management e Oracle Hyperion Profitability and Cost Management são invalidados quando você gera novamente a chave de Criptografia de Logon Único. Depois de gerar novamente a chave, abra e salve os fluxos de tarefas para revalidá-los.

Para gerar novamente as chaves Single Sign On Encryption, Provider Configuration ou Trusted Services:

1. Acesse o Oracle Hyperion Shared Services Console como Administrador do Sistema. Consulte [Iniciando o Shared Services Console](#).
2. Selecione **Administração** e **Configurar Diretórios de Usuário**.
3. Selecione **Opções de Criptografia**.
4. Em **Opções de Criptografia**, selecione a chave que deseja regerar.

Tabela 4-7 Opções de Criptografia do EPM System

Opção	Descrição
Token de Sign-on Único	<p>Selecione para regerar a chave de criptografia usada para criptografar e descriptografar tokens SSO do EPM System. Selecione um dos seguintes botões, se Habilitar Compatibilidade do SSO estiver selecionado em Opções de Segurança:</p> <ul style="list-style-type: none"> • Gerar nova chave para criar uma nova chave de criptografia de tokens SSO • Redefinir para Padrões para restaurar a chave de criptografia padrão de tokens SSO
Chave de Serviços Confiáveis	<p>Selecione esta opção para regerar a chave de autenticação confiável, usada pelos componentes do EPM System para verificar a autenticidade do serviço que está solicitando um token SSO.</p>
Chave da Configuração do Provedor	<p>Selecione esta opção para regerar a chave usada para criptografar a senha (senha DN de usuário para diretórios de usuários habilitados para LDAP) que a segurança do EPM System usa para se vincular a um diretório de usuários externos configurado. A senha é definida durante a configuração de um diretório de usuários externos.</p>

✎ Nota:

Se você reverter para a chave de criptografia padrão, será necessário excluir o arquivo de armazenamento de chaves (`EPM_ORACLE_HOME/common/CSS/ssHandlerTK`) de todas as máquinas host do EPM System.

5. Clique em **OK**.

6. Se você optar por gerar uma nova chave de criptografia SSO, execute esta etapa.
 - a. Clique em **Fazer Download**.
 - b. Clique em **OK** para salvar `ssHandlerTK`, o arquivo de keystore que aceita a nova chave de criptografia SSO, em uma pasta no servidor que hospeda o Oracle Hyperion Foundation Services.
 - c. Copie o `ssHandlerTK` para o `EPM_ORACLE_HOME/common/CSS` em todas as máquinas de host do EPM System
7. Reinicie o Foundation Services e outros componentes do EPM System

Uso de Caracteres Especiais

O Active Directory e outros diretórios de usuário baseados em LDAP permitem caracteres especiais em entidades como DNS, nomes de usuário, funções e nomes de grupo. Talvez seja necessário um tratamento especial do Oracle Hyperion Shared Services para entender esses caracteres.

Em geral, você deve usar caracteres de escape ao especificar caracteres especiais nas definições de diretório do usuário; por exemplo, URLs de usuários e grupos, e DN de Base. A tabela a seguir lista os caracteres especiais que podem ser usados em nomes de usuário, nomes de grupo, URLs de usuários, URLs de grupos e no valor de OU no DN de usuário.

Tabela 4-8 Caracteres Especiais Suportados

Caractere	Nome ou Significado	Caractere	Nome ou Significado
(parênteses de abertura	\$	dólar
)	parênteses de fechamento	+	mais
"	aspas	&	e comercial
'	aspas simples	\	barra invertida
,	vírgula	^	acento circunflexo
=	igual a	;	ponto-e-vírgula
<	menor que	#	cerquilha
>	maior que	@	arroba



Nota:

Não use / (barra) nos nomes das unidades organizacionais que vêm no DN de Base

- Os caracteres especiais não são permitidos no valor do atributo Usuário do Logon.
- O asterisco (*) não é permitido em nomes de usuário, nomes de grupo, URLs de usuário e de grupo e no nome da unidade organizacional no DN de Usuário.
- Não há suporte aos valores de atributo com uma combinação de caracteres especiais.
- O E comercial (&) pode ser usado sem um caractere de escape. Para configurações do Active Directory, o & deve ser especificado como `&`.

- Os nomes de usuário e de grupo não podem conter barra invertida (\) e barra (/). Por exemplo, não há suporte para nomes como `test/\user` e `new\test/user`.

Tabela 4-9 Caracteres que não precisam ter escape

Caractere	Nome ou Significado	Caractere	Nome ou Significado
(parênteses de abertura	'	aspas simples
)	parênteses de fechamento	^	acento circunflexo
\$	dólar	@	arroba
&	E comercial		

 **Nota:**

& deve ser inserido como `&`.

Estes caracteres devem ter escape se forem usados nas configurações do diretório de usuário (nomes de usuário, nomes de grupos, URLs de usuário, URLs de grupo e DN de Usuário).

Tabela 4-10 Escape de Caracteres Especiais nas Definições de Configuração do Diretório de Usuário

Caractere Especial	Escape	Definição de Exemplo	Exemplo com Escape
vírgula (,)	barra invertida (\)	<code>ou=test,ou</code>	<code>ou=test\,ou</code>
sinal de mais (+)	barra invertida (\)	<code>ou=test+ou</code>	<code>ou=test\+ou</code>
igual a (=)	barra invertida (\)	<code>ou=test=ou</code>	<code>ou=test\=ou</code>
cerquilha (#)	barra invertida (\)	<code>ou=test#ou</code>	<code>ou=test\#ou</code>
ponto-e-vírgula (;)	barra invertida (\)	<code>ou=test;ou</code>	<code>ou=test\;ou</code>
menor que (<)	barra invertida (\)	<code>ou=test<ou</code>	<code>ou=test\<<ou</code>
maior que (>)	barra invertida (\)	<code>ou=test>ou</code>	<code>ou=test\>ou</code>
aspas (")	duas barras invertidas(\ \)	<code>ou=test"ou</code>	<code>ou=test\\"ou</code>
barra invertida (\)	três barras invertidas(\\ \)	<code>ou=test\ou</code>	<code>ou=test\\ou</code>

 **Nota:**

- Em DN's de Usuário, as aspas (") devem ser usadas com uma barra invertida como caractere de escape. Por exemplo, `ou=test"ou` deve ser especificado como `ou=test\"ou`.
- Em DN's de Usuário, deve ser utilizada uma barra invertida (\) de escape com uma barra invertida. Por exemplo, `ou=test\ou` deve ser especificado como `ou=test\\ou`.

 **Cuidado:**

Se o URL de usuário não estiver especificado, os usuários criados dentro da raiz RDN não deverão conter / (barra) ou \ (barra invertida). Da mesma forma, esses caracteres não devem ser usados nos nomes de grupos criados dentro da raiz RDN se um URL de grupo não for especificado. Por exemplo, não há suporte para os nomes de grupo como `OU=child\ou`, `OU=parent/ou` ou `OU=child/ou`, `OU=parent\ou`. Esta questão não se aplica se você estiver usando um atributo exclusivo como `Atributo de ID` na configuração do diretório de usuários.

Caracteres Especiais no Native Directory

Caracteres especiais são suportados em nomes de usuário e grupo no Native Directory.

