

Oracle® Enterprise Performance Management System

Guide de configuration de la sécurité



Version 11.2
F28805-22
Décembre 2023

ORACLE®

Copyright © 2005, 2023, Oracle et/ou ses affiliés.

Auteur principal : EPM Information Development Team

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>.

Table des matières

Accessibilité de la documentation

Commentaires sur la documentation

1 A propos de la sécurité dans EPM System

A propos d'EPM System	1-1
Connaissances préalables requises	1-1
Composants d'infrastructure de sécurité	1-2
Authentification utilisateur	1-2
Provisionnement (autorisation basée sur les rôles)	1-6
Lancement de Shared Services Console	1-10

2 Activation SSL des composants EPM System

Hypothèses	2-1
Sources d'information	2-1
Références d'emplacement	2-2
A propos de l'activation SSL des produits EPM System	2-2
Scénarios SSL pris en charge	2-3
Certificats requis	2-4
Arrêt de SSL dans le programme de téléchargement SSL	2-5
Déploiement SSL complet d'EPM System	2-7
Architecture de déploiement	2-7
Hypothèses	2-8
Configuration d'EPM System pour le déploiement SSL complet	2-9
Reconfiguration des paramètres communs EPM System	2-10
Facultatif : installation d'un certificat CA racine pour WebLogic Server	2-12
Installation d'un certificat sur WebLogic Server	2-12
Configuration de WebLogic Server	2-13
Activation de la connexion au serveur HFM avec une base de données Oracle compatible SSL	2-15

Procédures Oracle HTTP Server	2-21
Configuration des composants Web EPM System déployés sur WebLogic Server	2-25
Mise à jour de la configuration de domaine	2-27
Redémarrage des serveurs et d'EPM System	2-28
Test du déploiement	2-29
Configuration des annuaires des utilisateurs externes compatibles SSL	2-29
Arrêt de SSL sur le serveur Web	2-30
SSL pour Essbase 11.1.2.4	2-33
Installation et déploiement des composants Essbase	2-35
Utilisation de certificats CA tiers sécurisés pour Essbase	2-36
Etablissement d'une connexion SSL par session	2-43
SSL pour Essbase 21c	2-44
Installation et déploiement des composants Essbase	2-47
Utilisation de certificats CA tiers sécurisés pour Essbase	2-47
Etablissement d'une connexion SSL par session	2-53

3 Activation de l'authentification unique (SSO) à l'aide des agents de sécurité

Méthodes d'authentification unique prises en charge	3-1
Authentification unique à partir d'Oracle Access Manager	3-4
Authentification unique OracleAS	3-5
Test du déploiement	3-7
Activation d'OSSO pour EPM System	3-7
Protection des produits EPM System pour l'authentification unique	3-11
Authentification unique basée sur un en-tête avec des produits de gestion des identités	3-16
Configuration d'EPM System pour l'authentification unique basée sur un en-tête avec Oracle Identity Cloud Service	3-18
Prérequis et exemples d'URL	3-18
Activation de l'authentification basée sur un en-tête pour EPM System	3-19
Ajout d'une application EPM System et d'une passerelle vers Oracle Identity Cloud Service	3-19
Configuration de la passerelle d'application	3-25
Configuration de l'annuaire des utilisateurs pour l'autorisation	3-25
Activation de l'authentification unique dans EPM System	3-25
Mise à jour des paramètres EPM Workspace	3-26
Authentification unique SiteMinder	3-26
Authentification unique Kerberos	3-29
Configuration de EPM System pour l'authentification unique	3-44
Options d'authentification unique pour Smart View	3-45

4 Configuration des annuaires des utilisateurs

Annuaire des utilisateurs et sécurité EPM System	4-1
Opérations associées à la configuration des annuaires des utilisateurs	4-2
Oracle Identity Manager et EPM System	4-2
Informations Active Directory	4-3
Configuration d'OID, d'Active Directory et d'autres annuaires des utilisateurs LDAP	4-4
Configuration des bases de données relationnelles en tant qu'annuaires des utilisateurs	4-19
Test des connexions de l'annuaire des utilisateurs	4-22
Modification des paramètres d'annuaire des utilisateurs	4-23
Suppression des configurations d'annuaires des utilisateurs	4-23
Gestion de l'ordre de recherche de l'annuaire des utilisateurs	4-24
Configuration des options de sécurité	4-26
Régénération des clés de cryptage	4-29
Utilisation des caractères spéciaux	4-31

5 Utilisation d'un module d'authentification personnalisé

Présentation	5-1
Exemples de cas d'utilisation et limitation	5-3
Prérequis	5-3
Remarques concernant la conception et le codage	5-3
Déploiement du module d'authentification personnalisé	5-9

6 Consignes générales de sécurité pour EPM System

Implémentation du protocole SSL	6-1
Modification du mot de passe d'administration	6-1
Régénération des clés de cryptage	6-2
Modification des mots de passe de base de données	6-2
Sécurité des cookies	6-3
Réduction du délai d'expiration du jeton SSO	6-4
Vérification des rapports de sécurité	6-4
Personnalisation du système d'authentification pour une authentification forte	6-4
Désactivation des utilitaires de débogage d'EPM Workspace	6-4
Modification des pages d'erreur par défaut du serveur Web	6-5
Prise en charge des logiciels tiers	6-5

A Exemple de code d'authentification personnalisé

Exemple de code 1	A-1
Exemple de code 2	A-2

B Implémentation d'une classe de connexion personnalisée

Exemple de code de classe de connexion personnalisée

B-1

Déploiement d'une classe de connexion personnalisée

B-4

C Migration d'utilisateurs et de groupes entre les annuaires des utilisateurs

Présentation

C-1

Prérequis

C-1

Procédure de migration

C-2

Mises à jour spécifiques du produit

C-5

Accessibilité de la documentation

Pour plus d'informations sur l'engagement d'Oracle pour l'accessibilité de la documentation, visitez le site Web Oracle Accessibility Program, à l'adresse : <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Accès aux services de support Oracle

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> ou le site <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> si vous êtes malentendant.

Commentaires sur la documentation

Pour envoyer des commentaires sur cette documentation, cliquez sur le bouton Commentaires situé en bas de la page de chaque rubrique du centre d'aide Oracle. Vous pouvez également envoyer un courriel à l'adresse epmdoc_ww@oracle.com.

1

A propos de la sécurité dans EPM System

Voir aussi :

- [A propos d'EPM System](#)
- [Connaissances préalables requises](#)
- [Composants d'infrastructure de sécurité](#)
- [Authentification utilisateur](#)
- [Provisionnement \(autorisation basée sur les rôles\)](#)
- [Lancement de Shared Services Console](#)

A propos d'EPM System

Les produits Oracle Enterprise Performance Management System constituent un système complet à l'échelle de l'entreprise, qui intègre des suites modulaires d'applications de planification et de gestion financière, ainsi que des fonctionnalités d'informatique décisionnelle permettant l'analyse et la création de rapports. Voici les principaux composants des produits EPM System :

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

Pour obtenir plus d'informations sur les produits et les composants de chacune de ces familles de produits, reportez-vous au guide *Avant l'installation d'Oracle Hyperion Enterprise Performance Management System*.

Connaissances préalables requises

Ce guide s'adresse aux administrateurs système chargés de configurer, de sécuriser et de gérer les composants Oracle Enterprise Performance Management System. Les compétences suivantes sont requises :

- Une bonne compréhension de l'infrastructure de sécurité de votre organisation, y compris des éléments suivants :
 - Les serveurs d'annuaire, par exemple, Oracle Internet Directory, Sun Java System Directory Server et Microsoft Active Directory
 - L'utilisation du protocole SSL (Secure Socket Layer) pour sécuriser les canaux de communication
 - Les systèmes de gestion d'accès, par exemple, Oracle Access Manager et SiteMinder
 - L'infrastructure SSO (Single sign-on), par exemple, Kerberos

- La connaissance des concepts de sécurité EPM System pertinents pour votre organisation

Composants d'infrastructure de sécurité

Oracle Enterprise Performance Management System intègre plusieurs composants de sécurité pour garantir la fiabilité de la sécurité des applications. Lorsqu'il est intégré à une infrastructure sécurisée, EPM System offre une suite d'applications hautement sécurisée qui garantit la sécurité de l'accès et des données. Les composants d'infrastructure que vous pouvez utiliser pour sécuriser EPM System incluent les éléments suivants :

- Un système de gestion d'accès facultatif, par exemple, Oracle Access Manager, pour fournir l'accès SSO aux composants EPM System
- Une infrastructure SSO intégrée, par exemple, Kerberos
Vous pouvez utiliser l'authentification Kerberos avec le système de gestion d'accès (SiteMinder) afin de vous assurer que les utilisateurs Windows peuvent se connecter de manière transparente à SiteMinder et aux composants EPM System.
- Le protocole SSL (Secure Socket Layer) pour sécuriser les canaux de communication entre les clients et les composants EPM System

Authentification utilisateur

L'authentification de l'utilisateur active la fonctionnalité d'authentification unique (SSO) dans les composants Oracle Enterprise Performance Management System en validant les informations de connexion de chaque utilisateur pour déterminer les utilisateurs authentifiés. L'authentification utilisateur, ainsi que l'autorisation propre aux composants, donnent à l'utilisateur un accès aux composants EPM System. Le processus d'autorisation est appelé provisionnement.

Composants d'authentification

Les sections suivantes décrivent les composants qui prennent en charge l'authentification unique :

- [Annuaire natif](#)
- [Annuaire des utilisateurs externes](#)

Annuaire natif

L'annuaire natif désigne la base de données relationnelle qu'Oracle Hyperion Shared Services utilise pour prendre en charge le provisionnement et stocker les données de départ telles que les comptes utilisateur par défaut.

Fonctions de l'annuaire natif :

- Conserver et gérer les comptes utilisateur EPM System par défaut
- Stocker toutes les informations de provisionnement EPM System (relations entre les utilisateurs, les groupes et les rôles)

Oracle Hyperion Shared Services Console permet d'accéder à l'annuaire natif et de le gérer. Reportez-vous à la section "Gestion de l'annuaire natif" du *Guide d'administration de la sécurité utilisateur d'Oracle Enterprise Performance Management System*.

Annuaire des utilisateurs externes

Les annuaires des utilisateurs font référence aux systèmes de gestion des identités et des utilisateurs d'entreprise compatibles avec les composants EPM System.

Les composants EPM System sont pris en charge par plusieurs annuaires des utilisateurs, notamment les annuaires des utilisateurs basés sur LDAP, tels qu'Oracle Internet Directory, Sun Java System Directory Server (anciennement SunONE Directory Server) et Microsoft Active Directory. Les bases de données relationnelles sont également prises en charge en tant qu'annuaires des utilisateurs. Les annuaires des utilisateurs autres que l'annuaire natif sont appelés annuaires des utilisateurs externes dans ce document.

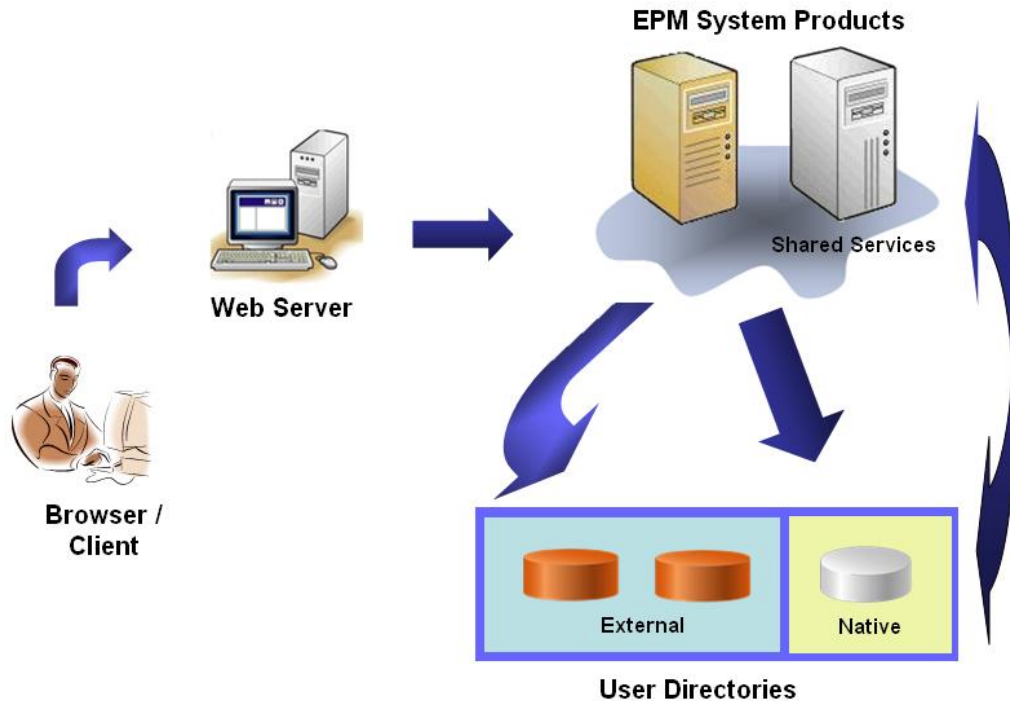
Pour obtenir la liste des annuaires des utilisateurs pris en charge, reportez-vous à la *Matrice de certification Oracle Enterprise Performance Management System* publiée sur la page [Configurations système prises en charge par Oracle Fusion Middleware](#) sur Oracle Technology Network (OTN).

Shared Services Console vous permet de configurer de nombreux annuaires des utilisateurs externes comme source pour les utilisateurs et les groupes EPM System. Chaque utilisateur EPM System doit disposer d'un compte unique dans un annuaire des utilisateurs configuré. En général, les utilisateurs EPM System sont affectés à des groupes pour faciliter le provisionnement.

Authentification unique EPM System par défaut

EPM System prend en charge SSO sur les applications Web EPM System en autorisant les utilisateurs authentifiés d'une application à accéder en toute transparence à d'autres applications sans avoir à entrer de nouveau des informations d'identification. SSO est implémenté par le biais de l'intégration d'un environnement de sécurité commun qui gère le provisionnement et l'authentification des utilisateurs (autorisation basée sur les rôles) pour les composants EPM System.

Le processus SSO par défaut est représenté dans l'illustration suivante.



1. A l'aide d'un navigateur, les utilisateurs accèdent à l'écran de connexion à un composant EPM System et saisissent un nom d'utilisateur et un mot de passe.
Le composant EPM System envoie une requête aux annuaires des utilisateurs configurés (y compris l'annuaire natif) pour vérifier les informations d'identification de l'utilisateur. Lorsque le compte utilisateur correspondant est trouvé dans un annuaire des utilisateurs, la recherche s'interrompt et les informations de l'utilisateur sont renvoyées au composant EPM System.
L'accès est refusé si aucun compte utilisateur n'est trouvé dans un annuaire des utilisateurs configuré.
2. A l'aide des informations d'utilisateur extraites, le composant EPM System envoie une requête à l'annuaire natif pour obtenir les détails de provisionnement de l'utilisateur.
3. Le composant EPM System vérifie la liste de contrôle d'accès (ACL) pour déterminer à quels artefacts d'application l'utilisateur peut accéder.

Dès réception des informations de provisionnement de l'annuaire natif, le composant EPM System devient disponible pour l'utilisateur. A ce stade, SSO est activé pour tous les composants EPM System pour lesquels l'utilisateur est provisionné.

Authentification unique à partir de systèmes de gestion d'accès

Afin de sécuriser davantage les composants EPM System, vous pouvez implémenter un système de gestion d'accès pris en charge, comme Oracle Access Manager ou SiteMinder, qui peut fournir des informations d'identification d'utilisateur authentifié aux composants EPM System et contrôler l'accès en fonction de privilèges d'accès prédéfinis.

L'authentification unique à partir d'agents de sécurité est disponible pour les applications Web EPM System uniquement. Dans ce scénario, les composants EPM System utilisent les informations utilisateur fournies par l'agent de sécurité pour

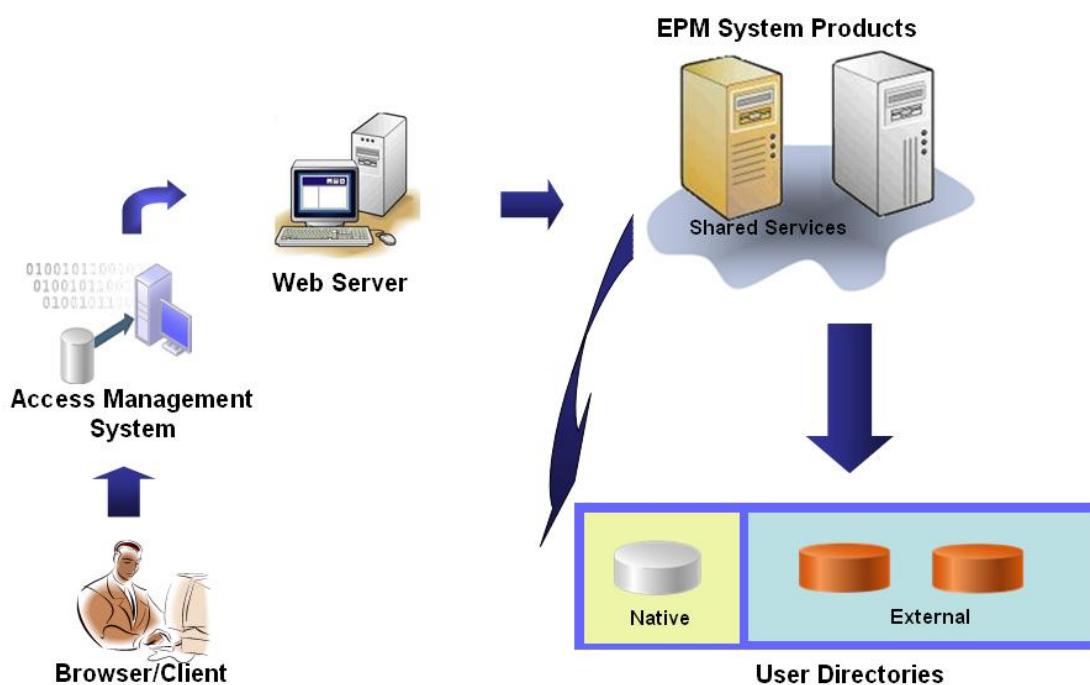
déterminer les autorisations d'accès des utilisateurs. Pour renforcer la sécurité, Oracle recommande que l'accès direct aux serveurs soit bloqué par des pare-feu. Ainsi, toutes les requêtes sont acheminées via un portail d'authentification unique.

L'authentification unique à partir de systèmes de gestion d'accès est prise en charge en acceptant les informations d'identification des utilisateurs authentifiés via un mécanisme d'authentification unique acceptable. Reportez-vous à la section [Méthodes d'authentification unique prises en charge](#). Le système de gestion d'accès authentifie les utilisateurs et transmet le nom de connexion à EPM System. EPM System vérifie le nom de connexion par rapport aux annuaires des utilisateurs configurés.

Reportez-vous aux sections suivantes.

- [Authentification unique à partir d'Oracle Access Manager](#)
- [Authentification unique OracleAS](#)
- [Authentification unique SiteMinder](#)
- [Authentification unique Kerberos](#)

Illustration du concept :



1. A l'aide d'un navigateur, les utilisateurs demandent l'accès à une ressource protégée par un système de gestion d'accès, par exemple, Oracle Access Manager ou SiteMinder.

 **Remarque :**

Les composants EPM System sont définis comme des ressources protégées par le système de gestion d'accès.

Le système de gestion d'accès intercepte la demande et présente un écran de connexion. Les utilisateurs entrent un nom d'utilisateur et un mot de passe, qui sont validés par rapport aux annuaires des utilisateurs configurés dans le système de gestion d'accès pour vérifier l'authenticité de l'utilisateur. Les composants EPM System sont également configurés pour fonctionner avec ces annuaires des utilisateurs.

Les informations sur l'utilisateur authentifié sont transmises au composant EPM System, qui accepte ces informations comme valides.

Le système de gestion d'accès transmet le nom de connexion de l'utilisateur (valeur `Attribut de connexion`) au composant EPM System à l'aide d'un mécanisme SSO acceptable. Reportez-vous à la section [Méthodes d'authentification unique prises en charge](#).

2. Pour vérifier les informations de connexion, le produit EPM System recherche l'utilisateur dans un annuaire des utilisateurs. Si un compte utilisateur correspondant est trouvé, les informations de l'utilisateur sont renvoyées au composant EPM System. La sécurité d'EPM System définit le jeton SSO qui permet d'activer l'authentification unique dans les composants EPM System.
3. A l'aide des informations d'utilisateur extraites, le composant EPM System envoie une requête à l'annuaire natif pour obtenir les détails de provisionnement de l'utilisateur.

Lorsqu'il reçoit les informations sur le provisionnement, le composant EPM System est disponible pour l'utilisateur. L'authentification unique est activée pour tous les produits EPM System pour lesquels l'utilisateur est provisionné.

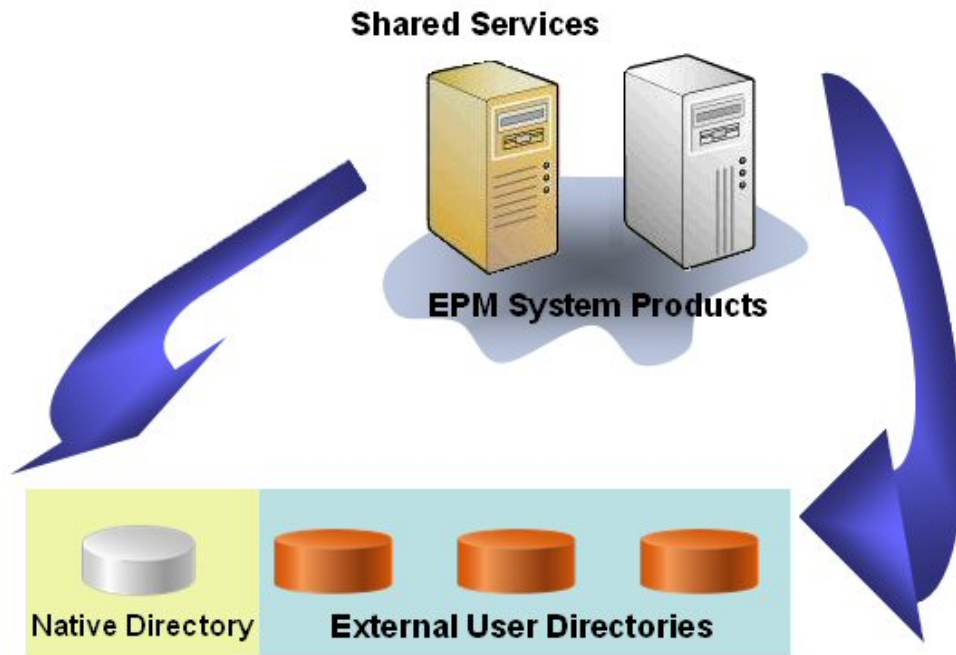
Provisionnement (autorisation basée sur les rôles)

La sécurité d'Oracle Enterprise Performance Management System détermine l'accès utilisateur aux applications via le concept de rôles. Les rôles correspondent à des autorisations qui déterminent l'accès utilisateur aux fonctions de l'application. Certains composants EPM System appliquent des listes ACL de niveau objet pour affiner davantage l'accès des utilisateurs à leurs artefacts, tels que les rapports et les membres.

Chaque composant EPM System fournit plusieurs rôles par défaut adaptés aux différents besoins métier. Chaque application appartenant à un composant EPM System hérite de ces rôles. Les rôles prédéfinis des applications enregistrées auprès d'Oracle Hyperion Shared Services sont disponibles dans Oracle Hyperion Shared Services Console. Vous pouvez aussi créer d'autres rôles qui agrègent les rôles par défaut pour répondre aux exigences spécifiques. Ces rôles sont utilisés pour le provisionnement. Le processus d'attribution de rôles spécifiques des applications EPM System et de leurs ressources aux utilisateurs et aux groupes est appelé *provisionnement*.

L'annuaire natif et les annuaires des utilisateurs configurés sont des sources d'informations sur les utilisateurs et les groupes pour le processus de provisionnement. Vous pouvez rechercher et provisionner des utilisateurs et des groupes à partir de tous les annuaires configurés sur Shared Services Console. Vous pouvez également utiliser des rôles agrégés spécifiques de l'application créés dans l'annuaire natif lors du processus de provisionnement.

Présentation illustrée du processus d'autorisation :



1. Une fois l'utilisateur authentifié, le composant EPM System envoie une requête aux annuaires des utilisateurs pour déterminer les groupes de l'utilisateur.
2. Le composant EPM System utilise les informations sur l'utilisateur et les groupes pour extraire les données de provisionnement de l'utilisateur à partir de Shared Services. Le composant utilise ces données pour déterminer les ressources auxquelles un utilisateur peut accéder.

Les tâches de provisionnement spécifiques du produit, telles que la configuration du contrôle de l'accès spécifique à un produit, sont effectuées pour chaque produit. Ces données sont combinées avec les données de provisionnement pour déterminer l'accès au produit pour les utilisateurs.

Le provisionnement basé sur les rôles de produits EPM System utilise ces concepts.

Roles

Un rôle est une construction (semblable à la liste des contrôles d'accès) qui définit les autorisations d'accès accordées aux utilisateurs et aux groupes pour effectuer les fonctions sur les ressources EPM System. Un rôle est une combinaison de ressources ou de types de ressource (ce à quoi les utilisateurs ont accès, par exemple, un rapport) et d'actions que les utilisateurs peuvent effectuer sur les ressources (par exemple, afficher et modifier).

L'accès aux ressources d'application EPM System est restreint. Les utilisateurs peuvent y accéder uniquement après qu'un rôle doté de privilèges d'accès a été affecté à l'utilisateur ou au groupe auquel appartient l'utilisateur. La restriction de l'accès basée sur les rôles permet aux administrateurs de contrôler et de gérer l'accès à l'application.

Rôles globaux

Les rôles globaux sont des rôles Shared Services qui couvrent plusieurs produits et permettent d'effectuer certaines tâches dans les produits EPM System. Par exemple, l'administrateur Shared Services peut provisionner les utilisateurs pour toutes les applications EPM System.

Rôles prédéfinis

Les rôles prédéfinis sont des rôles intégrés dans les produits EPM System. Vous ne pouvez pas les supprimer. Chaque instance d'application appartenant à un produit EPM System hérite de tous les rôles prédéfinis du produit. Ces rôles sont enregistrés avec Shared Services lors de la création de chaque application.

Rôles agrégés

Les rôles agrégés, également nommés rôles personnalisés, agrègent plusieurs rôles prédéfinis d'une application. Un rôle agrégé peut contenir d'autres rôles agrégés. Par exemple, un administrateur ou un gestionnaire de profils Shared Services peut créer un rôle agrégé combinant les rôles Planificateur et Utilisateur de la vue d'une application Oracle Hyperion Planning. L'agrégation des rôles permet de simplifier l'administration des applications possédant des rôles granulaires. Les rôles Shared Services globaux peuvent être inclus dans des rôles agrégés. Vous ne pouvez pas créer un rôle agrégé couvrant plusieurs applications ou produits.

Users

Les annuaires des utilisateurs stockent des informations sur les utilisateurs qui ont accès aux produits EPM System. Les processus d'authentification et d'autorisation utilisent les informations d'utilisateur. Vous pouvez créer et gérer des utilisateurs d'annuaire natif uniquement à partir de Shared Services Console.

Les utilisateurs de tous les annuaires configurés sont visibles à partir de Shared Services Console. Des privilèges d'accès peuvent être attribués individuellement à ces utilisateurs pour les applications EPM System enregistrées avec Shared Services. Oracle déconseille le provisionnement d'utilisateurs individuels.

Administrateur EPM System par défaut

Un compte d'administrateur, avec le nom par défaut `admin`, est créé dans l'annuaire natif lors du processus de déploiement. Il s'agit du compte EPM System offrant le plus de contrôle et il doit être utilisé uniquement pour configurer un administrateur système, qui est l'expert en informatique chargé de gérer la sécurité et l'environnement EPM System.

Le nom d'utilisateur et le mot de passe de l'administrateur EPM System sont définis lors du déploiement d'Oracle Hyperion Foundation Services. Etant donné que ce compte ne peut pas être soumis à des stratégies de mot de passe de compte d'entreprise, Oracle recommande de le désactiver après la création d'un compte d'administrateur système.

En règle générale, le compte d'administrateur EPM System par défaut est utilisé pour effectuer les tâches suivantes :

- Configurer l'annuaire de l'entreprise en tant qu'annuaire des utilisateurs externe. Reportez-vous à [Configuration des annuaires des utilisateurs](#).
- Créer un compte d'administrateur système en provisionnant un expert en informatique d'entreprise avec le rôle d'administrateur Shared Services. Reportez-vous à la section "Provisionnement des utilisateurs et des groupes" dans le *Guide d'administration de la sécurité utilisateur d'Oracle Enterprise Performance Management System*.

Administrateur système

L'administrateur système est généralement un expert en informatique d'entreprise qui dispose de droits d'accès en lecture, en écriture et en exécution sur tous les serveurs d'un déploiement EPM System.

En règle générale, l'administrateur système effectue les tâches suivantes :

- Désactiver le compte d'administrateur EPM System par défaut.
- Créer au moins un administrateur fonctionnel.
- Définir la configuration de la sécurité pour EPM System à l'aide de Shared Services Console.
- Eventuellement, configurer les annuaires des utilisateurs en tant qu'annuaire des utilisateurs externe.
- Surveiller EPM System en exécutant régulièrement l'outil d'analyse de journal.

Les tâches effectuées par l'administrateur fonctionnel sont décrites dans ce guide.

Procédures pour créer un administrateur fonctionnel :

- Configurer l'annuaire de l'entreprise en tant qu'annuaire des utilisateurs externe. Reportez-vous à la section [Configuration des annuaires des utilisateurs](#).
- Provisonnez un utilisateur ou un groupe avec les rôles requis pour créer un administrateur fonctionnel. Reportez-vous à la section "Provisionnement des utilisateurs et des groupes" dans le *Guide d'administration de la sécurité utilisateur d'Oracle Enterprise Performance Management System*.

L'administrateur fonctionnel doit être provisionné avec les rôles suivants :

- Rôle d'administrateur LCM de Shared Services
- Rôle d'administrateur et de gestionnaire de profils de chaque composant EPM System

Administrateurs fonctionnels

L'administrateur fonctionnel est un utilisateur d'entreprise qui est un expert EPM System. En général, il est défini dans l'annuaire d'entreprise qui est configuré dans Shared Services en tant qu'annuaire des utilisateurs externe.

L'administrateur fonctionnel exécute des tâches d'administration EPM System comme la création d'autres administrateurs fonctionnels, la configuration de l'administration déléguée, la création et le provisionnement d'applications et d'artefacts, et la configuration de l'audit d'EPM System. Les tâches effectuées par l'administrateur fonctionnel sont décrites dans le *Guide d'administration de la sécurité utilisateur d'Oracle Enterprise Performance Management System*.

Groups

Les groupes sont des conteneurs pour les utilisateurs ou les autres groupes. Vous pouvez créer et gérer des groupes d'annuaire natif à partir de Shared Services Console. Les groupes de tous les annuaires d'utilisateurs configurés sont affichés dans Shared Services Console. Vous pouvez provisionner ces groupes afin de donner les autorisations d'accès aux produits EPM System enregistrés auprès de Shared Services.

Lancement de Shared Services Console

Vous utilisez une option de menu dans Oracle Hyperion Enterprise Performance Management Workspace pour accéder à Oracle Hyperion Shared Services Console.

Pour lancer Shared Services Console :

1. Rendez-vous sur :

```
http://web_server_name:port_number/workspace
```

Dans l'URL, *web_server_name* indique le nom de l'ordinateur où le serveur Web utilisé par Oracle Hyperion Foundation Services est exécuté, et *port_number* indique le port du serveur Web utilisé (par exemple, `http://myWebserver:19000/workspace`).

Remarque :

Si vous accédez à EPM Workspace dans des environnements sécurisés, utilisez `https` (et non `http`) comme protocole et le numéro de port du serveur Web sécurisé. Par exemple, utilisez l'URL suivante : `https://myserver:19043/workspace`.

2. Cliquez sur **Lancer l'application**.

Remarque :

Les bloqueurs de fenêtres publicitaires peuvent empêcher l'ouverture d'EPM Workspace.

3. Dans l'écran de **connexion**, entrez votre nom d'utilisateur et votre mot de passe.
Initialement, le seul utilisateur pouvant accéder à Shared Services Console est l'administrateur Oracle Enterprise Performance Management System dont le nom d'utilisateur et le mot de passe ont été fournis au cours du processus de déploiement.
4. Cliquez sur **Connexion**.
5. Sélectionnez **Naviguer**, **Administrer**, puis **Shared Services Console**.

2

Activation SSL des composants EPM System

Voir aussi :

- [Hypothèses](#)
- [Sources d'information](#)
- [Références d'emplacement](#)
- [A propos de l'activation SSL des produits EPM System](#)
- [Scénarios SSL pris en charge](#)
- [Certificats requis](#)
- [Arrêt de SSL dans le programme de téléchargement SSL](#)
- [Déploiement SSL complet d'EPM System](#)
- [Arrêt de SSL sur le serveur Web](#)
- [SSL pour Essbase 11.1.2.4](#)
- [SSL pour Essbase 21c](#)

Hypothèses

- Vous avez déterminé la topologie de déploiement et identifié les liens de communication qui doivent être sécurisés à l'aide de SSL.
- Vous avez obtenu les certificats requis d'un CA (Certificate Authority, Autorité de certification), soit d'un CA reconnu ou de vous-même, ou créé des certificats auto-signés. Reportez-vous à [Certificats requis](#).
- Vous connaissez les procédures et les concepts liés à SSL comme l'import de certificats. Reportez-vous à la section [Sources d'information](#) pour obtenir la liste des documents de référence.

Sources d'information

L'activation SSL d'Oracle Enterprise Performance Management System nécessite que vous prépariez des composants tels que le serveur d'applications, le serveur Web, les bases de données et les annuaires des utilisateurs afin de communiquer à l'aide du protocole SSL. Ce document part du principe que vous connaissez les tâches associées à l'activation SSL de ces composants.

- **Oracle WebLogic Server** : reportez-vous à la section [Configuration du protocole SSL du guide de sécurisation de WebLogic Server](#).
- **Oracle HTTP Server** : reportez-vous aux sections suivantes dans le *Guide de l'administrateur Oracle HTTP Server* :
 - [Gestion de la sécurité](#)
 - [Enabling SSL for Oracle HTTP Server \(activation SSL pour Oracle HTTP Server\)](#)

- **Annuaire des utilisateurs** : reportez-vous à la documentation du fournisseur de l'annuaire des utilisateurs. Liens utiles :
 - **Oracle Internet Directory** : reportez-vous à [Guide de l'administrateur Oracle Internet Directory](#) et
 - **Sun Java System Directory Server** : reportez-vous à la section [Sécurité du serveur d'annuaire](#) du *guide d'administration de Sun Java System Directory Server*.
 - **Active Directory** : reportez-vous à la documentation Microsoft.
- **Bases de données** : reportez-vous à la documentation du fournisseur de bases de données.

Références d'emplacement

Ce document fait référence aux emplacements de déploiement et d'installation suivants :

- *MIDDLEWARE_HOME* se rapporte à l'emplacement des composants Middleware tels qu'Oracle WebLogic Server et, éventuellement, un ou plusieurs répertoires *EPM_ORACLE_HOME*. *MIDDLEWARE_HOME* est défini pendant l'installation du produit Oracle Enterprise Performance Management System. Le répertoire *MIDDLEWARE_HOME* par défaut est `Oracle/Middleware`.
- *EPM_ORACLE_HOME* se rapporte au répertoire d'installation contenant les fichiers requis pour prendre en charge les produits EPM System. *EPM_ORACLE_HOME* réside dans *MIDDLEWARE_HOME*. L'emplacement par défaut d'*EPM_ORACLE_HOME* est *MIDDLEWARE_HOME/EPMSys11R1*, par exemple, `Oracle/Middleware/EPMSys11R1`.

Les produits EPM System sont installés dans le répertoire *EPM_ORACLE_HOME/products*, par exemple, `Oracle/Middleware/EPMSys11R1/products`.

En outre, pendant la configuration des produits EPM System, certains produits déploient des composants vers *MIDDLEWARE_HOME/user_projects/epmsys11*, par exemple, `Oracle/Middleware/user_projects/epmsys11`.

- *EPM_ORACLE_INSTANCE* indique un emplacement qui est défini au cours du processus de configuration, lorsque certains produits déploient des composants. L'emplacement par défaut d'*EPM_ORACLE_INSTANCE* est *MIDDLEWARE_HOME/user_projects/epmsys11*, par exemple, `Oracle/Middleware/user_projects/epmsys11`.

A propos de l'activation SSL des produits EPM System

Le processus de déploiement d'Oracle Enterprise Performance Management System déploie automatiquement les produits Oracle EPM System de sorte qu'ils fonctionnent à la fois dans les modes SSL et non SSL.

 **Remarque :**

- EPM System prend en charge SSL sur HTTP et JDBC uniquement. Il ne prend en charge aucun autre protocole, par exemple Thrift et ODBC, pour sécuriser la communication.
- Afin d'éviter la vulnérabilité Poodle (Padding Oracle On Downgraded Legacy Encryption), qui est une attaque visant le protocole SSLv3, vous devez désactiver la prise en charge de SSLv3 sur vos serveurs et sur les navigateurs utilisés pour accéder aux composants EPM System. Reportez-vous à la documentation de vos serveurs et des navigateurs pour plus d'informations sur la désactivation de la prise en charge de SSLv3.
- Il se peut que les serveurs EPM System ne démarrent pas si vous désactivez le mode non SSL après avoir configuré SSL.
Activez la réplication sécurisée pour tous les serveurs EPM System dans le domaine afin qu'ils démarrent lorsque le mode non SSL est désactivé.

Lorsque vous spécifiez les paramètres communs pour EPM System, vous indiquez si SSL doit être activé pour l'ensemble de la communication entre serveurs dans votre déploiement.

La sélection des paramètres SSL au cours du déploiement ne configure pas automatiquement votre environnement pour SSL. Seul un indicateur s'affiche dans le registre Oracle Hyperion Shared Services pour indiquer que tous les composants EPM System qui font appel au registre Shared Services doivent utiliser le protocole sécurisé (HTTPS) pour la communication entre serveurs. Vous devez effectuer des procédures supplémentaires afin d'activer SSL pour votre environnement. Ces procédures sont abordées dans ce document.

 **Remarque :**

Le fait de redéployer vos applications efface les paramètres de serveur Web et de serveur d'applications que vous avez spécifiés pour activer SSL.

 **Remarque :**

Dans Enterprise Performance Management System version 11.2.x, SSL (Secure Sockets Layer) pour MS SQL Server dans l'utilitaire de création de référentiel (RCU) n'est pas pris en charge.

Scénarios SSL pris en charge

Les scénarios SSL suivants sont pris en charge :

- Arrêt de SSL dans le programme de déchargement SSL. Reportez-vous à [Arrêt de SSL dans le programme de déchargement SSL](#).
- Déploiement SSL complet. Reportez-vous à [Déploiement SSL complet d'EPM System](#).

Certificats requis

La communication SSL utilise des certificats pour établir l'approbation entre les composants. Oracle recommande d'utiliser les certificats émis par des organismes de certification tiers reconnus pour activer SSL pour Oracle Enterprise Performance Management System dans un environnement de production.

Remarque :

EPM System prend en charge l'utilisation de certificats génériques, ce qui permet de sécuriser plusieurs sous-domaines avec un seul certificat SSL. Les certificats génériques permettent de réduire les coûts et le temps de gestion.

Si vous utilisez des certificats génériques pour crypter la communication, vous devez désactiver la vérification de nom d'hôte dans Oracle WebLogic Server.

Vous avez besoin des certificats suivants pour chaque serveur hébergeant des composants EPM System :

- Un certificat CA racine

Remarque :

Vous n'avez pas besoin d'installer un certificat CA racine dans le fichier de clés d'accès Java si vos certificats proviennent d'un organisme de certification tiers reconnu dont le certificat racine est déjà installé dans le fichier de clés d'accès Java.