Tabela 4-11 Caracteres Especiais Suportados: Native Directory

Caractere	Nome ou Significado	Caractere	Nome ou Significado
@	arroba	,	vírgula
#	cerquilha	=	igual a
\$	dólar	+	mais
^	acento circunflexo	;	ponto-e-vírgula
(parênteses de abertura	!	exclamação
)	parênteses de fechamento	%	percentual
'	aspas simples		

5

Uso do Módulo de Autenticação Personalizada

Consulte Também:

- [Visão Geral](#)
- [Exemplos de Caso de Uso e Limitações](#)
- [Pré-requisitos](#)
- [Considerações de Codificação e Design](#)
- [Implantação do Módulo de Autenticação Personalizada](#)

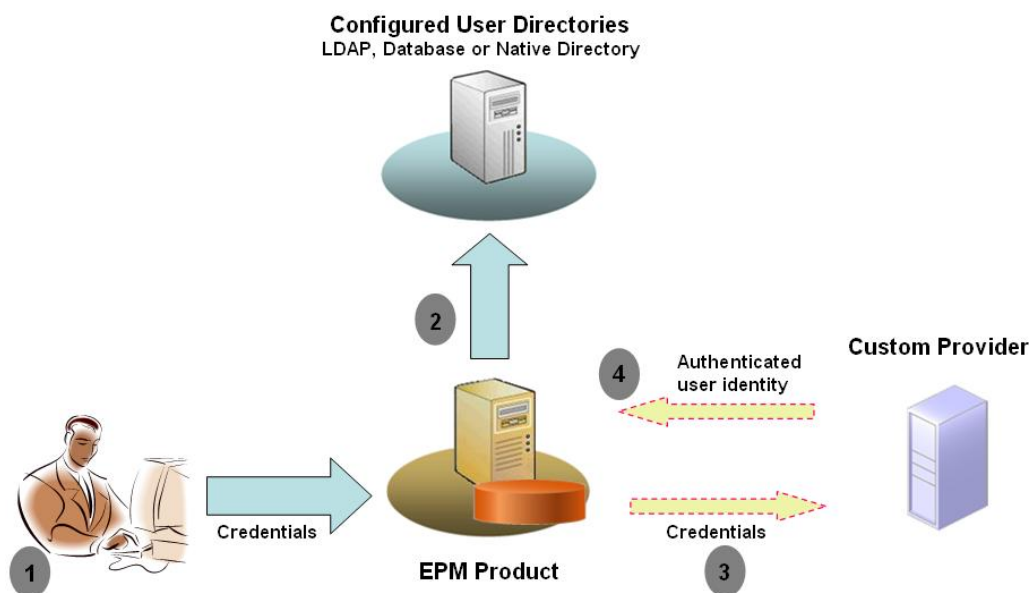
Visão Geral

Um módulo de autenticação personalizada é um módulo Java que os clientes desenvolvem e implementam para autenticar usuários do Oracle Enterprise Performance Management System. De modo geral, os produtos EPM System usam uma tela de logon para capturar o nome de usuário e a senha, que são usados para autenticar usuários. Em vez de usar a autenticação do EPM System, você pode usar um módulo de autenticação personalizada para autenticar e passar credenciais do usuário autenticado ao EPM System para futuro processamento. A implementação de um módulo de autenticação personalizada não envolve a modificação de produtos EPM System.

Você pode usar um módulo de autenticação personalizada com thick clients (por exemplo, Oracle Smart View para Office e Oracle Essbase Studio) e thin clients (por exemplo, Oracle Hyperion Enterprise Performance Management Workspace).

O módulo de autenticação personalizada usa as informações que um usuário insere ao fazer logon em um produto EPM System. Se habilitado para um diretório de usuário, ele autentica usuários por meio do módulo de autenticação personalizada. Após autenticar o usuário com êxito, o módulo de autenticação personalizada retorna o nome do usuário para o EPM System.

A seguinte ilustração apresenta um cenário de exemplo da autenticação personalizada:



Por exemplo, é possível usar a infraestrutura RSA SecurID como o provedor personalizado para garantir autenticação forte transparente para o EPM System. Uma visão geral:

1. O usuário insere credenciais (normalmente, o nome de usuário e senha) para acessar o produto EPM System. Essas credenciais devem identificar exclusivamente o usuário para o provedor usado pelo módulo de autenticação personalizada. Por exemplo, se você estiver usando uma infraestrutura RSA SecurID para autenticar usuários, o usuário irá inserir um ID de usuário e PIN RSA (não um ID de usuário e senha do EPM System).
2. Usando a ordem de pesquisa (consulte [Ordem de Pesquisa](#)), o EPM System percorre os diretórios de usuários configurados para localizar o usuário.
 - Se o diretório de usuários atual não estiver configurado para autenticação personalizada, o EPM System tentará localizar e autenticar o usuário por meio da autenticação do EPM System.
 - Se o diretório de usuários estiver configurado para autenticação personalizada, o EPM System delegará o processo de autenticação ao módulo personalizado.
3. Se o EPM System delegar a autenticação para o módulo personalizado, o módulo de autenticação personalizada aceitará as credenciais e usará sua própria lógica para direcionar a autenticação do usuário em um provedor personalizado; por exemplo, a infraestrutura RSA SecurID.
4. Se o módulo de autenticação personalizada autenticar o usuário no respectivo provedor, ele retornará o nome de usuário para o EPM System, ou retornará uma exceção Java.

O nome de usuário retornado pelo módulo de autenticação personalizada deve ser idêntico a um nome de usuário em um diretório de usuários que é habilitado para autenticação personalizada.

- Se o módulo de autenticação personalizada retornar um nome de usuário, o EPM System localizará o usuário em um diretório de usuários que está habilitado para autenticação personalizada. Nesse estágio, o EPM System

não pesquisa os diretórios de usuários que não são configurados para autenticação personalizada.

- Se o módulo de autenticação personalizada gerar uma exceção ou retornar um usuário nulo, o EPM System continuará pesquisando o usuário nos diretórios de usuários restantes da ordem de pesquisa que não estão habilitados para autenticação personalizada. Se um usuário que corresponde às credenciais não for encontrado, o EPM System exibirá um erro.

Exemplos de Caso de Uso e Limitações

Os cenários de implantação de autenticação personalizada incluem:

- Adição de suporte para senha ocasional
- Execução da autenticação em uma [Solução de Controle de Acesso a Recursos \(RACF\)](#)
- Adição de uma associação de Simple Authentication and Security Layer (SASL) aos diretórios de usuários habilitados para LDAP no lugar de associações LDAP simples

A autenticação com mecanismo de desafio/resposta pode não funcionar bem se você implementar um módulo de autenticação personalizada. As mensagens personalizadas emitidas pelo módulo de autenticação personalizada não são propagadas para os clientes. Uma vez que os clientes, por exemplo, Oracle Hyperion Enterprise Performance Management Workspace, substituem a mensagem de erro para exibir uma mensagem genérica, os seguintes cenários não são válidos:

- Dois PINs RSA SecurID consecutivos
- Variação de senha com desafios, como inserir primeiro, último e terceiro caracteres da senha

Pré-requisitos

- Um arquivo Java totalmente testado chamado `CustomAuth.jar` que contém bibliotecas de módulo de autenticação personalizada. `CustomAuth.jar` deve implementar a interface pública `CSSCustomAuthenticationIF`, definida no pacote `com.hyperion.css` como parte das APIs Oracle Hyperion Shared Services padrão. Consulte http://download.oracle.com/docs/cd/E12825_01/epm.111/epm_security_api_11111/client/com/hyperion/css/CSSCustomAuthenticationIF.html.
- Acesse o Shared Services como administrador do Shared Services

Considerações de Codificação e Design

Ordem de Pesquisa

Além do Native Directory, vários diretórios de usuários podem ser configurados no Oracle Hyperion Shared Services. Uma posição da ordem de pesquisa padrão é atribuída a todos os diretórios de usuários configurados. É possível modificar a ordem de pesquisa no Oracle Hyperion Shared Services Console. Com exceção do Native Directory, você pode remover diretórios de usuários configurados da ordem de pesquisa. O Oracle Enterprise Performance Management System não usa os diretórios de usuários que não estão incluídos na ordem de pesquisa. Consulte o *Guia de Administração da Segurança de Usuário do Sistema Oracle Enterprise Performance Management*.

A ordem de pesquisa determina a ordem na qual o EPM System circula pelos diretórios de usuários para autenticar usuários. Se o usuário for autenticado em um diretório de usuários, o EPM System interromperá a pesquisa e retornará o usuário. O EPM System negará a autenticação e retornará um erro se o usuário não puder ser autenticado nos diretórios de usuários na ordem de pesquisa.

Impacto da Autenticação Personalizada na Ordem de Pesquisa

A autenticação personalizada afeta como a segurança do EPM System interprete a ordem de pesquisa.

Se o módulo de autenticação personalizada retornar um nome de usuário, o EPM System localizará o usuário somente em um diretório de usuários que está habilitado para autenticação personalizada. Nesse estágio, o EPM System ignora os diretórios de usuários que não são configurados para autenticação personalizada.

Compreensão do Fluxo de Autenticação Personalizada

Os seguintes cenários de caso de uso são usados para explorar o fluxo de autenticação personalizada:

- [Cenário 1 de Caso de Uso](#)
- [Cenário 2 de Caso de Uso](#)
- [Cenário 3 de Caso de Uso](#)

Cenário 1 de Caso de Uso

A tabela a seguir detalha a configuração do diretório de usuários do EPM System e a ordem de pesquisa usada nesse cenário. Esse cenário supõe que o módulo de autenticação personalizada usa uma infraestrutura RSA para autenticar usuários.

Tabela 5-1 Configuração do Cenário 1

Tipo e Nome do Diretório de Usuários	Ordem de Pesquisa	Autenticação Personalizada	Nomes de Usuário de Exemplo	Senha ¹
Native Directory	1	Desabilitada	test_user_1 test_user_2 test_user_3	password
Habilitado para LDAP SunONE_West	2	Desabilitada	test_ldap1 test_ldap_2 test_user_3 test_ldap_4	ldappassword
Habilitado para LDAP SunONE_East	3	Habilitada	test_ldap1 test_ldap_2 test_user_3	ldappassword em SunONE e RSA PIN no módulo personalizado

¹ Para simplificar, é pressuposto que todos os usuários usem a mesma senha de diretório de usuários.

Para iniciar o processo de autenticação, um usuário insere um nome de usuário e senha na tela de logon de um produto EPM System. Nesse cenário, o módulo de autenticação personalizada executa as seguintes ações:

- Aceita um nome de usuário e RSA PIN como as credenciais de usuário
- Retorna um nome de usuário no formato *username@providername*; por exemplo, *test_ldap_2@SunONE_East*, para segurança do EPM System

Tabela 5-2 Resultados e interação do usuário

Nome de Usuário e Senha	Resultado da Autenticação	Diretório de Usuários do Logon
test_user_1/password	Êxito	Native Directory
test_user_3/password	Êxito	Native Directory
test_user_3/ ldappassword	Êxito	SunONE_West (ordem de pesquisa 2) ¹
test_user_3/RSA PIN	Êxito	SunONE_East (ordem de pesquisa 3) ²
test_ldap_2/ ldappassword	Êxito	SunONE_West (ordem de pesquisa 2)
test_ldap_4/RSA PIN	Falha O EPM System exibe um erro de autenticação. ³	

¹ A autenticação personalizada não pode autenticar esse usuário porque o usuário inseriu credenciais do EPM System. O EPM System pode identificar esse usuário somente em um diretório de usuários que não está habilitado para autenticação personalizada. O usuário não está no Native Directory (número da ordem de pesquisa), mas é identificado em SunONE West (número da ordem de pesquisa 2).

² O EPM System não encontra esse usuário no Native Directory (número da ordem de pesquisa 1) ou SunONE West (número da ordem de pesquisa 2). O módulo de autenticação personalizada valida o usuário no Servidor do RSA e retorna *test_user_3@SunONE_EAST* para EPM System. O EPM System localiza o usuário em SunONE East (número da ordem de pesquisa 3), que é um diretório de usuários habilitado para autenticação personalizada.

³ A Oracle recomenda que todos os usuários autenticados pelo módulo personalizado estejam presentes em um diretório de usuários habilitado para autenticação personalizada incluído na ordem de pesquisa. O logon falhará se o nome de usuário que é retornado pelo módulo de autenticação personalizada não estiver presente em um diretório de usuários habilitado para autenticação personalizada incluído na ordem de pesquisa.

Cenário 2 de Caso de Uso

A tabela a seguir detalha a configuração do diretório de usuários do EPM System e a ordem de pesquisa usada nesse cenário. Esse cenário supõe que o módulo de autenticação personalizada usa uma infraestrutura RSA para autenticar usuários.

Nesse cenário, o módulo de autenticação personalizada executa as seguintes ações:

- Aceita um nome de usuário e RSA PIN como as credenciais de usuário
- Retorna um nome de usuário, por exemplo, *test_ldap_2*, para segurança do EPM System

Tabela 5-3 Uma ordem de pesquisa de exemplo

Diretório de Usuários	Ordem de Pesquisa	Autenticação Personalizada	Nomes de Usuário de Exemplo	Senha ¹
Native Directory	1	Desabilitada	test_user_1 test_user_2 test_user_3	password
Habilitado para LDAP, por exemplo, SunONE	2	Habilitada	test_ldap1 test_ldap2 test_user_3	ldappassword em SunONE e RSA PIN no módulo personalizado

¹ Para simplificar, é pressuposto que todos os usuários usem a mesma senha de diretório de usuários.

Para iniciar o processo de autenticação, um usuário insere um nome de usuário e senha na tela de logon de um produto EPM System.

Tabela 5-4 Resultados e interação do usuário

Nome de Usuário e Senha	Resultado do Logon	Diretório de Usuários do Logon
test_user_1/password	Êxito	Native Directory
test_user_3/password	Êxito	Native Directory
test_user_3/ldappassword	Falha	SunONE ¹
test_user_3/RSA PIN	Êxito	SunONE ²

¹ A autenticação do usuário no Native Directory falha devido à incompatibilidade de senha. A autenticação do usuário que está usando o módulo de autenticação personalizada falha porque a senha usada não é um RSA PIN válido. O EPM System não tenta autenticar esse usuário no SunONE (ordem de pesquisa 2), pois as configurações de autenticação personalizada substituem a autenticação do EPM System nesse diretório.