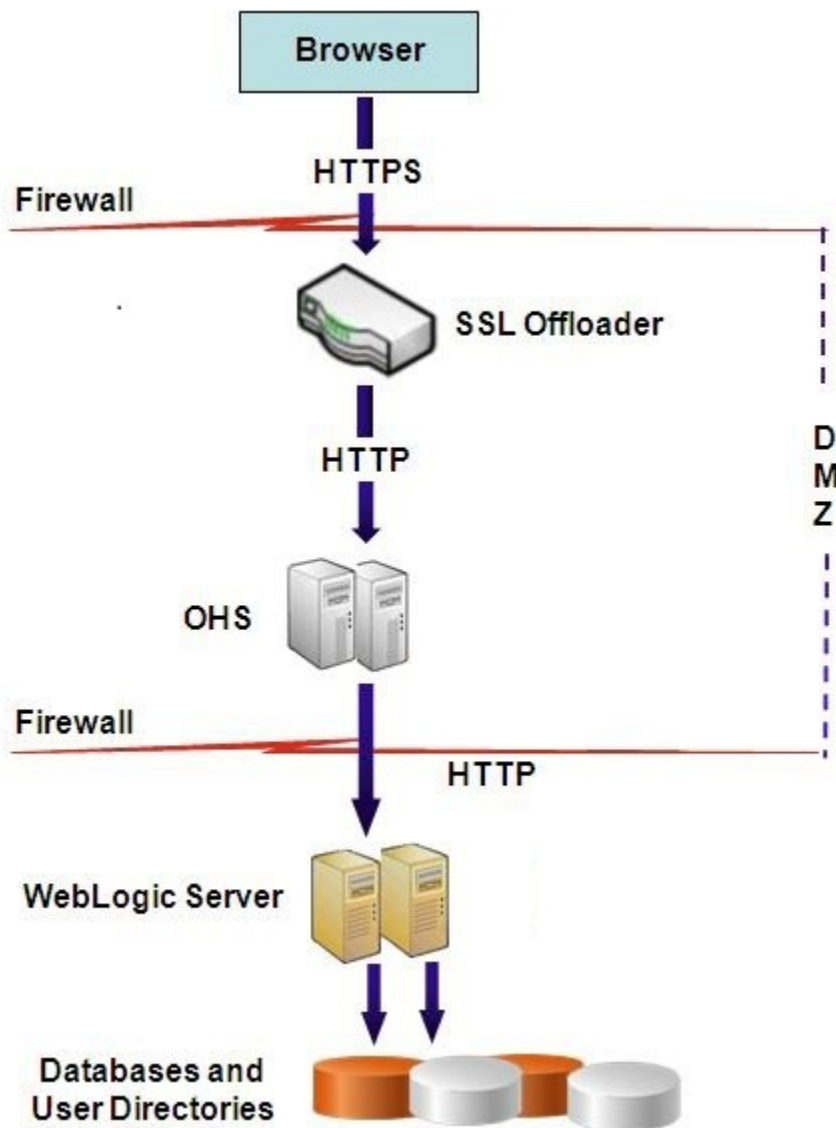
Des certificats provenant d'organismes de certification tiers reconnus sont préchargés pour Firefox et Internet Explorer. Si vous êtes votre propre organisme de certification, vous devez importer votre certificat CA racine dans le fichier de clés d'accès utilisé par les clients auxquels accèdent ces navigateurs. Si vous êtes votre propre organisme de certification, les clients Web ne peuvent pas établir de liaison SSL avec le serveur si votre certificat CA racine n'est pas disponible pour le navigateur à partir duquel s'effectue l'accès au client.

- Des certificats signés pour chaque serveur Oracle HTTP Server dans votre déploiement
- Un certificat signé pour l'ordinateur hôte WebLogic Server Les serveurs gérés sur cet ordinateur peuvent également utiliser ce certificat.
- Deux certificats pour le programme de déchargement/l'équilibreur de charge SSL. L'un de ces certificats est destiné à la communication externe et l'autre à la communication interne.

Arrêt de SSL dans le programme de déchargement SSL

Architecture de déploiement

Dans ce scénario, SSL est utilisé pour sécuriser le lien de communication entre les clients Oracle Enterprise Performance Management System (par exemple, un navigateur) et un programme de déchargement SSL. Illustration du concept :



Hypothèses

Programme de déchargement SSL et équilibreur de charge

Un programme de déchargement SSL entièrement configuré avec un équilibreur de charge doit être présent dans l'environnement de déploiement.

L'équilibreur de charge doit être configuré pour transmettre toutes les demandes reçues par les hôtes virtuels vers les serveurs Oracle HTTP Server.

Lorsque SSL est en cours d'arrêt au niveau d'Oracle HTTP Server (OHS) ou de l'équilibreur de charge, vous devez procéder comme suit :

- Définissez chaque application Web logique sur l'hôte virtuel non SSL de l'équilibreur de charge ou d'Oracle HTTP Server (par exemple, `empinternal.myCompany.com:80`, où 80 est le port non SSL). Ouvrez l'écran Configuration, puis effectuez les étapes suivantes :
 1. Développez la tâche de configuration **Hyperion Foundation**.
 2. Sélectionnez **Configurer une adresse logique pour les applications Web**.
 3. Indiquez le *nom d'hôte*, le numéro de port non SSL et le numéro de port SSL.
- Définissez l'URL externe sur l'hôte virtuel compatible SSL de l'équilibreur de charge ou d'Oracle HTTP Server (par exemple, `empexternal.myCompany.com:443`, où 443 est le port SSL). Ouvrez l'écran Configuration, puis effectuez les étapes suivantes :
 1. Développez la tâche de configuration **Hyperion Foundation**.
 2. Sélectionnez **Configurer les paramètres communs**.
 3. Sélectionnez **Activer le déchargement SSL** sous Détails d'URL externe.
 4. Indiquez l'*hôte d'URL externe* et le *port d'URL externe*.

 **Remarque :**

Le redéploiement des applications Web ou la reconfiguration du serveur Web à l'aide de **configtool** entraîne le remplacement des paramètres des URL externe et d'application Web logique.

Hôtes virtuels

L'arrêt de SSL lors de la configuration du programme de déchargement SSL utilise deux alias de serveur, par exemple `epm.myCompany.com` et `empinternal.myCompany.com`, sur le programme de déchargement/l'équilibreur de charge SSL, l'un pour la communication externe entre le programme de déchargement et les navigateurs, et l'autre pour la communication interne entre les serveurs EPM System. Assurez-vous que les alias de serveur pointent vers l'adresse IP de la machine et qu'ils peuvent être résolus via DNS.

Un certificat signé permettant de prendre en charge la communication externe entre le programme de déchargement et les navigateurs (via `epm.myCompany.com`) doit être installé sur l'équilibreur de charge/le programme de déchargement.

Configuration d'EPM System

Le déploiement par défaut des composants EPM System prend en charge l'arrêt de SSL dans le programme de déchargement SSL. Aucune action supplémentaire n'est nécessaire.

Lors de la configuration d'EPM System, assurez-vous que l'adresse logique pour les applications Web pointe vers l'alias (par exemple, `empinternal.myCompany.com`) ayant

été créé pour la communication interne. Reportez-vous aux sources d'information suivantes pour installer et configurer EPM System :

- *Guide d'installation et de configuration d'Oracle Enterprise Performance Management System*
- *Avant l'installation d'Oracle Hyperion Enterprise Performance Management System*
- *Guide de résolution des problèmes d'installation et de configuration d'Oracle Enterprise Performance Management System*

Test du déploiement

Après avoir terminé le processus de déploiement, vérifiez que tout fonctionne en vous connectant à l'URL sécurisée Oracle Hyperion Enterprise Performance Management Workspace :

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

Par exemple, `https://epm.myCompany.com:443/workspace/index.jsp`, où 443 est le port SSL.

Déploiement SSL complet d'EPM System

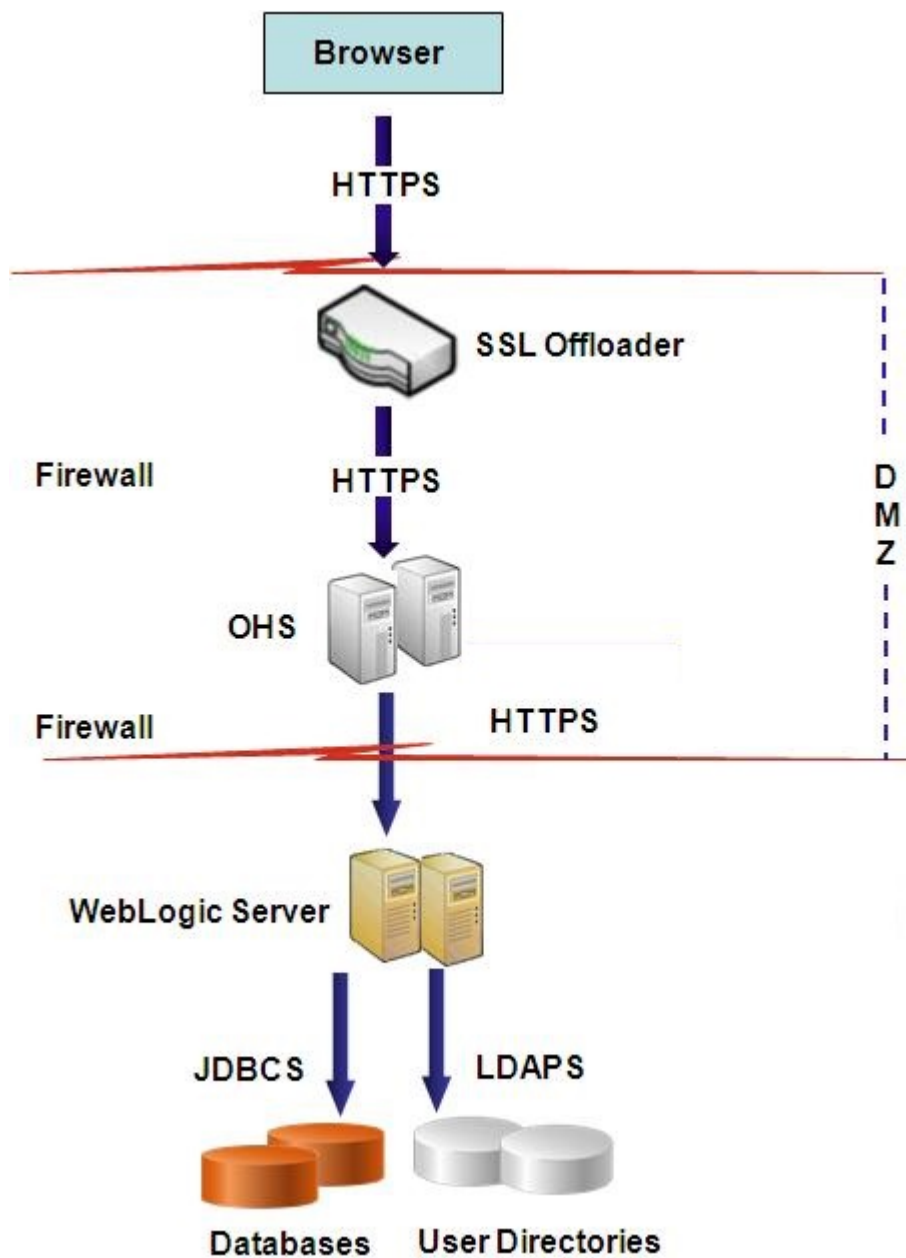
Voir aussi :

- [Architecture de déploiement](#)
- [Hypothèses](#)
- [Configuration d'EPM System pour le déploiement SSL complet](#)

Architecture de déploiement

En mode SSL complet, la communication entre tous les canaux pouvant être sécurisés est sécurisée à l'aide du protocole SSL. Ce scénario de déploiement Oracle Enterprise Performance Management System est le plus sécurisé.

Illustration du concept :



Hypothèses

Bases de données

SSL est activé pour les clients et les serveurs de base de données. Reportez-vous à la documentation portant sur votre base de données pour plus d'informations sur l'activation SSL du client et du serveur de base de données.

EPM System

Les composants Oracle Enterprise Performance Management System, y compris Oracle WebLogic Server et Oracle HTTP Server, sont installés et déployés. De plus,

voire environnement EPM System a été testé pour vérifier que tout fonctionne en mode non SSL. Reportez-vous aux sources d'informations suivantes :

- *Guide d'installation et de configuration d'Oracle Enterprise Performance Management System*
- *Avant l'installation d'Oracle Hyperion Enterprise Performance Management System*
- *Guide de résolution des problèmes d'installation et de configuration d'Oracle Enterprise Performance Management System*

Si vous prévoyez d'activer SSL pour les connexions de base de données, vous devez, au cours du processus de configuration, sélectionner le lien **Options avancées** pour chaque écran de configuration de base de données, puis spécifier les paramètres suivants, notamment :

- Sélectionnez **Utiliser une connexion sécurisée à la base de données (SSL)** et saisissez une URL de base de données sécurisée, par exemple,
`jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCPS)(HOST=myDBhost)(PORT=1529)(CONNECT_DATA=(SERVICE_NAME=myDBhost.myCompany.com)))`
- **Fichier de clés d'accès sécurisé**
- **Mot de passe du fichier de clés d'accès sécurisé**

Reportez-vous au *Guide d'installation et de configuration d'Oracle Enterprise Performance Management System* pour plus de détails.

Programme de déchargement SSL et équilibreur de charge

Un programme de déchargement SSL entièrement configuré avec un équilibreur de charge doit être présent dans l'environnement de déploiement.

La configuration SSL complète utilise deux alias de serveur, par exemple `epm.myCompany.com` et `empinternal.myCompany.com`, sur le programme de déchargement SSL. L'un est destiné à la communication externe entre le programme de déchargement et les navigateurs, et l'autre à la communication interne entre les serveurs EPM System. Assurez-vous que les alias de serveur pointent vers l'adresse IP de la machine et qu'ils peuvent être résolus via DNS.

L'équilibreur de charge doit être configuré pour transmettre toutes les demandes reçues par les hôtes virtuels vers les serveurs Oracle HTTP Server.

Les deux certificats signés, l'un pour prendre en charge la communication externe entre le programme de déchargement et les navigateurs (via `epm.myCompany.com`), et l'autre pour prendre en charge la communication interne (via `empinternal.myCompany.com`) entre plusieurs applications, doivent être installés sur l'équilibreur de charge/le programme de déchargement. Oracle recommande que ces certificats soient associés aux alias de serveur à des fins d'amélioration de la sécurité et afin que les noms de serveur ne soient pas visibles.

Configuration d'EPM System pour le déploiement SSL complet

Voir aussi :

- [Reconfiguration des paramètres communs EPM System](#)
- [Facultatif : installation d'un certificat CA racine pour WebLogic Server](#)
- [Installation d'un certificat sur WebLogic Server](#)
- [Configuration de WebLogic Server](#)

- Activation de la connexion au serveur HFM avec une base de données Oracle compatible SSL
- Procédures Oracle HTTP Server
- Configuration des composants Web EPM System déployés sur WebLogic Server
- Mise à jour de la configuration de domaine
- Redémarrage des serveurs et d'EPM System
- Test du déploiement
- Configuration de l'activation SSL pour les annuaires des utilisateurs externes

Reconfiguration des paramètres communs EPM System

Au cours de ce processus, vous sélectionnez les paramètres qui forcent les composants Oracle Enterprise Performance Management System à utiliser la communication SSL.

Remarque :

Si vous activez SSL pour le serveur Web Oracle Hyperion Financial Management : avant de configurer Financial Management, vous devez sécuriser le cookie en modifiant le descripteur de session de HFM WebApp dans `weblogic.xml`.

1. Développez l'archive Web Financial Management à l'aide d'un outil tel que 7-Zip. L'emplacement de `weblogic.xml` dans l'archive est `EPM_ORACLE_HOME\products\FinancialManagement\AppServer\InstallableApps\HFMMWebApplication.ear\HFMMWeb.war\WEB-INF\weblogic.xml`.
2. Incluez la directive suivante dans le descripteur de session de HFM WebApp dans `weblogic.xml` :

```
<cookie-secure>true</cookie-secure>
```
3. Enregistrez `weblogic.xml`.
4. Cliquez sur **Oui** lorsque 7 Zip demande si vous souhaitez mettre à jour l'archive.

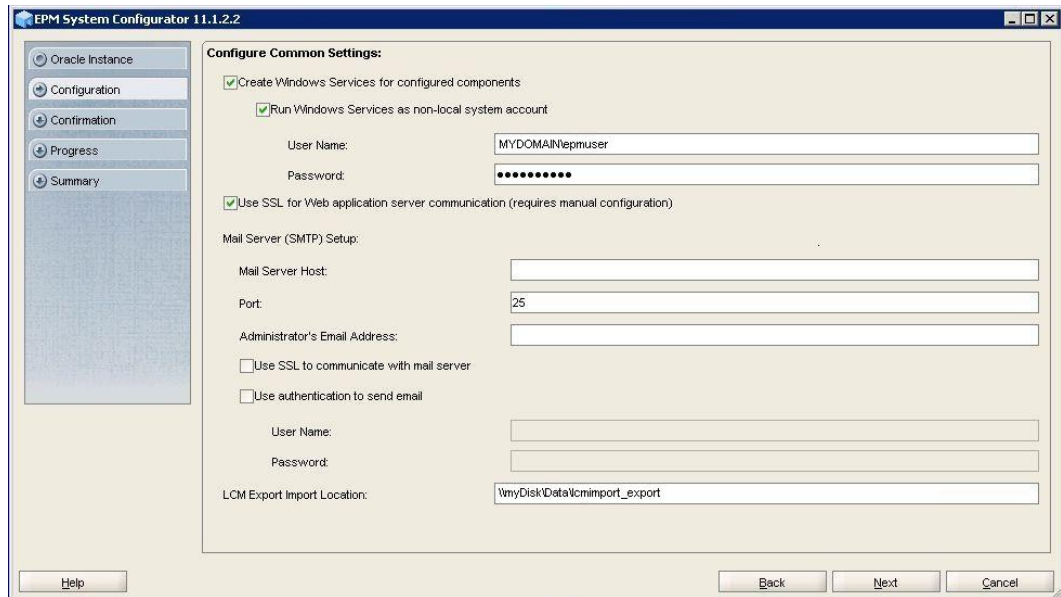
Pour reconfigurer EPM System pour SSL, procédez comme suit :

1. Lancez le Configurateur d'EPM System.
2. Dans **Sélectionner l'instance Oracle EPM à laquelle la configuration sera appliquée**, effectuez les étapes suivantes :
 - a. Dans **Nom de l'instance Oracle EPM**, entrez le nom d'instance que vous avez utilisé lors de la première configuration des composants EPM System.
 - b. Cliquez sur **Suivant**.
3. Dans l'écran Configuration, effectuez les étapes suivantes :
 - a. Effacez la sélection dans **Désélectionner tout**.
 - b. Développez la tâche de configuration **Hyperion Foundation**, puis sélectionnez **Configurer les paramètres communs**.

- c. Cliquez sur **Suivant**.
4. Dans **Configurer les paramètres communs**, effectuez les étapes suivantes :

Attention :

Assurez-vous que le serveur de messagerie est configuré pour SSL avant de sélectionner les paramètres permettant d'utiliser SSL pour communiquer avec lui.



- a. Sélectionnez **Utiliser le protocole SSL pour les communications du serveur d'applications Web Java (exige une configuration manuelle)** pour indiquer qu'EPM System doit utiliser SSL pour la communication.
- b. **Facultatif** : saisissez les informations adéquates dans **Hôte du serveur de messagerie** et **Port**. Vous devez spécifier le port sécurisé utilisé par le serveur de messagerie SMTP pour que la communication SSL soit prise en charge.
- c. **Facultatif** : sélectionnez **Utiliser SSL pour communiquer avec le serveur de messagerie** afin que la communication SSL soit prise en charge avec le serveur de messagerie SMTP.
- d. Sélectionnez ou entrez les paramètres nécessaires dans les champs restants.
- e. Cliquez sur **Suivant**.
5. Cliquez sur **Suivant** dans les écrans suivants du configurateur EPM System.
6. Lorsque le processus de déploiement est terminé, l'écran Récapitulatif s'affiche. Cliquez sur **Terminer**.

Facultatif : installation d'un certificat CA racine pour WebLogic Server

Les certificats racine de la plupart des organismes de certification tiers reconnus sont déjà installés dans le fichier de clés d'accès de la JVM. Effectuez les procédures de cette section si vous n'utilisez pas de certificats provenant d'un organisme de certification tiers reconnu (non recommandé). L'emplacement par défaut du fichier de clés d'accès de la JVM est `MIDDLEWARE_HOME/jdk/jre/lib/security/cacerts`.

Remarque :

Effectuez cette procédure sur chaque serveur Oracle Enterprise Performance Management System.

Pour installer le certificat CA racine, procédez comme suit :

1. Copiez le certificat CA racine dans un répertoire local de l'ordinateur sur lequel Oracle WebLogic Server est installé.
2. A partir d'une console, changez de répertoire pour passer à `MIDDLEWARE_HOME/jdk/jre/bin`.
3. Exécutez une commande `keytool` telle que la suivante afin d'installer le certificat CA racine dans le fichier de clés d'accès de la JVM :

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

Par exemple, vous pouvez utiliser la commande suivante pour ajouter un certificat `CAcert.crt` stocké dans le répertoire actuel au fichier de clés d'accès de la JVM avec l'alias de certificat `Blister` dans le fichier de clés d'accès. Le mot de passe `example_pwd` est supposé.

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

Remarque :

La commande et l'exemple précédents utilisent une partie de la syntaxe permettant d'importer des certificats à l'aide de `keytool`. Reportez-vous à la documentation relative à `keytool` pour obtenir la liste complète des syntaxes d'import.

Installation d'un certificat sur WebLogic Server

L'installation par défaut d'Oracle WebLogic Server utilise un certificat de démonstration pour prendre en charge SSL. Oracle recommande d'installer un certificat de tiers reconnu pour renforcer la sécurité de votre environnement.

Sur chaque ordinateur qui héberge WebLogic Server, utilisez un outil (par exemple, keytool) pour créer un fichier de clés d'accès personnalisé afin de stocker le certificat signé pour WebLogic Server et les composants Web Oracle Enterprise Performance Management System.

Pour créer un fichier de clés d'accès personnalisé et importer le certificat, procédez comme suit :

1. A partir d'une console, changez de répertoire pour passer à `MIDDLEWARE_HOME/jdk/jre/bin`.
2. Exécutez une commande keytool telle que la suivante pour créer le fichier de clés d'accès personnalisé (identifié par la directive `-keystore` dans la commande) dans un répertoire existant :

```
keytool -genkey -dname "cn=myserver, ou=EPM, o=myCompany, c=US" -alias
epm_ssl -keypass password -keystore
C:\oracle\Middleware\EPMSys11R1\ssl\keystore -storepass password -
validity 365 -keyalg RSA
```

Remarque :

Le nom commun (cn) que vous définissez doit correspondre au nom du serveur. Si vous utilisez un nom de domaine qualifié complet en tant que cn, vous devez l'utiliser lors du déploiement des composants Web.

3. Générez une demande de certificat.

```
keytool -certreq -alias epm_ssl -file C:/certs/epmssl_csr -keypass
password -storetype jks -keystore
C:\oracle\Middleware\EPMSys11R1\ssl\keystore -storepass password
```

4. Obtenez un certificat signé pour l'ordinateur WebLogic Server.
5. Importez le certificat signé dans le fichier de clés d'accès :

```
keytool -import -alias epm_ssl -file C:/certs/epmssl.crt -keypass
password -keystore C:\Oracle\Middleware\EPMSys11R1\ssl\keystore -
storepass password
```

Configuration de WebLogic Server

Après avoir déployé les composants Web Oracle Enterprise Performance Management System, vous devez les configurer pour la communication SSL.

Pour configurer les composants Web pour SSL, procédez comme suit :

1. Démarrez Oracle WebLogic Server en exécutant `MIDDLEWARE_HOME/user_projects/domains/EPMSys11R1/bin/startWebLogic.cmd` :
2. Lancez la console d'administration WebLogic Server en accédant à l'URL suivante :

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

Par exemple, pour accéder à la console WebLogic Server déployée sur le port par défaut sur `myServer`, vous devez utiliser `http://myServer:7001/console`.

3. Dans l'écran d'accueil, entrez le nom d'utilisateur de l'administrateur WebLogic Server et le mot de passe que vous avez spécifié dans le configurateur EPM System.
4. Dans **Centre des modifications**, cliquez sur **Verrouiller et modifier**.
5. Dans le volet de gauche de la console, développez **Environnement**, puis sélectionnez **Serveurs**.
6. Dans l'écran Récapitulatif des serveurs, cliquez sur le nom du serveur pour lequel vous souhaitez activer SSL.

Par exemple, pour activer SSL pour les composants Oracle Hyperion Foundation Services, vous travaillez avec le serveur `EPMServer0`.

7. Désélectionnez **Port d'écoute activé** pour désactiver le port d'écoute HTTP.
8. Assurez-vous que **Port d'écoute SSL activé** est sélectionné.
9. Dans **Port d'écoute SSL**, entrez le port d'écoute SSL sur lequel ce serveur doit écouter les demandes.
10. Pour spécifier l'identité et les fichiers de clés d'accès sécurisés à utiliser, sélectionnez **Fichiers de clés** pour ouvrir l'onglet Fichiers de clés.
11. Cliquez sur **Modifier**.
12. Sélectionnez une option :
 - **Identité personnalisée et sécurisation personnalisée** si vous n'utilisez pas un certificat de serveur provenant d'un organisme de certification tiers reconnu
 - **Identité personnalisée et sécurisation Java standard** si vous utilisez un certificat de serveur provenant d'un organisme de certification tiers reconnu
13. Cliquez sur **Enregistrer**.
14. Dans **Fichier de clés d'identité personnalisé**, entrez le chemin du fichier de clés d'accès où le certificat WebLogic Server signé est installé.
15. Dans **Type de fichier de clés d'identité personnalisé**, entrez `jks`.
16. Dans **Phrase de passe du fichier de clés d'identité personnalisé** et **Confirmer la phrase de passe du fichier de clés d'identité personnalisé**, entrez le mot de passe du fichier de clés d'accès.
17. Si vous avez sélectionné **Identité personnalisée et sécurisation personnalisée** dans **Fichiers de clés**, procédez comme suit :
 - Dans **Fichier de clés sécurisé personnalisé**, entrez le chemin du fichier de clés d'accès personnalisé dans lequel le certificat racine de l'organisme de certification ayant signé votre certificat de serveur est disponible.
 - Dans **Type de fichier de clés sécurisé personnalisé**, entrez `jks`.
 - Dans **Phrase de passe du fichier de clés sécurisé personnalisé** et **Confirmer la phrase de passe du fichier de clés sécurisé personnalisé**, entrez le mot de passe du fichier de clés d'accès.
18. Cliquez sur **Enregistrer**.
19. Spécifiez les paramètres SSL :
 - Sélectionnez **SSL**.

- Dans **Alias de clé privée**, entrez l'alias que vous avez spécifié lors de l'import du certificat WebLogic Server signé.
- Dans **Phrase de passe de la clé privée** et **Confirmer la phrase de passe de clé privée**, entrez le mot de passe à utiliser pour extraire la clé privée.
- Cliquez sur **Enregistrer**.

 **Remarque :**

Si vous utilisez des certificats SHA-2, vous devez sélectionner le paramètre **Utiliser l'implémentation SSL JSSE** pour tout serveur géré qui est utilisé pour prendre en charge EPM System. Le paramètre est disponible dans l'onglet Avancé de la page SSL. Vous devez redémarrer WebLogic Server pour activer cette modification.

20. Activez la réplication sécurisée pour le serveur :
 - a. Dans le volet de gauche de la console, développez **Environnement**, puis cliquez sur **Clusters**.
 - b. Dans Récapitulatif des clusters, cliquez sur le nom du serveur (par exemple, `Foundation Services`) pour lequel vous voulez activer la réplication sécurisée.
L'onglet Configuration de l'écran Paramètres correspondant au serveur sélectionné est affiché.
 - c. Cliquez sur **Réplication** pour ouvrir l'onglet Réplication.
 - d. Sélectionnez **Réplication sécurisée activée**. Il se peut que vous deviez cliquer sur **Verrouiller et modifier** pour pouvoir sélectionner cette option.
 - e. Cliquez sur **Enregistrer**.
21. Effectuez les étapes 6 à 20 pour chaque serveur géré appartenant à cet hôte.
22. Activez la réplication sécurisée pour fournir un canal aux appels de réplication pour le cluster.
Reportez-vous au document Oracle Metalink 1319381.1 pour obtenir plus de détails.
 - Dans la console d'administration, développez **Environnement**, puis sélectionnez **Clusters**.
 - Sélectionnez **Réplication**.
 - Dans **Réplication**, sélectionnez **Réplication sécurisée activée**.
 - Cliquez sur **Enregistrer**.
23. Dans **Centre des modifications**, cliquez sur **Activer les modifications**.

Activation de la connexion au serveur HFM avec une base de données Oracle compatible SSL

La connexion réseau entre la source de données HFM et la base de données Oracle peut être cryptée à l'aide de SSL. Pour que cela fonctionne, le portefeuille Oracle doit être configuré comme indiqué dans la [documentation Oracle](#). Le processus d'écoute TNS doit également être configuré de sorte à écouter sur un nouveau port pour les connexions cryptées SSL. Enfin, vous devez charger les certificats appropriés dans le fichier de clés

d'accès et le truststore sur les serveurs hébergeant la source de données HFM. Les instructions ci-dessous sont tirées de la [documentation Oracle Database](#).

Prérequis

Vérifiez que les prérequis suivants sont satisfaits avant de poursuivre avec les étapes ci-dessous :

- Un serveur de base de données opérationnel.
- Assurez-vous qu'aucun pare-feu local ou réseau ne bloque la communication avec le serveur sur le port sur lequel le processus d'écoute TNS compatible SSL est en cours d'exécution.

Dans les exemples ci-dessous, la version d'Oracle 12c (12.1.0.2) exécutée sur MS Windows Server 2016 a été utilisée. Ces instructions fonctionneront également sur une installation Linux, à condition que les chemins indiqués pour les fichiers de portefeuille soient des chemins de système de fichiers Linux et que les substitutions de variable d'environnement soient correctement modifiées pour l'interpréteur de commandes utilisé sur le serveur de base de données. Les mêmes instructions ont été utilisées sur des instances de développement et de prise en charge 19c.

Les exemples de cette section utilisent des certificats auto-signés mais vous pouvez également utiliser des certificats d'organisme de certification appropriés si vous préférez. Reportez-vous à la [documentation Oracle Database](#) pour connaître les étapes exactes à suivre lors de l'installation d'un certificat délivré par un organisme de certification.

Configuration de la base de données Oracle

Pour configurer la base de données Oracle, suivez les étapes ci-dessous :

1. Créez un portefeuille de connexion automatique sur le serveur de base de données.

Remarque :

Ces étapes sont requises uniquement si aucun portefeuille Oracle n'a été créé précédemment. Les étapes suivantes ne sont pas nécessaires si l'outil d'interface utilisateur graphique de portefeuille Oracle est utilisé sur le serveur de base de données.

```
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
```

Vous pouvez ignorer les messages vous invitant à utiliser `-auto_login_local` sur la ligne de commande `orapki`. Si vous rencontrez une erreur relative à un échec d'authentification SSL, reportez-vous à l'[ID de document 2238096.1](#) pour résoudre le problème.

Vérifiez également les autorisations de sécurité du fichier `cwallet.sso` (sous le répertoire du portefeuille) et assurez-vous que l'utilisateur du service de processus d'écoute Oracle possède une autorisation en lecture sur ce fichier. Sans

autorisation en lecture, la procédure d'établissement de liaison SSL échouera plus tard. Cette situation arrivera si la base de données Oracle a été installée avec l'utilisateur Oracle suggéré qui n'est pas autorisé à se connecter. Si la base de données Oracle a été installée avec l'utilisateur Oracle, le processus d'écoute TNS doit être exécuté sous un autre utilisateur.

2. Créez un certificat auto-signé et chargez-le dans le portefeuille.

```
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
```

Le mot de passe `password1` dans l'exemple ci-dessus doit correspondre au mot de passe indiqué à l'étape 1.

3. Exportez le certificat auto-signé que vous venez de créer.

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

4. Copiez le fichier de certificat Base64 exporté vers les serveurs HFM.

5. Configurez les processus d'écoute SQL*NET et TNS :

- a. Identifiez un port inutilisé sur le serveur de base de données. L'exemple ci-dessous crée le processus d'écoute sur le port 1522. Le port généralement utilisé pour les connexions SSL est 2484, mais vous pouvez utiliser n'importe quel port disponible. Vous devez vérifier que le port que vous voulez utiliser est disponible sur le serveur de base de données avant de poursuivre et l'ajuster si besoin.
- b. Mettez à jour `SQLNET.ORA`. L'élément `DIRECTORY` de la déclaration `WALLET_LOCATION` doit pointer vers le portefeuille créé lors de l'étape 1 ci-dessus.

```
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. Mettez à jour `LISTENER.ORA` pour définir un nouveau processus d'écoute. Utilisez le port identifié lors de l'étape 5a ci-dessus.

```
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. Créez une entrée dans TNSNAMES.ORA pour le nouveau port.

```

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

```

Vous devez indiquer le même port que celui identifié à l'étape 5a ci-dessus et utilisé à l'étape 5c.

e. Redémarrez le processus d'écoute TNS.

```

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

```

f. Vérifiez que le nouveau processus d'écoute TNS fonctionne.

```

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)
```

Configuration du serveur HFM de sorte à utiliser des connexions de base de données SSL

Ajout du certificat de base de données au truststore sur les serveurs HFM

Les étapes suivantes doivent être effectuées sur chaque serveur EPM sur lequel est exécutée la source de données HFM. La variable d'environnement `%MW_HOME%` utilisée ci-dessous est l'emplacement de l'installation Oracle Middleware. Cette variable d'environnement n'est pas créée par défaut lors de l'installation d'EPM et est utilisée ici pour montrer le répertoire parent de cette dernière.

L'emplacement de l'installation EPM est indiqué par la variable d'environnement `EMP_ORACLE_HOME`. L'exemple ci-dessous place le fichier de clés d'accès et le truststore dans un répertoire situé au même emplacement que l'installation EPM. Les fichiers de clés d'accès et de truststore peuvent se trouver n'importe où sur le système de fichiers du serveur HFM.

1. Créez un répertoire sous `%MW_HOME%` pour stocker le fichier de clés d'accès Java et le truststore PKCS12.
 - a. `cd %MW_HOME%`
 - b. `mkdir certs`
2. Copiez les certificats CA de fichier de clé d'accès Java à partir du JDK.
 - a. `cd %MW_HOME%\certs`
 - b. `copy %MW_HOME%\jdk1.8.0_181\jre\lib\security\cacerts testing_cacerts`
Il faut copier le fichier de clés d'accès du JDK et l'utiliser à la place du fichier de clés d'accès par défaut du JDK, car si le JDK est mis à niveau et que le précédent JDK est supprimé, les clés et les certificats insérés dans le fichier de clés d'accès par défaut seront perdus.
3. Copiez le certificat Base64 vers `%MW_HOME%\certs`.
4. Importez le certificat dans le fichier de clés d'accès Java `testing_cacerts`.
 - a. Par exemple, `keytool -importcert -file bur00cbb-certificate.crt -keystore testing_cacerts -alias "myserver"`.
 - i. Vous devrez indiquer le mot de passe du fichier de clés d'accès.
 - ii. Vous devez remplacer "myserver" par le nom de domaine qualifié complet du serveur de base de données.
 - b. Lorsque vous êtes invité à indiquer si le certificat doit être sécurisé, spécifiez `y`.
5. Créez le truststore au format PKCS12 à partir du fichier de clés d'accès Java du JDK. Par exemple :

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

Mise à jour des connexions JDBC HFM pour utiliser SSL

1. Reconfigurez la connexion JDBC de base de données HFM pour utiliser SSL.
 - a. Lancez l'outil de configuration EPM.

- i. Sélectionnez les noeuds **Configurer la base de données** et **Déployer vers le serveur d'applications** sous le noeud **Financial Management**.
 - ii. Cliquez sur **Suivant**.
 - iii. Effectuez chacune des étapes suivantes pour la connexion JDBC HFM :
 - i. Saisissez le port SSL, le nom du service, le nom d'utilisateur et le mot de passe pour la connexion dans les colonnes correspondantes.
 - ii. Cliquez sur (+) pour ouvrir les **options de base de données avancées**.
 - iii. Cochez la case **Utiliser des connexions sécurisées**.
 - iv. Saisissez l'emplacement du fichier de clés d'accès Java créé lors de l'étape 2.
 - v. Cliquez sur **Appliquer**.
 - vi. Cliquez sur (+) pour ouvrir les **options de base de données avancées**.
 - vii. Cliquez sur **Modifier l'URL JDBC et l'utiliser**. Aucune modification ne doit être apportée à l'URL JDBC affichée.
 - viii. Cliquez sur **Appliquer**.
 - ix. Cliquez sur **Suivant**.
 - b. Effectuez les étapes restantes pour déployer l'application HFM telles que décrites dans la documentation EPM.
 2. Ouvrez une fenêtre de commande ou un interpréteur de commandes pour mettre à jour manuellement le registre EPM de sorte que la connexion ODBC utilisée par la source de données puisse être compatible SSL.
Exécutez chaque commande répertoriée ci-dessous :

```
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
```

Dans les exemples ci-dessus, le chemin C:\Oracle\Middleware correspond à la valeur de %MW_HOME% dans les étapes 1, 2 et 3.

La propriété FINANCIAL_MANAGEMENT_PRODUCT/DATABASE_CONN/@ODBC_VALIDATESERVERCERTIFICATE ne doit être définie sur False que si un certificat auto-signé est utilisé. La valeur de FINANCIAL_MANAGEMENT_PRODUCT/DATABASE_CONN/@ODBC_TRUSTSTOREPASSWORD doit être le mot de passe du fichier de clés d'accès Java d'origine copié à l'étape 2.

Mise à jour de l'entrée de noms TNS utilisée par HFM

Modifiez `TNSNAMES.ORA` pour créer une entrée et renommez l'ancienne entrée. L'exemple suivant montre un fichier `TNSNAMES.ORA` mis à jour sur le serveur HFM auquel les modifications nécessaires ont été appliquées. Ces modifications ont été apportées car HFM recherche et utilise une entrée de noms TNS nommée `HFMTNS`. Le protocole et le port de cette entrée doivent être modifiés pour que `XFMDataSource` fonctionne correctement.

```
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)
)
)
```

L'entrée d'origine `HFMTNS` a été renommée en `HFMTNS_UNENC`. La nouvelle entrée `HFMTNS` a été réalisée en copiant l'entrée `HFMTNS_UNENC` et en la renommant `HFMTNS`. Le protocole a ensuite été mis à jour sur `TCPS` et le port a été remplacé par `1522`. Le port indiqué doit être le même que celui indiqué dans le fichier `TNS LISTENER.ORA`.

Procédures Oracle HTTP Server

Création d'un portefeuille et installation d'un certificat pour Oracle HTTP Server

Un portefeuille par défaut est automatiquement installé avec Oracle HTTP Server. Vous devez configurer un véritable portefeuille pour chaque serveur Oracle HTTP dans votre déploiement

Remarque : à compter de la version 11.2.x, Oracle Wallet Manager n'est pas installé avec Oracle HTTP Server. Oracle Wallet Manager est installé uniquement si vous installez le client Oracle Database. Vous devez utiliser le gestionnaire de portefeuille disponible avec le client Oracle Database pour créer le portefeuille et importer le certificat. Si vous configurez Oracle HTTP Server pour SSL, veillez à toujours installer le client Oracle Database 64 bits dans le cadre de l'installation de vos produits EPM System.

Pour créer et installer le certificat Oracle HTTP Server, procédez comme suit :

1. Sur chaque ordinateur hébergeant Oracle HTTP Server, lancez Wallet Manager.

Sélectionnez **Démarrer, Tous les programmes, Oracle-OHxxxxxx**, puis **Outils de gestion intégrés et Wallet Manager**.

xxxxxx est le numéro d'instance Oracle HTTP Server.

2. Créez un portefeuille vide.
 - a. Dans Oracle Wallet Manager, sélectionnez **Portefeuille**, puis **Nouveau**.
 - b. Cliquez sur **Oui** pour créer un répertoire de portefeuille par défaut ou sur **Non** pour créer le fichier de portefeuille à l'emplacement de votre choix.
 - c. Dans l'écran Nouveau portefeuille, dans **Mot de passe de portefeuille et Confirmer le mot de passe**, entrez le mot de passe que vous voulez utiliser.
 - d. Cliquez sur **OK**.
 - e. Dans la boîte de dialogue de confirmation, cliquez sur **Non**.
3. **Facultatif** : si vous n'utilisez pas un organisme de certification connu d'Oracle HTTP Server, importez le certificat CA racine dans le portefeuille.
 - a. Dans Oracle Wallet Manager, cliquez avec le bouton droit de la souris sur **Certificats sécurisés** et sélectionnez **Importer un certificat sécurisé**.
 - b. Recherchez et sélectionnez le certificat CA racine.
 - c. Sélectionnez **Ouvrir**.
4. Créez une demande de certificat.
 - a. Dans Oracle Wallet Manager, cliquez avec le bouton droit de la souris sur **Certificat : [vide]** et sélectionnez **Ajouter une demande de certificat**.
 - b. Dans Créer une demande de certificat, entrez les informations requises.
Pour le nom commun, entrez l'alias de serveur qualifié complet, par exemple, `epm.myCompany.com` ou `epminternal.myCompany.com`, disponibles dans le fichier `hosts` de votre système.
 - c. Cliquez sur **OK**.
 - d. Dans la boîte de dialogue de confirmation, cliquez sur **OK**.
 - e. Cliquez avec le bouton droit de la souris sur la demande de certificat que vous avez créée, puis sélectionnez **Exporter une demande de certificat**.
 - f. Spécifiez un nom pour le fichier de demande de certificat.
5. A l'aide des fichiers de demande de certificat, obtenez les certificats signés auprès de l'organisme de certification.
6. Importez les certificats signés.
 - a. Dans Oracle Wallet Manager, cliquez avec le bouton droit de la souris sur la demande de certificat utilisée pour obtenir le certificat signé, puis sélectionnez **Importer un certificat utilisateur**.
 - b. Dans Importer un certificat, cliquez sur **OK** pour importer le certificat à partir d'un fichier.
 - c. Dans Importer un certificat, sélectionnez le fichier de certificat, puis cliquez sur **Ouvrir**.
7. Enregistrez le portefeuille à un emplacement qui vous convient, par exemple, `EPM_ORACLE_INSTANCE/httpConfig/ohs/config/OHS/ohs_component/keystores/epmsystem`.

8. Sélectionnez **Portefeuille**, puis **Connexion automatique** pour activer la connexion automatique.

Configuration d'un portefeuille Oracle à l'aide d'ORAPKI (sous Linux)

Pour configurer un portefeuille Oracle à l'aide de la ligne de commande ORAPKI, procédez comme suit :

1. Créez un dossier pour votre portefeuille :

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

2. Ajoutez l'emplacement de l'utilitaire orapki à votre chemin :

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

3. Créez un portefeuille pour stocker votre certificat :

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

Cette commande vous invite à entrer à deux reprises un mot de passe de portefeuille si aucun mot de passe n'a été spécifié sur la ligne de commande. Elle crée un portefeuille à l'emplacement indiqué pour `-wallet`.

4. Générez une demande de signature de certificat et ajoutez-la à votre portefeuille :

```
$ 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. Ajoutez les certificats racine et intermédiaire au fichier de clés d'accès sécurisé :

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

6. Utilisez votre organisme de certification pour signer la demande de signature de certificat. Pour exporter la demande de certificat à partir d'un portefeuille Oracle, utilisez la commande suivante :

```
$ 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. Importez la demande de signature de certificat signée dans le portefeuille :

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

8. Pour afficher le contenu du portefeuille, utilisez la commande suivante :

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

Activation SSL d'Oracle HTTP Server

Après avoir reconfiguré le serveur Web sur chaque ordinateur hébergeant Oracle HTTP Server, mettez à jour le fichier de configuration d'Oracle HTTP Server en remplaçant l'emplacement du portefeuille par défaut par l'emplacement du portefeuille que vous avez créé.

Pour configurer Oracle HTTP Server pour SSL, procédez comme suit :

1. Reconfigurez le serveur Web sur chaque ordinateur hôte Oracle HTTP Server dans votre déploiement.
2. Démarrez le configurateur EPM System pour l'instance.
3. Dans l'écran de sélection des tâches de configuration, effectuez les tâches suivantes, puis cliquez sur **Suivant**.
 - a. Effacez la sélection dans **Désélectionner tout**.
 - b. Développez le groupe de tâches **Hyperion Foundation**, puis sélectionnez **Configurer le serveur Web**.
4. Dans **Configurer le serveur Web**, cliquez sur **Suivant**.
5. Dans **Confirmation**, cliquez sur **Suivant**.
6. Dans **Récapitulatif**, cliquez sur **Terminer**.
7. A l'aide d'un éditeur de texte, ouvrez *EPM_ORACLE_INSTANCE/httpConfig/ohs/config/fmwconfig/components/OHS/ohs_component/ssl.conf*.
8. Assurez-vous que le port SSL que vous utilisez est répertorié sous `OHS Listen port` de la manière suivante :

Si vous utilisez 19443 en tant que port de communication SSL, vous devez obtenir les entrées suivantes :


```
Listen 19443
```
9. Définissez la valeur de paramètre `SSLSessionCache` sur `none`.
10. Mettez à jour les paramètres de configuration de chaque serveur Oracle HTTP Server dans votre déploiement.
 - a. A l'aide d'un éditeur de texte, ouvrez *EPM_ORACLE_INSTANCE/httpConfig//ohs/config/fmwconfig/components/OHS/ohs_component/ssl.conf*.
 - b. Recherchez la directive `SSLWallet` et modifiez sa valeur de sorte qu'elle pointe vers le portefeuille dans lequel vous avez installé le certificat. Si vous avez créé le portefeuille dans *EPM_ORACLE_INSTANCEhttpConfig/ohs/*

config/OHS/ohs_component/keystores/epmsystem, il se peut que votre directive SSLWallet soit la suivante :

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

- c. Enregistrez et fermez ssl.conf.
- 11. Mettez à jour mod_wl_ohs.conf sur chaque serveur Oracle HTTP Server dans votre déploiement.
 - a. A l'aide d'un éditeur de texte, ouvrez *EPM_ORACLE_INSTANCE*/httpConfig/ohs/config/fmwconfig/components/OHS/ohs_component/mod_wl_ohs.conf.
 - b. Assurez-vous que la directive WLSSLWallet pointe vers le portefeuille Oracle dans lequel le certificat SSL est stocké.

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

Par exemple, C:/Oracle/Middleware/ohs/bin/wallets/myWallet

- c. Définissez la valeur de SecureProxy sur ON.
- ```
SecureProxy ON
```
- d. Assurez-vous que les définitions LocationMatch pour les composants Oracle Enterprise Performance Management System déployés sont semblables à l'exemple Oracle Hyperion Shared Services suivant, qui suppose l'existence d'un cluster Oracle WebLogic Server (sur myserver1 et myserver2 à l'aide du port SSL 28443) :

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

- e. Enregistrez et fermez mod\_wl\_ohs.conf.

## Configuration des composants Web EPM System déployés sur WebLogic Server

Après avoir déployé les composants Web Oracle Enterprise Performance Management System, vous devez les configurer pour la communication SSL.

Pour configurer les composants Web pour SSL, procédez comme suit :

1. Démarrez Oracle WebLogic Server en exécutant un fichier stocké dans *EPM\_ORACLE\_INSTANCE*/domains/EPMSysystem/bin/startWebLogic.cmd :
2. Lancez la console d'administration WebLogic Server en accédant à l'URL suivante :

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

Par exemple, pour accéder à la console WebLogic Server déployée sur le port par défaut sur myServer, vous devez utiliser http://myServer:7001/console.

3. Dans l'écran d'accueil, entrez le nom d'utilisateur et le mot de passe pour accéder à EPMSystem. Vous spécifiez le nom d'utilisateur et le mot de passe dans le configurateur EPM System au cours du processus de configuration.
4. Dans **Centre des modifications**, cliquez sur **Verrouiller et modifier**.
5. Dans le volet de gauche de la console, développez **Environnement**, puis sélectionnez **Serveurs**.
6. Dans l'écran Récapitulatif des serveurs, cliquez sur le nom du serveur pour lequel vous souhaitez activer SSL.

Par exemple, si vous avez installé tous les composants Oracle Hyperion Foundation Services, vous pouvez activer SSL pour les serveurs suivants :

- CalcManager
- FoundationServices

7. Désélectionnez **Port d'écoute activé** pour désactiver le port d'écoute HTTP.
8. Assurez-vous que **Port d'écoute SSL activé** est sélectionné.
9. Dans **Port d'écoute SSL**, entrez le port d'écoute SSL WebLogic Server.
10. Spécifiez l'identité et les fichiers de clés d'accès sécurisés à utiliser.
  - Sélectionnez **Fichiers de clés** pour ouvrir l'onglet Fichiers de clés.
  - Dans **Fichiers de clés**, sélectionnez une option :
    - a. Sélectionnez **Fichiers de clés** pour ouvrir l'onglet Fichiers de clés.
    - b. Dans **Fichiers de clés**, sélectionnez une option :
      - **Identité personnalisée et sécurisation personnalisée** si vous n'utilisez pas un certificat de serveur provenant d'un organisme de certification tiers reconnu
      - **Identité personnalisée et sécurisation Java standard** si vous utilisez un certificat de serveur provenant d'un organisme de certification tiers reconnu
    - c. Dans **Fichier de clés d'identité personnalisé**, entrez le chemin du fichier de clés d'accès où le certificat WebLogic Server signé est installé.
    - d. Dans **Type de fichier de clés d'identité personnalisé**, entrez `jks`.
    - e. Dans **Phrase de passe du fichier de clés d'identité personnalisé** et **Confirmer la phrase de passe du fichier de clés d'identité personnalisé**, entrez le mot de passe du fichier de clés d'accès.
    - f. Si vous avez sélectionné **Identité personnalisée et sécurisation personnalisée** dans **Fichiers de clés**, procédez comme suit :
      - Dans **Fichier de clés sécurisé personnalisé**, entrez le chemin du fichier de clés d'accès personnalisé dans lequel le certificat racine de l'organisme de certification ayant signé votre certificat de serveur est disponible.
      - Dans **Type de fichier de clés sécurisé personnalisé**, entrez `jks`.
      - Dans **Phrase de passe du fichier de clés sécurisé personnalisé** et **Confirmer la phrase de passe du fichier de clés sécurisé personnalisé**, entrez le mot de passe du fichier de clés d'accès.
    - g. Cliquez sur **Enregistrer**.

11. Spécifiez les paramètres SSL.
  - Sélectionnez **SSL**.
  - Dans **Alias de clé privée**, entrez l'alias que vous avez spécifié lors de l'import du certificat WebLogic Server signé.
  - Dans **Phrase de passe de la clé privée** et **Confirmer la phrase de passe de clé privée**, entrez le mot de passe à utiliser pour extraire la clé privée.
  - **Application Web Oracle Hyperion Provider Services uniquement** : si vous utilisez des certificats génériques pour crypter la communication entre WebLogic Server et les autres composants de serveur EPM System, désactivez la vérification de nom d'hôte pour l'application Web Provider Services.
    - Sélectionnez **Avancé**.
    - Dans **Vérification du nom d'hôte**, sélectionnez **Aucun**.
  - Cliquez sur **Enregistrer**.
12. Dans **Centre des modifications**, cliquez sur **Activer les modifications**.

## Mise à jour de la configuration de domaine

Ce processus met à jour la configuration de domaine. Avant de démarrer cette procédure, créez une sauvegarde complète de votre déploiement. Oracle vous recommande de tester cette procédure sur un déploiement de test avant d'apporter toute modification à un déploiement de production.

Pour mettre à jour la configuration de domaine, procédez comme suit :

1. Accédez au répertoire `MIDDLEWARE_HOME/oracle_common/bin` :  

```
cd MIDDLEWARE_HOME/oracle_common/bin
```
2. Définissez `ORACLE_HOME`, `WL_HOME` et `JAVA_HOME`.  

```
set ORACLE_HOME= /Oracle/Middleware
set WL_HOME= /Oracle/Middleware/wlserver
set JAVA_HOME= /Oracle/Middleware/jdk
```
3. Dans la console WebLogic, activez le port HTTP pour le serveur d'administration.
4. Créez un fichier de clés d'accès à l'aide d'une commande telle que celle-ci :  

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

Dans cette commande, remplacez `HOSTNAME` par le nom d'hôte du serveur WebLogic et `USERNAME` par le nom d'utilisateur de l'administrateur. Vérifiez que la sortie indique que le fichier de clés d'accès OVD a bien été créé.

5. Exportez le certificat SSL à partir du serveur d'administration.

### Note:

Cette étape concerne uniquement le serveur LDAP imbriqué (authentificateur par défaut). Pour les autres serveurs LDAP, le certificat doit être exporté à l'aide des commandes propres à LDAP appropriées. Le format du fichier de certificat doit être le suivant : **X.509 codé en base 64**

- a. Dans Internet Explorer, accédez à la console d'administration WebLogic en vous connectant à l'adresse `https://HOSTNAME:7002/console`
  - b. Cliquez sur **Afficher le certificat**, puis sur **Détails**, et sélectionnez **Copier vers un fichier** pour exporter le certificat SSL.
  - c. Enregistrez le certificat au format **X.509 codé en base 64** dans un répertoire local, par exemple, `C:\certificate\slc17rby.cer`.
  - d. Déplacez le certificat vers le serveur.
6. A l'aide de la commande `keytool`, importez le certificat dans le fichier de clés d'accès créé à l'étape 4. Utilisez une commande semblable à celle ci-dessous, qui part du principe que `JAVA_HOME` (de même que l'exécutable `keytool`) se trouve dans le chemin :

```
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, par
exemple :
```

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

 **Note:**

- Le mot de passe employé dans cette commande doit correspondre à celui utilisé lors de la génération du fichier de clés d'accès à l'étape 4.
- `CERTIFICATE_PATH` correspond à l'emplacement et au nom du certificat.
- L'alias est un alias de votre choix.

Une fois le certificat importé, la commande `keytool` affiche le message suivant :  
Certificat ajouté au fichier de clés.

7. Dans la console WebLogic, activez le port SSL pour le serveur d'administration en plus du port HTTP.
8. Redémarrez le serveur d'administration WebLogic et les serveurs gérés.
9. Connectez-vous à Oracle Hyperion Enterprise Performance Management Workspace via une connexion sécurisée afin de vérifier que tout fonctionne correctement.

## Redémarrage des serveurs et d'EPM System

Redémarrez tous les serveurs dans le déploiement, puis démarrez Oracle Enterprise Performance Management System sur chaque serveur.

## Test du déploiement

Après avoir terminé le déploiement SSL, vérifiez que tout fonctionne.

Pour tester votre déploiement, procédez comme suit :

1. A l'aide d'un navigateur, accédez à l'URL sécurisée Oracle Hyperion Enterprise Performance Management Workspace :

Si vous avez utilisé `epm.myCompany.com` comme alias de serveur pour la communication externe et 4443 comme port SSL, l'URL EPM Workspace est la suivante :

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

2. Dans l'écran de connexion, entrez un nom d'utilisateur et un mot de passe.
3. Cliquez sur **Connexion**.
4. Vérifiez que vous pouvez accéder de manière sécurisée aux composants Oracle Enterprise Performance Management System déployés.

## Configuration des annuaires des utilisateurs externes compatibles SSL

### Hypothèses

- Les annuaires des utilisateurs externes que vous prévoyez de configurer dans Oracle Hyperion Shared Services Console sont compatibles SSL.
- Si vous n'avez pas utilisé un certificat provenant d'un organisme de certification tiers reconnu pour l'activation SSL de l'annuaire des utilisateurs, vous disposez d'une copie du certificat racine de l'organisme de certification ayant signé le certificat de serveur.

### Import du certificat CA racine

Si vous n'avez pas utilisé un certificat provenant d'un organisme de certification tiers reconnu pour l'activation SSL de l'annuaire des utilisateurs, vous devez importer le certificat racine de l'organisme de certification ayant signé le certificat de serveur dans les fichiers de clés d'accès suivants :

#### Remarque :

Pendant le déploiement de l'application, WebLogic ajoute la directive -  
`Djavax.net.ssl.trustStore` pointant vers `DemoTrust.jks` dans `setDomainEnv.sh`  
ou `setDomainEnv.cmd`. Enlevez `-Djavax.net.ssl.trustStore` de `setDomainEnv.sh`  
ou de `setDomainEnv.cmd` si vous n'utilisez pas le certificat WebLogic par défaut.

Utilisez un outil tel que keytool pour importer le certificat CA racine.

- Tous les serveurs Oracle Enterprise Performance Management System :  
**Fichier de clés d'accès de la JVM :** `MIDDLEWARE_HOME/jdk/jre/lib/security/cacerts`
- Le fichier de clés d'accès utilisé par la JVM sur chaque ordinateur hôte de composant EPM System. Par défaut, les composants EPM System utilisent le fichier de clés d'accès suivant :

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

### Configuration des annuaires des utilisateurs externes

Vous configurez les annuaires des utilisateurs à l'aide de Shared Services Console. Lors de la configuration des annuaires des utilisateurs, vous devez sélectionner l'option `Protocole SSL activé` qui indique à la sécurité EPM System d'utiliser le protocole sécurisé pour communiquer avec l'annuaire des utilisateurs. Vous pouvez activer SSL pour une connexion entre la sécurité EPM System et les annuaires des utilisateurs compatibles LDAP, par exemple, Oracle Internet Directory et Microsoft Active Directory.

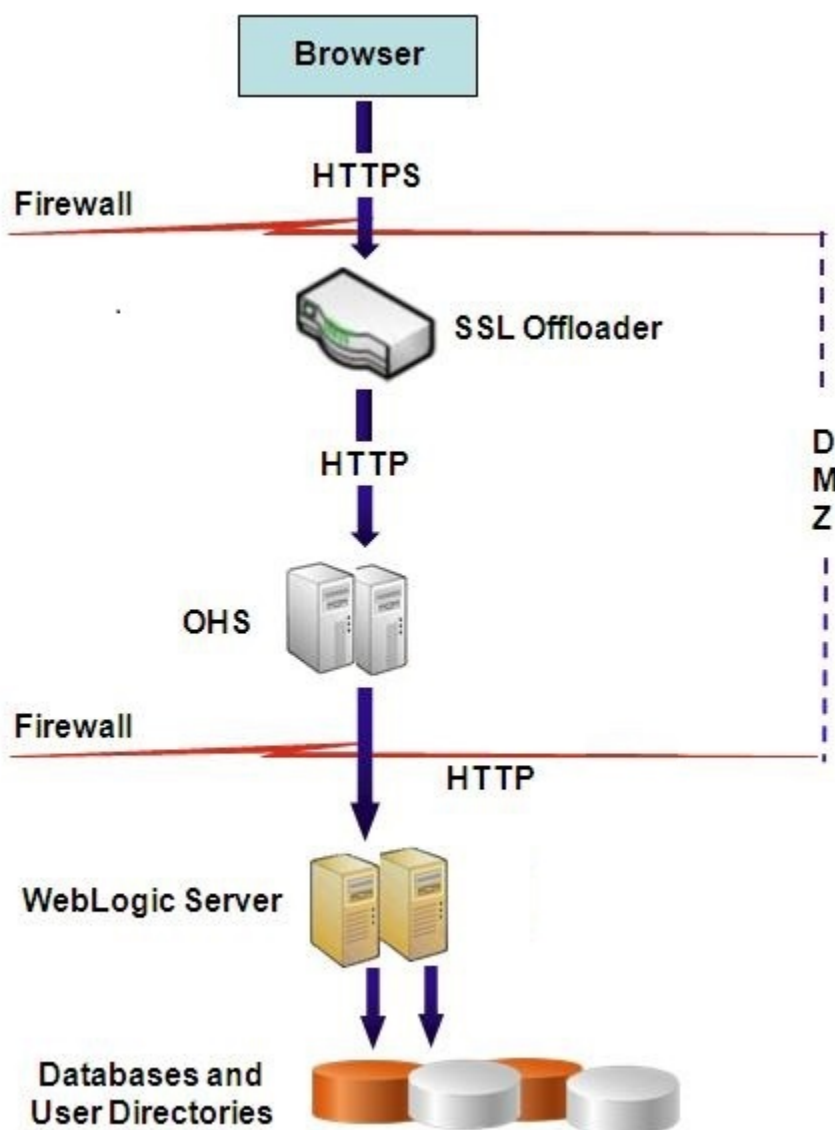
Reportez-vous à la section "Configuration des annuaires des utilisateurs" du *Guide d'administration de la sécurité utilisateur d'Oracle Enterprise Performance Management System*.

## Arrêt de SSL sur le serveur Web

### Architecture de déploiement

Dans ce scénario, SSL est utilisé pour sécuriser le lien de communication entre les clients Oracle Enterprise Performance Management System (par exemple, un navigateur) et Oracle HTTP Server. Illustration du concept :





### Hypothèses

Cette configuration utilise deux alias de serveur, par exemple `epm.myCompany.com` et `empinternal.myCompany.com`, sur le serveur Web, l'un pour la communication externe entre le serveur Web et les navigateurs, et l'autre pour la communication interne entre les serveurs EPM System. Assurez-vous que les alias de serveur pointent vers l'adresse IP de la machine et qu'ils peuvent être résolus via DNS.

Un certificat signé permettant de prendre en charge la communication externe avec les navigateurs (par exemple, via `epm.myCompany.com`) doit être installé sur le serveur Web (là où est défini l'hôte virtuel prenant en charge la communication externe sécurisée). L'hôte virtuel doit arrêter SSL et transmettre les demandes HTTP à Oracle HTTP Server.

Lorsque SSL est en cours d'arrêt au niveau d'Oracle HTTP Server (OHS) ou de l'équilibreur de charge, vous devez procéder comme suit :

- Définissez chaque application Web logique sur l'hôte virtuel non SSL de l'équilibreur de charge ou d'Oracle HTTP Server (par exemple, `empinternal.myCompany.com:80`, où 80 est le port non SSL). Ouvrez l'écran Configuration, puis effectuez les étapes suivantes :

1. Développez la tâche de configuration **Hyperion Foundation**.
  2. Sélectionnez **Configurer une adresse logique pour les applications Web**.
  3. Indiquez le *nom d'hôte*, le numéro de port non SSL et le numéro de port SSL.
- Définissez l'URL externe sur l'hôte virtuel compatible SSL de l'équilibreur de charge ou d'Oracle HTTP Server (par exemple, `empexternal.myCompany.com:443`, où 443 est le port SSL). Ouvrez l'écran Configuration, puis effectuez les étapes suivantes :
    1. Développez la tâche de configuration **Hyperion Foundation**.
    2. Sélectionnez **Configurer les paramètres communs**.
    3. Sélectionnez **Activer le téléchargement SSL** sous Détails d'URL externe.
    4. Indiquez l'*hôte d'URL externe* et le *port d'URL externe*.

 **Remarque :**

Le redéploiement des applications Web ou la reconfiguration du serveur Web à l'aide de **configtool** entraîne le remplacement des paramètres des URL externe et d'application Web logique.

### Configuration d'EPM System

Le déploiement par défaut des composants EPM System prend en charge l'arrêt de SSL sur le serveur Web. Aucune action supplémentaire n'est nécessaire.

Lors de la configuration d'EPM System, assurez-vous que les applications Web logiques pointent vers l'hôte virtuel (par exemple, `empinternal.myCompany.com`) ayant été créé pour la communication interne. Reportez-vous aux sources d'information suivantes pour installer et configurer EPM System :

- *Guide d'installation et de configuration d'Oracle Enterprise Performance Management System*
- *Avant l'installation d'Oracle Hyperion Enterprise Performance Management System*

### Test du déploiement

Après avoir terminé le processus de déploiement, vérifiez que tout fonctionne en vous connectant à l'URL sécurisée Oracle Hyperion Enterprise Performance Management Workspace :

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

Par exemple, `https://epm.myCompany.com:443/workspace/index.jsp`, où 443 est le port SSL.

## SSL pour Essbase 11.1.2.4

### Présentation

Cette section explique les procédures de remplacement des certificats par défaut qui sont utilisés pour sécuriser la communication entre une instance Oracle Essbase et des composants tels que MaxL, le serveur Oracle Essbase Administration Services, le serveur Oracle Essbase Studio, Oracle Hyperion Provider Services, Oracle Hyperion Foundation Services, Oracle Hyperion Planning, Oracle Hyperion Financial Management et Oracle Hyperion Shared Services Registry.

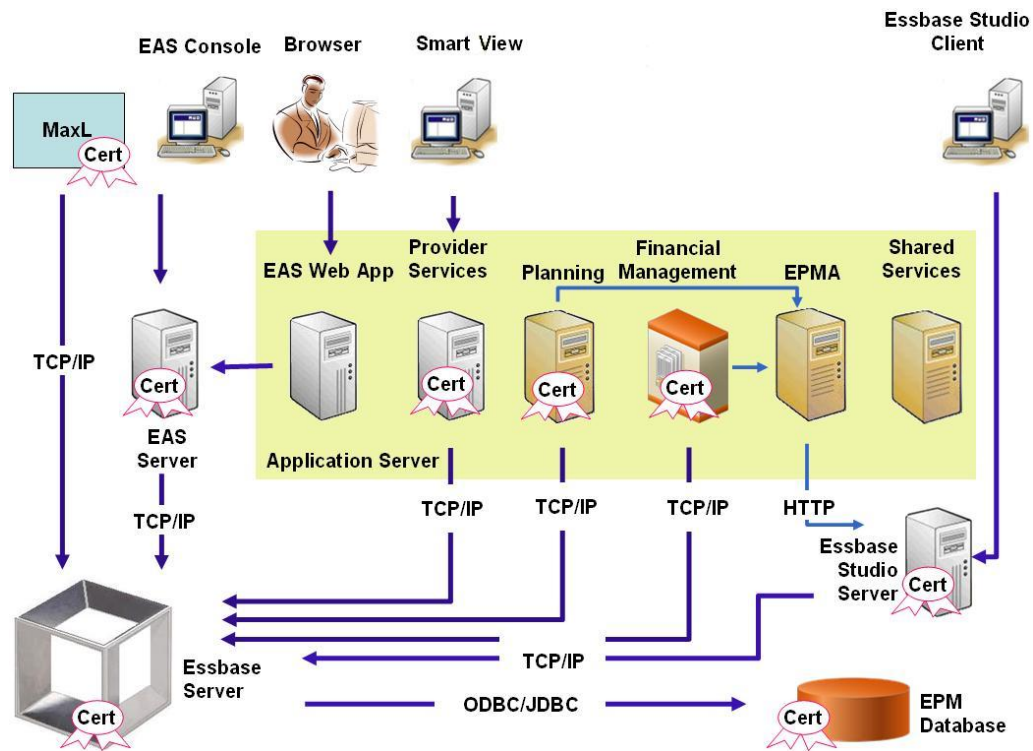
### Déploiement par défaut

Essbase peut être déployé pour fonctionner en mode SSL et non SSL. L'agent Essbase écoute sur un port non sécurisé, mais il peut aussi être configuré pour écouter sur un port sécurisé. Toutes les connexions accédant au port sécurisé sont traitées comme des connexions SSL. Si un client se connecte à l'agent Essbase sur le port non SSL, la connexion est traitée comme une connexion non SSL. Les composants peuvent établir des connexions simultanées non SSL et SSL à un agent Essbase.

Vous pouvez contrôler le mode SSL par session en spécifiant le protocole sécurisé et le port lorsque vous vous connectez. Reportez-vous à [Etablissement d'une connexion SSL par session](#).

Si SSL est activé, toutes les communications au sein d'une instance Essbase sont cryptées pour assurer la sécurité des données.

Les déploiements par défaut de composants Essbase en mode sécurisé font appel à des certificats auto-signés pour activer la communication SSL, principalement à des fins de test. Oracle recommande d'utiliser les certificats émis par des organismes de certification tiers reconnus pour activer SSL pour Essbase dans des environnements de production.



En règle générale, un portefeuille Oracle stocke le certificat qui active la communication SSL avec les clients utilisant le client en temps réel Essbase et un fichier de clés d'accès Java stocke le certificat qui active la communication SSL avec les composants utilisant JAPI pour la communication. Pour établir la communication SSL, les outils et les clients Essbase stockent le certificat racine de l'organisme de certification ayant signé les certificats de l'agent et du serveur Essbase. Reportez-vous à la section [Certificats requis et leur emplacement](#).

### Certificats requis et leur emplacement

Oracle recommande d'utiliser les certificats émis par des organismes de certification tiers reconnus pour activer SSL pour Essbase dans un environnement de production. Vous pouvez utiliser les certificats auto-signés par défaut à des fins de test.

#### Remarque :

Essbase prend en charge l'utilisation de certificats génériques, ce qui permet de sécuriser plusieurs sous-domaines avec un seul certificat SSL. Les certificats génériques permettent de réduire les coûts et le temps de gestion.

Les certificats génériques ne peuvent pas être utilisés si la vérification de nom d'hôte est activée.

Vous avez besoin des certificats suivants :

- Un certificat CA racine  
Les composants qui utilisent le client en temps réel Essbase pour établir une connexion à Essbase nécessitent que le certificat CA racine soit stocké dans un portefeuille Oracle. Les composants qui utilisent JAPI pour établir une connexion

nécessitent que le certificat CA racine soit stocké dans un fichier de clés d'accès Java. Les certificats requis et leur emplacement sont indiqués dans le tableau suivant.

 **Remarque :**

Il se peut que vous n'ayez pas besoin d'installer un certificat CA racine si vos certificats proviennent d'un organisme de certification tiers reconnu dont le certificat racine est déjà installé dans le portefeuille Oracle.

- Un certificat signé pour le serveur Essbase et l'agent Essbase

**Tableau 2-1 Certificats requis et leur emplacement**

| Composant <sup>1</sup>                                          | Fichier de clés d'accès                                                                                         | Certificat <sup>2</sup>                                                                                                                 |
|-----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| MaxL                                                            | Portefeuille Oracle                                                                                             | Certificat CA racine                                                                                                                    |
| Serveur Administration Services                                 | Portefeuille Oracle                                                                                             | Certificat CA racine                                                                                                                    |
| Provider Services                                               | Portefeuille Oracle                                                                                             | Certificat CA racine                                                                                                                    |
| Base de données Oracle Enterprise Performance Management System | Portefeuille Oracle                                                                                             | Certificat CA racine                                                                                                                    |
| Serveur Essbase Studio                                          | Fichier de clés d'accès Java                                                                                    | Certificat CA racine                                                                                                                    |
| Planning                                                        | <ul style="list-style-type: none"> <li>• Portefeuille Oracle</li> <li>• Fichier de clés d'accès Java</li> </ul> | Certificat CA racine                                                                                                                    |
| Financial Management                                            | Fichier de clés d'accès Java                                                                                    | Certificat CA racine                                                                                                                    |
| Essbase (serveur et agent) <sup>3</sup>                         | <ul style="list-style-type: none"> <li>• Portefeuille Oracle</li> <li>• Fichier de clés d'accès Java</li> </ul> | <ul style="list-style-type: none"> <li>• Certificat CA racine</li> <li>• Certificat signé pour le serveur et l'agent Essbase</li> </ul> |
| Référentiel Oracle Hyperion Shared Services                     |                                                                                                                 |                                                                                                                                         |

<sup>1</sup> Vous n'avez besoin que d'une seule instance du fichier de clés d'accès pour prendre en charge plusieurs composants utilisant un fichier de clés d'accès similaire.

<sup>2</sup> Plusieurs composants peuvent utiliser un certificat racine installé dans un fichier de clés d'accès.

<sup>3</sup> Les certificats doivent être installés dans le portefeuille Oracle par défaut et dans le fichier de clés d'accès Java.

## Installation et déploiement des composants Essbase

Le processus de configuration vous permet de sélectionner un port d'agent sécurisé (par défaut, il s'agit du port 6423) que vous pouvez modifier lors de la configuration d'Oracle Essbase. Par défaut, le processus de déploiement installe les certificats auto-signés requis pour créer un déploiement sécurisé fonctionnel à des fins de test.

Le programme d'installation d'EPM System installe un portefeuille Oracle et un certificat auto-signé dans `ARBOR_PATH` sur l'ordinateur qui héberge l'instance Essbase si Oracle HTTP Server est installé. Dans les déploiements d'hôte unique, tous les composants Essbase partagent ce certificat.

## Utilisation de certificats CA tiers sécurisés pour Essbase

### Création de demandes de certificats et obtention de certificats

Générez une demande de certificat afin d'obtenir un certificat pour le serveur qui héberge le serveur Oracle Essbase et l'agent Essbase. Une demande de certificat contient des informations cryptées propres à votre nom distinctif (DN). Vous pouvez soumettre une demande de certificat à une autorité signataire pour obtenir un certificat SSL.

Pour créer une demande de certificat, utilisez un outil tel que keytool ou Oracle Wallet Manager. Pour plus d'informations sur la création d'une demande de certificat, reportez-vous à la documentation de l'outil en question.

Pour créer une demande de certificat avec keytool, utilisez une commande semblable à la suivante :

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

### Obtention et installation d'un certificat CA racine

Le certificat CA racine vérifie la validité du certificat utilisé pour prendre en charge SSL. Il contient la clé publique avec laquelle la clé privée utilisée pour signer le certificat est mise en correspondance pour vérifier le certificat. Vous pouvez obtenir le certificat CA racine auprès de l'autorité de certification qui a signé vos certificats SSL.

Installez le certificat racine de l'autorité de certification qui a signé le certificat du serveur Essbase sur les clients qui se connectent au serveur ou à l'agent Essbase. Vérifiez que le certificat racine est installé dans le fichier de clés approprié pour le client. Reportez-vous à la section [Certificats requis et leur emplacement](#).

#### Remarque :

Plusieurs composants peuvent utiliser un certificat CA racine installé sur un ordinateur serveur.

### Portefeuille Oracle

Reportez-vous à [Certificats requis et leur emplacement](#) pour obtenir la liste des composants qui requièrent le certificat CA racine dans Oracle Wallet. Vous pouvez créer un portefeuille ou installer le certificat dans le portefeuille de démo où le certificat auto-signé par défaut est installé.

Reportez-vous à la documentation d'Oracle Wallet Manager pour connaître le détail des procédures de création de portefeuille et d'import de certificat CA racine.

### Fichier de clés d'accès Java

Reportez-vous à [Certificats requis et leur emplacement](#) pour obtenir la liste des composants qui requièrent le certificat CA racine dans un fichier de clés Java. Vous

pouvez ajouter le certificat dans le fichier de clés où est installé le certificat auto-signé par défaut ou créer un fichier de clés pour y stocker le certificat.

 **Remarque :**

Les certificats CA racine de nombreuses autorités de certification tierces reconnues sont déjà installés dans le fichier de clés Java.

Reportez-vous à la documentation de l'outil que vous utilisez pour obtenir des instructions détaillées. Pour importer un certificat racine avec keytool, utilisez une commande semblable à la suivante :

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

### Installation de certificats signés

Vous installez les certificats SSL signés sur le serveur qui héberge le serveur Essbase et l'agent Essbase. Pour les composants qui utilisent Essbase RTC (API C) pour établir une connexion au serveur ou à l'agent Essbase, le certificat doit être stocké dans Oracle Wallet avec le certificat CA racine. Pour les composants qui utilisent JAPI pour établir une connexion au serveur ou à l'agent Essbase, le certificat CA racine et le certificat SSL signé doivent être stockés dans un fichier de clés Java. Pour connaître le détail des procédures, consultez ces sources d'information :

- Documentation Oracle Wallet Manager
- Documentation ou aide en ligne de l'outil (par exemple, keytool, qui sert à importer le certificat)

Pour importer un certificat avec keytool, utilisez une commande semblable à la suivante :

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

### Mise à jour des valeurs de registre de serveur Essbase

#### Windows

1. Dans une invite de commande, changez de répertoire pour passer à `EPM_ORACLE_INSTANCE/epmsystem1/bin`.
2. Exécutez les commandes suivantes pour mettre à jour le registre Windows :
 

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

Veillez à remplacer <Object ID> par l'ID de composant de serveur Essbase, qui est disponible dans le rapport de registre généré à la fin du processus de configuration du serveur Essbase.

#### Linux

1. Dans une console, changez de répertoire pour passer à `EPM_ORACLE_INSTANCE/epmsystem1/bin`.
2. Exécutez les commandes suivantes pour mettre à jour le registre :  

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

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

Veillez à remplacer `<Object ID>` par l'ID de composant de serveur Essbase, qui est disponible dans le rapport de registre généré à la fin du processus de configuration du serveur Essbase.

### Mise à jour des paramètres SSL Essbase

Afin de personnaliser les paramètres SSL des clients et du serveur Essbase, indiquez des valeurs pour les éléments suivants dans `essbase.cfg`.

- Paramètre permettant d'activer le mode sécurisé
- Paramètre permettant d'activer le mode d'effacement
- Mode privilégié pour communiquer avec les clients (utilisé uniquement par les clients)
- Port sécurisé
- Mécanismes de cryptage
- Chemin d'Oracle Wallet

#### Remarque :

Dans le fichier `essbase.cfg`, veillez à bien inclure tous les paramètres obligatoires, en particulier `EnableSecureMode` et `AgentSecurePort`, et à définir leur valeur.

Pour mettre à jour le fichier `essbase.cfg`, procédez comme suit :

1. Copiez le portefeuille Oracle contenant les certificats pour le serveur Essbase vers `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin/wallet`. Il s'agit de l'unique emplacement Oracle Wallet acceptable pour le serveur Essbase.
2. A l'aide d'un éditeur de texte, ouvrez `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin/essbase.cfg`.
3. Entrez les paramètres nécessaires. Les paramètres Essbase par défaut sont implicites. Si vous devez modifier le comportement par défaut, ajoutez les paramètres du comportement personnalisé dans le fichier `essbase.cfg`. Par exemple, `EnableClearMode` est appliqué par défaut, ce qui permet au serveur Essbase de communiquer sur un canal non crypté. Pour empêcher le serveur Essbase de communiquer sur un canal non crypté, vous devez indiquer `EnableClearMode FALSE` dans le fichier `essbase.cfg`. Reportez-vous au tableau suivant.