² A autenticação do usuário no Native Directory falha devido à incompatibilidade de senha. O módulo de autenticação personalizada autentica o usuário e retorna o nome de usuário test_user_3 para EPM System.

Cenário 3 de Caso de Uso

A tabela a seguir detalha a configuração do diretório de usuários do EPM System e a ordem de pesquisa usada nesse cenário. Esse cenário supõe que o módulo de autenticação personalizada usa uma infraestrutura RSA para autenticar usuários.

Para clareza em tais cenários, a Oracle recomenda que seu módulo de autenticação personalizada retorne o nome de usuário no formato `username@providernome`; por exemplo, `test_ldap_4@SunONE`.

Tabela 5-5 Uma ordem de pesquisa de exemplo

Diretório de Usuários	Ordem de Pesquisa	Autenticação Personalizada	Nomes de Usuário de Exemplo	Senha ¹
Native Directory	1	Habilitada	test_user_1 test_user_2 test_user_3	RSA_PIN
Habilitado para LDAP, por exemplo, MSAD	2	Desabilitada	test_ldap1 test_ldap4 test_user_3	ldappassword
Habilitado para LDAP, por exemplo, SunONE	3	Habilitada	test_ldap1 test_ldap4 test_user_3	ldappassword em SunONE e RSA PIN no módulo personalizado

¹ Para simplificar, é pressuposto que todos os usuários usem a mesma senha de diretório de usuários.

Para iniciar o processo de autenticação, um usuário insere um nome de usuário e senha na tela de logon de um produto EPM System.

Tabela 5-6 Resultados e interação do usuário

Nome de Usuário e Senha	Resultado da Autenticação	Diretório de Usuários do Logon
test_user_1/password	Êxito	Native Directory
test_user_3/RSA_PIN	Êxito	Native Directory
test_user_3/ldappassword	Êxito	MSAD (ordem de pesquisa 2)
test_ldap_4/ldappassword	Êxito	MSAD (ordem de pesquisa 2)
test_ldap_4/RSA PIN	Êxito	SunONE (ordem de pesquisa 3)

Diretórios de Usuários e Módulo de Autenticação Personalizada

Para usar o módulo de autenticação personalizada, os diretórios de usuários que contêm as informações de usuário e grupo do EPM System podem ser configurados individualmente para delegar a autenticação ao módulo personalizado.

Os usuários do EPM System que são autenticados usando um módulo personalizado devem estar presentes em um dos diretórios de usuários incluídos na ordem de pesquisa (consulte [Ordem de Pesquisa](#)). Além disso, o diretório de usuário deve ser configurado para delegar autenticação ao módulo personalizado.

A identidade do usuário no provedor personalizado, (por exemplo, 1357642 na infraestrutura RSA SecurID) pode ser diferente do nome de usuário no diretório de usuários (por exemplo, jDoe em um Oracle Internet Directory) configurado no Shared Services. Após autenticação do usuário, o módulo de autenticação personalizada deve retornar o nome de usuário jDoe para EPM System.

 **Nota:**

Como prática recomendada, a Oracle recomenda que o nome de usuário nos diretórios de usuários configurados no EPM System seja idêntico aos disponíveis no diretório de usuários usados pelo módulo de autenticação personalizada.

Interface Java `CSSCustomAuthenticationIF`

O módulo de autenticação personalizada deve usar a interface Java `CSSCustomAuthenticationIF` para integração à estrutura de segurança do EPM System. Ele deverá retornar uma string de nome de usuário se a autenticação personalizada for bem-sucedida ou uma mensagem de erro se a autenticação for malsucedida. Para que o processo de autenticação seja concluído, o nome de usuário retornado pelo módulo de autenticação personalizada deve estar presente em um dos diretórios de usuários incluídos na ordem de pesquisa do Shared Services. A estrutura de segurança do EPM System dá suporte ao formato `username@providerName`.

 **Nota:**

Assegure-se de que o nome de usuário que o módulo de autenticação personalizada retorna não contenha um * (asterisco), pois a estrutura de segurança do EPM System o interpreta como um caractere curinga durante a pesquisa por usuários.

Consulte [Código de Exemplo 1](#) em busca da assinatura da interface `CSSCustomAuthenticationIF`.

Seu módulo de autenticação personalizada (pode ser um arquivo de classe) deve ser incluído em `CustomAuth.jar`. A estrutura do pacote não é importante.

Para obter informações detalhadas sobre a interface `CSSCustomAuthenticationIF`, consulte [Documentação da API de segurança](#).

O método `authenticate` de `CSSCustomAuthenticationIF` aceita a autenticação personalizada. O método `authenticate` aceita credenciais (nome de usuário e senha) que o usuário inseriu ao tentar acessar o EPM System como parâmetros de entrada. Esse método retornará uma string (nome de usuário) se a autenticação personalizada for bem-sucedida. Ele vai gerar `java.lang.Exception` se a autenticação for malsucedida. O nome de usuário retornado pelo método deve identificar exclusivamente um usuário em um dos diretórios de usuários incluídos na ordem de pesquisa do Shared Services. A estrutura de segurança do EPM System dá suporte ao formato `username@providerName`.



Nota:

Para inicializar recursos, por exemplo, um pool de conexões JDBC, use o construtor de classe. Fazer isso melhora o desempenho ao não carregar recursos para cada autenticação.

Implantação do Módulo de Autenticação Personalizado

Somente um módulo personalizado é permitido para uma implantação do Oracle Enterprise Performance Management System. É possível habilitar a autenticação personalizada para um ou mais diretórios de usuários na ordem de pesquisa.

O módulo de autenticação personalizada deve implementar a interface pública `CSSCustomAuthenticationIF`, definida no pacote `com.hyperion.css`. Este documento supõe que você tenha um módulo personalizado completamente funcional que define a lógica para autenticar usuários em relação ao provedor de usuário de sua escolha. Depois que você desenvolve e testa um módulo de autenticação personalizada, é preciso implementá-lo no ambiente do EPM System.

Visão Geral das Etapas

Seu código de autenticação personalizada não deve usar `log4j` para registro de erro. Se o código que você usou em uma versão anterior usar `log4j`, será preciso removê-lo do código antes de usá-lo com essa versão.

Para implementar o módulo de autenticação personalizada, conclua as seguintes etapas:

- Interrompa os produtos EPM System, incluindo o Oracle Hyperion Shared Services e todos os sistemas que usam APIs do Shared Services.
- Copie o arquivo Java do módulo de autenticação personalizada `CustomAuth.jar` na implantação:
 - **WebLogic:** Copie `CustomAuth.jar` em `MIDDLEWARE_HOME/user_projects/domains/WEBLOGIC_DOMAIN/lib`, normalmente, `C:/Oracle/Middleware/user_projects/domains/EPMSysstem/lib`.

Se estiver atualizando da Versão 11.1.2.0 ou 11.1.2.1 que tinha uma implementação do módulo de autenticação personalizada, mova `CustomAuth.jar` de `EPM_ORACLE_HOME/common/jlib/11.1.2.0` para `MIDDLEWARE_HOME/user_projects/domains/WEBLOGIC_DOMAIN/lib`.