**Tableau 2-2 Paramètres SSL Essbase**

| Paramètre                        | Description <sup>1</sup>                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EnableClearMode <sup>2</sup>     | <p>Permet la communication non cryptée entre les applications Essbase et l'agent Essbase. Si cette propriété est définie sur FALSE, Essbase ne traite que les demandes SSL.</p> <p><b>Valeur par défaut :</b> EnableClearMode TRUE</p> <p><b>Exemple :</b> EnableClearMode FALSE</p>                                                                                                                                                                                                                  |
| EnableSecureMode                 | <p>Active la communication cryptée SSL entre les clients Essbase et l'agent Essbase. Cette propriété doit être définie sur TRUE pour prendre en charge SSL.</p> <p><b>Valeur par défaut :</b> FALSE</p> <p><b>Exemple :</b> EnableSecureMode TRUE</p>                                                                                                                                                                                                                                                 |
| SSLCipherSuites                  | <p>Liste des mécanismes de cryptage, par ordre de préférence, à utiliser pour la communication SSL. L'agent Essbase utilise l'un de ces mécanismes de cryptage pour la communication SSL. Le premier mécanisme de cryptage de la liste reçoit la priorité la plus élevée lorsque l'agent choisit un mécanisme.</p> <p><b>Valeur par défaut :</b> SSL_RSA_WITH_RC4_128_MD5</p> <p><b>Exemple :</b> SSLCipherSuites<br/>SSL_RSA_WITH_AES_256_CBC_SHA256,SSL_RSA_WITH_AES_256_GCM_SHA384</p>             |
| APSRESOLVER                      | <p>URL d'Oracle Hyperion Provider Services. Si vous utilisez plusieurs serveurs Provider Services, séparez chaque URL à l'aide d'un point-virgule.</p> <p><b>Exemple :</b> APSRESOLVER https://<br/>exampleAPShost1:PORT/aps;https://<br/>exampleAPShost2:PORT/aps</p>                                                                                                                                                                                                                                |
| AgentSecurePort                  | <p>Port sécurisé sur lequel écoute l'agent.</p> <p><b>Valeur par défaut :</b> 6423</p> <p><b>Exemple :</b> AgentSecurePort 16001</p>                                                                                                                                                                                                                                                                                                                                                                  |
| WalletPath                       | <p>Emplacement d'Oracle Wallet (moins de 1 024 caractères) qui contient le certificat CA racine et le certificat signé.</p> <p><b>Valeur par défaut :</b> ARBORPATH/bin/wallet</p> <p><b>Exemple :</b> WalletPath/usr/local/wallet</p>                                                                                                                                                                                                                                                                |
| ClientPreferredMode <sup>3</sup> | <p>Mode (SECURE ou CLEAR) de la session client. Si la propriété est définie sur SECURE, le mode SSL est utilisé pour toutes les sessions.</p> <p>Si la propriété est définie sur CLEAR, le choix du transport dépend de la présence du mot-clé de transport sécurisé dans la demande de connexion du client. Reportez-vous à la section <a href="#">Etablissement d'une connexion SSL par session</a>.</p> <p><b>Valeur par défaut :</b> CLEAR</p> <p><b>Exemple :</b> ClientPreferredMode SECURE</p> |

**Tableau 2-2 (suite) Paramètres SSL Essbase**

| Paramètre | Description <sup>1</sup>                                                                                                                         |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------|
|           | <sup>1</sup> La valeur par défaut est appliquée si ces propriétés ne sont pas disponibles dans <code>essbase.cfg</code> .                        |
|           | <sup>2</sup> Essbase cesse de fonctionner si <code>EnableClearMode</code> et <code>EnableSecureMode</code> sont définis sur <code>FALSE</code> . |
|           | <sup>3</sup> Les clients utilisent ce paramètre pour déterminer s'ils doivent établir une connexion sécurisée ou non sécurisée à Essbase.        |

4. Enregistrez et fermez `essbase.cfg`.

### Mise à jour des noeuds Essbase distribués pour SSL

#### Remarque :

Cette section s'applique uniquement au déploiement distribué d'Essbase.

Assurez-vous que le dossier de portefeuille (par exemple, `WalletPath/usr/local/wallet`) contenant le certificat CA racine et le certificat signé se trouve à l'emplacement requis sur chaque noeud distribué.

1. Copiez le dossier de portefeuille vers les emplacements suivants dans chaque noeud distribué :
  - `EPM_ORACLE_HOME/common/EssbaseRTC/11.1.2.0/bin`
  - `EPM_ORACLE_HOME/common/EssbaseRTC-64/11.1.2.0/bin`
2. Copiez le dossier de portefeuille vers les emplacements suivants, le cas échéant, dans chaque noeud distribué :
  - `EPM_ORACLE_HOME/products/Essbase/EssbaseServer/bin`
  - `EPM_ORACLE_HOME/products/Essbase/EssbaseServer-32/bin`
  - `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin`
3. Copiez `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin/essbase.cfg` vers les emplacements suivants sur chaque noeud distribué :
  - `EPM_ORACLE_HOME/common/EssbaseRTC/11.1.2.0/bin`
  - `EPM_ORACLE_HOME/common/EssbaseRTC-64/11.1.2.0/bin`
4. Copiez `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin/essbase.cfg` vers les emplacements suivants, le cas échéant, sur chaque noeud distribué :
  - `EPM_ORACLE_HOME/products/Essbase/EssbaseServer/bin`
  - `EPM_ORACLE_HOME/products/Essbase/EssbaseServer-32/bin`
  - `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin`
5. Copiez le dossier de portefeuille vers les emplacements d'installation client Essbase suivants sur chaque noeud distribué :
  - `EPM_ORACLE_HOME/products/Essbase/EssbaseClient/bin`

- *EPM\_ORACLE\_HOME*/products/Essbase/EssbaseClient-32/bin
6. Copiez *EPM\_ORACLE\_INSTANCE*/EssbaseServer/essbaseserver1/bin/essbase.cfg vers les emplacements d'installation client Essbase suivants sur chaque noeud distribué :
- *EPM\_ORACLE\_HOME*/products/Essbase/EssbaseClient/bin
  - *EPM\_ORACLE\_HOME*/products/Essbase/EssbaseClient-32/bin
7. Ajoutez les propriétés suivantes au fichier *essbase.properties* :
- *essbase.sseverywhere=true*
  - *olap.server.ssl.alwaysSecure=true*
  - *APSRESOLVER=http[s]://host:httpsPort/aps*  
Veillez à remplacer cette valeur par l'URL appropriée.

Vous devez mettre à jour le fichier *essbase.properties* aux emplacements suivants, le cas échéant, dans chaque noeud distribué :

- *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. Copiez *EPM\_ORACLE\_HOME*/products/Essbase/aps/bin/essbase.properties vers le répertoire *EPM\_ORACLE\_HOME*/products/Essbase/eas, si disponible, sur chaque noeud distribué :
9. **Pour Oracle Hyperion Planning uniquement.** Ajoutez les trois propriétés suivantes au fichier *essbase.properties* :
- *essbase.sseverywhere=true*
  - *olap.server.ssl.alwaysSecure=true*
  - *APSRESOLVER=APS\_URL*  
Remplacez *APS\_URL* par l'URL Provider Services. Si vous utilisez plusieurs serveurs Provider Services, séparez chaque URL à l'aide d'un point-virgule. Par exemple, *https://exampleAPShost1:PORT/aps;https://exampleAPShost2:PORT/aps*.
- Vous devez mettre à jour le fichier *essbase.properties* aux emplacements suivants dans chaque noeud distribué :
- *EPM\_ORACLE\_HOME*/products/Planning/config/essbase.properties
  - *EPM\_ORACLE\_HOME*/products/Planning/lib/essbase.properties
10. **Pour Oracle Hyperion Financial Reporting uniquement.** Ajoutez les trois propriétés suivantes au fichier *EPM\_ORACLE\_HOME*/products/financialreporting/bin/EssbaseJAPI/bin/essbase.properties :
- *essbase.sseverywhere=true*
  - *olap.server.ssl.alwaysSecure=true*
  - *APSRESOLVER=APS\_URL*  
Remplacez *APS\_URL* par l'URL Provider Services. Si vous utilisez plusieurs serveurs Provider Services, séparez chaque URL à l'aide d'un point-virgule. Par exemple, *https://exampleAPShost1:PORT/aps;https://exampleAPShost2:PORT/aps*.

 **Remarque :**

Dans les environnements entièrement SSL, Financial Reporting nécessite le nom du cluster Essbase pour établir une connexion. Les connexions échouent si le nom d'hôte est utilisé.

11. a. Définissez les variables d'environnement :
  - **Windows** : créez une variable système nommée `API_DISABLE_PEER_VERIFICATION` et définissez sa valeur sur 1.
  - **Linux** : ajoutez la directive `API_DISABLE_PEER_VERIFICATION=1` dans `setCustomParamsPlanning.sh`.
- b. Ajoutez la directive `API_DISABLE_PEER_VERIFICATION=1` dans `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin/setEssbaseenv.bat` ou `EPM_ORACLE_INSTANCE/EssbaseServer/essbaseserver1/bin/setEssbaseenv.sh`.

Définissez des variables d'environnement :

### Personnalisation des propriétés SSL des clients JAPI

Plusieurs propriétés par défaut sont prédéfinies pour les composants Essbase basés sur JAPI. Il est possible de passer outre ces propriétés par défaut en incluant des propriétés dans le fichier `essbase.properties`.

 **Remarque :**

Seules quelques-unes des propriétés SSL identifiées dans le tableau suivant sont externalisées dans `essbase.properties`. Vous devez ajouter les propriétés qui ne sont pas externalisées.

Pour mettre à jour les propriétés SSL des clients JAPI, procédez comme suit :

1. A l'aide d'un éditeur de texte, ouvrez `EPM_ORACLE_HOME/common/EssbaseJavaAPI/11.1.2.0/bin/essbase.properties`.
2. Mettez à jour les propriétés selon vos besoins. Reportez-vous au tableau suivant pour obtenir une description des propriétés client JAPI personnalisables. Si la propriété souhaitée ne figure pas dans le fichier `essbase.properties`, ajoutez-la.

**Tableau 2-3 Propriétés SSL par défaut pour les clients JAPI**

| Propriété                                 | Description                                                                                                                                                                                                                   |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>olap.server.ssl.alwaysSecure</code> | Définit le mode que les clients doivent utiliser pour toutes les instances Essbase. Remplacez la valeur de cette propriété par <code>true</code> pour appliquer le mode SSL.<br><b>Valeur par défaut</b> : <code>false</code> |

**Tableau 2-3 (suite) Propriétés SSL par défaut pour les clients JAPI**

| Propriété                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>olap.server.ssl.securityHandler</code>   | Nom de package pour le traitement du protocole. Vous pouvez modifier cette valeur afin d'indiquer un autre gestionnaire.<br><b>Valeur par défaut :</b><br><code>java.protocol.handler.pkgs</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <code>olap.server.ssl.securityProvider</code>  | Oracle utilise l'implémentation de protocole SSL Sun. Vous pouvez modifier cette valeur afin d'indiquer un autre fournisseur.<br><b>Valeur par défaut :</b><br><code>com.sun.net.ssl.internal.www.protocol</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <code>olap.server.ssl.supportedCiphers</code>  | Liste de cryptages supplémentaires, séparés par des virgules, à activer pour une communication sécurisée. Vous ne devez indiquer que des cryptages pris en charge par Essbase.<br><b>Exemple :</b><br><code>SSL_RSA_WITH_AES_256_CBC_SHA256,SSL_RSA_WITH_AES_256_GCM_SHA384</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <code>olap.server.ssl.trustManagerClass</code> | Classe <code>TrustManager</code> à utiliser pour valider le certificat SSL, en vérifiant la signature et la date d'expiration du certificat.<br>Par défaut, cette propriété n'applique pas toutes les vérifications.<br>Pour ignorer les vérifications, définissez la valeur de ce paramètre sur <code>com.essbase.services.olap.security.EssDefaultTrustManager</code> , qui est la classe <code>TrustManager</code> par défaut permettant le succès de toutes les validations.<br>Pour mettre en oeuvre une classe <code>TrustManager</code> personnalisée, indiquez un nom de classe qualifié complet pour la classe <code>TrustManager</code> qui implémente l'interface <code>javax.net.ssl.X509TrustManager</code> .<br><b>Exemple :</b><br><code>com.essbase.services.olap.security.EssDefaultTrustManager</code> |

3. Enregistrez et fermez `essbase.properties`.
4. Redémarrez tous les composants Essbase.

## Etablissement d'une connexion SSL par session

Les composants Oracle Essbase (par exemple, MaxL) peuvent contrôler le protocole SSL au niveau de la session en se connectant à l'agent Essbase à l'aide du mot-clé de transport

secure. Par exemple, vous pouvez établir une connexion sécurisée entre MaxL et l'agent Essbase en exécutant l'une des commandes suivantes à partir d'une console MaxL :

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

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

Le contrôle par session est prioritaire sur les paramètres de configuration spécifiés dans `essbase.cfg`. Si aucun mot-clé de transport n'est spécifié, les clients Essbase utilisent la valeur définie pour `ClientPreferredMode` afin de déterminer si une connexion sécurisée avec Essbase doit être lancée. Si le paramètre `ClientPreferredMode` n'est pas défini pour être sécurisé, la communication s'effectue sur un canal non sécurisé.

## SSL pour Essbase 21c

### Présentation

Cette section explique les procédures de remplacement des certificats par défaut qui sont utilisés pour sécuriser la communication entre une instance Oracle Essbase et des composants tels que MaxL, le serveur Oracle Essbase Administration Services, Oracle Hyperion Provider Services, Oracle Hyperion Foundation Services, Oracle Hyperion Planning, Oracle Hyperion Financial Management et Oracle Hyperion Shared Services Registry.

#### Remarque :

Essbase Administration Services (EAS) Lite n'utilise pas le port SSL du serveur HTTP (par exemple, 443) configuré à l'aide du configurateur EPM. L'URL sécurisée dans le fichier `easconsole.jnlp` est définie par défaut sur le port non SSL (80).

**Solution de contournement :** remplacez le port non SSL par défaut dans l'URL sécurisée identifiée dans `easconsole.jnlp` par l'URL sécurisée mise à jour :

URL sécurisée par défaut : `https://myserver:SECURE_PORT/easconsole/console.html`. Par exemple : `https://myserver:80/easconsole/console.html`.

URL sécurisée mise à jour : `https://myserver:SECURE_PORT/easconsole/console.html`. Par exemple : `https://myserver:443/easconsole/console.html`.

Pour plus d'informations, reportez-vous à l'article My Oracle Support (MOS) : [SSL Port Not Included In easconsole.jnlp of the EAS Web Console \(ID de document 1926558.1\)](#).

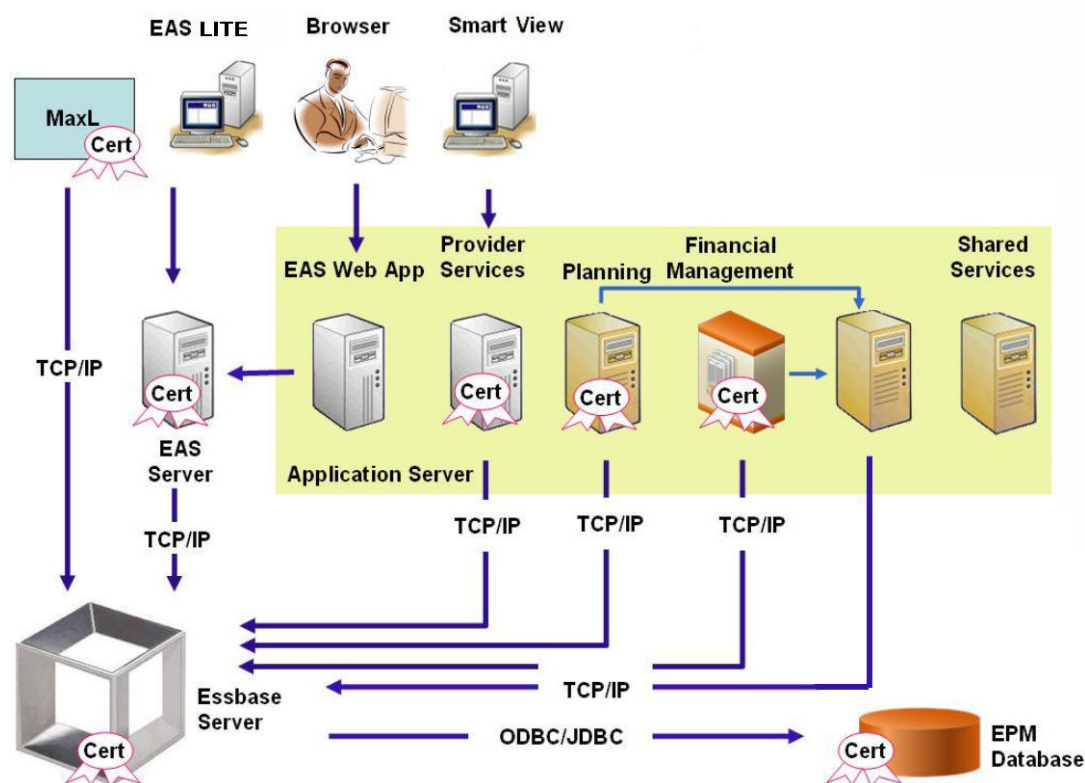
## Déploiement par défaut

Essbase peut être déployé pour fonctionner en mode SSL et non SSL. L'agent Essbase écoute sur un port non sécurisé, mais il peut aussi être configuré pour écouter sur un port sécurisé. Toutes les connexions accédant au port sécurisé sont traitées comme des connexions SSL. Si un client se connecte à l'agent Essbase sur le port non SSL, la connexion est traitée comme une connexion non SSL. Les composants peuvent établir des connexions simultanées non SSL et SSL à un agent Essbase.

Vous pouvez contrôler le mode SSL par session en spécifiant le protocole sécurisé et le port lorsque vous vous connectez. Reportez-vous à [Etablissement d'une connexion SSL par session](#).

Si SSL est activé, toutes les communications au sein d'une instance Essbase sont cryptées pour assurer la sécurité des données.

Les déploiements par défaut de composants Essbase en mode sécurisé font appel à des certificats auto-signés pour activer la communication SSL, principalement à des fins de test. Oracle recommande d'utiliser les certificats émis par des organismes de certification tiers reconnus pour activer SSL pour Essbase dans des environnements de production.



En règle générale, un portefeuille Oracle stocke le certificat qui active la communication SSL avec les clients utilisant le client en temps réel Essbase et un fichier de clés d'accès Java stocke le certificat qui active la communication SSL avec les composants utilisant JAPI pour la communication. Pour établir la communication SSL, les outils et les clients Essbase stockent le certificat racine de l'organisme de certification ayant signé les certificats de l'agent et du serveur Essbase.

## Certificats requis et leur emplacement

Oracle recommande d'utiliser les certificats émis par des organismes de certification tiers reconnus pour activer SSL pour Essbase dans un environnement de production. Vous pouvez utiliser les certificats auto-signés par défaut à des fins de test.

### Remarque :

Essbase prend en charge l'utilisation de certificats génériques, ce qui permet de sécuriser plusieurs sous-domaines avec un seul certificat SSL. Les certificats génériques permettent de réduire les coûts et le temps de gestion.

Les certificats génériques ne peuvent pas être utilisés si la vérification de nom d'hôte est activée.

Vous avez besoin des certificats suivants :

- Un certificat CA racine  
Les composants qui utilisent le client en temps réel Essbase pour établir une connexion à Essbase nécessitent que le certificat CA racine soit stocké dans un portefeuille Oracle. Les composants qui utilisent JAPI pour établir une connexion nécessitent que le certificat CA racine soit stocké dans un fichier de clés d'accès Java. Les certificats requis et leur emplacement sont indiqués dans le tableau suivant.

### Remarque :

Il se peut que vous n'ayez pas besoin d'installer un certificat CA racine si vos certificats proviennent d'un organisme de certification tiers reconnu dont le certificat racine est déjà installé dans le portefeuille Oracle.

- Un certificat signé pour le serveur Essbase et l'agent Essbase

**Tableau 2-4 Certificats requis et leur emplacement**

| Composant <sup>1</sup>                                          | Fichier de clés d'accès                                                                                         | Certificat <sup>2</sup>                                                                                                                 |
|-----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| MaxL                                                            | Portefeuille Oracle                                                                                             | Certificat CA racine                                                                                                                    |
| Serveur Administration Services                                 | Portefeuille Oracle                                                                                             | Certificat CA racine                                                                                                                    |
| Provider Services                                               | Portefeuille Oracle                                                                                             | Certificat CA racine                                                                                                                    |
| Base de données Oracle Enterprise Performance Management System | Portefeuille Oracle                                                                                             | Certificat CA racine                                                                                                                    |
| Planning                                                        | <ul style="list-style-type: none"> <li>• Portefeuille Oracle</li> <li>• Fichier de clés d'accès Java</li> </ul> | Certificat CA racine                                                                                                                    |
| Financial Management                                            | Fichier de clés d'accès Java                                                                                    | Certificat CA racine                                                                                                                    |
| Essbase (serveur et agent) <sup>3</sup>                         | <ul style="list-style-type: none"> <li>• Portefeuille Oracle</li> <li>• Fichier de clés d'accès Java</li> </ul> | <ul style="list-style-type: none"> <li>• Certificat CA racine</li> <li>• Certificat signé pour le serveur et l'agent Essbase</li> </ul> |
| Référentiel Oracle Hyperion Shared Services                     |                                                                                                                 |                                                                                                                                         |



Tableau 2-4 (suite) Certificats requis et leur emplacement

| Composant <sup>1</sup>                                                                                                                                                                                                                                                                                                                                                                                                                      | Fichier de clés d'accès | Certificat <sup>2</sup> |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|-------------------------|
| <sup>1</sup> Vous n'avez besoin que d'une seule instance du fichier de clés d'accès pour prendre en charge plusieurs composants utilisant un fichier de clés d'accès similaire.<br><sup>2</sup> Plusieurs composants peuvent utiliser un certificat racine installé dans un fichier de clés d'accès.<br><sup>3</sup> Les certificats doivent être installés dans le portefeuille Oracle par défaut et dans le fichier de clés d'accès Java. |                         |                         |

## Installation et déploiement des composants Essbase

Le processus de configuration vous permet de sélectionner un port d'agent sécurisé (par défaut, il s'agit du port 6423) que vous pouvez modifier lors de la configuration d'Oracle Essbase. Par défaut, le processus de déploiement installe les certificats auto-signés requis pour créer un déploiement sécurisé fonctionnel à des fins de test.

Le programme d'installation d'EPM System installe un portefeuille Oracle et un certificat auto-signé dans *ARBOR\_PATH* sur l'ordinateur qui héberge l'instance Essbase si Oracle HTTP Server est installé. Dans les déploiements d'hôte unique, tous les composants Essbase partagent ce certificat.

## Utilisation de certificats CA tiers sécurisés pour Essbase

### Création de demandes de certificats et obtention de certificats

Générez une demande de certificat afin d'obtenir un certificat pour le serveur qui héberge le serveur Oracle Essbase et l'agent Essbase. Une demande de certificat contient des informations cryptées propres au nom commun (CN=) de votre serveur. Vous pouvez soumettre une demande de certificat à une autorité signataire pour obtenir un certificat SSL.

Pour créer une demande de certificat, utilisez un outil tel que keytool ou Oracle Wallet Manager. Pour plus d'informations sur la création d'une demande de certificat, reportez-vous à la documentation de l'outil en question.

### Exemples avec keytool :

Créez un fichier de clés d'accès Java et générez une clé privée :

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

Générez une demande de certificat:

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

Exportez la clé privée (vous aurez besoin de l'utilitaire `openssl` pour effectuer ces étapes) :

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. Signez la nouvelle demande de certificat générée à l'aide de votre autorité de certification et copiez-la dans le fichier suivant :  
C:\oracle\Middleware\EPMSysstem11R1\ssl\essbase.cer.

### Obtention et installation d'un certificat CA racine

Le certificat CA racine vérifie la validité du certificat utilisé pour prendre en charge SSL. Il contient la clé publique avec laquelle la clé privée utilisée pour signer le certificat est mise en correspondance pour vérifier le certificat. Vous pouvez obtenir le certificat CA racine auprès de l'autorité de certification qui a signé vos certificats SSL.

Installez le certificat racine de l'autorité de certification qui a signé le certificat du serveur Essbase sur les clients qui se connectent au serveur ou à l'agent Essbase. Vérifiez que le certificat racine est installé dans le fichier de clés approprié pour le client. Reportez-vous à la section [Certificats requis et leur emplacement](#).



#### Remarque :

Plusieurs composants peuvent utiliser un certificat CA racine installé sur un ordinateur serveur.

### Installation de certificats signés par une autorité de certification

Pour installer des certificats signés par une autorité de certification, reportez-vous aux sections suivantes :

- [Configuration de connexion TLS WebLogic pour Essbase](#)
- [Mise à jour de certificats TLS](#)

Mettez à jour le fichier `tls.properties` sous

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

Où :

```
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.
```

Exécutez les commandes suivantes pour mettre à jour le serveur Essbase avec les nouveaux certificats :

```
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
```

### Mise à jour des paramètres SSL Essbase

Afin de personnaliser les paramètres SSL des clients et du serveur Essbase, indiquez des valeurs pour les éléments suivants dans `essbase.cfg`.

- Paramètre permettant d'activer le mode sécurisé
- Paramètre permettant d'activer le mode d'effacement
- Mode privilégié pour communiquer avec les clients (utilisé uniquement par les clients)
- Port sécurisé
- Mécanismes de cryptage
- Chemin d'Oracle Wallet

#### Remarque :

Dans le fichier `essbase.cfg`, veillez à bien inclure tous les paramètres obligatoires, en particulier `EnableSecureMode` et `AgentSecurePort`, et à définir leur valeur.

Pour mettre à jour `essbase.cfg` dans l'emplacement ci-dessous, procédez comme suit :

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

1. Entrez les paramètres nécessaires. Les paramètres Essbase par défaut sont implicites. Si vous devez modifier le comportement par défaut, ajoutez les paramètres du comportement personnalisé dans le fichier `essbase.cfg`. Par exemple, `EnableClearMode` est appliqué par défaut, ce qui permet au serveur Essbase de communiquer sur un canal non crypté. Pour empêcher le serveur Essbase de communiquer sur un canal non crypté, vous devez indiquer `EnableClearMode FALSE` dans le fichier `essbase.cfg`. Reportez-vous au tableau suivant:

**Tableau 2-5 Paramètres SSL Essbase**

| Paramètre                                 | Description <sup>1</sup>                                                                                                                                                                                                                                                                                      |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>EnableClearMode</code> <sup>2</sup> | Permet la communication non cryptée entre les applications Essbase et l'agent Essbase. Si cette propriété est définie sur <code>FALSE</code> , Essbase ne traite que les demandes SSL.<br><b>Valeur par défaut :</b> <code>EnableClearMode TRUE</code><br><b>Exemple :</b> <code>EnableClearMode FALSE</code> |

**Tableau 2-5 (suite) Paramètres SSL Essbase**

| Paramètre                        | Description <sup>1</sup>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EnableSecureMode                 | Active la communication cryptée SSL entre les clients Essbase et l'agent Essbase. Cette propriété doit être définie sur <code>TRUE</code> pour prendre en charge SSL.<br><b>Valeur par défaut :</b> <code>FALSE</code><br><b>Exemple :</b> <code>EnableSecureMode TRUE</code>                                                                                                                                                                                                                                 |
| SSLCipherSuites                  | Liste des mécanismes de cryptage, par ordre de préférence, à utiliser pour la communication SSL. L'agent Essbase utilise l'un de ces mécanismes de cryptage pour la communication SSL. Le premier mécanisme de cryptage de la liste reçoit la priorité la plus élevée lorsque l'agent choisit un mécanisme.<br><b>Valeur par défaut :</b> <code>SSL_RSA_WITH_RC4_128_MD5</code><br><b>Exemple :</b> <code>SSLCipherSuites<br/>SSL_RSA_WITH_AES_256_CBC_SHA256,SSL_RSA_WITH_AES_256_GCM_SHA384</code>          |
| APSPRESOLVER                     | URL d'Oracle Hyperion Provider Services. Si vous utilisez plusieurs serveurs Provider Services, séparez chaque URL à l'aide d'un point-virgule.<br><b>Exemple :</b> <code>https://exampleAPShost1:PORT/essbase;https://exampleAPShost2:PORT/essbase</code>                                                                                                                                                                                                                                                    |
| AgentSecurePort                  | Port sécurisé sur lequel écoute l'agent.<br><b>Valeur par défaut :</b> <code>6423</code><br><b>Exemple :</b> <code>AgentSecurePort 16001</code>                                                                                                                                                                                                                                                                                                                                                               |
| WalletPath                       | Emplacement d'Oracle Wallet (moins de 1 024 caractères) qui contient le certificat CA racine et le certificat signé.<br><b>Valeur par défaut :</b> <code>ARBORPATH/bin/wallet</code><br><b>Exemple :</b> <code>WalletPath/usr/local/wallet</code>                                                                                                                                                                                                                                                             |
| ClientPreferredMode <sup>3</sup> | Mode (SECURE ou CLEAR) de la session client. Si la propriété est définie sur SECURE, le mode SSL est utilisé pour toutes les sessions.<br>Si la propriété est définie sur CLEAR, le choix du transport dépend de la présence du mot-clé de transport sécurisé dans la demande de connexion du client. Reportez-vous à la section <a href="#">Etablissement d'une connexion SSL par session</a> .<br><b>Valeur par défaut :</b> <code>CLEAR</code><br><b>Exemple :</b> <code>ClientPreferredMode SECURE</code> |

- <sup>1</sup> La valeur par défaut est appliquée si ces propriétés ne sont pas disponibles dans `essbase.cfg`.
- <sup>2</sup> Essbase cesse de fonctionner si `EnableClearMode` et `EnableSecureMode` sont définis sur `FALSE`.
- <sup>3</sup> Les clients utilisent ce paramètre pour déterminer s'ils doivent établir une connexion sécurisée ou non sécurisée à Essbase.

2. Enregistrez et fermez `essbase.cfg`.

## Mise à jour des noeuds Essbase distribués pour SSL

### Remarque :

Cette section s'applique uniquement au déploiement distribué d'Essbase.

Assurez-vous que le dossier de portefeuille (par exemple, `WalletPath/usr/local/wallet`) contenant le certificat CA racine et le certificat signé se trouve à l'emplacement requis sur chaque noeud distribué.

#### 1. Importez tous les nouveaux certificats d'autorité de certification à l'aide d'outils TLS.

Pour plus d'informations, reportez-vous aux sections suivantes :

- [Configuration de connexion TLS WebLogic pour Essbase](#)
- [Mise à jour de certificats TLS](#)

#### 2. Accédez à l'emplacement source

`ESSBASE_DOMAIN_HOME\config\fmwconfig\essconfig\essbase` et modifiez les propriétés suivantes dans le fichier `essbase.properties` :

- `essbase.sseverywhere=true`
- `olap.server.ssl.alwaysSecure=true`
- `APSRESOLVER=APS_URL`  
Remplacez `APS_URL` par l'URL Provider Services. Si vous utilisez plusieurs serveurs Provider Services, séparez chaque URL par un point-virgule.

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

#### 3. Copiez les dossiers `Wallet` et `Walletssl`, ainsi que les fichiers `essbase.cfg` et `essbase.properties` dans les chemins de destination ci-après.

**Tableau 2-6 Chemins de destination**

| Chemins de destination                                                       | Wallet | Walletssl | essbase.cfg | essbase.properties |
|------------------------------------------------------------------------------|--------|-----------|-------------|--------------------|
| <code>EPM_ORACLE_HOME\common\EssbaseRTC-21c\11.1.2.0\bin</code>              | Oui    | Oui       | Oui         | Oui                |
| <code>EPM_ORACLE_HOME\common\EssbaseJavaAPI-21c\11.1.2.0\bin</code>          | Oui    | Oui       | Oui         | Oui                |
| <code>ESSBASE_DOMAIN_HOME\config\fmwconfig\essconfig\aps</code>              | Oui    | Oui       | Oui         | Oui                |
| <code>ESSBASE_DOMAIN_HOME\config\fmwconfig\essconfig\essbase</code>          | Oui    | Oui       | Oui         | Oui                |
| <code>MIDDLEWARE_HOME\essbase\products\Essbase\template_files\essbase</code> | Oui    | Oui       | Oui         | Oui                |

Tableau 2-6 (suite) Chemins de destination

| Chemins de destination                                                                                                                                                                                                                                                                                                                             | Wallet | Wallet ssl | essbase.cfg | essbase.properties |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|------------|-------------|--------------------|
| MIDDLEWARE_HOME\essbase\products\Essbase\EssbaseServer\bin                                                                                                                                                                                                                                                                                         | Oui    | Oui        | Oui         | Oui                |
| MIDDLEWARE_HOME\essbase\products\Essbase\aps\bin                                                                                                                                                                                                                                                                                                   | Oui    | Oui        | Oui         | Oui                |
| MIDDLEWARE_HOME\essbase\products\Essbase\eas                                                                                                                                                                                                                                                                                                       | Oui    | Oui        | Oui         | Oui                |
| MIDDLEWARE_HOME\essbase\common\EssbaseJavaAPI\bin                                                                                                                                                                                                                                                                                                  | Oui    | Oui        | Oui         | Oui                |
| <p><b>Uniquement pour Oracle Hyperion Financial Reporting</b><br/>EPM_ORACLE_HOME/products/financialreporting/bin/EssbaseJAPI/bin/</p> <p><b>Remarque :</b> dans les environnements entièrement SSL, Financial Reporting nécessite le nom du cluster Essbase pour établir une connexion. Les connexions échouent si le nom d'hôte est utilisé.</p> | Oui    | Oui        | Oui         | Oui                |
| <p><b>Uniquement pour Oracle Hyperion Planning</b><br/>EPM_ORACLE_HOME/products/Planning/config/<br/>EPM_ORACLE_HOME/products/Planning/lib/</p>                                                                                                                                                                                                    | Oui    | Oui        | Oui         | Oui                |

4. Définissez les variables d'environnement :

- **Windows :** créez une variable système nommée `API_DISABLE_PEER_VERIFICATION` et définissez sa valeur sur 1.
- **Linux :** ajoutez la directive `API_DISABLE_PEER_VERIFICATION=1` dans `setCustomParamsPlanning.sh`.

**Personnalisation des propriétés SSL des clients JAPI**

Plusieurs propriétés par défaut sont prédéfinies pour les composants Essbase basés sur JAPI. Il est possible de passer outre ces propriétés par défaut en incluant des propriétés dans le fichier `essbase.properties`.

 **Remarque :**

Seules quelques-unes des propriétés SSL identifiées dans le tableau suivant sont externalisées dans `essbase.properties`. Vous devez ajouter les propriétés qui ne sont pas externalisées.

Pour mettre à jour les propriétés SSL des clients JAPI, procédez comme suit :

1. A l'aide d'un éditeur de texte, ouvrez `EPM_ORACLE_HOME/common/EssbaseJavaAPI-21c/11.2.0/bin/essbase.properties`.
2. Mettez à jour les propriétés selon vos besoins. Reportez-vous au tableau suivant pour obtenir une description des propriétés client JAPI personnalisables.

Si la propriété souhaitée ne figure pas dans le fichier `essbase.properties`, ajoutez-la.

**Tableau 2-7 Propriétés SSL par défaut pour les clients JAPI**

| Propriété                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>olap.server.ssl.alwaysSecure</code>      | Définit le mode que les clients doivent utiliser pour toutes les instances Essbase. Remplacez la valeur de cette propriété par <code>true</code> pour appliquer le mode SSL.<br><b>Valeur par défaut :</b> <code>false</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <code>olap.server.ssl.securityHandler</code>   | Nom de package pour le traitement du protocole. Vous pouvez modifier cette valeur afin d'indiquer un autre gestionnaire.<br><b>Valeur par défaut :</b> <code>java.protocol.handler.pkgs</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <code>olap.server.ssl.securityProvider</code>  | Oracle utilise l'implémentation de protocole SSL Sun. Vous pouvez modifier cette valeur afin d'indiquer un autre fournisseur.<br><b>Valeur par défaut :</b><br><code>com.sun.net.ssl.internal.www.protocol</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <code>olap.server.ssl.supportedCiphers</code>  | Liste de cryptages supplémentaires, séparés par des virgules, à activer pour une communication sécurisée. Vous ne devez indiquer que des cryptages pris en charge par Essbase.<br><b>Exemple :</b><br><code>SSL_RSA_WITH_AES_256_CBC_SHA256,SSL_RSA_WITH_AES_256_GCM_SHA384</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <code>olap.server.ssl.trustManagerClass</code> | Classe <code>TrustManager</code> à utiliser pour valider le certificat SSL, en vérifiant la signature et la date d'expiration du certificat.<br>Par défaut, cette propriété n'applique pas toutes les vérifications.<br>Pour ignorer les vérifications, définissez la valeur de ce paramètre sur <code>com.essbase.services.olap.security.EssDefaultTrustManager</code> , qui est la classe <code>TrustManager</code> par défaut permettant le succès de toutes les validations.<br>Pour mettre en oeuvre une classe <code>TrustManager</code> personnalisée, indiquez un nom de classe qualifié complet pour la classe <code>TrustManager</code> qui implémente l'interface <code>javax.net.ssl.X509TrustManager</code> .<br><b>Exemple :</b><br><code>com.essbase.services.olap.security.EssDefaultTrustManager</code> |

3. Enregistrez et fermez `essbase.properties`.
4. Redémarrez tous les composants Essbase.

## Etablissement d'une connexion SSL par session

Les composants Oracle Essbase (par exemple, MaxL) peuvent contrôler le protocole SSL au niveau de la session en se connectant à l'agent Essbase à l'aide du mot-clé de transport

`secure`. Par exemple, vous pouvez établir une connexion sécurisée entre MaxL et l'agent Essbase en exécutant l'une des commandes suivantes à partir d'une console MaxL :

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

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

Le contrôle par session est prioritaire sur les paramètres de configuration spécifiés dans `essbase.cfg`. Si aucun mot-clé de transport n'est spécifié, les clients Essbase utilisent la valeur définie pour `ClientPreferredMode` afin de déterminer si une connexion sécurisée avec Essbase doit être lancée. Si le paramètre `ClientPreferredMode` n'est pas défini pour être sécurisé, la communication s'effectue sur un canal non sécurisé.



# 3

## Activation de l'authentification unique (SSO) à l'aide des agents de sécurité

### Voir aussi :

- [Méthodes d'authentification unique prises en charge](#)
- [Authentification unique à partir d'Oracle Access Manager](#)
- [Authentification unique OracleAS](#)
- [Protection des produits EPM System pour l'authentification unique](#)
- [Authentification unique basée sur un en-tête avec des produits de gestion des identités](#)
- [Configuration d'EPM System pour l'authentification unique basée sur un en-tête avec Oracle Identity Cloud Service](#)
- [Authentification unique SiteMinder](#)
- [Authentification unique Kerberos](#)
- [Configuration de EPM System pour l'authentification unique](#)
- [Options d'authentification unique pour Smart View](#)

## Méthodes d'authentification unique prises en charge

L'authentification unique (SSO) exige que la solution de gestion des identités Web transfère le nom de connexion des utilisateurs authentifiés aux produits Oracle Enterprise Performance Management System. Vous pouvez utiliser les méthodes standard EPM System suivantes pour intégrer EPM System à des solutions SSO sur le Web commerciales et personnalisées.

- [En-tête HTTP](#)
- [Classe de connexion personnalisée](#)
- [En-tête d'autorisation HTTP](#)
- [Obtenir les utilisateurs à distance à partir d'une requête HTTP](#)
- [Authentification basée sur un en-tête avec des produits de gestion des identités](#)

### ▲ Attention :

Par mesure de sécurité, Oracle recommande d'implémenter l'authentification des certificats client (SSL bidirectionnel) entre le serveur Web et le serveur d'applications si votre organisation utilise des méthodes dans lesquelles l'identité de l'utilisateur est véhiculée dans l'en-tête pour la propagation d'identité.

## En-tête HTTP

Si Oracle Single Sign-on (OSSO), SiteMinder ou Oracle Access Manager est votre solution de gestion des identités Web, la sécurité d'EPM System sélectionne automatiquement un en-tête HTTP personnalisé afin de transmettre le nom de connexion des utilisateurs authentifiés aux composants EPM System.

Le nom de connexion de l'utilisateur d'un produit EPM System est déterminé par la valeur `Attribut de connexion` spécifiée au moment de la configuration des annuaires des utilisateurs dans Oracle Hyperion Shared Services. Reportez-vous à la section "Configuration d'OID, d'Active Directory et d'autres annuaires des utilisateurs LDAP" du *Guide d'administration de la sécurité utilisateur d'Oracle Enterprise Performance Management System* pour obtenir une brève description de la valeur `Attribut de connexion`.

L'en-tête HTTP doit contenir la valeur de l'attribut défini dans `Attribut de connexion`. Par exemple, si la valeur `Attribut de connexion` est `uid`, l'en-tête HTTP doit comporter la valeur de l'attribut `uid`.