- **Todas as Implantações do Cliente:** Copie `CustomAuth.jar` em todas as implantações do cliente EPM System, no seguinte local:

`EPM_ORACLE_HOME/common/jlib/11.1.2.0`, geralmente, `Oracle/Middleware/common/jlib/11.1.2.0`. Confirme que o arquivo `CustomAuth.jar` esteja sempre no diretório `EPM_ORACLE_HOME/common/jlib/11.1.2.0`.

Para que todos os servidores e clientes trabalhem com autenticação personalizada, o arquivo `CustomAuth.jar` deve estar presente nos dois seguintes locais:

- * `MIDDLEWARE_HOME/user_projects/domains/WEBLOGIC_DOMAIN/lib`
- * `EPM_ORACLE_HOME/common/jlib/11.1.2.0`

- Atualize as configurações de diretório de usuários no Shared Services. Consulte [Atualização das Configurações no Shared Services](#).
- Inicie o Shared Services, seguido por outros produtos do EPM System.
- Teste sua implementação. Consulte [Teste da Implantação](#).

Atualização das Configurações no Shared Services

Por padrão, a autenticação personalizada está desativada para todos os diretórios de usuários. É possível substituir o comportamento padrão para habilitar a autenticação personalizada para diretórios de usuários externos ou para o Native Directory.

Atualização das Configurações do Diretório de Usuários

Você deve atualizar a configuração do diretório de usuários para o qual a autenticação personalizada deve ser habilitada.

Para atualizar a configuração de diretório de usuário:

1. Inicie o Oracle Hyperion Foundation Services.
2. Acesse o Oracle Hyperion Shared Services Console como Administrador do Sistema.
3. Selecione **Administração e Configurar Diretórios de Usuário**.
4. Na tela Diretórios de Usuários Definidos, selecione o diretório de usuários para o qual deseja alterar a configuração de autenticação personalizada.

 **Nota:**

O EPM System usa apenas diretórios de usuário incluídos na ordem de pesquisa.

5. Clique em **Editar**.
6. Selecione **Mostrar Opções Avançadas**.
7. Em **Módulo Personalizado**, selecione **Módulo de Autenticação** a fim de habilitar o módulo personalizado para o diretório de usuários atual.
8. Clique em **Concluir**.
9. Repita este procedimento para atualizar a configuração de outros diretórios de usuário na ordem de pesquisa.

Atualização das Opções de Segurança

Assegure-se de que `CustomAuth.jar` esteja disponível em `EPM_ORACLE_HOME/user_projects/domains/WEBLOGIC_DOMAIN/lib` antes de iniciar o procedimento a seguir.

Para atualizar as opções de segurança:

1. Acesse o Shared Services Console como Administrador do Sistema.
2. Selecione **Administração e Configurar Diretórios de Usuário**.
3. Selecione **Opções de Segurança**.

4. Selecione **Mostrar Opções Avançadas**.
5. No **Módulo de Autenticação**, insira o nome da classe totalmente qualificado personalizado do módulo de autenticação personalizada que deve ser usado para autenticar usuários em todos os diretórios de usuários para os quais o módulo de autenticação personalizada está selecionado. Por exemplo,
`com.mycompany.epm.CustomAuthenticationImpl.`
6. Clique em **OK**.

Teste da Implantação

Se o Native Directory não estiver configurado para autenticação personalizada, não use os usuários do Native Directory para testar a autenticação personalizada.

Nota:

É sua responsabilidade identificar e corrigir todos os problemas com o módulo de autenticação personalizada. A Oracle supõe que seu módulo personalizado funcione perfeitamente para mapear um usuário do diretório de usuários usado pelo módulo personalizado para um usuário em um diretório de usuários habilitado para autenticação personalizada disponível na ordem de pesquisa do EPM System.

Para testar sua implantação, faça logon no EPM System usando credenciais de usuário do diretório de usuários; por exemplo, uma infraestrutura SecurID RSA, usada pelo módulo personalizado. Essas credenciais podem ser diferentes das credenciais do EPM System.

Sua implementação será considerada bem-sucedida se os produtos EPM System permitirem que você acesse seus recursos. Um erro indicando que o usuário não foi encontrado nem sempre é um indicador de uma implementação malsucedida. Nesses casos, verifique se as credenciais que você inseriu estão presentes no armazenamento de usuários personalizado e se um usuário correspondente está presente em um dos diretórios de usuários habilitados para autenticação personalizada na ordem de pesquisa do EPM System.

Para testar a autenticação personalizada:

1. Verifique se os produtos EPM System estão em execução.
2. Acesse um componente do EPM System; por exemplo, Oracle Hyperion Enterprise Performance Management Workspace.
3. Faça logon como um usuário definido em um diretório de usuários para o qual a autenticação personalizada está habilitada.
 - a. Em **Nome de Usuário**, informe o identificador do usuário; por exemplo, um ID de Usuário RSA.
 - b. Em **Senha**, informe uma senha; por exemplo, um PIN RSA.
 - c. Clique em **Logon**.
4. Verifique se você pode acessar os recursos do produto EPM System.

6

Diretrizes de Segurança do EPM System

Consulte Também:

- [Implementação de SSL](#)
- [Alteração da Senha de Administração](#)
- [Nova Geração de Chaves de Criptografia](#)
- [Alteração das Senhas de Banco de Dados](#)
- [Proteção de Cookies](#)
- [Redução do Tempo Limite do Token SSO](#)
- [Revisão de Relatórios de Segurança](#)
- [Personalização do Sistema de Autenticação para Autenticação Forte](#)
- [Desativação de Utilitários de Depuração do EPM Workspace](#)
- [Alteração de Páginas de Erro do Servidor Web Padrão](#)
- [Suporte para Software de Terceiros](#)

Implementação de SSL

O SSL usa um sistema de criptografia que criptografa dados. O SSL cria uma conexão segura entre um cliente e um servidor, sobre o qual os dados podem ser enviados com segurança.

Para proteger seu ambiente do Oracle Enterprise Performance Management System, proteja todos os canais de comunicação usados pelos seus aplicativos Web e conexões de diretório de usuários usando SSL. Consulte [Componentes do EPM System com Habilitação para SSL](#).

Além disso, proteja todas as portas de agente, por exemplo, porta 6861, que é a porta do agente do Oracle Hyperion Reporting and Analysis, usando um firewall. Os usuários finais não precisam acessar as portas do agente do EPM System.

Alteração da Senha de Administração

A conta de usuário administrativa padrão do Native Directory fornece acesso a todas as funções do Oracle Hyperion Shared Services. Essa senha é definida quando você implanta o Oracle Hyperion Foundation Services. É preciso alterar periodicamente a senha dessa conta.

Edite a conta do usuário *admin* para alterar a senha. Consulte o tópico sobre modificação de contas de usuário no *Guia de Administração da Segurança de Usuário do Sistema Oracle Enterprise Performance Management*.

Nova Geração de Chaves de Criptografia

Use o Oracle Hyperion Shared Services Console para gerar periodicamente o seguinte:

- Token de logon único

 **Cuidado:**

Os fluxos de tarefas usados pelo Oracle Hyperion Financial Management e Oracle Hyperion Profitability and Cost Management são invalidados quando você gera um novo keystore. Depois de gerar novamente o armazenamento de chaves, abra e salve os fluxos de tarefas para revalidá-los.