Pour plus d'informations sur la définition et l'affectation d'en-têtes HTTP personnalisés, reportez-vous à la documentation relative à votre solution de gestion des identités Web.

La sécurité d'EPM System analyse l'en-tête HTTP et valide le nom de connexion qu'il contient par rapport aux annuaires des utilisateurs configurés dans Shared Services.

## Classe de connexion personnalisée

Lorsqu'un utilisateur se connecte, la solution de gestion des identités Web l'authentifie à l'aide du serveur d'annuaires et encapsule les informations d'identification de l'utilisateur authentifié dans un mécanisme SSO afin d'activer l'authentification unique avec des systèmes en aval. Si la solution de gestion des identités Web utilise un mécanisme non pris en charge par les produits EPM System ou si la valeur `Attribut de connexion` n'est pas disponible dans le mécanisme SSO, utilisez une classe de connexion personnalisée pour dériver la valeur `Attribut de connexion` et la transmettre aux produits EPM System.

Une classe de connexion personnalisée permet l'intégration d'EPM System aux agents de sécurité qui utilisent l'authentification basée sur le certificat X509. L'utilisation de ce mécanisme d'authentification requiert l'implémentation d'API Shared Services standard pour définir l'interface SSO entre les composants EPM System et la solution de gestion des identités Web. La classe de connexion personnalisée doit transmettre la valeur `Attribut de connexion` aux produits EPM System. Reportez-vous à la section "Configuration d'OID, d'Active Directory et d'autres annuaires des utilisateurs LDAP" du *Guide d'administration de la sécurité utilisateur d'Oracle Enterprise Performance Management System* pour obtenir une brève description de la valeur `Attribut de connexion`. Pour obtenir un exemple de code et consulter les étapes d'implémentation, reportez-vous à la section [Implémentation d'une classe de connexion personnalisée](#).

Pour utiliser une classe de connexion personnalisée (dont le nom par défaut est `com.hyperion.css.sso.agent.X509CertificateSecurityAgentImpl`), une implémentation de l'interface `com.hyperion.css.CSSSecurityAgentIF` doit être disponible dans le classpath. `CSSSecurityAgentIF` définit la méthode d'extraction du nom et du mot de passe de l'utilisateur (facultatif). Si l'interface renvoie un mot de passe NULL, l'authentification de sécurité traite le fournisseur comme étant sécurisé et

vérifie l'existence de l'utilisateur dans les fournisseurs configurés. Si elle renvoie une valeur non NULL pour le mot de passe, EPM System tente d'authentifier la demande à l'aide du nom et du mot de passe de l'utilisateur renvoyés par cette implémentation.

CSSSecurityAgentIF comprend deux méthodes : `getUserName` et `getPassword`.

### Méthode `getUserName`

Cette méthode renvoie le nom de l'utilisateur pour l'authentification.

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

Le paramètre `req` identifie la requête HTTP qui contient les informations utilisées pour déterminer le nom de l'utilisateur. Le paramètre `res` n'est pas utilisé (prédéfini pour la compatibilité ascendante).

### Méthode `getPassword`

Cette méthode renvoie un mot de passe en texte clair pour l'authentification. L'extraction du mot de passe est facultative.

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

Le paramètre `req` identifie la requête HTTP qui contient les informations utilisées pour déterminer le mot de passe. Le paramètre `res` n'est pas utilisé (prédéfini pour la compatibilité ascendante).

### En-tête d'autorisation HTTP

La sécurité d'EPM System prend en charge l'utilisation d'un en-tête d'autorisation HTTP pour transmettre la valeur `Attribut de connexion` aux produits EPM System à partir de solutions de gestion des identités Web. Les produits EPM System analysent l'en-tête d'autorisation pour extraire le nom de connexion de l'utilisateur.

### Obtenir les utilisateurs à distance à partir d'une requête HTTP

La sécurité d'EPM System prend en charge l'utilisation d'une demande HTTP pour transmettre la valeur `Attribut de connexion` aux produits EPM System à partir de solutions de gestion des identités Web. Utilisez cette méthode SSO si la solution de gestion des identités Web transmet une demande HTTP contenant la valeur `Attribut de connexion`, qui est définie à l'aide de la fonction `setRemoteUser`.

### Authentification basée sur un en-tête avec des produits de gestion des identités

EPM System prend en charge tous les produits de gestion des identités, comme Oracle Identity Cloud Service, Microsoft Azure AD et Okta, qui prennent en charge l'authentification basée sur un en-tête. Le workflow conceptuel est le suivant :

- Une application de passerelle faisant office de proxy inverse protège les composants EPM System en limitant l'accès au réseau non authentifié.
- L'application de passerelle intercepte les demandes HTTP(S) aux composants EPM System et vérifie que le produit de gestion des identités authentifie les utilisateurs avant de transmettre les demandes aux composants EPM System.
- Lors du transfert des demandes aux composants EPM System, l'application de passerelle propage l'identité de l'utilisateur authentifié au composant EPM System via des demandes d'en-tête HTTP.

Pour prendre en charge ce scénario d'authentification, EPM System doit être configuré pour fonctionner avec l'identité de l'utilisateur authentifié propagée via les demandes d'en-tête HTTP(S).

## Authentification unique à partir d'Oracle Access Manager

Oracle Enterprise Performance Management System s'intègre à Oracle Access Manager en acceptant un en-tête HTTP personnalisé (nom par défaut : `HYPLOGIN`) qui contient la valeur d'attribut de connexion. L'attribut de connexion est défini lorsque vous configurez un annuaire des utilisateurs externe dans Oracle Hyperion Shared Services. Reportez-vous à la section "Configuration d'OID, d'Active Directory et d'autres annuaires des utilisateurs LDAP" du *Guide d'administration de la sécurité utilisateur d'Oracle Enterprise Performance Management System* pour obtenir une brève description de la valeur `Attribut de connexion`.

Vous pouvez utiliser n'importe quel nom d'en-tête fournissant la valeur de l'attribut de connexion à EPM System. Vous utilisez le nom d'en-tête lors de la configuration de Shared Services pour SSO à partir d'Oracle Access Manager.

EPM System utilise la valeur de l'attribut de connexion pour authentifier l'utilisateur par rapport à un annuaire des utilisateurs configuré (dans ce cas, l'annuaire des utilisateurs par rapport auquel Oracle Access Manager authentifie les utilisateurs), puis génère un jeton SSO EPM qui active SSO dans EPM System. Les informations de provisionnement de l'utilisateur sont vérifiées dans l'annuaire natif afin d'accorder une autorisation à l'utilisateur pour les ressources EPM System.

### Remarque :

La console Oracle Essbase Administration Services, qui est un client lourd, ne prend pas en charge SSO à partir d'Oracle Access Manager.

Les informations relatives à la configuration d'Oracle Access Manager et à la réalisation de tâches telles que la configuration de l'en-tête HTTP et des domaines de stratégie sont disponibles dans la documentation Oracle Access Manager. Ce guide suppose que le déploiement d'Oracle Access Manager est fonctionnel lorsque vous avez effectué les tâches suivantes :

- Vous avez configuré les domaines de stratégie requis pour les composants EPM System.
- Vous avez configuré un en-tête HTTP pour transmettre la valeur d'attribut de connexion à EPM System.

- Vous avez protégé les ressources EPM System répertoriées dans la section [Ressources à protéger](#). Les demandes d'accès aux ressources protégées font l'objet d'un mécanisme de question/réponse de vérification avec Oracle Access Manager.
- Vous avez déprotégé les ressources EPM System répertoriées dans la section [Ressources à déprotéger](#). Les demandes d'accès aux ressources non protégées font l'objet d'un mécanisme de question/réponse de vérification avec Oracle Access Manager.

Pour configurer EPM System pour SSO à partir d'Oracle Access Manager, procédez comme suit :

1. Ajoutez l'annuaire des utilisateurs qu'Oracle Access Manager utilise pour authentifier les utilisateurs en tant qu'annuaire des utilisateurs externe dans EPM System. Reportez-vous à la section "Configuration d'OID, d'Active Directory et d'autres annuaires des utilisateurs LDAP" du *Guide d'administration de la sécurité utilisateur d'Oracle Enterprise Performance Management System*.

 **Remarque :**

Assurez-vous que la case à cocher **Sécurisé** dans l'écran Informations de connexion est sélectionnée pour indiquer que l'annuaire des utilisateurs est une source SSO fiable.

2. Configurez EPM System pour SSO. Reportez-vous à la section [Configuration de EPM System pour l'authentification unique](#).

Sélectionnez Oracle Access Manager dans la liste **Fournisseur ou agent d'authentification unique**. Si l'en-tête HTTP d'Oracle Access Manager utilise un nom différent de `HYPROGIN`, entrez le nom de l'en-tête personnalisé dans la zone de texte en regard de la liste **Mécanisme SSO**.

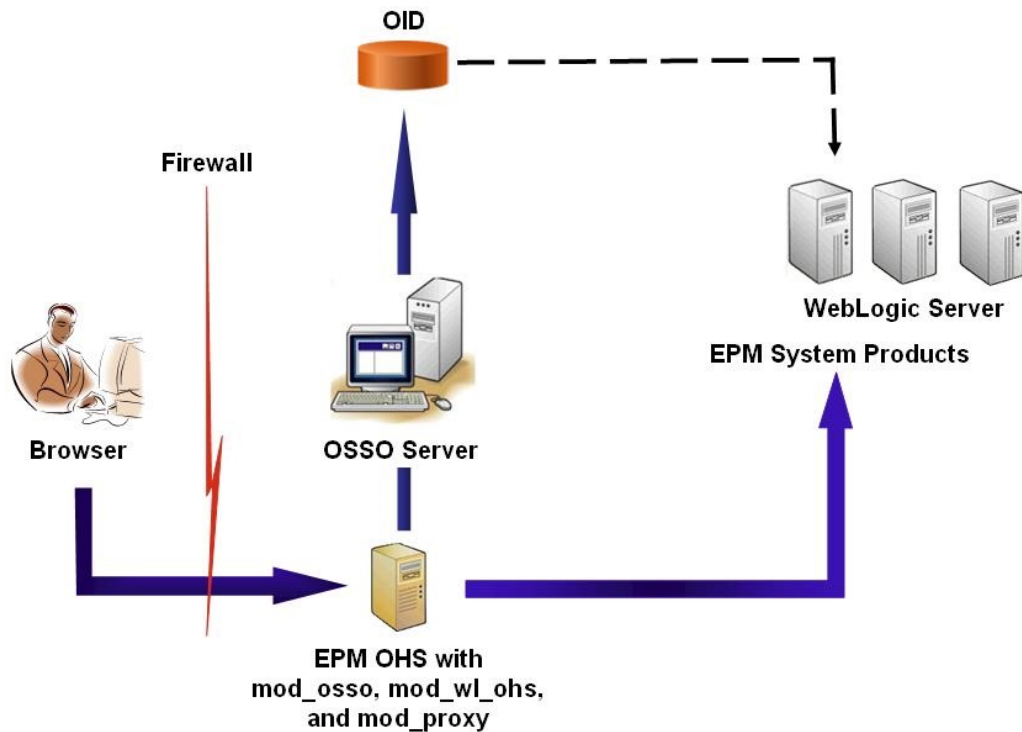
3. Oracle Data Relationship Management uniquement :
  - a. Configurez Data Relationship Management pour l'authentification Shared Services.
  - b. Activez SSO dans la console Data Relationship Management.

Reportez-vous à la documentation Data Relationship Management pour obtenir des informations détaillées.

## Authentification unique OracleAS

La solution OracleAS Single Sign-on (OSSO) fournit un accès SSO aux applications Web en utilisant Oracle Internet Directory (OID) comme annuaire des utilisateurs. Les utilisateurs emploient un nom d'utilisateur et un mot de passe définis dans OID pour se connecter aux produits Oracle Enterprise Performance Management System.

### Flux de processus



Le processus OSSO :

1. A l'aide d'une URL EPM System, par exemple, `http://OSSO_OHS_Server_NAME:OSSO_OHS_Server_PORT/interop/index.jsp`, les utilisateurs accèdent à un composant EPM System qui est défini en tant qu'application protégée OSSO.
2. Etant donné que l'URL est protégée via OSSO, `mod_osso`, déployé sur Oracle HTTP Server, intercepte la demande. A l'aide de `mod_osso`, Oracle HTTP Server recherche un cookie valide. Si aucun cookie valide n'est disponible dans la demande, Oracle HTTP Server redirige les utilisateurs vers le serveur OSSO, qui invite les utilisateurs à fournir des informations d'identification qu'il authentifie par rapport à OID.
3. Le serveur OSSO crée l'élément `obSSOCookie` et redonne le contrôle au module `mod_osso` sur le serveur Oracle HTTP Server qui définit l'élément `obSSOCookie` dans le navigateur. Il redirige également la demande vers la ressource EPM System via `mod_wl_ohs` (Oracle WebLogic Server). Avant de transmettre la demande à une ressource EPM System, Oracle HTTP Server définit l'en-tête `Proxy-Remote-User`, que la sécurité d'EPM System utilise pour activer SSO.
4. Le composant EPM System vérifie que l'utilisateur dont l'identité a été extraite de `Proxy-Remote-User` est présent dans OID. Pour que le processus fonctionne, l'annuaire OID configuré avec le serveur OSSO doit être configuré en tant qu'annuaire des utilisateurs externes dans Oracle Hyperion Shared Services.

### Prérequis

1. Une infrastructure Oracle Application Server entièrement fonctionnelle.  
Pour établir une infrastructure Oracle Application Server, installez et configurez l'infrastructure d'Oracle Identity Management 10.1.4. Assurez-vous qu'OSSO est

activé. L'installation de l'infrastructure d'Oracle Identity Management Infrastructure 10.1.4 inclut les composants suivants afin de prendre en charge OSSO.

- Un serveur OSSO Oracle 10g
- OID, que le serveur OSSO utilise pour valider les informations d'identification. Reportez-vous aux guides suivants :
  - *Guide d'installation d'Oracle Fusion Middleware pour Oracle Identity Management*
  - *Guide de l'administrateur Oracle Fusion Middleware pour Oracle Internet Directory*
- Oracle HTTP Server en tant que serveur frontal pour le serveur OSSO. Cette installation inclut l'élément `mod_osso`, qui vous permet de définir des applications partenaires pour OSSO.

 **Remarque :**

Cette instance Oracle HTTP Server fait partie de l'infrastructure OSSO. Elle n'est pas directement utilisée pour la configuration d'OSSO pour les composants EPM System.

Pendant le processus d'installation, assurez-vous que `mod_osso` est enregistré auprès du serveur OSSO en tant qu'application partenaire.

2. Un déploiement EPM System entièrement fonctionnel.  
Lorsque vous configurez le serveur Web pour les composants EPM System, le configurateur EPM System configure `mod_wl_ohs.conf` sur Oracle HTTP Server pour agir en tant que proxy sur les demandes à WebLogic Server.

## Test du déploiement

Après avoir terminé le déploiement SSL, vérifiez que tout fonctionne.

Pour tester votre déploiement, procédez comme suit :

1. A l'aide d'un navigateur, accédez à l'URL sécurisée Oracle Hyperion Enterprise Performance Management Workspace :

Si vous avez utilisé `epm.myCompany.com` comme alias de serveur pour la communication externe et 4443 comme port SSL, l'URL EPM Workspace est la suivante :

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

2. Dans l'écran de connexion, entrez un nom d'utilisateur et un mot de passe.
3. Cliquez sur **Connexion**.
4. Vérifiez que vous pouvez accéder de manière sécurisée aux composants Oracle Enterprise Performance Management System déployés.

## Activation d'OSSO pour EPM System

Cette section part du principe que vous avez déjà complètement configuré l'infrastructure OSSO. Reportez-vous au *Guide de l'administrateur d'Oracle Application Server*.

## Inscription du serveur Web EPM System en tant qu'application partenaire

L'outil d'inscription SSO Oracle Identity Manager (`ssoreg.sh` ou `ssoreg.bat`) sert à inscrire le serveur Web Oracle Enterprise Performance Management System en tant qu'application partenaire sur l'instance Oracle HTTP Server qui fait office de serveur frontal avec le serveur OSSO.

Exécutez cette procédure sur le serveur hébergeant l'instance Oracle HTTP Server qui fait office de serveur frontal avec le serveur OSSO. Ce processus génère et stocke un fichier `osso.conf` brouillé à l'emplacement de votre choix.

Pour inscrire le serveur Web EPM System en tant qu'application partenaire, procédez comme suit :

1. Ouvrez une console sur le serveur hébergeant l'instance Oracle HTTP Server qui fait office de serveur frontal avec le serveur OSSO et accédez au répertoire `ORACLE_HOME/sso/bin` d'Oracle HTTP Server, par exemple `C:\OraHome_1\sso\bin` (Windows).
2. Exécutez une commande semblable à la suivante avec l'option `-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
```

Le texte ci-dessous explique les paramètres utilisés dans cette commande. Dans cette description, le terme d'application partenaire désigne l'instance Oracle HTTP Server utilisée comme serveur Web EPM System.

- `-site_name` identifie le site Web de l'application partenaire (par exemple, `epm.myCompany.com`).
- `-mod_osso_url` indique l'URL de l'application partenaire, au format `PROTOCOL://HOST_NAME:PORT`. Il s'agit de l'URL à laquelle le serveur Web EPM System accepte les demandes client entrantes (par exemple, `http://epm.myCompany.com:19000`).
- `-config_mod_osso` indique si l'application partenaire utilise `mod_osso`. Vous devez inclure le paramètre `config_mod_osso` pour générer `osso.conf`.
- `-update_mode` indique le mode de mise à jour. Utilisez la valeur par défaut `CREATE` pour générer un nouvel enregistrement.
- `-remote_midtier` indique que l'application partenaire `mod_osso` est à un niveau intermédiaire distant. Utilisez cette option lorsque l'application partenaire est à un autre emplacement `ORACLE_HOME` que le serveur OSSO.
- `-virtualhost` indique que l'URL de l'application partenaire est un hôte virtuel. Utilisez ce paramètre uniquement si vous avez recours à un hôte virtuel. Si vous inscrivez une URL d'application partenaire liée à un hôte virtuel, vous devez définir l'hôte virtuel dans `httpd.conf`. Reportez-vous à [Facultatif : définition de l'hôte virtuel](#).



- `-config_file` indique le chemin de l'emplacement où le fichier `osso.conf` doit être généré.

### Facultatif : définition de l'hôte virtuel

Si vous avez utilisé une URL d'hôte virtuel lors de l'inscription de l'application partenaire, vous devez définir l'hôte virtuel en mettant à jour le fichier `httpd.conf` sur l'instance Oracle HTTP Server utilisée comme serveur Web EPM System.

Pour définir un hôte virtuel, procédez comme suit :

1. A l'aide d'un éditeur de texte, ouvrez `EPM_ORACLE_INSTANCE/httpConfig/ohs/config/OHS/ohs_component/httpd.conf`.
2. Ajoutez une définition semblable à celle ci-dessous. Cette définition suppose que le serveur Web est exécuté sur le serveur virtuel `epm.myCompany.com` sur le port `epm.myCompany.com:19400`. Modifiez les paramètres selon les besoins.

```
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>
```

### Création du fichier `mod_osso.conf`

Créez le fichier `mod_osso.conf` sur l'instance Oracle HTTP Server qui fait office de serveur frontal avec le serveur Web EPM System.

Pour créer le fichier `mod_osso.conf`, procédez comme suit :

1. Créez un fichier à l'aide d'un éditeur de texte.
2. Copiez le contenu suivant dans le fichier et modifiez-le en fonction de l'environnement.

```
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. Dans la définition `<IfModule mod_osso.c>`, incluez des définitions d'emplacement semblables à celles ci-dessous pour identifier chaque ressource que vous voulez protéger avec OSSO.

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

4. Enregistrez le fichier sous le nom `mod_osso.conf`.

#### Déplacement du fichier `osso.conf`

Le processus d'inscription du serveur Web EPM System en tant qu'application partenaire (voir [Inscription du serveur Web EPM System en tant qu'application partenaire](#)) crée un fichier `osso.conf` brouillé à l'emplacement identifié par la directive `-config_file`.

Pour déplacer le fichier `osso.conf`, procédez comme suit :

1. Localisez le fichier `osso.conf` créé lors de l'inscription du serveur Web EPM System en tant qu'application partenaire (voir [Inscription du serveur Web EPM System en tant qu'application partenaire](#)).
2. Copiez le fichier `osso.conf` dans le répertoire (sur l'instance Oracle HTTP Server qui fait office de serveur frontal avec le serveur OSSO) identifié par la propriété `OsoConfigFile` définie dans `mod_osso.conf` (voir [Création du fichier `mod\_osso.conf`](#)).

#### Configuration d'EPM System pour OSSO

Configurez l'instance OID intégrée à la solution OSSO en tant qu'annuaire des utilisateurs externe dans EPM System, puis activez l'authentification unique.

Pour configurer EPM System pour OSSO, procédez comme suit :

1. Configurez l'instance OID utilisée par la solution OSSO comme annuaire des utilisateurs externe. Reportez-vous à la section "Configuration d'OID, d'Active Directory et d'autres annuaires des utilisateurs LDAP" du *Guide d'administration de la sécurité utilisateur d'Oracle Enterprise Performance Management System*.
2. Activez l'authentification unique dans EPM System. [Configuration de EPM System pour l'authentification unique](#)

#### Remarque :

Pour configurer OSSO en tant que solution de gestion des identités, vous devez choisir `Autre` dans **Fournisseur ou agent d'authentification unique**, `En-tête HTTP personnalisé` dans **Mécanisme SSO**, puis saisir le nom de l'en-tête HTTP personnalisé, `Proxy-Remote-User`.

3. Provisionnez au moins un utilisateur OID comme administrateur Oracle Hyperion Shared Services.
4. Redémarrez les produits EPM System et les applications personnalisées qui utilisent les API de sécurité Shared Services.

#### Remarque :

Vérifiez que l'instance OID configurée avec Shared Services est en cours d'exécution avant de lancer les produits EPM System.

### Facultatif : activation des messages de débogage sur le serveur OSSO

Pour enregistrer les messages de débogage sur le serveur OSSO, modifiez `policy.properties`. Les messages de débogage sont écrits dans `ORACLE_HOME/sso/log/ssoServer.log`.

Pour enregistrer les messages de débogage, procédez comme suit :

1. A l'aide d'un éditeur de texte, ouvrez `ORACLE_HOME/sso/conf/policy.properties` (par exemple, `C:\OraHome_1\sso\conf\policy.properties`) sur le serveur OSSO.
2. Définissez la valeur de la propriété `debugLevel` sur `DEBUG`.

```
debugLevel = DEBUG
```

3. Enregistrez et fermez `policy.properties`.

### Facultatif : activation des messages de débogage pour les ressources protégées

Pour enregistrer les messages de débogage OSSO pour les ressources protégées à l'aide de `mod_osso.conf`, modifiez `httpd.conf` sur le serveur Web EPM System. Les messages de débogage sont écrits dans `EPM_ORACLE_INSTANCE/httpConfig/ohs/diagnostics/logs/OHS/ohs_component/ohs_component.log`.

Pour enregistrer les messages de débogage pour les ressources protégées, procédez comme suit :

1. A l'aide d'un éditeur de texte, ouvrez `EPM_ORACLE_INSTANCE/httpConfig/ohs/config/OHS/ohs_component/httpd.conf`.
2. Définissez la valeur de la propriété `OraLogSeverity` sur `TRACE`.

```
OraLogSeverity TRACE:32
```

3. Enregistrez et fermez `httpd.conf`.

## Protection des produits EPM System pour l'authentification unique

Vous devez protéger les ressources Oracle Enterprise Performance Management System de sorte que les demandes SSO en provenance d'utilisateurs soient redirigées vers l'agent de sécurité (OAS, OSSO ou SiteMinder).

Oracle HTTP Server utilise `mod_osso` pour rediriger les utilisateurs vers le serveur OSSO. Les utilisateurs sont redirigés uniquement si les URL qu'ils demandent sont configurées dans `mod_osso` pour être protégées. Reportez-vous à la section [Gestion de la sécurité](#) dans le *Guide de l'administrateur Oracle HTTP Server*.

Pour plus d'informations sur la protection des ressources pour l'authentification unique SiteMinder, reportez-vous à la documentation relative à SiteMinder.

### OAM uniquement : prévention de l'ajout des en-têtes par défaut aux réponses

Par défaut, OAM ajoute deux en-têtes (`Pragma: no-cache` et `Cache-Control: no-cache`) aux URL protégées. Etant donné que ces en-têtes entrent en conflit avec les directives de mise

en cache similaires ajoutées par les applications Web et EPM System, les navigateurs peuvent ne pas mettre en cache le contenu des URL protégées entraînant un ralentissement des performances.

Pour obtenir des informations détaillées sur la procédure permettant d'empêcher l'ajout de ces en-têtes OAM aux réponses, reportez-vous à la rubrique *Réglage des agents OAM* de la section [Réglage des performances d'Oracle Access Management](#) du *guide de l'administrateur Fusion Middleware pour Oracle Access Manager avec Oracle Security Token Service*.

### Ressources à protéger

Le tableau suivant répertorie les contextes devant être protégés. La syntaxe pour la protection d'une ressource (en utilisant `interop` comme exemple) pour OSSO est la suivante :

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

Le paramètre `allow from` (autoriser depuis) spécifie les serveurs à partir desquels la protection du contexte peut être ignorée.

Pour Oracle Hyperion Enterprise Performance Management Workspace et Oracle Hyperion Financial Reporting, vous devez définir uniquement les paramètres indiqués dans l'exemple suivant :

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

**Tableau 3-1 Ressources EPM System à protéger**

| Produit EPM System                     | Contexte à protéger                                                                                  |
|----------------------------------------|------------------------------------------------------------------------------------------------------|
| Oracle Hyperion Shared Services        | <ul style="list-style-type: none"> <li>/interop</li> <li>/interop/.../*</li> </ul>                   |
| EPM Workspace                          | <ul style="list-style-type: none"> <li>/workspace</li> <li>/workspace/.../*</li> </ul>               |
| Financial Reporting                    | <ul style="list-style-type: none"> <li>/hr</li> <li>/hr/.../*</li> </ul>                             |
| Oracle Hyperion Planning               | <ul style="list-style-type: none"> <li>/HyperionPlanning</li> <li>/HyperionPlanning/.../*</li> </ul> |
| Oracle Integrated Operational Planning | <ul style="list-style-type: none"> <li>/interlace</li> <li>/interlace/.../*</li> </ul>               |

**Tableau 3-1 (suite) Ressources EPM System à protéger**

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

**Ressources à déprotéger**

Le tableau suivant répertorie les contextes devant être déprotégés. La syntaxe d'annulation de la protection d'une ressource (à l'aide de `/interop/framework(.*)`, par exemple) pour OSSO est la suivante :

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

```

 allow from all
 satisfy any
</LocationMatch>

```

**Tableau 3-2 Ressources EPM System à déprotéger**

| Produit EPM System | Contextes à déprotéger                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Shared Services    | <ul style="list-style-type: none"> <li>• /interop/framework</li> <li>• /interop/framework*</li> <li>• /interop/framework.*</li> <li>• /interop/framework/.../*</li> <li>• /interop/Audit</li> <li>• /interop/Audit*</li> <li>• /interop/Audit.*</li> <li>• /interop/Audit/.../*</li> <li>• /interop/taskflow</li> <li>• /interop/taskflow*</li> <li>• /interop/taskflow/.../*</li> <li>• /interop/WorkflowEngine</li> <li>• /interop/WorkflowEngine/*</li> <li>• /interop/WorkflowEngine/.../*</li> <li>• /interop/TaskReceiver</li> <li>• /framework/lcm/HSSMigration</li> </ul>                                                        |
| EPM Workspace      | <ul style="list-style-type: none"> <li>• /epmstatic/.../*</li> <li>• /workspace/bpmstatic/.../*</li> <li>• /workspace/static/.../*</li> <li>• /workspace/cache/.../*</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Planning           | <ul style="list-style-type: none"> <li>• /HyperionPlanning/Smartview</li> <li>• /HyperionPlanning/faces/PlanningCentral</li> <li>• /HyperionPlanning/servlet/<br/>HspDataTransfer</li> <li>• /HyperionPlanning/servlet/HspLCMServlet</li> <li>• /HyperionPlanning/servlet/<br/>HspADMServlet/.../*</li> <li>• /HyperionPlanning/servlet/<br/>HspADMServlet/**</li> <li>• /HyperionPlanning/servlet/<br/>HspADMServlet*</li> <li>• /HyperionPlanning/servlet/<br/>HspAppManagerServlet/.../*</li> <li>• /HyperionPlanning/servlet/<br/>HspAppManagerServlet/**</li> <li>• /HyperionPlanning/servlet/<br/>HspAppManagerServlet*</li> </ul> |

Tableau 3-2 (suite) Ressources EPM System à déprotéger

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

Tableau 3-2 (suite) Ressources EPM System à déprotéger

| Produit EPM System                | Contextes à déprotéger                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Integrated Operational Planning   | <ul style="list-style-type: none"> <li>• /interlace/services/</li> <li>• /interlace/services/*</li> <li>• /interlace/services/*</li> <li>• /interlace/services/.../*</li> <li>• /interlace/anteros</li> <li>• /interlace/anteros/*</li> <li>• /interlace/anteros/*</li> <li>• /interlace/anteros/.../*</li> <li>• /interlace/interlace</li> <li>• /interlace/interlace/*</li> <li>• /interlace/interlace/*</li> <li>• /interlace/interlace/.../*</li> <li>• /interlace/WebHelp</li> <li>• /interlace/WebHelp/*</li> <li>• /interlace/WebHelp/*</li> <li>• /interlace/WebHelp/.../*</li> <li>• /interlace/html</li> <li>• /interlace/html/*</li> <li>• /interlace/html/*</li> <li>• /interlace/html/.../*</li> <li>• /interlace/email-book</li> <li>• /interlace/email-book/*</li> <li>• /interlace/email-book/*</li> <li>• /interlace/email-book/.../*</li> </ul> |
| Profitability and Cost Management | <ul style="list-style-type: none"> <li>• /profitability/cesagent</li> <li>• /profitability/lcm</li> <li>• /profitability/control</li> <li>• /profitability/ApplicationListener</li> <li>• /profitability/HPMApplicationListener</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Oracle Essbase                    | <ul style="list-style-type: none"> <li>• /essbase/agent/.../*</li> <li>• /essbase/jet/logout.html</li> <li>• /essbase/jet/.\.(js   css   gif   jpe?g   png)\$</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| FDMEE                             | <ul style="list-style-type: none"> <li>• /aif/services/FDMRuleService</li> <li>• /aif/services/RuleService</li> <li>• /aif/LCMServlet</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## Authentification unique basée sur un en-tête avec des produits de gestion des identités

### Prérequis

- Une instance Oracle Enterprise Performance Management System entièrement configurée. Pour autoriser des utilisateurs, le serveur d'annuaire du produit de gestion des identités doit être configuré dans EPM System en tant qu'annuaire des utilisateurs.



- Un produit de gestion des identités entièrement configuré (Microsoft Azure AD, Okta, etc.) qui prend en charge l'authentification basée sur un en-tête.

Les processus génériques suivants sont impliqués dans la configuration d'EPM System pour l'authentification unique basée sur un en-tête avec un produit de gestion des identités compatible. Les étapes spécifiques nécessaires varient selon le produit utilisé, consultez les manuels de votre produit de gestion des identités pour obtenir les étapes détaillées.

Pour obtenir les étapes détaillées de la configuration de l'authentification basée sur un en-tête avec Oracle Identity Cloud Service, reportez-vous à [Configuration d'EPM System pour l'authentification unique basée sur un en-tête avec Oracle Identity Cloud Service](#).

1. Enregistrez EPM System en tant qu'application d'entreprise dans le produit de gestion des identités. Cette étape permet à l'administrateur de gestion des identités de configurer l'authentification sur l'application d'entreprise, y compris des fonctionnalités telles que l'authentification à plusieurs facteurs.

Utilisez le nom de domaine qualifié complet de la passerelle avec le suffixe `workspace/index.jsp` (exemple : `https://gateway.server.example.com:443/workspace/index.jsp`) en tant qu'URL de l'application d'entreprise pour EPM System.

Configurez l'application d'entreprise EPM System pour propager un en-tête HTTP. Vous pouvez choisir n'importe quel nom d'en-tête non réservé comme nom d'en-tête HTTP. La valeur de l'en-tête doit être la propriété qui identifie de manière unique les utilisateurs EPM System.

2. Installez, configurez et enregistrez une passerelle d'application pour vous assurer que l'application d'entreprise transmet uniquement les demandes authentifiées à EPM System.

Utilisez les paramètres de configuration suivants :

- Nom de domaine qualifié complet du serveur de passerelle (exemple : `gateway.server.example.com:443`) en tant que point d'accès.
- Nom de domaine qualifié complet d'EPM System (exemple : `epm.server.example.com:443`) en tant que ressource à laquelle les demandes HTTP(S) authentifiées doivent être transmises.

3. Activez l'authentification unique dans EPM System pour respecter les en-têtes HTTP(S) propagés par la passerelle d'application. Pour obtenir des informations détaillées, reportez-vous à [Configuration des options de sécurité](#).

Pour activer l'authentification unique, procédez comme suit :

- a. Accédez à la console Oracle Hyperion Shared Services en tant qu'administrateur système. Reportez-vous à la section [Lancement de Shared Services Console](#).
- b. Sélectionnez **Administration**, puis **Configurer les annuaires des utilisateurs**.
- c. Cliquez sur **Options de sécurité**.
- d. Dans la section **Configuration de l'authentification unique**, procédez comme suit :
  - i. Cochez la case **Activer l'authentification unique**.
  - ii. Dans la liste déroulante **Fournisseur ou agent d'authentification unique**, sélectionnez **Autre**.
  - iii. Dans la liste déroulante **Mécanisme SSO**, sélectionnez **En-tête HTTP personnalisé**, puis indiquez le nom de l'en-tête transmis par l'agent de sécurité à EPM System.
- e. Cliquez sur **OK**.

4. Mettez à jour le paramètre d'URL post-déconnexion d'Oracle Hyperion Enterprise Performance Management Workspace avec celui de la page Web que les utilisateurs doivent voir lorsqu'ils se déconnectent d'EPM System. Pour mettre à jour le paramètre d'URL post-déconnexion dans EPM Workspace, procédez comme suit :
  - a. Accédez à EPM Workspace en tant qu'administrateur système. Reportez-vous à la section [Accès à EPM Workspace](#).
  - b. Sélectionnez **Naviguer**, puis **Paramètres Workspace**, puis **Paramètres du serveur**.
  - c. Dans **Paramètres du serveur Workspace**, remplacez l'**URL post-déconnexion** par celle de la page Web que les utilisateurs doivent voir lorsqu'ils se déconnectent d'EPM System.
  - d. Cliquez sur **OK**.
5. Redémarrez Oracle Hyperion Foundation Services et tous les serveurs gérés EPM System.

## Configuration d'EPM System pour l'authentification unique basée sur un en-tête avec Oracle Identity Cloud Service

Dans ce scénario, Oracle Identity Cloud Service authentifie les utilisateurs d'Oracle Enterprise Performance Management System et propage les en-têtes HTTP requis pour l'activation de l'authentification unique.

Cette section présente les étapes nécessaires à la configuration d'EPM System pour la prise en charge de l'authentification unique avec Oracle Identity Cloud Service. Vous pouvez suivre ces instructions pour activer la prise en charge de l'authentification basée sur un en-tête d'EPM System avec tous les systèmes de gestion des identités (par exemple, Azure AD) ou les fournisseurs Infrastructure-as-a-Service (IaaS) qui prennent en charge ce type d'authentification.

Le workflow conceptuel est le suivant :

- Une application de passerelle faisant office de proxy inverse protège les composants EPM System en limitant l'accès au réseau non authentifié.
- L'application de passerelle intercepte les demandes HTTP(S) aux composants EPM System et vérifie que le produit de gestion des identités authentifie les utilisateurs avant de transmettre les demandes aux composants EPM System.
- Lors du transfert des demandes aux composants EPM System, l'application de passerelle propage l'identité de l'utilisateur authentifié au composant EPM System via des demandes d'en-tête HTTP.

### Prérequis et exemples d'URL

Pour établir l'authentification unique basée sur un en-tête avec Oracle Identity Cloud Service, les prérequis sont les suivants :

- Une instance Oracle Enterprise Performance Management System entièrement configurée.

- Un hôte ou conteneur avec une passerelle d'application Oracle entièrement configurée, qui sert de proxy inverse pour protéger EPM System en limitant les accès non autorisés. Une passerelle d'application Oracle doit être configurée pour intercepter les demandes HTTP vers les composants EPM System et vérifier que les utilisateurs sont authentifiés par Oracle Identity Cloud Service avant la transmission des demandes à EPM System. Lors de l'envoi des demandes aux composants EPM System, une passerelle d'application Oracle doit propager l'identité de l'utilisateur authentifié via des demandes d'en-tête HTTP.
- Un accès en tant qu'administrateur de domaine à Oracle Identity Cloud Service.

Les exemples d'URL suivants sont utilisés dans cette discussion :

- URL de base du nom de domaine qualifié complet du serveur d'Oracle Identity Cloud Service (fournisseur d'identités) :  
`https://identity.server.example.com:443/`
- Nom de domaine qualifié complet du serveur de la passerelle d'application Oracle (qui héberge l'application de passerelle) :  
`https://gateway.server.example.com:443/`
- URL d'application d'entreprise pour EPM System. Il s'agit du nom de domaine qualifié complet du serveur de passerelle d'application Oracle avec le suffixe `workspace/index.jsp` :  
`https://gateway.server.example.com:443/workspace/index.jsp`



#### Note:

Oracle Identity Cloud Service et la passerelle d'application Oracle sont configurés avec la prise en charge HTTPS. La prise en charge HTTPS pour EPM System est facultative.

Il est supposé ici qu'EPM System a été configuré avec la prise en charge HTTPS.

## Activation de l'authentification basée sur un en-tête pour EPM System

L'activation de l'authentification basée sur un en-tête pour Oracle Enterprise Performance Management System nécessite les étapes suivantes :

- [Ajout d'une application EPM System et d'une passerelle vers Oracle Identity Cloud Service](#)
- [Configuration de la passerelle d'application](#)
- [Configuration de l'annuaire des utilisateurs pour l'autorisation](#)
- [Activation de l'authentification unique dans EPM System](#)
- [Mise à jour des paramètres EPM Workspace](#)

## Ajout d'une application EPM System et d'une passerelle vers Oracle Identity Cloud Service

Pour configurer l'authentification basée sur un en-tête, vous devez créer une instance Oracle Enterprise Performance Management System en tant qu'application d'entreprise.

## Ajout d'EPM System en tant qu'application d'entreprise dans la console de gestion des identités Oracle Cloud

Pour ajouter EPM System en tant qu'application d'entreprise, procédez comme suit :

1. Accédez à la console de gestion des identités Oracle Cloud en tant qu'administrateur de domaine.
  - a. A l'aide d'un navigateur, accédez à <https://www.oracle.com/cloud/sign-in.html>.
  - b. Entrez le nom de votre compte Oracle Fusion Cloud EPM.
  - c. Sur la page de connexion au compte Oracle Fusion Cloud EPM, entrez votre nom d'utilisateur et votre mot de passe, puis cliquez sur **Connexion**.
  - d. Dans le **volet de navigation**, cliquez sur **Utilisateurs**, puis sur **Identité (principale)**.
  - e. Cliquez sur **Console de gestion des identités**.
2. Ajoutez EPM System en tant qu'application d'entreprise.
  - a. Dans le volet de navigation, cliquez sur **Applications**.
  - b. Cliquez sur **Ajouter**, puis sur **Application d'entreprise**.

The screenshot shows the Oracle Identity Cloud Service console interface for adding an enterprise application. The left sidebar contains navigation options: Dashboard, Users, Groups, Applications (selected), Oracle Cloud Services, Jobs, Reports, Settings, and Security. The main content area is titled 'Add Enterprise Application' and features a progress indicator with three steps: 1. Details (active), 2. OAuth Configuration, and 3. SSO Configuration. The 'Details' section includes the following fields:

- Name:** EPM System
- Description:** On-Premises EPM 11.2
- Application Icon:** A default icon is shown with an 'Upload' button below it.
- Application URL:** r.example.com:443/workspace/index.jsp
- Custom Login URL:** (empty)
- Custom Logout URL:** (empty)
- Custom Error URL:** (empty)
- Linking callback URL:** (empty)

Below the form, there is a 'Tags' section with the instruction: 'Add tags to your applications to organize and identify them. A tag consists of a key-value pair.' and an 'Add Tag' button. The 'Settings' section at the bottom contains three checkboxes:

- Display in My Apps
- User can request access
- User must be granted the app

3. Ajoutez les détails de l'application comme suit :
  - a. Dans **Nom**, entrez un nom unique pour identifier l'application d'entreprise EPM System.

- b. Entrez une description facultative.
  - c. Chargez éventuellement une icône d'application pour EPM System. Cliquez sur **Télécharger** pour sélectionner et télécharger l'icône.
  - d. Dans **URL d'application**, entrez l'URL de lancement vers laquelle la passerelle doit rediriger les utilisateurs. L'URL est le nom de domaine qualifié complet de la passerelle d'application Oracle avec le suffixe `workspace/index.jsp`, qui est le contexte de l'application EPM System.
  - e. Sous **Paramètres**, sélectionnez **Afficher dans Mes applications** pour afficher l'application d'entreprise EPM System sur l'onglet **Configuration SSO** de la page **Mes applications** dans la console de gestion des identités Oracle Cloud.
  - f. Cliquez sur **Suivant**.
4. Indiquez les détails de configuration de l'authentification unique.
    - a. Cliquez sur **Configuration SSO**.
    - b. Ajoutez une ressource pour l'application d'entreprise. Dans **Configuration SSO**, développez **Ressources**.
      - i. Cliquez sur **Ajouter**.

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

- Resource Name:** A text input field containing the value "EPM".
- Resource URL:** A text input field containing the value "/\*".
- 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.

An "OK" button is located at the bottom right of the dialog box.

- ii. Indiquez un nom de ressource unique.
  - iii. Dans **URL de ressource**, entrez `/*`.
  - iv. Cochez la case **Expression régulière**.
  - v. Cliquez sur **OK**.
  - vi. Dans **Configuration SSO**, développez **Ressources**.
- c. Ajoutez une stratégie d'authentification. Dans **Configuration SSO**, développez **Stratégie d'authentification**.
    - i. Cochez les cases **Autoriser CORS** et **Exiger des cookies sécurisés**.

- ii. Cliquez sur **Ajouter** sous **Ressources gérées** et définissez **Formulaire ou jeton d'accès** en tant que méthode d'authentification pour la ressource d'authentification unique.

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

- Resource:** A text input field containing "EPM".
- Authentication Method:** A dropdown menu showing "Form or Access Token".
- Authentication Method Overrides:** A plus sign (+) icon.
- Headers:** A plus sign (+) icon.
- Header Table:** A table with two columns: "Name" and "Value". One row is visible with "Name" as "HYPLOGIN" and "Value" as "Work Email".
- Buttons:** An "Add" button at the bottom right and a close (X) button at the top right.

- iii. Dans **Ressource**, sélectionnez la ressource d'authentification unique que vous avez ajoutée à l'étape précédente.
  - iv. Développez **En-têtes**.
  - v. Entrez le nom de l'en-tête HTTP qui sera propagé vers EPM System. Le nom d'en-tête d'authentification par défaut est `HYPLOGIN`. Vous pouvez utiliser le nom de votre choix.
  - vi. Dans **Valeur**, sélectionnez la propriété qui identifie de manière unique les utilisateurs d'EPM System. La valeur de ce champ doit correspondre à l'identité de l'utilisateur dans EPM System. Par exemple, si l'identité de l'utilisateur dans EPM System est l'adresse électronique, sélectionnez Adresse électronique professionnelle comme valeur.
  - vii. Cliquez sur **Enregistrer**.
5. Cliquez sur **Terminer** pour créer l'application d'entreprise.
  6. Cliquez sur **Activer** pour activer l'application.
  7. Enregistrez une passerelle d'application, et configurez l'hôte et l'application pour EPM System.
    - a. Dans le **volet de navigation**, cliquez sur **Sécurité**, puis sur **Passerelles d'application**.
    - b. Cliquez sur **Ajouter**.
    - c. Dans **Détails**, entrez un nom unique pour la passerelle et éventuellement une description.
    - d. Cliquez sur **Suivant** pour ouvrir l'écran Hôtes.
    - e. Ajoutez un hôte de passerelle d'application pour EPM System.
      - i. Dans l'écran Hôtes, cliquez sur **Ajouter**.

The screenshot shows a dialog box titled "Add Host" with the following fields and values:

- 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;
```

A green "Save" button is located at the bottom right of the dialog.

- ii. Dans **Identificateur d'hôte**, entrez EPMAppGateway.
- iii. Dans **Hôte**, entrez le nom de domaine qualifié complet de l'ordinateur qui héberge le serveur de passerelle d'application, par exemple, gateway.server.example.com.
- iv. Dans **Port**, entrez le port sur lequel le serveur de passerelle d'application répond aux demandes HTTPS.
- v. Cochez la case **SSL activé**.
- vi. Dans **Propriétés supplémentaires**, entrez les éléments suivants :
  - Emplacement du certificat SSL
  - Clé du certificat SSL
  - Fichier de mots de passe SSL (le cas échéant)

Pour plus d'informations, reportez-vous à la rubrique [Enregistrement d'une passerelle d'application](#) de la section "Configuration d'une passerelle d'application" du guide *Administration d'Oracle Identity Cloud Service*.
- vii. Cliquez sur **Enregistrer**.
- viii. Cliquez sur **Suivant** pour ouvrir l'écran Applications.
- f. Ajoutez l'application d'entreprise EPM System à la passerelle d'application.
  - i. Sur **Applications**, cliquez sur **Ajouter**.
  - ii. Dans **Application**, sélectionnez l'application d'entreprise EPM System que vous avez précédemment ajoutée à la console de gestion des identités Oracle Cloud.

- iii. Dans **Sélectionner un hôte**, sélectionnez EPMAAppGateway (l'hôte EPM System que vous avez ajouté à la passerelle d'application).
  - iv. Dans **Préfixe de ressource**, saisissez / pour transmettre toutes les demandes à l'hôte EPM System.
  - v. Dans **Serveur d'origine**, entrez le nom de domaine qualifié complet de l'ordinateur qui héberge Oracle Hyperion Enterprise Performance Management Workspace et le numéro du port qu'EPM Workspace utilise.
  - vi. Cliquez sur **Enregistrer**.
8. Enregistrez l'ID et la clé secrète du client de la passerelle d'application. Ces valeurs sont requises pour configurer la passerelle d'application.
    - a. Dans le **volet de navigation**, cliquez sur **Sécurité**, puis sur **Passerelles d'application**.
    - b. Cliquez sur le nom de la passerelle que vous avez ajoutée pour l'application d'entreprise EPM System.
    - c. Copiez l'ID du client (chaîne alphanumérique) dans un éditeur de texte.
    - d. Cliquez sur **Afficher la clé secrète** pour afficher le code secret du client.
    - e. Copiez la clé secrète du client (chaîne alphanumérique) dans un éditeur de texte.
    - f. Enregistrez le fichier texte.

 **Note:**

Vous devez redémarrer le serveur de passerelle d'application chaque fois qu'une mise à jour de configuration est appliquée à Oracle Identity Cloud Service. Pour démarrer et arrêter le serveur de passerelle d'application, reportez-vous à la section [Démarrage et arrêt d'une passerelle d'application](#).



## Configuration de la passerelle d'application

Pour obtenir des informations détaillées, reportez-vous à la section [Configuration d'une passerelle d'application](#) de l'*Administration d'Oracle Identity Cloud Service*.

Vous aurez besoin de l'ID et de la clé secrète de client que vous avez enregistrés dans la section précédente pour configurer le serveur de passerelle d'application.

## Configuration de l'annuaire des utilisateurs pour l'autorisation

Certains produits de gestion des identités, par exemple Oracle Identity Cloud Service et Microsoft Azure, ne peuvent pas être directement configurés en tant qu'annuaires des utilisateurs dans Oracle Enterprise Performance Management System. Vous pouvez configurer ces produits avec Oracle Unified Directory ou Oracle Virtual Directory, puis configurer ce dernier en tant qu'annuaire des utilisateurs dans EPM System. Afin d'obtenir les étapes détaillées pour la configuration d'annuaires des utilisateurs, reportez-vous à [Configuration des annuaires des utilisateurs](#).

## Activation de l'authentification unique dans EPM System

Vous configurez des options de sécurité dans Oracle Enterprise Performance Management System pour activer l'authentification unique. Pour des instructions détaillées, reportez-vous à [Configuration des options de sécurité](#).

Pour activer l'authentification unique, procédez comme suit :

1. Accédez à la console Oracle Hyperion Shared Services en tant qu'administrateur système. Reportez-vous à [Lancement de Shared Services Console](#).
2. Sélectionnez **Administration**, puis **Configurer les annuaires des utilisateurs**.
3. Cliquez sur **Options de sécurité**.
4. Dans la section **Configuration de l'authentification unique**, procédez comme suit :
  - a. Cochez la case **Activer l'authentification unique**.
  - b. Dans la liste déroulante **Fournisseur ou agent d'authentification unique**, sélectionnez **Autre**.
  - c. Dans la liste déroulante **Mécanisme SSO**, sélectionnez **En-tête HTTP personnalisé**, puis indiquez le nom de l'en-tête transmis par l'agent de sécurité à EPM System (`HYPLOGIN` ou le nom personnalisé que vous avez indiqué lors de l'ajout d'une ressource pour l'application d'entreprise dans la console de gestion des identités Oracle Cloud).
5. Cliquez sur **OK**.

### Note:

Veillez à redémarrer tous les services EPM System après chaque modification de configuration SSO.

## Mise à jour des paramètres EPM Workspace

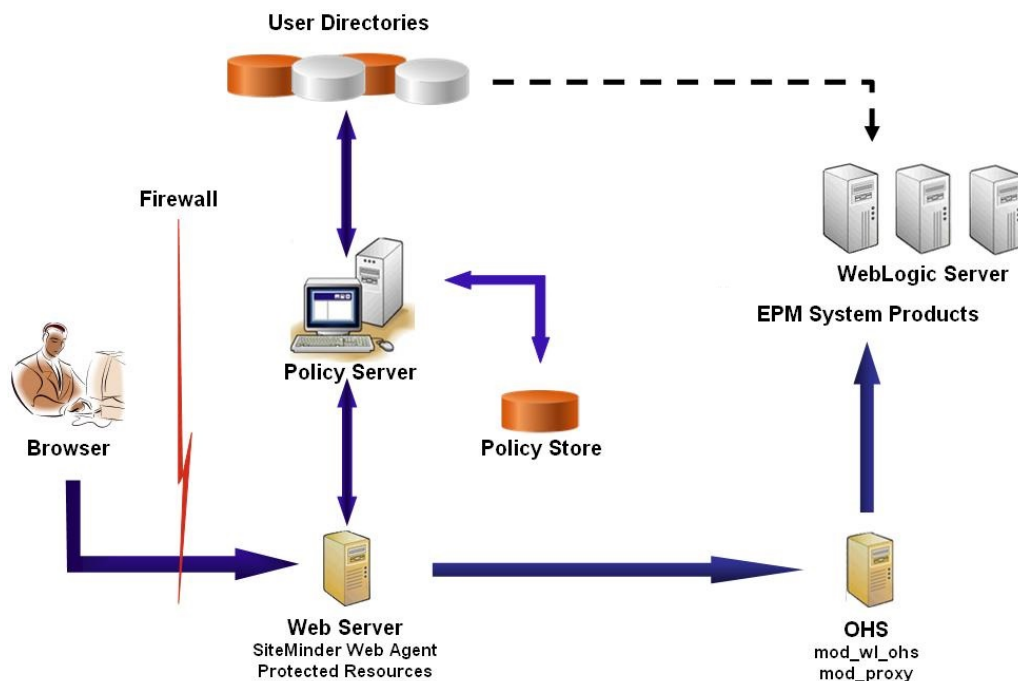
1. Accédez à Oracle Hyperion Enterprise Performance Management Workspace en tant qu'administrateur système. Reportez-vous à [Accès à EPM Workspace](#).
2. Sélectionnez **Naviguer**, puis **Paramètres Workspace**, puis **Paramètres du serveur**.
3. Dans **Paramètres du serveur Workspace**, remplacez l'**URL post-déconnexion** par celle de la page Web que les utilisateurs doivent voir lorsqu'ils se déconnectent d'Oracle Enterprise Performance Management System.
4. Cliquez sur **OK**.
5. Redémarrez Oracle Hyperion Foundation Services et tous les composants EPM System.

## Authentification unique SiteMinder

SiteMinder est une solution Web uniquement. Les applications de bureau et leurs compléments (par exemple, Microsoft Excel et Concepteur de rapports) ne peuvent pas utiliser l'authentification via SiteMinder. Toutefois, Oracle Smart View for Office peut utiliser une authentification SiteMinder.

### Flux de processus

Présentation illustrée de l'activation SSO pour SiteMinder



Le processus SSO pour SiteMinder :

1. Les utilisateurs tentent d'accéder à une ressource Oracle Enterprise Performance Management System protégée par SiteMinder. Ils utilisent une URL qui les

connecte au serveur Web faisant office de serveur frontal pour le serveur de stratégie SiteMinder, par exemple `http://`

`WebAgent_Web_Server_Name:WebAgent_Web_ServerPort/interop/index.jsp.`

2. Le serveur Web redirige les utilisateurs vers le serveur de stratégie qui invite les utilisateurs à fournir des informations d'identification. Après avoir vérifié les informations d'identification par rapport aux annuaires des utilisateurs configurés, le serveur de stratégie les transmet au serveur Web qui héberge l'agent Web SiteMinder.
3. Le serveur Web qui héberge l'agent Web SiteMinder redirige la demande vers le serveur Oracle HTTP Server qui fait office de serveur frontal pour EPM System. Oracle HTTP Server redirige les utilisateurs vers l'application demandée, déployée sur Oracle WebLogic Server.
4. Le composant EPM System vérifie les informations de provisionnement et transmet le contenu. Pour que ce processus fonctionne, les annuaires des utilisateurs utilisés par SiteMinder pour authentifier les utilisateurs doivent être configurés en tant qu'annuaires des utilisateurs externes dans EPM System. Ces annuaires doivent être configurés en tant que source sécurisée.

### Remarques particulières

SiteMinder est une solution Web uniquement. Les applications de bureau et leurs compléments (par exemple, Microsoft Excel et Concepteur de rapports) ne peuvent pas utiliser l'authentification via SiteMinder. Toutefois, Smart View peut utiliser une authentification SiteMinder.

### Prérequis

1. Une installation SiteMinder entièrement fonctionnelle comprenant les composants suivants :
  - Un serveur de stratégie SiteMinder sur lequel les stratégies et les objets d'agent sont définis
  - Un agent Web SiteMinder installé sur le serveur Web faisant office de serveur frontal pour le serveur de stratégie SiteMinder
2. Un déploiement EPM System entièrement fonctionnel.  
Lorsque vous configurez le serveur Web pour les composants EPM System, le configurateur EPM System configure `mod_wl_ohs.conf` pour les demandes proxy du serveur WebLogic.

### Activation de l'agent Web SiteMinder

L'agent Web est installé sur un serveur Web qui intercepte les demandes de ressources EPM System. Les tentatives d'accès à des ressources EPM System protégées par des utilisateurs non authentifiés force l'agent Web à inviter les utilisateurs à fournir des informations d'identification SSO. Lorsqu'un utilisateur est authentifié, le serveur de stratégies ajoute le nom de connexion de l'utilisateur authentifié, qui est contenu dans l'en-tête. Ensuite, la demande HTTP est transmise au serveur Web EPM System, qui redirige les demandes. Les composants EPM System extraient les informations d'identification des utilisateurs authentifiés à partir des en-têtes.

SiteMinder prend en charge l'authentification unique entre les produits EPM System en cours d'exécution sur des plates-formes de serveur Web hétérogènes. Si les produits EPM System utilisent des serveurs Web différents, vous devez vous assurer que le cookie SiteMinder peut être transmis entre les serveurs Web du même domaine. Pour ce faire, vous spécifiez le

domaine d'application EPM System approprié comme valeur de la propriété `Cookiedomain` dans le fichier `WebAgent.conf` de chaque serveur Web.

Reportez-vous à la section "Configuration des agents Web" dans le *Guide de l'agent Netegrity SiteMinder*.

 **Remarque :**

Etant donné qu'Oracle Hyperion Shared Services utilise l'authentification de base pour protéger son contenu, le serveur Web qui intercepte les demandes à Shared Services doit activer l'authentification de base pour prendre en charge SSO avec SiteMinder.

Vous configurez l'agent Web en exécutant l'assistant de configuration de l'agent Web SiteMinder (en exécutant `WEBAGENT_HOME/install_config_info/nete-wa-config`, par exemple, `C:\netegrity\webagent\install_config_info\nete-wa-config.exe` sur Windows). Le processus de configuration crée un élément `WebAgent.conf` pour le serveur Web SiteMinder.

Pour activer l'agent Web SiteMinder, procédez comme suit :

1. A l'aide d'un éditeur de texte, ouvrez le fichier `WebAgent.conf`. L'emplacement de ce fichier dépend du serveur Web que vous utilisez.
2. Définissez la valeur de la propriété `enableWebAgent` sur `Yes`.  
`enableWebAgent="YES"`
3. Enregistrez et fermez le fichier de configuration de l'agent Web.

### Exemple 3-1 Configuration du serveur de stratégie SiteMinder

Un administrateur SiteMinder doit configurer le serveur de stratégies pour activer l'authentification unique aux produits EPM System.

Le processus de configuration implique les opérations suivantes :

- Créer un agent Web SiteMinder et ajouter les objets de configuration adéquats pour le serveur Web SiteMinder.
- Créer un domaine pour chaque ressource EPM System qui doit être protégée et ajouter l'agent Web au domaine. Reportez-vous à la section [Ressources à protéger](#).
- Dans le domaine créé pour les ressources EPM System protégées, créer des domaines pour les ressources non protégées. Reportez-vous à la section [Ressources à déprotéger](#).
- Créer une référence d'en-tête HTTP. L'en-tête doit fournir la valeur `Attribut de connexion` aux applications EPM System. Reportez-vous à la section "Configuration d'OID, d'Active Directory et d'autres annuaires des utilisateurs LDAP" du *Guide d'administration de la sécurité utilisateur d'Oracle Enterprise Performance Management System* pour obtenir une brève description de la valeur `Attribut de connexion`.
- Créer des règles dans les domaines avec `Get`, `Post` et `Put` comme actions d'agent Web.

- Créer un attribut de réponse avec `hyplogin=<%userattr="SM_USERLOGINNAME"%>` en tant que valeur.
- Créer une stratégie, affecter l'accès à l'annuaire des utilisateurs et ajouter les règles que vous avez créées pour EPM System à la liste Membres en cours.
- Définir les réponses pour les règles que vous avez créées pour les composants EPM System

### Exemple 3-2 Configuration du serveur Web SiteMinder pour transmettre les demandes au serveur Web EPM System

Configurez le serveur Web qui héberge l'agent Web SiteMinder pour transmettre les demandes provenant d'utilisateurs authentifiés (qui contiennent l'en-tête identifiant l'utilisateur) au serveur Web EPM System.

Pour les serveurs Web Apache, utilisez des directives semblables à ce qui suit pour transmettre les demandes authentifiées :

```
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
```

Dans cette directive, remplacez `EPM_WEB_SERVER` et `EPM_WEB_SERVER_PORT` par les valeurs réelles correspondant à votre environnement.

### Exemple 3-3 Activation de SiteMinder dans EPM System

L'intégration avec SiteMinder exige que vous activiez l'authentification de SiteMinder pour les produits EPM System. Reportez-vous à la section [Configuration de EPM System pour l'authentification unique](#).

## Authentification unique Kerberos

### Présentation

Les produits Oracle Enterprise Performance Management System prennent en charge l'authentification unique Kerberos si le serveur d'applications qui héberge les produits EPM System est configuré pour l'authentification Kerberos.

Kerberos est un service d'authentification sécurisé dans lequel chaque client Kerberos approuve les identités d'autres clients Kerberos (utilisateurs, services réseau, etc.).

Voici ce qui se produit lorsqu'un utilisateur accède à un produit EPM System :

1. Sur un ordinateur Windows, l'utilisateur se connecte à un domaine Windows, qui est également un domaine de sécurité Kerberos.
2. A l'aide d'un navigateur configuré pour utiliser Integrated Windows Authentication, l'utilisateur essaie de se connecter aux produits EPM System en cours d'exécution sur le serveur d'applications.
3. Le serveur d'applications (asserteur de négociation d'identités) intercepte la demande et obtient le jeton SPNEGO (mécanisme de négociation simple et protégé) de l'API Generic Security Services (GSSAPI) avec le ticket Kerberos issu de l'en-tête d'autorisation du navigateur.

4. L'asserteur valide l'identité de l'utilisateur incluse dans le jeton à l'aide de sa banque d'identités, afin de transmettre les informations relatives à cet utilisateur au produit EPM System. Le produit EPM System valide le nom d'utilisateur à l'aide d'un annuaire Active Directory. Le produit EPM System émet un jeton SSO qui prend en charge l'authentification unique sur tous les produits EPM System.

### Limites de la prise en charge

L'authentification unique Kerberos est prise en charge pour tous les produits EPM System, sauf dans les cas suivants:

- L'authentification unique Kerberos n'est pas prise en charge sur les clients lourds autres qu'Oracle Smart View for Office.
- Smart View prend en charge l'intégration Kerberos pour les fournisseurs Oracle Essbase, Oracle Hyperion Planning et Oracle Hyperion Financial Management uniquement.

### Hypothèses

Ce document, qui contient les étapes de configuration de Kerberos au niveau de l'application, requiert des connaissances préalables quant à la configuration de Kerberos au niveau du système. Avant de commencer ces procédures, confirmez que les prérequis de ces tâches sont remplis.

Ce document suppose que vous travaillez dans un environnement réseau complètement fonctionnel et compatible avec Kerberos, dans lequel les machines clientes Windows sont configurées pour l'authentification Kerberos.

- L'annuaire Active Directory de l'entreprise est configuré pour l'authentification Kerberos. Reportez-vous à [Documentation de Microsoft Windows Server](#).
- Les navigateurs utilisés pour accéder aux produits EPM System sont configurés pour négocier à l'aide de tickets Kerberos.
- Synchronisation temporelle avec un décalage maximal de cinq minutes entre KDC et les machines clientes. Reportez-vous à la section "Authentication Errors are Caused by Unsynchronized Clocks" (Erreurs d'authentification causées par des horloges non synchronisées) sur [http://technet.microsoft.com/en-us/library/cc780011\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc780011(WS.10).aspx).

### Authentification unique Kerberos avec WebLogic Server

L'authentification unique Kerberos avec Oracle WebLogic Server utilise l'asserteur de négociation d'identités pour négocier et décoder les jetons SPNEGO afin d'activer l'authentification unique avec les clients Microsoft. WebLogic Server décode les jetons SPNEGO pour obtenir un ticket Kerberos, puis valide ce ticket et le mappe avec un utilisateur WebLogic Server. Vous pouvez utiliser l'authentificateur Active Directory de WebLogic Server avec l'asserteur de négociation d'identités afin de configurer Active Directory comme annuaire pour les utilisateurs WebLogic Server.

Lorsque le navigateur demande l'accès à un produit EPM System, KDC envoie un ticket Kerberos au navigateur, qui crée un jeton SPNEGO contenant les types de jeton GSS pris en charge. L'asserteur de négociation d'identités décode le jeton SPNEGO et utilise les API GSS pour accepter le contexte de sécurité. L'identité de l'utilisateur à l'origine de la requête est mappée sur un nom d'utilisateur et renvoyée au serveur WebLogic. Par ailleurs, WebLogic Server détermine les groupes auxquels appartient l'utilisateur. A ce stade, le produit EPM System demandé devient disponible pour l'utilisateur.

 **Remarque :**

Les utilisateurs doivent disposer d'un navigateur qui prend en charge SPNEGO (par exemple, Internet Explorer ou Firefox) pour accéder aux produits EPM System en cours d'exécution sur WebLogic Server.

A l'aide de l'ID utilisateur dérivé du processus d'authentification, le processus d'autorisation du produit EPM System vérifie les données de provisionnement. L'accès au produit EPM System est restreint en fonction des données de provisionnement.

### Procédures WebLogic Server permettant de prendre en charge l'authentification Kerberos

Un administrateur doit réaliser ces tâches pour permettre la prise en charge de l'authentification Kerberos :

- Créez le domaine WebLogic pour EPM System. Reportez-vous à la section [Création du domaine WebLogic pour EPM System](#).
- Créez un fournisseur d'authentification. Reportez-vous à la section [Création d'un fournisseur d'authentification LDAP dans WebLogic Server](#).
- Créez un asserteur de négociation d'identités. Reportez-vous à la section [Création d'un asserteur de négociation d'identités](#).
- Créez une identification Kerberos. Reportez-vous à la section [Création de l'identification Kerberos pour WebLogic Server](#).
- Mettez à jour les options de JVM pour Kerberos. Reportez-vous à la section [Mise à jour des options de JVM pour Kerberos](#).
- Configurez les stratégies d'autorisation. Reportez-vous à la section [Configuration des stratégies d'autorisation](#).
- Déployez et utilisez SSODiag pour vérifier que WebLogic Server est prêt à prendre en charge l'authentification Kerberos pour EPM System. Reportez-vous à la section [Utilisation de SSODiag pour tester l'environnement Kerberos](#).

#### Création du domaine WebLogic pour EPM System

En règle générale, les composants EPM System sont déployés dans le domaine WebLogic EPMSystem (l'emplacement par défaut est `MIDDLEWARE_HOME/user_projects/domains/EPMSystem`).

Pour configurer le domaine WebLogic EPM System pour l'authentification Kerberos, procédez comme suit :

1. Installez les composants EPM System.
2. Déployez Oracle Hyperion Foundation Services uniquement.  
Le déploiement Foundation Services crée le domaine WebLogic EPM System par défaut.
3. Connectez-vous à Oracle Hyperion Shared Services Console pour vérifier que le déploiement Foundation Services a été effectué. Reportez-vous à la section [Lancement de Shared Services Console](#).

### Création d'un fournisseur d'authentification LDAP dans WebLogic Server

Un administrateur WebLogic Server crée le fournisseur d'authentification LDAP, qui stocke les informations sur les utilisateurs et les groupes sur un serveur LDAP externe. Les serveurs compatibles LDAP v2 ou v3 fonctionnent avec WebLogic Server. Reportez-vous aux références suivantes :

- [Configuration des fournisseurs d'authentification LDAP](#) dans le *guide Oracle Fusion Middleware sur la sécurisation d'Oracle WebLogic Server*.
- [Configuration des fournisseurs d'authentification et d'assertion d'identité](#) dans l'*aide en ligne Oracle Fusion Middleware sur la console d'administration d'Oracle WebLogic Server*.

### Création d'un asserteur de négociation d'identités

Le fournisseur d'assertion de négociation d'identités active l'authentification unique avec les clients Microsoft. Il décode les jetons SPNEGO pour obtenir des jetons Kerberos, valide les jetons Kerberos et les mappe avec les utilisateurs WebLogic. Le fournisseur d'assertion de négociation d'identités, implémentation de l'interface du fournisseur de services de sécurité (SSPI) comme défini dans la structure de sécurité WebLogic, fournit la logique requise pour l'authentification d'un client à l'aide de son jeton SPNEGO.

- [Configuration d'un fournisseur d'assertion de négociation d'identités](#) dans le *guide Oracle Fusion Middleware sur la sécurisation d'Oracle WebLogic Server*.
- [Configuration des fournisseurs d'authentification et d'assertion d'identité](#) dans l'*aide en ligne Oracle Fusion Middleware sur la console d'administration d'Oracle WebLogic Server*.

Lors de la création d'un fournisseur d'assertion de négociation d'identités, définissez l'option d'indicateur de contrôle JAAS sur `SUFFICIENT` pour tous les éléments d'authentification. Reportez-vous à la section "[Définir l'indicateur de contrôle JAAS](#)" dans l'[Aide en ligne Oracle Fusion Middleware sur la console d'administration d'Oracle WebLogic Server](#).

### Création de l'identification Kerberos pour WebLogic Server

Sur l'ordinateur du contrôleur de domaine Active Directory, créez des objets utilisateur qui représentent WebLogic Server et le serveur Web EPM System, puis mappez-les avec les noms de principal de service (SPN) qui représentent votre instance WebLogic Server et votre serveur Web dans le domaine de sécurité Kerberos. Les clients ne peuvent pas localiser un service qui n'a pas de SPN. Vous stockez les SPN dans des fichiers keytab qui sont copiés dans le domaine WebLogic Server utilisé dans le processus de connexion.

Pour connaître les procédures détaillées, reportez-vous à la section [Création de l'identification pour WebLogic Server](#) dans le *guide Oracle Fusion Middleware sur la sécurisation d'Oracle WebLogic Server*.

Pour créer l'identification Kerberos pour WebLogic Server, procédez comme suit :

1. Sur l'ordinateur du contrôleur de domaine Active Directory, créez un compte utilisateur (par exemple, `epmHost`) pour l'ordinateur qui héberge le domaine WebLogic Server.



 **Remarque :**

Créez l'identification en tant qu'objet utilisateur, et non comme un ordinateur. Utilisez le nom simple de l'ordinateur (par exemple, `epmHost` si l'hôte s'appelle `epmHost.example.com`).

Enregistrez le mot de passe employé lors de la création de l'objet utilisateur. Vous devrez créer des SPN.

Ne sélectionnez aucune option de mot de passe, en particulier L'utilisateur doit modifier son mot de passe lors de la prochaine connexion.

2. Modifiez l'objet utilisateur pour qu'il soit conforme au protocole Kerberos. Le compte doit exiger la pré-authentification Kerberos.
  - Dans l'onglet **Compte**, sélectionnez le cryptage à utiliser.
  - Vérifiez qu'aucune autre option de compte (en particulier Ne pas exiger de pré-authentification Kerberos) n'est sélectionnée.
  - La configuration du type de cryptage risque de corrompre le mot de passe de l'objet. Par conséquent, réinitialisez le mot de passe sur la valeur que vous avez définie lors de la création de l'objet.
3. Sur l'ordinateur qui héberge le contrôleur de domaine Active Directory, ouvrez une fenêtre d'invite de commande et accédez au répertoire où sont installés les outils de prise en charge d'Active Directory.
4. Créez et configurez les SPN nécessaires.
  - a. Utilisez une commande semblable à celle ci-dessous pour vérifier que les SPN sont associés à l'objet utilisateur (`epmHost`) que vous avez créé à l'étape 1 de cette procédure.

```
setspn -L epmHost
```

- b. A l'aide d'une commande comme celle ci-dessous, configurez le SPN de WebLogic Server dans Active Directory Domain Services (AD DS) et générez un fichier keytab qui contient la clé secrète partagée.

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

5. Créez un fichier keytab sur l'ordinateur qui héberge WebLogic Server.
  - a. Ouvrez une invite de commande.
  - b. Accédez à `MIDDLEWARE_HOME/jdk/bin`.
  - c. Exécutez une commande telle que la suivante :

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

- d. A l'invite, saisissez le mot de passe que vous avez défini lors de la création de l'utilisateur à l'étape 1 de cette procédure.
6. Copiez le fichier keytab dans le répertoire de démarrage du domaine WebLogic (par exemple, dans `C:\Oracle\Middleware\user_projects\domains\EPMSys`).

7. Vérifiez que l'authentification Kerberos fonctionne correctement.

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

Dans cette commande, `account-name` indique le principal Kerberos (par exemple, `HTTP/epmHost.example.com@EXAMPLE.COM`). La sortie de cette commande doit ressembler à ceci :

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

**Mise à jour des options de JVM pour Kerberos**

Reportez-vous aux sections [Utilisation d'arguments de démarrage pour l'authentification Kerberos avec WebLogic Server](#) et [Création d'un fichier de connexion JAAS](#) dans le *guide Oracle Fusion Middleware sur la sécurisation d'Oracle WebLogic Server 11g version 1 (10.3.1)*.

Si les serveurs gérés EPM System sont exécutés en tant que services Windows, mettez à jour le registre Windows pour définir les options de démarrage de JVM.

Pour mettre à jour les options de démarrage de JVM dans le registre Windows, procédez comme suit :

1. Ouvrez l'éditeur de registre Windows.
2. Sélectionnez successivement **Poste de travail, HKEY\_LOCAL\_MACHINE, Logiciels, Solutions Hyperion, Foundationservices0 et HyS9EPMServer\_epmsystem1**.
3. Créez les valeurs de chaîne suivantes :



**Remarque :**

Les noms répertoriés dans le tableau suivant sont des exemples.

**Tableau 3-3 Options de démarrage de JVM pour l'authentification Kerberos**

| Nom         | Type   | Données                                                                                                     |
|-------------|--------|-------------------------------------------------------------------------------------------------------------|
| JVMOption44 | REG_SZ | -Djava.security.krb5.realm= <i>Nom du domaine de sécurité Active Directory</i>                              |
| JVMOption45 | REG_SZ | -Djava.security.krb5.kdc= <i>Adresse IP ou nom d'hôte pour Active Directory</i>                             |
| JVMOption46 | REG_SZ | -<br>Djava.security.auth.login.config= <i>Emplacement du fichier de configuration de connexion Kerberos</i> |
| JVMOption47 | REG_SZ | -<br>Djavax.security.auth.useSubjectCredsOnly= <i>false</i>                                                 |

- Mettez à jour la valeur de JVMOptionCount DWord pour refléter l'ajout de JVMOptions (ajoutez 4 à la valeur décimale actuelle).

### Configuration des stratégies d'autorisation

Reportez-vous à la section [Options de sécurisation de l'application Web et des ressources EJB](#) dans le *guide Oracle Fusion Middleware sur la sécurisation des ressources à l'aide de rôles et de stratégies pour Oracle WebLogic Server* afin d'obtenir des informations sur la configuration de stratégies d'autorisation pour les utilisateurs Active Directory qui accèdent à EPM System.

Pour des exemples d'étapes de configuration de stratégies, reportez-vous à la section [Création de stratégies pour SSODiag](#).

### Utilisation de SSODiag pour tester l'environnement Kerberos

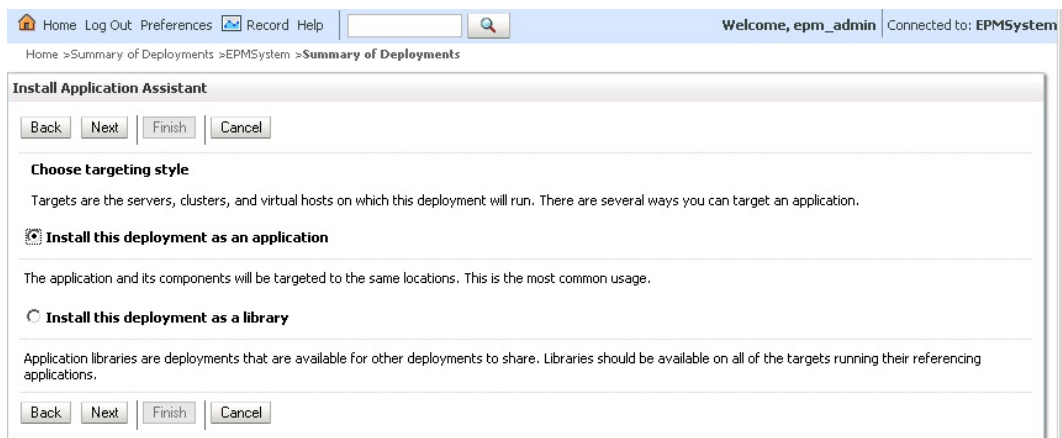
SSODiag est une application Web de diagnostic qui permet de tester si l'instance WebLogic Server de votre environnement Kerberos est prête à prendre en charge EPM System.

### Déploiement de SSODiag

Pour déployer SSODiag, utilisez les informations d'identification de l'administrateur WebLogic Server (le nom d'utilisateur par défaut est `epm_admin`) que vous avez indiquées lors du déploiement de Foundation Services.

Pour déployer et configurer SSODiag, procédez comme suit :

- Connectez-vous à la console d'administration WebLogic Server du domaine EPM System.
- Dans le centre de modifications, sélectionnez **Verrouiller et modifier**.
- Sous **EPMSystem** dans **Structure du domaine**, cliquez sur **Déploiements**.
- Dans **Récapitulatif des déploiements**, cliquez sur **Installer**.
- Dans **Chemin**, sélectionnez `EPM_ORACLE_HOME/products/Foundation/AppServer/InstallableApps/common/SSODiag.war`.
- Cliquez sur **Suivant**.
- Dans **Choisir un style de ciblage**, vérifiez que l'option **Installer ce déploiement en tant qu'application** est sélectionnée, puis cliquez sur **Suivant**.



8. Dans **Sélectionner des cibles de déploiement**, sélectionnez les options ci-dessous, puis cliquez sur **Suivant**.

- **EPMServer**
- **Tous les serveurs du cluster**

The screenshot shows the 'Install Application Assistant' dialog box in a web browser. The title bar includes 'Home Log Out Preferences Record Help' and 'Welcome, epm\_admin Connected to: EPMSystem'. The breadcrumb trail is 'Home > Summary of Deployments > EPMSystem > Summary of Deployments'. The main heading is 'Install Application Assistant' with buttons for 'Back', 'Next', 'Finish', and 'Cancel'. Below this is the section 'Select deployment targets' with the instruction: 'Select the servers and/or clusters to which you want to deploy this application. (You can reconfigure deployment targets later)'. Underneath is 'Available targets for SSODiag'. There are two sections: 'Servers' with a checkbox for 'AdminServer' (unchecked), and 'Clusters' with a checked radio button for 'EPMServer', and two unchecked radio buttons for 'All servers in the cluster' and 'Part of the cluster'. At the bottom are 'Back', 'Next', 'Finish', and 'Cancel' buttons.

9. Dans **Paramètres facultatifs**, sélectionnez **Rôles et stratégies personnalisés** : **utilisez uniquement les rôles et stratégies définis dans la console d'administration** comme modèle de sécurité.

The screenshot shows the 'Install Application Assistant' dialog box in a web browser. The title bar includes 'Home Log Out Preferences Record Help' and 'Welcome, epm\_admin Connected to: EPMSystem'. The breadcrumb trail is 'Home > Summary of Deployments > EPMSystem > Summary of Deployments'. The main heading is 'Install Application Assistant' with buttons for 'Back', 'Next', 'Finish', and 'Cancel'. Below this is the section 'Optional Settings' with the instruction: 'You can modify these settings or accept the defaults'. There are two sections: 'General' with the question 'What do you want to name this deployment?' and a text input field containing 'SSODiag'; and 'Security' with the question 'What security model do you want to use with this application?' and four radio button options: 'DD Only: Use only roles and policies that are defined in the deployment descriptors.', 'Custom Roles: Use roles that are defined in the Administration Console; use policies that are defined in the deployment descriptor.', 'Custom Roles and Policies: Use only roles and policies that are defined in the Administration Console.', and 'Advanced: Use a custom model that you have configured on the realm's configuration page.' The third option is selected.

10. Cliquez sur **Suivant**.

11. Dans l'écran de vérification, sélectionnez **Non, je vérifierai la configuration ultérieurement**.

12. Cliquez sur **Terminer**.

13. Dans le centre de modifications, sélectionnez **Activer les modifications**.

## Configuration d'Oracle HTTP Server pour SSODiag

Mettez à jour `mod_wl_ohs.conf` pour configurer Oracle HTTP Server afin qu'il transmette les demandes d'URL SSODiag à WebLogic Server.

Pour configurer la transmission d'URL dans Oracle HTTP Server, procédez comme suit :

1. Ouvrez `EPM_ORACLE_INSTANCE/httpConfig/ohs/config/fmwconfig/components/OHS/ohs_component/mod_wl_ohs.conf` dans un éditeur de texte.
2. Ajoutez une définition `LocationMatch` pour SSODiag :

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

Dans l'exemple précédent, `myServer` désigne l'ordinateur hôte de Foundation Services, et `28080` représente le port sur lequel Oracle Hyperion Shared Services écoute les demandes.

3. Enregistrez et fermez `mod_wl_ohs.conf`.
4. Redémarrez Oracle HTTP Server.

## Création de stratégies pour SSODiag

Créez une stratégie dans la console d'administration WebLogic Server pour protéger l'URL SSODiag suivante.

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

Dans cet exemple, `OHS_HOST_NAME` indique le nom du serveur qui héberge Oracle HTTP Server, et `PORT` représente le port sur lequel Oracle HTTP Server écoute les demandes.

Pour créer des stratégies visant à protéger SSODiag :

1. Dans le centre de modifications de la console d'administration WebLogic Server pour le domaine EPM System, sélectionnez **Verrouiller et modifier**.
2. Sélectionnez successivement **Déploiements, SSODiag, Sécurité, URLPatterns et Stratégies**.
3. Créez les modèles d'URL suivants :
  - /
  - /index.jsp
4. Modifiez chaque modèle d'URL que vous avez créé :
  - a. Dans la liste des modèles d'URL sous **Modèles d'URL d'application Web autonome**, cliquez sur le modèle (/) que vous avez créé pour l'ouvrir.
  - b. Sélectionnez **Ajouter des conditions**.
  - c. Dans **Liste de prédicats**, sélectionnez **Utilisateur**.
  - d. Sélectionnez **Suivant**.

- e. Dans **Nom d'argument utilisateur**, indiquez l'utilisateur Active Directory dont le compte sert à accéder à un bureau client configuré pour l'authentification Kerberos (par exemple, `krbuser1`). Ensuite, sélectionnez **Ajouter**. `krbuser1` est un utilisateur de bureau Windows ou Active Directory.
  - f. Sélectionnez **Terminer**.
5. Sélectionnez **Enregistrer**.

### Utilisation de SSODiag pour tester la configuration de WebLogic Server pour l'authentification Kerberos

Si la configuration de WebLogic Server pour l'authentification Kerberos fonctionne correctement, la page de *l'utilitaire de diagnostic SSO Oracle Hyperion Kerberos V 1.0* apparaît avec le message suivant :

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

#### **Attention :**

Ne configurez pas les composants EPM System pour l'authentification Kerberos si SSODiag ne peut pas extraire le nom de principal Kerberos.

Pour tester la configuration de WebLogic Server pour l'authentification Kerberos, procédez comme suit :

1. Démarrez Foundation Services et Oracle HTTP Server.
2. A l'aide de la console d'administration WebLogic Server, lancez l'application Web SSODiag pour traiter toutes les demandes.
3. Connectez-vous à un ordinateur client configuré pour l'authentification Kerberos à l'aide d'informations d'identification Active Directory valides.
4. A l'aide d'un navigateur, connectez-vous à l'URL SSODiag suivante :

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

Dans cet exemple, `OHS_HOST_NAME` indique le nom du serveur qui héberge Oracle HTTP Server, et `PORT` représente le port sur lequel Oracle HTTP Server écoute les demandes.

Si l'authentification Kerberos fonctionne correctement, SSODiag affiche les informations suivantes :

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

Si l'authentification Kerberos ne fonctionne pas correctement, SSODiag affiche les informations suivantes :

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

## Modification du modèle de sécurité

Le modèle de sécurité par défaut des applications Web protégées par le domaine de sécurité est `DDOnly`. Vous devez remplacer le modèle de sécurité par `CustomRolesAndPolicies`.

Pour modifier le modèle de sécurité, procédez comme suit :

1. A l'aide d'un éditeur de texte, ouvrez `MIDDLEWARE_HOME/user_projects/domains/EPMSysSystem/config/config.xml`.
2. Localisez l'élément suivant dans le descripteur de déploiement d'application de chaque composant Foundation Services :

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

3. Pour chaque composant, modifiez le modèle de sécurité de la façon suivante :

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

4. Enregistrez et fermez `config.xml`.

## Mise à jour de la configuration de sécurité d'EPM System

Modifiez la configuration de sécurité d'EPM System pour activer l'authentification Kerberos.

Pour configurer EPM System pour l'authentification Kerberos, procédez comme suit :

1. Connectez-vous à Shared Services Console en tant qu'administrateur.
2. Ajoutez le domaine Active Directory configuré pour l'authentification Kerberos comme annuaire des utilisateurs externe dans Shared Services. Reportez-vous à la section "Configuration d'OID, d'Active Directory et d'autres annuaires des utilisateurs LDAP" dans le *Guide d'administration de la sécurité utilisateur d'Oracle Enterprise Performance Management System*.
3. Activez l'authentification unique. Reportez-vous à la section [Configuration d'OID, Active Directory et d'autres annuaires des utilisateurs LDAP](#). Dans **Options de sécurité**, sélectionnez les paramètres du tableau suivant pour activer l'authentification unique Kerberos.

**Tableau 3-4 Paramètres permettant d'activer l'authentification unique Kerberos**

| Champ                                          | Paramètre obligatoire                                           |
|------------------------------------------------|-----------------------------------------------------------------|
| Activer l'authentification unique              | Sélectionné                                                     |
| Fournisseur ou agent d'authentification unique | Autre                                                           |
| Mécanisme SSO                                  | Obtenir les utilisateurs à distance à partir d'une requête HTTP |

4. Redémarrez Foundation Services.

## Test de l'authentification unique Kerberos

Connectez-vous à Foundation Services pour vérifier que l'authentification unique Kerberos fonctionne correctement.

Pour tester l'authentification unique Kerberos, procédez comme suit :

1. Vérifiez que Foundation Services et Oracle HTTP Server sont en cours d'exécution.
2. Connectez-vous à un ordinateur client configuré pour l'authentification Kerberos à l'aide d'informations d'identification Active Directory valides.
3. A l'aide d'un navigateur, connectez-vous à l'URL Foundation Services.

### Configuration des composants EPM System

A l'aide du configurateur EPM System, configurez et déployez d'autres composants EPM System dans le domaine WebLogic où Foundation Services est déployé.

### Configuration des serveurs gérés EPM System pour l'authentification Kerberos

Dans les environnements Microsoft Windows, les serveurs gérés EPM System sont exécutés en tant que services Windows. Vous devez modifier les options de démarrage de JVM pour chaque serveur géré WebLogic. Liste exhaustive des serveurs gérés en mode de déploiement non compact :

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

Si les applications Web EPM System sont déployées en mode de déploiement compact, vous devez mettre à jour les options de démarrage de JVM du serveur géré `EPMSys0` uniquement. Si vous avez plusieurs serveurs gérés compacts, vous devez mettre à jour les options de démarrage de JVM pour tous les serveurs gérés.

Reportez-vous à la section [Utilisation d'arguments de démarrage pour l'authentification Kerberos avec WebLogic Server](#) dans le *guide Oracle Fusion Middleware sur la sécurisation d'Oracle WebLogic Server*.

#### Remarque :

La procédure suivante décrit la configuration des options de démarrage de JVM pour le serveur géré FoundationServices. Vous devez effectuer cette tâche pour chaque serveur géré WebLogic du déploiement.

Pour obtenir des procédures détaillées de configuration des options de JVM dans les scripts de démarrage WebLogic Server, reportez-vous à la section [Mise à jour des options de JVM pour Kerberos](#).



Pour configurer les options de JVM dans les scripts de démarrage WebLogic Server, procédez comme suit :

### Configuration des stratégies d'autorisation

Configurez les stratégies d'autorisation pour les utilisateurs Active Directory qui ont accès à des composants EPM System autres que Foundation Services. Pour plus d'informations sur la configuration des stratégies de sécurité dans la console d'administration WebLogic, reportez-vous à la section [Configuration des stratégies d'autorisation](#).

### Modification du modèle de sécurité par défaut des composants EPM System

Pour modifier le modèle de sécurité par défaut, vous devez modifier le fichier de configuration EPM System. Pour les déploiements EPM System non compacts, vous devez modifier le modèle de sécurité par défaut de chaque application Web EPM System enregistrée dans `config.xml`. Liste des applications Web EPM System :

- AIF
- APS
- CALC
- EAS
- FINANCIALREPORTING
- PLANNING
- PROFITABILITY
- SHAREDSEVICES
- WORKSPACE

Pour modifier le modèle de sécurité, procédez comme suit :

1. A l'aide d'un éditeur de texte, ouvrez `MIDDLEWARE_HOME/user_projects/domains/EPMSystem/config/config.xml`
2. Dans la définition de déploiement d'application de chaque composant EPM System, définissez la valeur de `<security-dd-model>` sur `CustomRolesAndPolicies`, comme dans l'exemple suivant :