- Chave de Serviços Confiável
- Chave de Configuração do Provedor

Consulte [Nova Geração de Chaves de Criptografia](#).

 **Nota:**

O Oracle Hyperion Shared Services e o subsistema de segurança do Oracle Enterprise Performance Management System usam criptografia AES com restrição de chave de 128 bits.

Alteração das Senhas de Banco de Dados

Mude periodicamente a senha de todos os bancos de dados de produto Oracle Enterprise Performance Management System. O procedimento de alteração da senha do banco de dados no Oracle Hyperion Shared Services Registry é detalhado nesta seção.

Para ver os procedimentos detalhados de como alterar a senha do banco de dados de um produto EPM System, consulte o *Guia de Configuração e Instalação do Sistema Oracle Enterprise Performance Management*.

Para alterar as senhas de banco de dados do produto EPM System no Shared Services Registry:

1. Usando o console de administração de banco de dados, altere a senha da conta de usuário que foi usada para configurar o banco de dados de produtos do Shared Services.
2. Interrompa os produtos EPM System (aplicativos Web, serviços e processos).
3. Usando o EPM System Configurator, reconfigure o banco de dados através de um dos seguintes procedimentos.

Apenas Oracle Hyperion Shared Services:

 **Nota:**

Em ambientes distribuídos onde os produtos EPM System estão em máquinas diferentes das do Shared Services, você deve realizar esse procedimento em todos os servidores.

- a. Nas tarefas Foundation do EPM System Configurator, selecione **Configurar Banco de Dados**.
- b. Na página “Configuração de Banco de Dados e Registro do Shared Services”, selecione **Conectar a um banco de dados do Shared Services previamente configurado**.
- c. Especifique a nova senha do usuário cuja conta foi usada para configurar o banco de dados dos Shared Services. Não altere outras configurações.
- d. Continue a configuração e clique em **Concluir** quando terminar.

Produtos do **EPM System** que não sejam o **Shared Services**:

 **Nota:**

Siga estas etapas para os produtos EPM System implantados apenas no servidor atual.

Consulte o *Guia de Configuração e Instalação do Sistema Oracle Enterprise Performance Management* para obter instruções detalhadas.

4. Inicie os produtos e serviços do EPM System.

Proteção de Cookies

O aplicativo Web do Oracle Enterprise Performance Management System define um cookie para rastrear a sessão. Ao definir um cookie, especialmente um cookie de sessão, o servidor pode definir o sinalizador de segurança, que força o navegador a enviar o cookie por um canal de segurança. Esse comportamento reduz o risco de sequestro da sessão.

 **Nota:**

Proteja cookies somente se os produtos EPM System forem implantados em um ambiente habilitado para SSL.

Modifique o descritor da sessão do Oracle WebLogic Server para proteger os cookies do WebLogic Server. Defina o valor do atributo `cookieSecure` no elemento `session-param` como `true`. Consulte Proteção de Aplicativos Web em [Segurança de Programação do Oracle Fusion Middleware para Oracle WebLogic Server 11g](#).

Redução do Tempo Limite do Token SSO

O tempo limite padrão do token SSO é de 480 minutos. Você deve reduzir o tempo limite do token SSO, por exemplo, para 60 minutos, a fim de minimizar a reutilização do token se ele for exposto. Consulte "Configuração de Opções de Segurança" no *Guia de Administração da Segurança de Usuário do Sistema Oracle Enterprise Performance Management*.

Revisão de Relatórios de Segurança

O Relatório de Segurança contém informações de auditoria relacionadas às tarefas de segurança para as quais a auditoria está configurada. Gere e revise esse relatório no Oracle Hyperion Shared Services Console regularmente, especialmente para identificar tentativas de logon que falharam nos produtos Oracle Enterprise Performance Management System e alterações de provisionamento. Selecione **Modo de exibição detalhado** como opção de geração de relatório para agrupar os dados do relatório com base em atributos modificados e nos novos valores de atributos. Consulte o tópico sobre geração de relatórios no *Guia de Administração da Segurança de Usuário do Sistema Oracle Enterprise Performance Management*.

Personalização do Sistema de Autenticação para Autenticação Forte

Você pode usar um módulo de autenticação personalizado para adicionar autenticação forte ao EPM System. Por exemplo, você pode usar a autenticação de dois fatores do RSA SecurID no modo de resposta sem desafio. O módulo de autenticação personalizada é transparente para thin e thick clients, e não exige alterações de implantação no lado do cliente. Consulte [Uso do Módulo de Autenticação Personalizada](#).

Desabilitação dos Utilitários de Depuração do EPM Workspace

- Para fins de solução de problemas, o Oracle Hyperion Enterprise Performance Management Workspace é enviado com arquivos JavaScript não processados. Por motivos de segurança, você deve remover esses arquivos JavaScript não processados do seu ambiente de produção:
 - Crie uma cópia de backup do diretório `EPM_ORACLE_HOME/common/epmstatic/wspace/js/`.
 - Com exceção do arquivo `DIRECTORY_NAME.js`, exclua os arquivos `.js` de cada subdiretório de `EPM_ORACLE_HOME/common/epmstatic/wspace/js`.
Cada subdiretório contém um arquivo `.js` que leva o nome do diretório. Por exemplo, `EPM_ORACLE_HOME/common/epmstatic/wspace/js/com/hyperion/bpm/web/common` contém `Common.js`. Exclua todos os arquivos `.js`, exceto aquele que leva o nome do diretório, nesse caso; `Common.js`.

- O EPM Workspace fornece alguns utilitários de depuração e aplicativos de teste, que se tornarão acessíveis se o EPM Workspace for implantado no modo de depuração. Por motivos de segurança, os administradores devem desativar a depuração do lado do cliente no EPM Workspace.

Para desativar o modo de depuração:

1. Faça login no EPM Workspace como Administrador.
2. Selecione **Navegar, Administrar e Configurações do Servidor do Workspace**.
3. Em **ClientDebugEnabled** nas Configurações do Servidor do Workspace, selecione **Não**.
4. Clique em **OK**.

Alteração de Páginas de Erro do Servidor Web Padrão

Quando os servidores de aplicativos estiverem indisponíveis para aceitar solicitações, o plug-in de servidor Web para o servidor de aplicativos de back-end (por exemplo, plug-in Oracle HTTP Server para o Oracle WebLogic Server) vai gerar uma página de erro padrão que exibe as informações de criação do plug-in. Os servidores Web também exibem suas páginas de erro padrão em outras ocasiões. Os hackers podem usar essas informações para descobrir vulnerabilidades conhecidas em sites públicos.

Personalize as páginas de erro (do plug-in do servidor de aplicativos Web e do servidor Web) para que elas não contenham informações sobre componentes do sistema de produção; por exemplo, versão do servidor, tipo de servidor, data de criação do plug-in e tipo de plug-in. Consulte mais informações na documentação do fornecedor do servidor de aplicativos e do servidor Web.

Suporte para Software de Terceiros

A Oracle confirma e aceita as declarações de compatibilidade com versões anteriores feitas por fornecedores de terceiros. Portanto, se os fornecedores declararem compatibilidade com versões anteriores, versões de manutenção e service packs subsequentes poderão ser usados. Se alguma incompatibilidade for identificada, a Oracle especificará uma versão de patch na qual o produto deverá ser implantado (e removerá a versão incompatível da matriz aceita) ou fornecerá uma versão de manutenção ou uma correção de serviço para o produto Oracle.

Atualizações do Servidor: O suporte a upgrades para componentes de servidor de terceiros é regido pela Política de Versões Subsequentes de Manutenção. Normalmente, a Oracle contempla a atualização de componentes de servidor de terceiros para a versão de manutenção seguinte do service pack da versão suportada atualmente. Não há suporte para atualizações do próximo lançamento importante.

Atualizações de cliente: A Oracle permite atualizações automáticas de componentes de clientes, inclusive atualizações para a versão principal seguinte de componentes de cliente de terceiros. Por exemplo, é possível atualizar a versão JRE do navegador para a versão JRE atualmente suportada.

A

Código de Exemplo da Autenticação Personalizada

Código de Exemplo 1



Nota:

Seu código de autenticação personalizada não deve usar log4j para registro de erro. Se o código de autenticação personalizada que você usou em uma versão anterior usou log4j, será preciso removê-lo do código antes de usá-lo com essa versão.

O seguinte trecho de código é uma implementação vazia do 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;
    }
}
```

Parâmetros de entrada:

- Contexto: Um mapa que contém as informações do par de chave/valor de localidade
- Nome de usuário: Um identificador que identifica exclusivamente o usuário para o diretório de usuários onde o módulo personalizado autentica o usuário. O usuário insere o valor desse parâmetro ao fazer logon em um componente do Oracle Enterprise Performance Management System.
- Senha: A senha definida para o usuário no diretório de usuários onde o módulo personalizado autentica o usuário. O usuário insere o valor desse parâmetro ao fazer logon em um componente do EPM System.

Código de Exemplo 2

O exemplo de código a seguir demonstra a autenticação personalizada dos usuários usando o nome de usuário e a senha contidos em um arquivo simples. Você deve inicializar listas de usuários e senhas no construtor de classe para que a autenticação personalizada funcione.

```
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)
    ey))
        .append("@").append(PROVIDER_NAME).toString(
    );
    return userNameStr;
else throw new Exception("Invalid User Credentials");
    }
}

```

Arquivo de Dados para Código de Exemplo 2

Assegure-se de que o nome do arquivo de dados seja `datafile.txt`, que é o nome do código de exemplo, e que ele seja incluído no arquivo Java que você cria.

Use o seguinte como o conteúdo do arquivo simples que é usado como o diretório de usuários personalizado para dar suporte ao módulo de autenticação personalizada implementado pelo Código de Exemplo 2 (Consulte [Código de Exemplo 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

```


Use o seguinte como o conteúdo do arquivo simples que é usado como o diretório de usuários personalizado se você pretende retornar nome de usuário no 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

Implementação de uma Classe de Logon Personalizada

O Oracle Enterprise Performance Management System fornece `com.hyperion.css.sso.agent.X509CertificateSecurityAgentImpl` para extrair a identidade do usuário (DN) dos certificados x509.

Se você deve derivar a identidade do usuário de um atributo no certificado que não seja o DN, será preciso desenvolver e implementar uma classe de logon personalizada semelhante a `com.hyperion.css.sso.agent.X509CertificateSecurityAgentImpl`, conforme descrito neste apêndice.