```
<app-deployment>
 <name>SHAREDSEVICES#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. Enregistrez et fermez `config.xml`.
4. Redémarrez WebLogic Server.

### Création de stratégies de protection d'URL pour les composants EPM System

Créez une stratégie de protection d'URL dans la console d'administration WebLogic Server pour protéger toutes les URL des composants EPM System. Pour plus de détails, reportez-

vous à la section [Options de sécurisation des applications Web et des ressources EJB](#) dans le *guide Oracle Fusion Middleware sur la sécurisation des ressources à l'aide de rôles et de stratégies pour Oracle WebLogic Server*.

Pour créer des stratégies de protection d'URL, procédez comme suit :

1. Dans le centre de modifications de la console d'administration WebLogic Server pour le domaine EPM System, cliquez sur **Verrouiller et modifier**.
2. Cliquez sur **Déploiements**.
3. Développez une application d'entreprise EPM System (par exemple, `PLANNING`) dans votre déploiement, puis cliquez sur l'application Web correspondante (par exemple, `HyperionPlanning`). Reportez-vous à la section [Modification du modèle de sécurité par défaut des composants EPM System](#) pour obtenir la liste des composants EPM System.

 **Remarque :**

Certaines applications d'entreprise, comme Oracle Essbase Administration Services, comprennent plusieurs applications Web dont les modèles d'URL doivent être définis.

4. Créez une stratégie portant sur les modèles d'URL pour l'application Web.
  - AIF
  - APS
  - CALC
  - EAS
  - FINANCIALREPORTING
  - PLANNING
  - PROFITABILITY
  - SHARED SERVICES
  - WORKSPACE
  - a. Cliquez sur **Sécurité, Stratégies**, puis **Nouveau**.
  - b. Dans **Modèle d'URL**, entrez les URL protégées et non protégées pour les produits EPM System. Pour plus de détails, reportez-vous à la section [Protection et annulation de la protection des ressources EPM System](#).
  - c. Cliquez sur **OK**.
  - d. Cliquez sur le modèle d'URL que vous venez de créer.
  - e. Cliquez sur **Ajouter des conditions**.
  - f. Dans **Liste de prédicats**, sélectionnez une condition de stratégie, puis cliquez sur **Suivant**.  
Oracle recommande d'utiliser la condition `Groupe`, qui applique cette condition de sécurité à tous les membres d'un groupe spécifique.
  - g. Indiquez les arguments correspondant au prédicat choisi. Par exemple, si vous avez choisi `Groupe` à l'étape précédente, procédez comme suit :

- h. Dans **Nom d'argument de groupe**, saisissez le nom du groupe qui contient les utilisateurs auxquels vous voulez donner accès à l'application Web. Ce nom doit être identique au nom de groupe Active Directory.
    - Cliquez sur **Ajouter**.
    - Répétez les étapes précédentes pour ajouter d'autres groupes.
  - i. Cliquez sur **Terminer**.  
WebLogic Server affiche un message d'erreur s'il ne parvient pas à localiser le groupe dans Active Directory. Vous devez corriger cette erreur avant de continuer.
  - j. Sélectionnez **Enregistrer**.
5. Répétez les étapes 3 et 4 de cette procédure pour les autres composants EPM System du déploiement.
  6. Dans le centre de modifications, cliquez sur **Libérer la configuration**.
  7. Redémarrez WebLogic Server.

### Activer l'authentification par certificat client dans les applications Web

Insérez la définition `login-config` dans le fichier de configuration des archives d'application suivantes dans `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`

Pour activer l'authentification par certificat client, procédez comme suit :

1. Arrêtez les processus et les composants EPM System.
2. A l'aide de 7 Zip, développez l'archive Web contenue dans l'archive Enterprise, par exemple, `EPM_ORACLE_HOME/products/Essbase/eas/server/AppServer/InstallableApps/Common/eas.ear/eas.war`.
3. Accédez à `WEB-INF`.
4. Modifiez le fichier `web.xml` en ajoutant la définition `login_config` suivante juste avant l'élément `</webapp>` :

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

5. Enregistrez `web.xml`.
6. Cliquez sur **Oui** lorsque 7 Zip demande si vous souhaitez mettre à jour l'archive.

### Mise à jour de la configuration de sécurité d'EPM System

Configurez la sécurité EPM System dans l'optique de l'authentification unique. Reportez-vous à la section [Configuration de EPM System pour l'authentification unique](#).

## Configuration de EPM System pour l'authentification unique

Les produits Oracle Enterprise Performance Management System doivent être configurés afin de prendre en charge l'agent de sécurité pour l'authentification unique. La configuration spécifiée dans Oracle Hyperion Shared Services détermine les conditions suivantes pour tous les produits EPM System :

- Acceptation d'authentification unique à partir d'un agent de sécurité
- Mécanisme d'authentification pour accepter SSO

Dans un environnement SSO, le produit EPM System qui est accédé en premier par l'utilisateur analyse le mécanisme SSO pour extraire l'ID utilisateur authentifié qu'il contient. Le produit EPM System vérifie l'ID utilisateur, en le comparant aux annuaires des utilisateurs configurés dans Shared Services, pour déterminer si l'utilisateur est un utilisateur EPM System valide. Il affecte également un jeton qui active l'authentification unique pour tous les produits EPM System.

La configuration spécifiée dans Shared Services active l'authentification unique et détermine le mécanisme d'authentification afin d'accepter l'authentification unique pour tous les produits EPM System.

Pour activer la connexion unique à partir d'une solution de gestion des identités Web, procédez comme suit :

1. Lancez Oracle Hyperion Shared Services Console en tant qu'administrateur Shared Services. Reportez-vous à [Lancement de Shared Services Console](#).
2. Sélectionnez **Administration**, puis **Configurer les annuaires des utilisateurs**.
3. Vérifiez que les annuaires des utilisateurs utilisés par la solution de gestion des identités Web sont configurés en tant qu'annuaires des utilisateurs externes dans Shared Services.

Par exemple, pour activer l'authentification unique Kerberos, vous devez configurer l'annuaire Active Directory configuré pour l'authentification Kerberos en tant qu'annuaire des utilisateurs externe.

Pour obtenir des instructions, reportez-vous à la section Configuration des annuaires des utilisateurs.

4. Sélectionnez **Options de sécurité**.
5. Sélectionnez **Afficher les options avancées**.
6. Dans **Configuration de l'authentification unique**, dans l'écran Annuaires des utilisateurs définis, effectuez les étapes suivantes ::
  - a. Sélectionnez **Activer la connexion unique**.
  - b. Dans **Fournisseur ou agent d'authentification unique**, sélectionnez une solution de gestion des identités Web. Choisissez **Autre** si vous configurez l'authentification unique à l'aide du protocole Kerberos.

Le mécanisme SSO recommandé est automatiquement sélectionné. Reportez-vous au tableau suivant. Reportez-vous également à la section [Méthodes d'authentification unique prises en charge](#).

 **Remarque :**

Si vous n'utilisez pas le mécanisme SSO recommandé, vous devez sélectionner *Autre* dans **Fournisseur ou agent d'authentification unique**. Par exemple, si vous souhaitez utiliser un mécanisme autre qu'un en-tête HTTP pour SiteMinder, sélectionnez *Autre* dans **Fournisseur ou agent d'authentification unique**, puis sélectionnez le mécanisme SSO à utiliser dans **Mécanisme SSO**.

**Tableau 3-5 Mécanismes SSO par défaut pour les solutions de gestion des identités Web**

Solution de gestion des identités Web	Mécanisme SSO recommandé
Oracle Access Manager	En-tête HTTP personnalisé <sup>1</sup>
OSSO	En-tête HTTP personnalisé
SiteMinder	En-tête HTTP personnalisé
Kerberos	Obtenir les utilisateurs à distance à partir d'une requête HTTP

<sup>1</sup> Le nom de l'en-tête HTTP par défaut est HYPLOGIN. Si vous utilisez un en-tête HTTP personnalisé, remplacez le nom.

7. Cliquez sur **OK**.

## Options d'authentification unique pour Smart View

Bien qu'Oracle Smart View for Office soit un client lourd et non un navigateur, il se connecte aux composants de serveur avec HTTP et se comporte davantage comme un navigateur du point de vue du système. Smart View prend en charge toutes les méthodes d'intégration basées sur le Web prises en charge par les interfaces de navigateur. Il existe cependant certaines limitations :

- Si Smart View est lancé à partir d'une session de navigateur existante qui est connectée à un composant Oracle Enterprise Performance Management System, les utilisateurs doivent se connecter à nouveau à Smart View, car celui-ci ne partage pas le cookie de la session existante.
- Si vous utilisez un formulaire de connexion personnalisé basé sur HTML au lieu du formulaire de connexion par défaut Oracle Access Manager, assurez-vous que la source du formulaire personnalisé inclut la chaîne `loginform`. Ceci est obligatoire pour que l'intégration de Smart View à Oracle Access Manager fonctionne.

# 4

## Configuration des annuaires des utilisateurs

### Voir aussi :

- [Annuaires des utilisateurs et sécurité EPM System](#)
- [Opérations associées à la configuration des annuaires des utilisateurs](#)
- [Oracle Identity Manager et EPM System](#)
- [Informations Active Directory](#)
- [Configuration d'OID, Active Directory et d'autres annuaires des utilisateurs LDAP](#)
- [Configuration des bases de données relationnelles en tant qu'annuaires des utilisateurs](#)
- [Test des connexions de l'annuaire des utilisateurs](#)
- [Modification des paramètres d'annuaire des utilisateurs](#)
- [Suppression des configurations d'annuaires des utilisateurs](#)
- [Gestion de l'ordre de recherche de l'annuaire des utilisateurs](#)
- [Configuration des options de sécurité](#)
- [Régénération des clés de cryptage](#)
- [Utilisation des caractères spéciaux](#)

## Annuaires des utilisateurs et sécurité EPM System

Les produits Oracle Enterprise Performance Management System sont pris en charge sur un certain nombre de systèmes de gestion des utilisateurs et des identités, regroupés sous le nom d'annuaires des utilisateurs. Ceux-ci regroupent les annuaires des utilisateurs LDAP (Lightweight Directory Access Protocol), tels que Sun Java System Directory Server (anciennement SunONE Directory Server) et Microsoft Active Directory. EPM System prend également en charge les bases de données relationnelles en tant qu'annuaires d'utilisateurs externes.

En règle générale, les produits EPM System utilisent l'annuaire natif et les annuaires des utilisateurs externes lors du provisionnement. Reportez-vous à [Matrice de certification Oracle Enterprise Performance Management System](#) pour obtenir la liste des annuaires des utilisateurs pris en charge.

Les produits EPM System requièrent un compte d'annuaire des utilisateurs pour chaque utilisateur qui accède aux produits. Ces utilisateurs peuvent être affectés à des groupes pour faciliter le provisionnement. Vous pouvez attribuer aux utilisateurs et aux groupes des listes ACL de rôles et d'objets EPM System. En raison de la charge administrative que cela représente, Oracle déconseille le provisionnement d'utilisateurs individuels. Les utilisateurs et les groupes de tous les annuaires d'utilisateurs configurés sont visibles dans Oracle Hyperion Shared Services Console.

Par défaut, le configurateur EPM System configure le référentiel Shared Services comme annuaire natif pour la prise en charge des produits EPM System. Les gestionnaires d'annuaires accèdent à l'annuaire natif et le gèrent via Shared Services Console.

## Opérations associées à la configuration des annuaires des utilisateurs

Pour prendre en charge SSO et les autorisations, les administrateurs système doivent configurer des annuaires des utilisateurs externes. Dans Oracle Hyperion Shared Services Console, les administrateurs système peuvent effectuer plusieurs tâches relatives à la configuration et à la gestion des annuaires des utilisateurs. Pour plus d'instructions, consultez les rubriques suivantes :

- Configuration des annuaires des utilisateurs :
  - [Configuration d'OID, Active Directory et d'autres annuaires des utilisateurs LDAP](#)
  - [Configuration des bases de données relationnelles en tant qu'annuaires des utilisateurs](#)
- [Test des connexions de l'annuaire des utilisateurs](#)
- [Modification des paramètres d'annuaire des utilisateurs](#)
- [Suppression des configurations d'annuaires des utilisateurs](#)
- [Gestion de l'ordre de recherche de l'annuaire des utilisateurs](#)
- [Configuration des options de sécurité](#)

## Oracle Identity Manager et EPM System

Oracle Identity Manager est une solution d'administration d'utilisateurs et de rôles qui automatise le processus d'ajout, de mise à jour et de suppression des comptes d'utilisateur et des habilitations de niveau attribut dans les ressources Enterprise. Oracle Identity Manager est disponible séparément ou avec la solution Oracle Identity and Access Management Suite Plus.

Oracle Enterprise Performance Management System s'intègre à Oracle Identity Manager en utilisant des rôles Enterprise qui sont des groupes LDAP. Les rôles des composants EPM System peuvent être affectés à des rôles Enterprise. Les utilisateurs ou les groupes ajoutés aux rôles Enterprise d'Oracle Identity Manager héritent automatiquement des rôles EPM System affectés.

Par exemple, supposons que vous disposez d'une application Oracle Hyperion Planning nommée *Budget Planning*. Pour prendre en charge cette application, vous pouvez créer trois rôles Enterprise (Utilisateur interactif Budget Planning, Utilisateur final Budget Planning et Administrateur Budget Planning) dans Oracle Identity Manager. Lors du provisionnement des rôles EPM System, assurez-vous que les gestionnaires de profils provisionnent les rôles Enterprise d'Oracle Identity Manager avec les rôles obligatoires de *Budget Planning* et d'autres composants EPM System comme Shared Services. Tous les utilisateurs et les groupes affectés aux rôles Enterprise dans Oracle Identity Manager héritent des rôles EPM System. Reportez-vous à la documentation Oracle Identity Manager pour plus d'informations sur le déploiement et la gestion d'Oracle Identity Manager.

Pour intégrer Oracle Identity Manager à EPM System, les administrateurs doivent effectuer les étapes suivantes :

- Assurez-vous que les membres (utilisateurs et groupes) des rôles Enterprise d'Oracle Identity Manager qui doivent être utilisés pour le provisionnement d'EPM System sont définis dans un annuaire des utilisateurs LDAP, par exemple OID ou Active Directory.
- Configurez l'annuaire des utilisateurs LDAP dans lequel les membres des rôles Enterprise sont définis en tant qu'annuaire d'utilisateurs externe dans EPM System. Reportez-vous à [Configuration d'OID, Active Directory et d'autres annuaires des utilisateurs LDAP](#).

## Informations Active Directory

Cette section explique certains concepts Microsoft Active Directory utilisés dans ce document.

### Recherche DNS et recherche de nom d'hôte

Les administrateurs système peuvent configurer Active Directory afin qu'Oracle Hyperion Shared Services puisse effectuer une consultation de nom d'hôte statique ou une consultation DNS pour identifier Active Directory. La consultation de nom d'hôte statique ne prend pas en charge le basculement d'Active Directory.

La consultation DNS garantit la haute disponibilité d'Active Directory dans les scénarios où ce dernier est configuré sur plusieurs contrôleurs de domaine pour garantir la haute disponibilité. Lorsqu'il est configuré pour effectuer une recherche DNS, Shared Services envoie une requête au serveur DNS pour identifier les contrôleurs de domaine enregistrés et se connecte au contrôleur de domaine le plus important. En cas de défaillance du contrôleur de domaine auquel Shared Services est connecté, Shared Services bascule de façon dynamique vers le second contrôleur de domaine le plus important disponible.

#### Remarque :

La consultation DNS peut être configurée uniquement si une installation Active Directory redondante qui prend en charge le basculement est disponible. Pour plus d'informations, reportez-vous à la documentation Microsoft.

### Catalogue global

Un catalogue global est un contrôleur de domaine qui stocke une copie de tous les objets Active Directory dans une forêt. Il stocke une copie complète de tous les objets dans l'annuaire pour son domaine hôte et une copie partielle de tous les objets pour tous les autres domaines dans la structure, qui sont généralement utilisés dans les opérations de recherche d'utilisateurs. Reportez-vous à la documentation Microsoft pour des informations sur la configuration d'un catalogue global.

Si votre organisation utilise un catalogue global, utilisez l'une des méthodes suivantes pour configurer Active Directory :

- Configurer le serveur de catalogue global en tant qu'annuaire des utilisateurs externe (recommandé)
- Configurer chaque domaine Active Directory en tant qu'annuaire des utilisateurs externe séparé.



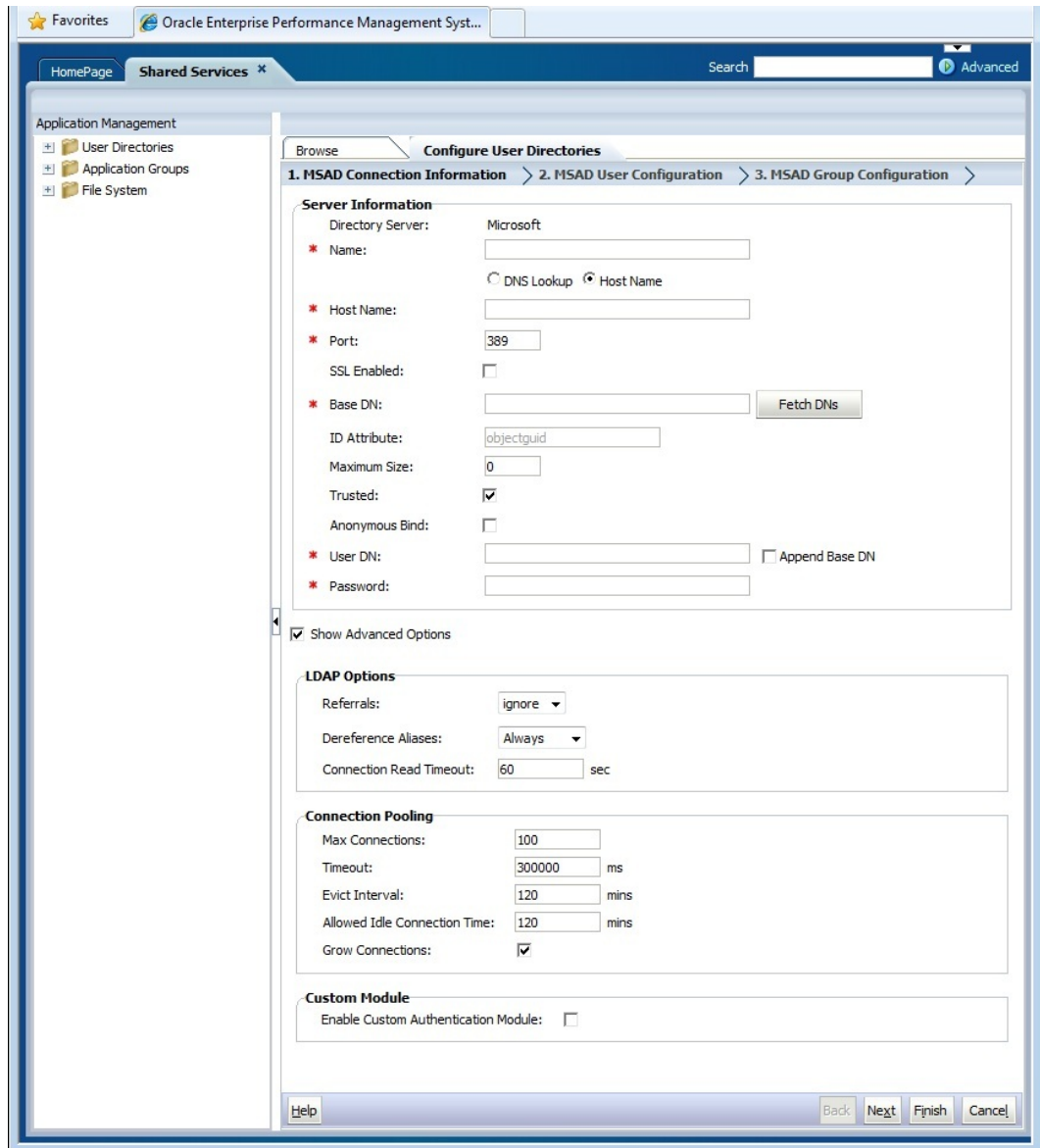
La configuration du catalogue global au lieu des domaines Active Directory individuels permet aux produits Oracle Enterprise Performance Management System d'accéder aux groupes locaux et universels de la forêt.

## Configuration d'OID, d'Active Directory et d'autres annuaires des utilisateurs LDAP

Les administrateurs système utilisent les procédures décrites dans cette section pour configurer les annuaires des utilisateurs d'entreprise LDAP, tels qu'OID, Sun Java System Directory Server, Oracle Virtual Directory, Active Directory, IBM Tivoli Directory Server ou un annuaire des utilisateurs LDAP qui ne figure pas dans l'écran de configuration.


Pour configurer OID, Active Directory et d'autres annuaires des utilisateurs LDAP, procédez comme suit :

1. Accédez à Oracle Hyperion Shared Services Console en tant qu'administrateur système. Reportez-vous à [Lancement de Shared Services Console](#).
2. Sélectionnez **Administration**, puis **Configurer les annuaires des utilisateurs**.  
L'onglet Configuration du fournisseur s'ouvre. Il répertorie tous les annuaires des utilisateurs configurés, notamment l'annuaire natif.
3. Cliquez sur **Nouveau**.
4. Dans **Type d'annuaire**, sélectionnez une option :
  - **LDAP (Lightweight Directory Access Protocol)** pour configurer un annuaire des utilisateurs LDAP autre qu'Active Directory. Sélectionnez cette option pour configurer Oracle Virtual Directory.
  - **Microsoft Active Directory (MSAD)** pour configurer Active Directory.  
**Active Directory et Active Directory Application Mode (ADAM) uniquement** : si vous souhaitez utiliser un attribut d'ID personnalisé (un attribut autre que `ObjectGUID` ; par exemple `sAMAccountName`) avec Active Directory ou ADAM, sélectionnez **LDAP (Lightweight Directory Access Protocol)** et configurez-le en tant que type d'annuaire `Other`.
5. Cliquez sur **Suivant**.





6. Entrez les paramètres requis.

**Tableau 4-1 Ecran Informations de connexion**

Libellé	Description
Serveur d'annuaire	<p>Choisissez un annuaire des utilisateurs. La valeur <b>Attribut d'ID</b> adopte l'attribut d'identité unique constant recommandé pour le produit sélectionné.</p> <p>Cette propriété est automatiquement sélectionnée si vous choisissez Active Directory à l'étape 4.</p> <p>Sélectionnez <i>Autre</i> dans les scénarios suivants :</p> <ul style="list-style-type: none"> <li>• Vous configurez un type d'annuaire des utilisateurs non répertorié ; par exemple, Oracle Virtual Directory.</li> <li>• Vous configurez un annuaire des utilisateurs LDAP répertorié (par exemple, OID), mais vous voulez utiliser un attribut d'ID personnalisé.</li> <li>• Vous configurez Active Directory ou ADAM pour utiliser un attribut d'ID personnalisé.</li> </ul> <div style="border: 1px solid #0070C0; padding: 10px; margin-top: 10px;"> <p> <b>Remarque :</b></p> <p>Comme Oracle Virtual Directory fournit une abstraction virtualisée des répertoires LDAP et des référentiels de données SGBDR dans une vue d'annuaire unique, Oracle Enterprise Performance Management System le considère comme un seul annuaire des utilisateurs externe sans tenir compte du nombre et du type d'annuaires des utilisateurs qu'Oracle Virtual Directory prend en charge.</p> </div> <p><b>Exemple :</b> Oracle Internet Directory</p>
Nom	<p>Nom descriptif de l'annuaire des utilisateurs. Utilisé pour identifier un annuaire des utilisateurs spécifique si plusieurs annuaires sont configurés. Le nom ne doit pas contenir de caractères spéciaux, à l'exception des espaces et des traits de soulignement.</p> <p><b>Exemple :</b> Corporate_OID</p>

**Tableau 4-1 (suite) Ecran Informations de connexion**

Libellé	Description
Consultation DNS	<p><b>Active Directory uniquement</b> : sélectionnez cette option pour activer la recherche DNS. Reportez-vous à la section <a href="#">Recherche DNS et recherche de nom d'hôte</a>. Oracle recommande de configurer la consultation DNS comme méthode de connexion à Active Directory dans les environnements de production afin d'éviter les échecs de connexion.</p>
	<div style="border: 1px solid #0070C0; padding: 10px; background-color: #E6F2FF;"> <p> <b>Remarque :</b></p> <p>Ne sélectionnez pas cette option si vous configurez un catalogue global.</p> </div>
	<p>Lorsque vous sélectionnez cette option, les champs suivants apparaissent :</p> <ul style="list-style-type: none"> <li>• <b>Domaine</b> : nom de domaine d'une forêt Active Directory.  <b>Exemples</b> : <code>example.com</code> ou <code>us.example.com</code></li> <li>• <b>Site AD</b> : nom du site Active Directory. En général, il s'agit du nom distinctif relatif de l'objet de site stocké dans le conteneur de configuration Active Directory. Habituellement, ce champ identifie un lieu (ville, département, région ou pays).  <b>Exemples</b> : <code>Santa Clara</code> ou <code>US_West_region</code></li> <li>• <b>Serveur DNS</b> : nom DNS du serveur prenant en charge la recherche de serveur DNS pour les contrôleurs de domaine.</li> </ul>
Nom d'hôte	<p><b>Active Directory uniquement</b> : sélectionnez cette option pour activer la recherche de nom d'hôte statique. Reportez-vous à la section <a href="#">Recherche DNS et recherche de nom d'hôte</a>.</p>
	<div style="border: 1px solid #0070C0; padding: 10px; background-color: #E6F2FF;"> <p> <b>Remarque :</b></p> <p>Sélectionnez cette option si vous configurez un catalogue global Active Directory.</p> </div>

**Tableau 4-1 (suite) Ecran Informations de connexion**




Libellé	Description
Nom d'hôte	<p>Nom DNS du serveur d'annuaire des utilisateurs. Utilisez le nom qualifié complet du domaine si l'annuaire des utilisateurs doit être utilisé pour prendre en charge l'authentification unique à partir de SiteMinder. Oracle recommande d'utiliser le nom d'hôte pour établir une connexion Active Directory à des fins de test uniquement.</p> <div data-bbox="667 506 1380 747"><p> <b>Remarque :</b></p><p>Si vous configurez un catalogue global Active Directory, indiquez le nom d'hôte du serveur du catalogue global. Reportez-vous à la section <a href="#">Catalogue global</a>.</p></div> <p><b>Exemple :</b> MyServer</p>
Port	<p>Numéro du port où l'annuaire des utilisateurs est en cours d'exécution.</p> <div data-bbox="667 926 1380 1167"><p> <b>Remarque :</b></p><p>Si vous configurez un catalogue global Active Directory, indiquez le port utilisé par le serveur du catalogue global (le port par défaut est 3268). Reportez-vous à la section <a href="#">Catalogue global</a>.</p></div> <p><b>Exemple :</b> 389</p>
SSL activé	<p>Case à cocher qui active la communication sécurisée avec cet annuaire des utilisateurs. L'annuaire des utilisateurs doit être configuré pour une communication sécurisée.</p>

Tableau 4-1 (suite) Ecran Informations de connexion

Libellé	Description
DN de base	<p>Le nom distinctif (DN ou Distinguished Name) du noeud où la recherche des utilisateurs et des groupes doit commencer. Vous pouvez également utiliser le bouton <b>Récupérer les DN</b> pour répertorier les DN de base disponibles, puis sélectionner le nom distinctif de base approprié dans la liste.</p> <div style="border: 1px solid #0070c0; padding: 10px; margin: 10px 0;"> <p> <b>Remarque :</b></p> <p>Si vous configurez un catalogue global, spécifiez le nom distinctif de base de la forêt.</p> </div> <p>Pour plus d'informations sur les restrictions d'utilisation des caractères spéciaux, reportez-vous à la section <a href="#">Utilisation des caractères spéciaux</a>.</p> <p>Oracle recommande de sélectionner le DN le plus bas contenant tous les utilisateurs et groupes de produits EPM System.</p> <p><b>Exemple :</b> dc=example,dc=com</p>
Attribut d'ID	<p>La valeur d'attribut ne peut être modifiée que si l'option <i>Autre</i> est sélectionnée dans <b>Type d'annuaire</b>. Cet attribut doit être un attribut commun qui existe dans les objets d'utilisateur et de groupe sur le serveur d'annuaire.</p> <p>La valeur recommandée pour cet attribut est automatiquement définie pour OID (<code>orclguid</code>), SunONE (<code>nsuniqueid</code>), IBM Directory Server (<code>Ibm-entryUuid</code>), Novell eDirectory (<code>GUID</code>) et Active Directory (<code>ObjectGUID</code>).</p> <p><b>Exemple :</b> <code>orclguid</code></p> <p>La valeur d'attribut d'ID, si vous la définissez manuellement après avoir choisi <i>Autre</i> dans <b>Serveur d'annuaire</b>, par exemple pour configurer une instance Oracle Virtual Directory, doit :</p> <ul style="list-style-type: none"> <li>• pointer vers un attribut unique</li> <li>• ne pas être propre à un emplacement</li> <li>• ne pas changer dans le temps</li> </ul>
Taille maximale	<p>Nombre maximal de résultats pouvant être renvoyé par une recherche. Si cette valeur est supérieure à celle qui est prise en charge par les paramètres d'annuaire des utilisateurs, la valeur de l'annuaire des utilisateurs la remplace.</p> <p>Pour les annuaires des utilisateurs LDAP autres qu'Active Directory, laissez ce champ vide afin d'extraire tous les utilisateurs et groupes qui répondent aux critères de recherche.</p> <p>Pour Active Directory, définissez cette valeur sur 0 pour extraire tous les utilisateurs et groupes qui répondent aux critères de recherche.</p> <p>Si vous configurez Oracle Hyperion Shared Services en mode Administration déléguée, définissez cette valeur sur 0.</p>

**Tableau 4-1 (suite) Ecran Informations de connexion**


Libellé	Description
Sécurisé	Case à cocher permettant d'indiquer que ce fournisseur est une source SSO sécurisée. Les jetons SSO de sources sécurisées ne contiennent pas le mot de passe de l'utilisateur.
Liaison anonyme	Case à cocher permettant d'indiquer que Shared Services peut être lié de manière anonyme à l'annuaire des utilisateurs pour rechercher des utilisateurs et des groupes. Peut être utilisée uniquement si l'annuaire des utilisateurs autorise la liaison anonyme. Si vous ne sélectionnez pas cette option, vous devez spécifier, dans le champ DN de l'utilisateur, un compte disposant des autorisations d'accès suffisantes pour effectuer une recherche dans le répertoire de stockage des informations utilisateur. Oracle recommande de ne pas utiliser la liaison anonyme.
 <b>Remarque :</b> La liaison anonyme n'est pas prise en charge pour OID.	
DN de l'utilisateur	Cette option est désactivée si vous sélectionnez <b>Liaison anonyme</b> . Nom distinctif de l'utilisateur que Shared Services doit utiliser pour être lié à l'annuaire des utilisateurs. Cet utilisateur doit disposer de privilèges de recherche sur l'attribut de nom distinctif relatif dans le nom distinctif. Par exemple, dans le nom distinctif : <code>cn=John Doe, ou=people, dc=myCompany, dc=com</code> , l'utilisateur de la liaison doit disposer d'un accès en recherche à l'attribut <code>cn</code> . Vous devez faire précéder les caractères spéciaux dans le nom distinctif de l'utilisateur par des caractères d'échappement. Pour plus d'informations sur les restrictions, reportez-vous à la section <a href="#">Utilisation des caractères spéciaux</a> . <b>Exemple :</b> <code>cn=admin, dc=myCompany, dc=com</code>
Ajouter le nom distinctif de base	La case à cocher pour ajouter le DN de base au DN de l'utilisateur. Si vous utilisez le compte Gestionnaire d'annuaire en tant que DN de l'utilisateur, n'ajoutez pas de nom distinctif de base. Cette case à cocher est désactivée si vous sélectionnez l'option Liaison anonyme.
Mot de passe	Mot de passe du nom distinctif (DN) de l'utilisateur Cette zone est désactivée si vous sélectionnez l'option Liaison anonyme. <b>Exemple :</b> <code>UserDNpassword</code>
Afficher les options avancées	Case à cocher pour afficher les options avancées.