Código de Exemplo de Classe de Logon Personalizada

Este código de exemplo ilustra a implementação do `com.hyperion.css.sso.agent.X509CertificateSecurityAgentImpl` padrão. De modo geral, você deve personalizar o método `parseCertificate(String sCertificate)` para essa implementação a fim de derivar o nome de usuário de um atributo de certificado diferente de 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
```

Implantação de uma Classe de Logon Personalizada

Para implementar a classe de logon personalizado, conclua as seguintes etapas:

1. Crie e teste a classe de logon personalizada. Assegure-se de que não tenha referências a `log4j` no seu código. Consulte [Código de Exemplo de Classe de Logon Personalizada](#).

É possível usar qualquer nome da sua classe personalizada.

2. Empacote a classe de logon personalizada em `CustomAuth.jar`
3. Copie `CustomAuth.jar` na implantação:
 - **WebLogic:** Copie `CustomAuth.jar` em `MIDDLEWARE_HOME/user_projects/domains/WEBLOGIC_DOMAIN/lib`, normalmente, `Oracle/Middleware/user_projects/domains/EPMSysstem/lib`.

Nota:

Se estiver atualizando da Versão 11.1.2.0 ou 11.1.2.1 que tinha uma implementação de classe de logon personalizada, mova `CustomAuth.jar` de `EPM_ORACLE_HOME/common/jlib/11.1.2.0` para `MIDDLEWARE_HOME/user_projects/domains/WEBLOGIC_DOMAIN/lib`.

- **Implantações do cliente:** Copie `CustomAuth.jar` em todas as implantações do cliente Oracle Enterprise Performance Management System, no seguinte local:

`EPM_ORACLE_HOME/common/jlib/11.1.2.0`, geralmente, `Oracle/Middleware/common/jlib/11.1.2.0`

A Oracle recomenda habilitar a Autenticação de Certificado de Cliente se você estiver usando uma classe de logon personalizada.

C

Migração de Usuários e Grupos entre Diretórios de Usuários

Visão Geral

Muitos cenários podem fazer com que as identidades de usuário e grupo dos usuários provisionados do Oracle Enterprise Performance Management System se tornem obsoletas. Os componentes do EPM System se tornarão inacessíveis se as informações de provisionamento disponíveis para eles estiverem obsoletas. Os cenários que podem criar dados de provisionamento obsoletos incluem:

- Retirada de um diretórios de usuários: As organizações podem retirar um diretório de usuários após mover os usuários para outro diretório.
- Atualização da versão: A atualização da versão do diretório de usuários pode envolver alterações no nome da máquina host ou nos ambiente do sistema operacional.
- Alteração de fornecedor: As organização podem descontinuar o uso de um diretório de usuários em favor de um diretório de outro fornecedor. Por exemplo, uma organização pode substituir seu Oracle Internet Directory por um Servidor de Diretórios SunONE.

Nota:

- Neste apêndice, o diretório de usuários que você está suprimindo gradualmente é conhecido como o diretório de usuários de *origem*, e o diretório de usuários para o qual você moveu as contas de usuário é conhecido como diretório de usuários de *destino*.
- Este procedimento de Migração não suporta a migração de contas de usuário de um diretório de usuários de origem para um diretório de usuários de destino, mas apenas a associação deles em aplicativos EPM. Os usuários devem ser criados manualmente no diretório de usuários de destino. Esse processo é aplicável a usuários de qualquer diretório de usuários de origem, inclusive o Native Directory.

Se um diretório de usuários de origem configurado com o Hyperion Shared Services tiver grupos, exceto grupos do Native Directory, esses grupos também deverão ser criados dentro do diretório de usuários de destino.

Pré-requisitos

- Os usuários e grupos do Oracle Enterprise Performance Management System cujos dados de provisionamento estão sendo migrados pelos diretórios de usuários devem estar disponíveis no diretório de usuários de destino.

Os relacionamentos de grupo que existem no diretório de usuários de origem devem ser mantidos no diretório de usuários de destino.

- Os nomes dos usuários do EPM System devem ser idênticos entre os diretórios de usuários de origem e destino.

Procedimento de Migração

Exportar Dados do Native Directory

Siga estas etapas no ambiente de origem:

Use Oracle Hyperion Enterprise Performance Management System Lifecycle Management para exportar somente os seguintes artefatos Shared Services a partir do Native Directory:

- Grupos do Native Directory
- Funções atribuídas
- Listas delegadas

O Lifecycle Management cria vários arquivos de exportação, geralmente em `EPM_ORACLE_INSTANCE/import_export/USER_NAME/EXPORT_DIR/resource/` Native Directory, onde `USER_NAME` é a identidade do usuário; por exemplo, `admin`, que executou a operação de exportação, e `EXPORT_DIR` é o nome do diretório de exportação. Normalmente, são criados estes arquivos:

- `Groups.csv`
- `Assigned Roles.csv`
- `Delegated Lists.csv`
- `Assigned Roles/PROD_NAME.csv` para cada aplicativo implantado, onde `PROD_NAME` é o nome de um componente do Oracle Enterprise Performance Management System; por exemplo, `Shared Services`.

Nota:

- Consulte o *Guia do Oracle Enterprise Performance Management System Lifecycle Management* para obter instruções detalhadas sobre exportação de dados usando o Lifecycle Management.
- Certifique-se de que o arquivo `Users.csv` não foi exportado.

Após a exportação dos artefatos, verifique se o Relatório de Status de Migração exibe o status da última operação de exportação como `Completed`.

Para exportar dados do Native Directory:

1. No Painel de exibição do Oracle Hyperion Shared Services Console, no grupo de aplicativos **Foundation**, selecione o aplicativo do **Shared Services**.
2. Para migrar, selecione apenas os artefatos necessários a partir da lista abaixo:
 - Grupos do Native Directory

- Funções Atribuídas
 - Listas Delegadas
3. Clique em **Exportar**.
 4. Insira um nome para o arquivo de exportação. O padrão é `admin DATE`; por exemplo `admin 13-03-18`.
 5. Clique em **Exportar**.

Importar Dados do Native Directory

Siga estas etapas no ambiente de destino:

1. Crie manualmente:
 - a. Usuários no diretório de usuários externos de destino, semelhante ao diretório de usuários de origem.
 - b. Grupos no diretório de usuários externos de destino, semelhante ao diretório de usuários de origem, exceto os grupos do Native Directory.
2. Configure o Diretório de Usuários de Destino.
 Adicione o diretório de usuários de destino como um diretório de usuários externo no EPM System se você moveu as contas de usuário do diretório de usuários de origem para outro diretório de usuários. Por exemplo, se você moveu as contas de usuário do Oracle Internet Directory para o Servidor de Diretórios do SunONE, adicione o Servidor de Diretórios do SunONE como um diretório de usuários externos. Consulte "Capítulo 3, Configuração de Diretórios de Usuários" no *Guia de Administração da Segurança de Usuário do Sistema Oracle Enterprise Performance Management*.

Nota:

Assegure-se de que o diretório de usuários de destino contenha contas de usuários e grupos para todos os usuários do EPM System cujos dados estão sendo migrados do diretório de usuários de origem.

Se você moveu os usuários para um diretório de usuários que já está definido como um diretório de usuários externo, verifique se as contas de usuário estão visíveis para Oracle Hyperion Shared Services. Você pode fazer isso pesquisando usuários no Shared Services Console. Consulte "Pesquisa de Usuários, Grupos, Funções e Listas Delegadas" no *Guia de Administração da Segurança de Usuário do Sistema Oracle Enterprise Performance Management*.

Ao configurar o diretório de usuários de destino como um diretório de usuários externo, verifique se a propriedade Atributo de Logon aponta para o atributo cujo valor foi originalmente usado como o nome de usuário no diretório de usuários de origem. Consulte [Pré-requisitos](#).

3. Mova o Diretório de Usuários de Destino para o topo da Ordem de Pesquisa.

 **Nota:**

Se o nome do diretório de usuários de destino for idêntico ao nome do diretório de origem, você deverá excluir o diretório de usuários de origem da configuração do EPM System.

O Shared Services atribui uma prioridade de ordem de pesquisa mais baixa a um diretório de usuários recentemente adicionado em comparação com a ordem de pesquisa atribuída aos diretórios existentes. Altere a ordem de pesquisa para que o diretório de usuários de destino tenha uma prioridade mais alta de ordem de pesquisa do que o diretório de usuários de origem. Essa ordem permite que o Shared Services descubra usuários no diretório de usuários de destino antes de pesquisar a origem. Consulte "Gerenciamento da Ordem de Pesquisa do Diretório de Usuários" no *Guia de Administração da Segurança de Usuário do Sistema Oracle Enterprise Performance Management*.

4. Reinicie o Oracle Hyperion Foundation Services e outros componentes do EPM System para impor as alterações realizadas.
5. Importe os Dados do Native Directory (exportados do ambiente de origem): Execute o Lifecycle Management com a opção `create/update` para importar os dados que você exportou anteriormente (conforme a lista abaixo) a partir do Native Directory.
 - `Groups.csv`
 - `Assigned Roles.csv`
 - `Delegated Lists.csv`

 **Nota:**

- Consulte o *Guia do Oracle Enterprise Performance Management System Lifecycle Management* para obter instruções detalhadas sobre importação de dados usando o Lifecycle Management.
- Certifique-se de que o arquivo `Users.csv` não foi importado.

Após a importação dos dados, verifique se o Relatório de Status de Migração exibe o status da última operação de importação como `Completed`.

Para importar dados do Native Directory:

- a. No Painel de exibição do Shared Services Console, expanda **Sistema de Arquivos**.
- b. Selecione o local do sistema de arquivos dos arquivos de importação.
- c. Selecione o tipo de artefato para o qual deseja importar informações de provisionamento.
- d. Clique em **Importar**.
- e. Clique em **OK**.

Atualizações Específicas de Produto

▲ **Cuidado:**

A Oracle recomenda que você faça backup dos dados de usuário e grupo no repositório usado pelo componente do Oracle Enterprise Performance Management System antes de iniciar as atualizações específicas do produto. Após a atualização das informações no repositório de produtos local, só é possível reverter para os dados antigos de usuário e grupo no repositório de produtos local usando backups.

Planning

O Oracle Hyperion Planning armazena informações sobre usuários e grupos provisionados no repositório do Planning. Se a identidade de um usuário foi alterada no Native Directory como resultado da migração de usuários e grupos entre diretórios de usuários, você deverá sincronizar as informações no repositório do Planning com o do Native Directory selecionando Migrar Usuários/Grupos. Esse botão está disponível no Planning ao atribuir acesso a formulários de dados, membros e listas de tarefas.

Financial Management

O Oracle Hyperion Financial Management registra informações sobre usuários e grupos provisionados para acessar objetos em um repositório local do Financial Management. Se as informações de usuário e grupo no Native Directory foram alteradas como resultado da migração de usuários e grupos entre diretórios de usuários, você deverá sincronizar as informações no repositório do Financial Management com o do Native Directory.