Tableau 4-1 (suite) Ecran Informations de connexion

Libellé	Description
Références	<b>Active Directory uniquement :</b> Si Active Directory est configuré afin de suivre des références, sélectionnez <code>suivre</code> pour suivre automatiquement les références LDAP. Sélectionnez <code>ignorer</code> pour ne pas utiliser les références.
Déréférencer les alias	Sélectionnez la méthode que les recherches Shared Services doivent utiliser pour déréférencer les alias dans l'annuaire des utilisateurs afin que les recherches extraient l'objet vers lequel pointe le DN de l'alias. Sélectionnez : <ul style="list-style-type: none"> <li>• <b>Toujours</b> : toujours déréférencer les alias</li> <li>• <b>Jamais</b> : ne jamais déréférencer les alias.</li> <li>• <b>Recherche</b> : déréférencer les alias uniquement au cours de la résolution du nom.</li> <li>• <b>Recherche en cours</b> : déréférencer les alias uniquement après la résolution du nom.</li> </ul>
Délai d'expiration de lecture de connexion	Intervalle (en secondes) au bout duquel le fournisseur LDAP abandonne la tentative de lecture LDAP s'il n'obtient pas de réponse. <b>Valeur par défaut</b> : 60 secondes
Nombre maximal de connexions	Nombre maximal de connexions dans le pool de connexions. La valeur par défaut est 100 pour les annuaires des utilisateurs LDAP, notamment Active Directory. <b>Valeur par défaut</b> : 100
Délai d'expiration	Délai d'expiration avant d'obtenir une connexion à partir du pool. Une exception est générée après ce délai. <b>Valeur par défaut</b> : 300 000 millisecondes (5 minutes)
Intervalle d'exclusion	<b>Facultatif</b> : intervalle d'exécution du processus d'exclusion pour nettoyer le pool. Ce processus supprime les connexions qui dépassent la durée d'inactivité autorisée pour la connexion. <b>Valeur par défaut</b> : 120 minutes
Durée d'inactivité autorisée pour la connexion	<b>Facultatif</b> : durée après laquelle le processus d'exclusion supprime les connexions inactives du pool. <b>Valeur par défaut</b> : 120 minutes
Augmenter les connexions	Cette option indique si le pool de connexions peut augmenter au-delà de la valeur <code>Nombre maximal de connexions</code> . Elle est sélectionnée par défaut. Dans ce cas, le système renvoie une erreur si une connexion n'est pas disponible dans le délai défini pour le paramètre <code>Dépassement du délai</code> .
Activer le module d'authentification personnalisé	La case à cocher pour activer l'utilisation d'un module d'authentification personnalisé pour authentifier les utilisateurs définis dans cet annuaire des utilisateurs. Vous devez également saisir le nom de classe Java qualifié complet du module d'authentification dans l'écran Options de sécurité. Reportez-vous à la section <a href="#">Configuration des options de sécurité</a> . Le module d'authentification personnalisé est transparent aux clients légers et lourds et ne requiert aucune modification du déploiement du client. Reportez-vous à la section "Utilisation d'un module d'authentification personnalisé" du <i>Guide de configuration de la sécurité d'Oracle Enterprise Performance Management System</i> .



7. Cliquez sur **Suivant**.

Shared Services utilise les propriétés définies dans l'écran Configuration de l'utilisateur pour créer une URL d'utilisateur qui permet de déterminer le noeud où la recherche des utilisateurs doit commencer. L'utilisation de cette URL accélère la recherche.

**Attention :**

L'URL d'utilisateur ne doit pas pointer sur un alias. La sécurité EPM System exige que l'URL d'utilisateur pointe vers l'utilisateur en question.

Oracle recommande d'utiliser la zone Configuration automatique de l'écran pour extraire les informations requises.

**Remarque :**

Pour obtenir la liste des caractères spéciaux pouvant être utilisés dans la configuration des utilisateurs, reportez-vous à la section [Utilisation des caractères spéciaux](#).

8. Dans **Configuration automatique**, entrez un identifiant utilisateur unique en utilisant le format *attribute=identifiant* (par exemple, *uid=jdoe*).

Les attributs de l'utilisateur sont affichés dans la zone Configuration de l'utilisateur.

Si vous configurez OID, vous ne pouvez pas configurer automatiquement le filtre utilisateur, car le DSE racine d'OID ne contient pas d'entrée dans l'attribut des contextes de dénomination. Reportez-vous à la section [Gestion des contextes de dénomination](#) dans le *Guide de l'administrateur Oracle Fusion Middleware pour Oracle Internet Directory*.

 **Remarque :**

Vous pouvez entrer manuellement les attributs de l'utilisateur requis dans les zones de texte de la zone Configuration de l'utilisateur.

**Tableau 4-2 Ecran Configuration de l'utilisateur**

Libellé	Description <sup>1</sup>
DN relatif de l'utilisateur	<p>DN relatif de l'utilisateur. Chaque composant d'un DN est appelé DN relatif et représente une branche dans l'arborescence du répertoire. Le DN relatif d'un utilisateur est en général équivalent à <code>uid</code> ou <code>cn</code>.</p> <p>Pour plus d'informations sur les restrictions, reportez-vous à la section <a href="#">Utilisation des caractères spéciaux</a>.</p> <p><b>Exemple :</b> <code>ou=People</code></p>
Attribut de connexion	<p>Attribut unique (il peut s'agir d'un attribut personnalisé) qui stocke le nom de connexion de l'utilisateur. Les utilisateurs utilisent la valeur de cet attribut en tant que nom d'utilisateur lorsqu'ils se connectent aux produits EPM System.</p> <p>Les ID utilisateur (valeur de l'attribut de connexion) doivent être identiques pour tous les annuaires des utilisateurs. Par exemple, vous pouvez utiliser <code>uid</code> et <code>sAMAccountName</code> respectivement en tant qu'attribut de connexion pour vos configurations SunONE et Active Directory. Les valeurs de ces attributs doivent être uniques pour tous les annuaires des utilisateurs, notamment l'annuaire natif.</p>

 **Remarque :**

Les ID utilisateur ne respectent pas la casse.


 **Remarque :**

Si vous configurez OID en tant qu'annuaire des utilisateurs externe pour les produits EPM System déployés sur Oracle Application Server, dans un environnement Kerberos, vous devez attribuer à cette propriété la valeur `userPrincipalName`.

**Valeur par défaut**

- **Active Directory :** `cn`
- **Annuaire LDAP différents d'Active Directory :** `uid`

Tableau 4-2 (suite) Ecran Configuration de l'utilisateur

Libellé	Description <sup>1</sup>
Attribut de prénom	Attribut qui stocke le prénom de l'utilisateur. <b>Valeur par défaut</b> : <code>givenName</code>
Attribut de nom de famille	Attribut qui stocke le nom de famille de l'utilisateur. <b>Valeur par défaut</b> : <code>sn</code>
Attribut de courriel	<b>Facultatif</b> : attribut qui stocke l'adresse électronique de l'utilisateur. <b>Valeur par défaut</b> : <code>mail</code>
Classe d'objet	Classes d'objet de l'utilisateur (attributs obligatoires et facultatifs qui peuvent être associés à l'utilisateur). Shared Services utilise les classes d'objet répertoriées dans cet écran dans le filtre de recherche. Grâce à elles, Shared Services est à même de trouver tous les utilisateurs auxquels des privilèges d'accès doivent être attribués.
	<div style="border: 1px solid #0070C0; padding: 10px; background-color: #E6F2FF;"> <p> <b>Remarque :</b></p> <p>Si vous configurez Active Directory ou ADAM comme type d'annuaire des utilisateurs <code>Autre</code> afin d'utiliser un attribut d'ID personnalisé, vous devez définir cette valeur sur <code>user</code>.</p> </div>
	<p>Si nécessaire, vous pouvez ajouter des classes d'objet manuellement. Pour ajouter une classe d'objet, entrez le nom de la classe d'objet dans la zone <b>Classe d'objet</b>, puis cliquez sur <b>Ajouter</b>.</p> <p>Pour enlever des classes d'objet, sélectionnez la classe d'objet, puis cliquez sur <b>Enlever</b>.</p> <p><b>Valeur par défaut</b></p> <ul style="list-style-type: none"> <li>• <b>Active Directory</b> : <code>user</code></li> <li>• <b>Annuaire LDAP différents d'Active Directory</b> : <code>person</code>, <code>organizationalPerson</code>, <code>inetorgperson</code></li> </ul>
Filtrer pour limiter les utilisateurs	<p>Requête LDAP qui extrait uniquement les utilisateurs auxquels des privilèges d'accès propres aux rôles des produits EPM System doivent être attribués. Par exemple, la requête LDAP (<code>uid=Hyp*</code>) extrait uniquement les utilisateurs dont le nom commence par <code>Hyp</code>.</p> <p>L'écran Configuration de l'utilisateur valide le DN relatif de l'utilisateur et recommande l'utilisation d'un filtre utilisateur, s'il est requis.</p> <p>Le filtre utilisateur limite le nombre d'utilisateurs renvoyés au cours d'une requête. Il est particulièrement important si le noeud identifié par le DN relatif de l'utilisateur contient de nombreux utilisateurs pour lesquels aucun privilège d'accès n'est à attribuer. Ces filtres peuvent être conçus pour exclure les utilisateurs ne nécessitant pas de privilège d'accès et améliorer ainsi les performances.</p>

**Tableau 4-2 (suite) Ecran Configuration de l'utilisateur**

Libellé	Description <sup>1</sup>
Attribut de recherche d'utilisateur pour le nom distinctif relatif multi-attribut	<p><b>Annuaire des utilisateurs LDAP autres qu'Active Directory uniquement</b> : définissez cette valeur seulement si le serveur d'annuaire est configuré pour utiliser un nom distinctif relatif multi-attribut. La valeur que vous définissez doit correspondre à l'un des attributs de nom distinctif relatif. La valeur de l'attribut spécifié doit être unique et l'attribut doit pouvoir faire l'objet d'une recherche.</p> <p>Par exemple, supposons qu'un serveur d'annuaire SunONE est configuré de manière à combiner les attributs <code>cn</code> (<code>cn=John Doe</code>) et <code>uid</code> (<code>uid=jDoe12345</code>) pour créer un nom distinctif relatif multi-attribut semblable à l'exemple suivant :</p> <pre>cn=John Doe+uid=jDoe12345, ou=people, dc=myCompany, dc=com</pre> <p>Dans ce cas, vous pouvez utiliser <code>cn</code> ou <code>uid</code> si ces attributs remplissent les conditions suivantes :</p> <ul style="list-style-type: none"> <li>• L'attribut peut être recherché par l'utilisateur identifié dans le nom distinctif de l'utilisateur enregistré sur l'onglet Informations de connexion.</li> <li>• L'attribut exige que vous définissiez une valeur unique dans l'annuaire des utilisateurs.</li> </ul>
Résoudre les groupes principaux personnalisés	<p><b>Active Directory uniquement</b> : cette case à cocher indique si les groupes d'utilisateurs principaux doivent être identifiés pour définir les rôles en vigueur. Elle est activée par défaut. Oracle recommande de laisser ce paramètre tel quel.</p>
Afficher un avertissement si le mot de passe de l'utilisateur expire dans	<p><b>Active Directory uniquement</b> : cette case à cocher indique si un message d'avertissement doit être affiché en cas d'expiration du mot de passe de l'utilisateur Active Directory après le nombre de jours spécifié.</p>

<sup>1</sup> La sécurité EPM System peut utiliser des valeurs par défaut pour certains champs dont les valeurs de configuration sont facultatives. Si vous n'entrez pas de valeur dans ces champs, les valeurs par défaut sont utilisées au moment de l'exécution.

**9. Cliquez sur [Suivant](#).**

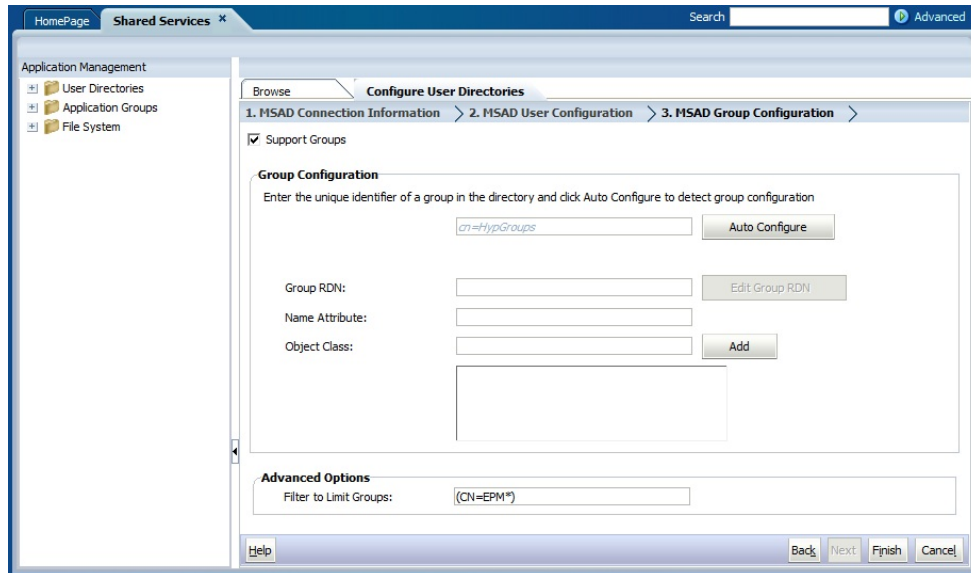
L'écran Configuration de groupe s'ouvre. Shared Services utilise les propriétés définies dans cet écran pour créer l'URL de groupe qui détermine le noeud où la recherche de groupes doit commencer. L'utilisation de cette URL accélère la recherche.

**▲ Attention :**

L'URL de groupe ne doit pas pointer vers un alias. La sécurité d'EPM System requiert que l'URL de groupe pointe vers un groupe réel. Si vous configurez un annuaire d'utilisateurs Novell eDirectory qui utilise des alias de groupe, les alias et comptes de groupe doivent être disponibles dans l'URL de groupe.

 **Remarque :**

La saisie de données dans l'écran Configuration de groupe est facultative. Si vous n'entrez pas de paramètres d'URL de groupe, Shared Services effectue une recherche dans le nom distinctif de base pour trouver des groupes, ce qui peut affecter la performance de manière négative, surtout si l'annuaire des utilisateurs contient de nombreux groupes.



10. Désactivez l'option **Prendre en charge les groupes** si votre organisation ne prévoit pas de provisionner des groupes ou si les utilisateurs ne sont pas répartis en groupes dans l'annuaire des utilisateurs. Cette action désactive les champs de cet écran.

Si vous prenez en charge les groupes, Oracle recommande d'utiliser la fonction de configuration automatique pour extraire les informations requises.

Si vous configurez OID en tant qu'annuaire des utilisateurs, vous ne pouvez pas utiliser la fonction de configuration automatique, car le DSE racine d'OID ne contient pas d'entrée dans l'attribut des contextes de dénomination. Reportez-vous à la section [Gestion des contextes de dénomination](#) dans le *Guide de l'administrateur Oracle Fusion Middleware pour Oracle Internet Directory*.

11. Dans la zone de texte **Configuration automatique**, entrez un identifiant de groupe unique, puis cliquez sur **Aller**.

L'identifiant de groupe doit être exprimé au format *attribute=identifieur* (par exemple, *cn=western\_region*).

Les attributs de groupe sont affichés dans la zone Configuration de groupe.

 **Remarque :**

Vous pouvez entrer les attributs de groupe requis dans les zones de texte Configuration de groupe.

 **Attention :**

Si l'URL de groupe n'est pas définie pour les annuaires des utilisateurs qui contiennent une barre oblique (/) ou une barre oblique inverse (\) dans le nom de leurs noeuds, la recherche d'utilisateurs et de groupes échoue. Par exemple, les opérations permettant de répertorier des utilisateurs ou des groupes échouent si l'URL de groupe n'est pas spécifiée pour un annuaire contenant des utilisateurs et des groupes dans un noeud tel que `OU=child\ou,OU=parent/ou` ou `OU=child/ou,OU=parent \ ou`.

**Tableau 4-3 Ecran Configuration de groupe**

Libellé	Description <sup>1</sup>
DN relatif du groupe	<p>Nom distinctif relatif du groupe. Cette valeur, qui est le chemin relatif au nom distinctif de base, est utilisée comme URL du groupe.</p> <p>Spécifiez un DN relatif du groupe qui identifie le noeud d'annuaire des utilisateurs le plus bas dans lequel tous les groupes que vous souhaitez provisionner sont disponibles.</p> <p>Si vous utilisez un groupe principal Active Directory pour le provisionnement, assurez-vous qu'il figure dans le DN relatif du groupe. Shared Services n'extrait pas le groupe principal s'il n'appartient pas à l'URL du groupe.</p> <p>Le DN relatif du groupe a un effet important sur les performances de connexion et de recherche. Dans la mesure où il est le point de départ de toutes les recherches de groupes, vous devez identifier le noeud le plus bas possible dans lequel tous les groupes des produits EPM System sont disponibles. Pour garantir une performance optimale, le nombre de groupes présents dans le DN relatif du groupe ne doit pas dépasser 10 000. Si plus de groupes sont présents, utilisez un filtre de groupe pour extraire uniquement les groupes à affecter.</p>


 **Remarque :**

Shared Services génère un avertissement si le nombre de groupes disponibles dans le DN relatif du groupe dépasse 10 000.

Pour plus d'informations sur les restrictions, reportez-vous à la section [Utilisation des caractères spéciaux](#).

**Exemple :** `ou=Groups`

**Tableau 4-3 (suite) Ecran Configuration de groupe**

Libellé	Description <sup>1</sup>
Attribut de nom	<p>Attribut qui stocke le nom du groupe</p> <p><b>Valeur par défaut</b></p> <ul style="list-style-type: none"> <li>• <b>Annuaire LDAP, y compris Active Directory</b> : cn</li> <li>• <b>Annuaire natif</b> : cssDisplayNameDefault</li> </ul>
Classe d'objet	<p>Classes d'objet du groupe. Shared Services utilise les classes d'objet répertoriées dans cet écran dans le filtre de recherche. Grâce à elles, Shared Services est à même de trouver tous les groupes associés à l'utilisateur.</p>
	<div style="border: 1px solid #0070C0; padding: 10px; background-color: #E6F2FF;"> <p> <b>Remarque :</b></p> <p>Si vous configurez Active Directory ou ADAM comme type d'annuaire des utilisateurs Autre afin d'utiliser un attribut d'ID personnalisé, vous devez définir cette valeur sur group?member.</p> </div> <p>Si nécessaire, vous pouvez ajouter des classes d'objet manuellement. Pour ce faire, entrez le nom de la classe d'objet dans la zone de texte Classe d'objet, puis cliquez sur <b>Ajouter</b>. Pour supprimer des classes d'objet, sélectionnez la classe d'objet, puis cliquez sur <b>Enlever</b>.</p> <p><b>Valeur par défaut</b></p> <ul style="list-style-type: none"> <li>• <b>Active Directory</b> : group?member</li> <li>• <b>Annuaire LDAP différents d'Active Directory</b> : groupofuniquenames?uniquemember, groupOfNames?member</li> <li>• <b>Annuaire natif</b> : groupofuniquenames?uniquemember, cssGroupExtend?cssIsActive</li> </ul>
Filtrer pour limiter les groupes	<p>Requête LDAP qui extrait uniquement les groupes auxquels des privilèges d'accès propres aux rôles des produits EPM System doivent être attribués. Par exemple, la requête LDAP ( (cn=Hyp*)(cn=Admin*)) extrait uniquement les groupes dont le nom commence par Hyp ou Admin.</p> <p>Le filtre de groupe permet de limiter le nombre de groupes renvoyés au cours d'une requête. Il est particulièrement important si le noeud identifié par le DN relatif du groupe contient de nombreux groupes pour lesquels aucun privilège d'accès n'est à attribuer. Ces filtres peuvent être conçus pour exclure les groupes ne nécessitant pas de privilège d'accès et améliorer ainsi la performance.</p> <p>Si vous utilisez le groupe principal Active Directory pour le provisionnement, assurez-vous que tous les filtres de groupe que vous définissez peuvent extraire le groupe principal contenu dans l'URL du groupe. Par exemple, le filtre ( (cn=Hyp*)(cn=Domain Users)) extrait les groupes dont le nom commence par Hyp et dont le groupe principal est nommé Domain Users.</p>

<sup>1</sup> La sécurité EPM System peut utiliser des valeurs par défaut pour certains champs dont les valeurs de configuration sont facultatives. Si vous n'entrez pas de valeur dans ces champs, les valeurs par défaut sont utilisées au moment de l'exécution.

**12.** Cliquez sur **Terminer**.

Shared Services enregistre la configuration et retourne à l'écran Annuaires des utilisateurs définis qui affiche désormais l'annuaire des utilisateurs que vous configuré.

**13.** Testez la configuration. Reportez-vous à la section [Test des connexions de l'annuaire des utilisateurs](#).

**14.** Si nécessaire, changez l'affectation de l'ordre de recherche. Pour plus d'informations, reportez-vous à la section [Gestion de l'ordre de recherche de l'annuaire des utilisateurs](#).

**15.** Si nécessaire, spécifiez les paramètres de sécurité. Pour plus d'informations, reportez-vous à la section [Configuration des options de sécurité](#).

**16.** Redémarrez Oracle Hyperion Foundation Services et d'autres composants EPM System.

## Configuration des bases de données relationnelles en tant qu'annuaires des utilisateurs

Les informations sur l'utilisateur et le groupe provenant des tables système des bases de données relationnelles Oracle, SQL Server et IBM DB2 peuvent être utilisées pour prendre en charge le provisionnement. Si les informations sur les groupes ne peuvent pas être dérivées du schéma de système de la base de données, Oracle Hyperion Shared Services ne prend pas en charge le provisionnement des groupes à partir de ce fournisseur de bases de données. Par exemple, Shared Services ne peut pas extraire les informations de groupe à partir d'anciennes versions d'IBM DB2, car cette base de données utilise les groupes définis sur le système d'exploitation. Toutefois, les gestionnaires de profils peuvent ajouter ces utilisateurs aux groupes dans l'annuaire natif et provisionner ces groupes. Pour plus d'informations sur les plates-formes prises en charge, reportez-vous à la *Matrice de certification Oracle Enterprise Performance Management System* publiée sur la page [Configurations système prises en charge par Oracle Fusion Middleware](#) sur Oracle Technology Network (OTN).

 **Remarque :**

Si vous utilisez une base de données DB2, le nom d'utilisateur doit comporter au moins huit caractères. Les noms d'utilisateurs ne doivent pas dépasser 256 caractères pour les bases de données Oracle et SQL Server, et 1 000 caractères pour les bases de données DB2.

Configurez Shared Services pour vous connecter à la base de données en tant qu'administrateur ; par exemple, l'utilisateur d'Oracle `SYSTEM`, pour extraire la liste des utilisateurs et des groupes.

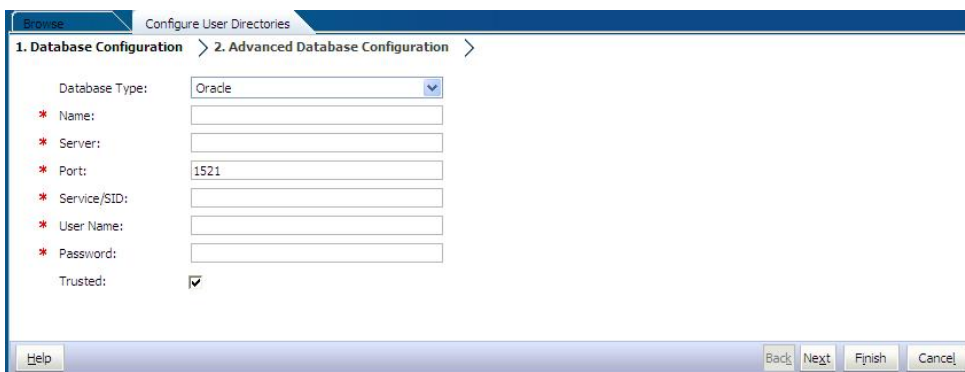


 **Remarque :**

Shared Services n'extrait que les utilisateurs de base de données actifs pour le provisionnement. Les comptes d'utilisateurs de base de données inactifs et verrouillés sont ignorés.

Pour configurer les fournisseurs de bases de données :

1. Accédez à Oracle Hyperion Shared Services Console en tant qu'administrateur système. Reportez-vous à la section [Lancement de Shared Services Console](#).
2. Sélectionnez **Administration**, puis **Configurer les annuaires des utilisateurs**.
3. Cliquez sur **Nouveau**.
4. Dans l'écran **Type d'annuaire**, sélectionnez **Base de données relationnelle (Oracle, DB2, SQL Server)**.
5. Cliquez sur **Suivant**.



The screenshot shows a web-based configuration window titled 'Configure User Directories'. It is currently on the 'Advanced Database Configuration' step. The 'Database Type' dropdown is set to 'Oracle'. Below it are several required fields marked with a red asterisk: 'Name', 'Server', 'Port' (containing '1521'), 'Service/SID', 'User Name', and 'Password'. There is also a 'Trusted' checkbox which is checked. At the bottom of the window, there are buttons for 'Help', 'Back', 'Next', 'Finish', and 'Cancel'.

6. Dans l'onglet Configuration de la base de données, saisissez les paramètres de configuration.

**Tableau 4-4 Onglet Configuration de la base de données**

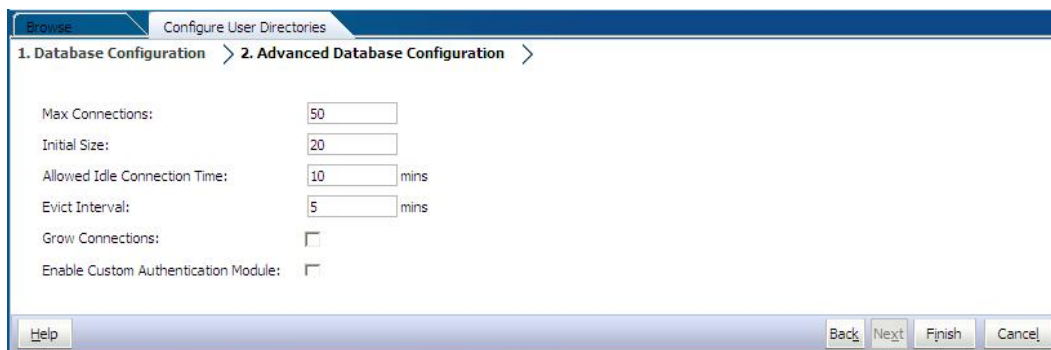
Libellé	Description
Type de base de données	Le fournisseur de bases de données relationnelles. Shared Services prend en charge uniquement les bases de données Oracle et SQL Server comme fournisseurs de bases de données. <b>Exemple :</b> Oracle
Nom	Nom de configuration unique pour le fournisseur de la base de données. <b>Exemple :</b> Oracle_DB_FINANCE
Serveur	Nom DNS de l'ordinateur sur lequel le serveur de bases de données est en cours d'exécution. <b>Exemple :</b> myserver
Port	Numéro de port du serveur de bases de données. <b>Exemple :</b> 1521

Tableau 4-4 (suite) Onglet Configuration de la base de données

Libellé	Description
Service/SID (Oracle uniquement)	L'identificateur du système (la valeur par défaut est <code>orcl</code> ). <b>Exemple</b> : <code>orcl</code>
Base de données (SQL Server et DB2 uniquement)	Base de données à laquelle Shared Services doit se connecter. <b>Exemple</b> : <code>master</code>
Nom d'utilisateur	Le nom d'utilisateur que Shared Services doit utiliser pour accéder à la base de données. Cet utilisateur de base de données doit avoir des privilèges d'accès aux tables système de base de données. Oracle vous recommande d'utiliser le compte <code>system</code> pour les bases de données Oracle et le nom d'utilisateur de l'administrateur de la base de données pour les bases de données SQL Server. <b>Exemple</b> : <code>SYSTEM</code>
Mot de passe	Mot de passe de l'utilisateur identifié dans <b>Nom d'utilisateur</b> . <b>Exemple</b> : <code>system_password</code>
Sécurisé	Case qui indique que ce fournisseur est une source SSO sécurisée. Les jetons SSO de sources sécurisées ne contiennent pas le mot de passe de l'utilisateur.

7. **Facultatif** : cliquez sur **Suivant** pour configurer le pool de connexions.

L'onglet Configuration avancée de la base de données s'affiche.



8. Dans Configuration avancée de la base de données, saisissez les paramètres de pool de connexions.

Tableau 4-5 Onglet Configuration avancée de la base de données

Libellé	Description
Nombre maximal de connexions	Nombre maximal de connexions dans le pool. La valeur par défaut est 50.
Taille initiale	Connexions disponibles quand le pool est initialisé. La valeur par défaut est 20.
Durée d'inactivité autorisée pour la connexion	<b>Facultatif</b> : durée après laquelle le processus d'exclusion supprime les connexions inactives du pool. La valeur par défaut est 10 minutes.

Tableau 4-5 (suite) Onglet Configuration avancée de la base de données

Libellé	Description
Intervalle d'exclusion	<b>Facultatif</b> : intervalle d'exécution du processus d'exclusion pour nettoyer le pool. L'exclusion supprime les connexions inactives qui ont dépassé la durée d'inactivité autorisée pour la connexion. La valeur par défaut est cinq minutes.
Augmenter les connexions	Indique si le pool de connexions peut augmenter au-delà du nombre maximal de connexions. Par défaut, cette option est désactivée, ce qui indique que le pool ne peut pas augmenter. Dans ce cas, le système renvoie une erreur si une connexion n'est pas disponible dans le délai défini pour le paramètre Dépassement du délai.
Activer le module d'authentification personnalisé	La case à cocher pour activer l'utilisation d'un module d'authentification personnalisé pour authentifier les utilisateurs définis dans cet annuaire des utilisateurs. Vous devez également saisir le nom de classe Java qualifié complet du module d'authentification dans l'écran Options de sécurité. Reportez-vous à la section <a href="#">Configuration des options de sécurité</a> . L'authentification via un module d'authentification personnalisé est transparente pour les clients lourds et légers. Reportez-vous à la section "Utilisation d'un module d'authentification personnalisé" du <i>Guide de configuration de la sécurité d'Oracle Enterprise Performance Management System</i> .

9. Cliquez sur **Terminer**.
10. Cliquez sur **OK** pour revenir à l'écran Annuaire des utilisateurs définis.
11. Testez la configuration du fournisseur de bases de données. Reportez-vous à la section [Test des connexions de l'annuaire des utilisateurs](#).
12. Changez l'affectation de l'ordre de recherche, si nécessaire. Pour plus d'informations, reportez-vous à la section [Gestion de l'ordre de recherche de l'annuaire des utilisateurs](#).
13. Spécifiez les paramètres de sécurité, si nécessaire. Reportez-vous à la section [Configuration des options de sécurité](#).
14. Redémarrez Oracle Hyperion Foundation Services et les autres composants Oracle Enterprise Performance Management System.

## Test des connexions de l'annuaire des utilisateurs

Une fois un annuaire des utilisateurs configuré, testez la connexion afin de vous assurer qu'Oracle Hyperion Shared Services peut se connecter à l'annuaire des utilisateurs à l'aide des paramètres actuels.

Pour tester la connexion d'un annuaire des utilisateurs :

1. Accédez à Oracle Hyperion Shared Services Console en tant qu'administrateur système. Reportez-vous à [Lancement de Shared Services Console](#).
2. Sélectionnez **Administration**, puis **Configurer les annuaires des utilisateurs**.
3. Dans la liste des annuaires des utilisateurs, sélectionnez la configuration d'un annuaire d'utilisateurs externe à tester.
4. Cliquez sur **Tester**, puis sur **OK**.

## Modification des paramètres d'annuaire des utilisateurs

Les administrateurs peuvent modifier tous les paramètres, autres que le nom, d'une configuration d'annuaire des utilisateurs. Oracle recommande de ne pas modifier les données de configuration des annuaires des utilisateurs utilisés pour le provisionnement.

### Attention :

La modification de certains paramètres, `Attribut d'ID` par exemple, dans la configuration de l'annuaire des utilisateurs rend non valides les données de provisionnement. Soyez très prudent lorsque vous modifiez les paramètres d'un annuaire d'utilisateurs auquel des privilèges d'accès ont été attribués.

Pour modifier la configuration d'un annuaire des utilisateurs :

1. Accédez à Oracle Hyperion Shared Services Console en tant qu'administrateur système. Reportez-vous à [Lancement de Shared Services Console](#).
2. Sélectionnez **Administration**, puis **Configurer les annuaires des utilisateurs**.
3. Sélectionnez un annuaire des utilisateurs à modifier.
4. Cliquez sur **Modifier**.
5. Modifiez les paramètres de configuration.

### Remarque :

Vous ne pouvez pas modifier le nom de la configuration. Si vous modifiez la configuration d'un annuaire des utilisateurs LDAP, vous pouvez choisir un serveur d'annuaire différent ou l'option `Autre` (pour les annuaires LDAP personnalisés) dans la liste des serveurs d'annuaire. Vous ne pouvez pas modifier les paramètres de l'annuaire natif.

Pour obtenir des explications sur les paramètres que vous pouvez modifier, consultez les tables suivantes :

- Active Directory et autres annuaires des utilisateurs LDAP : reportez-vous aux tableaux de la section [Configuration d'OID, Active Directory et d'autres annuaires des utilisateurs LDAP](#).
  - Bases de données : reportez-vous au tableau de la section [Configuration des bases de données relationnelles en tant qu'annuaires des utilisateurs](#)
6. Cliquez sur **OK** pour enregistrer les modifications.

## Suppression des configurations d'annuaires des utilisateurs

Les administrateurs système peuvent à tout moment supprimer la configuration d'un annuaire des utilisateurs externe. La suppression de la configuration d'une annuaire rend non valides

toutes les informations sur le provisionnement pour les utilisateurs et les groupes dérivés de l'annuaire des utilisateurs et retire l'annuaire de l'ordre de recherche.

 **Conseil :**

Si vous ne voulez pas utiliser un annuaire des utilisateurs configuré qui a été utilisé pour le provisionnement, retirez-le de l'ordre de recherche afin qu'il ne fasse pas l'objet d'une recherche d'utilisateurs et de groupes. Cette action conserve l'intégrité des informations sur le provisionnement et vous permet d'utiliser l'annuaire des utilisateurs plus tard.

Pour supprimer une configuration d'annuaire, procédez comme suit :

1. Accédez à Oracle Hyperion Shared Services Console en tant qu'administrateur système. Reportez-vous à [Lancement de Shared Services Console](#).
2. Sélectionnez **Administration**, puis **Configurer les annuaires des utilisateurs**.
3. Sélectionnez un répertoire.
4. Cliquez sur **Supprimer**.
5. Cliquez sur **OK**.
6. Cliquez à nouveau sur **OK**.
7. Redémarrez Oracle Hyperion Foundation Services et les autres composants Oracle Enterprise Performance Management System.

## Gestion de l'ordre de recherche de l'annuaire des utilisateurs

Lorsqu'un administrateur système configure un annuaire des utilisateurs externe, Oracle Hyperion Shared Services l'ajoute automatiquement à l'ordre de recherche et lui affecte la séquence de recherche disponible suivante juste avant celle de l'annuaire natif. L'ordre de recherche est utilisé pour effectuer un cycle complet sur les annuaires des utilisateurs configurés quand Oracle Enterprise Performance Management System recherche des utilisateurs et des groupes.

Les administrateurs système peuvent supprimer un annuaire des utilisateurs de l'ordre de recherche. Dans ce cas, Shared Services réaffecte automatiquement l'ordre de recherche des annuaires restants. Les annuaires des utilisateurs non inclus dans l'ordre de recherche ne sont pas utilisés pour prendre en charge l'authentification et le provisionnement.

 **Remarque :**

Shared Services met fin à la recherche de l'utilisateur ou du groupe lorsqu'il rencontre le compte indiqué. Oracle recommande de placer l'annuaire d'entreprise qui contient la majeure partie des utilisateurs EPM System en premier dans l'ordre de recherche.

Par défaut, l'annuaire natif est défini comme dernier annuaire de l'ordre de recherche. Les administrateurs peuvent effectuer les tâches suivantes pour gérer l'ordre de recherche :

- [Ajout d'un annuaire des utilisateurs à l'ordre de recherche](#)
- [Modification de l'ordre de recherche](#)
- [Suppression de l'affectation d'un ordre de recherche](#)

### Ajout d'un annuaire des utilisateurs à l'ordre de recherche

Un annuaire des utilisateurs qui vient d'être configuré est automatiquement ajouté à l'ordre de recherche. Si vous avez supprimé un annuaire de l'ordre de recherche, vous pouvez l'ajouter à la fin de l'ordre de recherche.

Pour ajouter un annuaire des utilisateurs à l'ordre de recherche :

1. Accédez à Oracle Hyperion Shared Services Console en tant qu'administrateur système. Reportez-vous à la section [Lancement de Shared Services Console](#).
2. Sélectionnez **Administration**, puis **Configurer les annuaires des utilisateurs**.
3. Sélectionnez un annuaire des utilisateurs désactivé à ajouter à l'ordre de recherche.
4. Cliquez sur **Inclure**.  
Ce bouton est disponible seulement si vous avez sélectionné un utilisateur qui ne figure pas dans l'ordre de recherche.
5. Cliquez sur **OK** pour revenir à l'écran Annuaires des utilisateurs définis.
6. Redémarrez Oracle Hyperion Foundation Services et d'autres composants EPM System.

### Suppression de l'affectation d'un ordre de recherche

Le retrait d'un annuaire d'utilisateurs de l'ordre de recherche ne rend pas la configuration de l'annuaire non valide. Elle enlève cet annuaire de la liste des annuaires analysés pour authentifier les utilisateurs. Un annuaire qui n'est pas inclus dans l'ordre de recherche a le statut **Désactivé**. Lorsqu'un administrateur supprime un annuaire des utilisateurs de l'ordre de recherche, la séquence de recherche affectée aux autres annuaires des utilisateurs est automatiquement mise à jour.

#### **Remarque :**

L'annuaire natif ne peut pas être enlevé de l'ordre de recherche.

Pour supprimer un annuaire des utilisateurs de l'ordre de recherche :

1. Accédez à Shared Services Console en tant qu'administrateur système. Reportez-vous à la section [Lancement de Shared Services Console](#).
2. Sélectionnez **Administration**, puis **Configurer les annuaires des utilisateurs**.
3. Sélectionnez un annuaire à enlever de l'ordre de recherche.
4. Cliquez sur **Exclure**.
5. Cliquez sur **OK**.
6. Cliquez sur **OK** dans l'écran Résultat de la configuration de l'annuaire.

7. Redémarrez Foundation Services et d'autres composants EPM System.

### Modification de l'ordre de recherche

L'ordre de recherche par défaut affecté à chaque annuaire des utilisateurs est basé sur la séquence selon laquelle l'annuaire a été configuré. Par défaut, l'annuaire natif est défini comme dernier annuaire de l'ordre de recherche.

Pour modifier l'ordre de recherche :

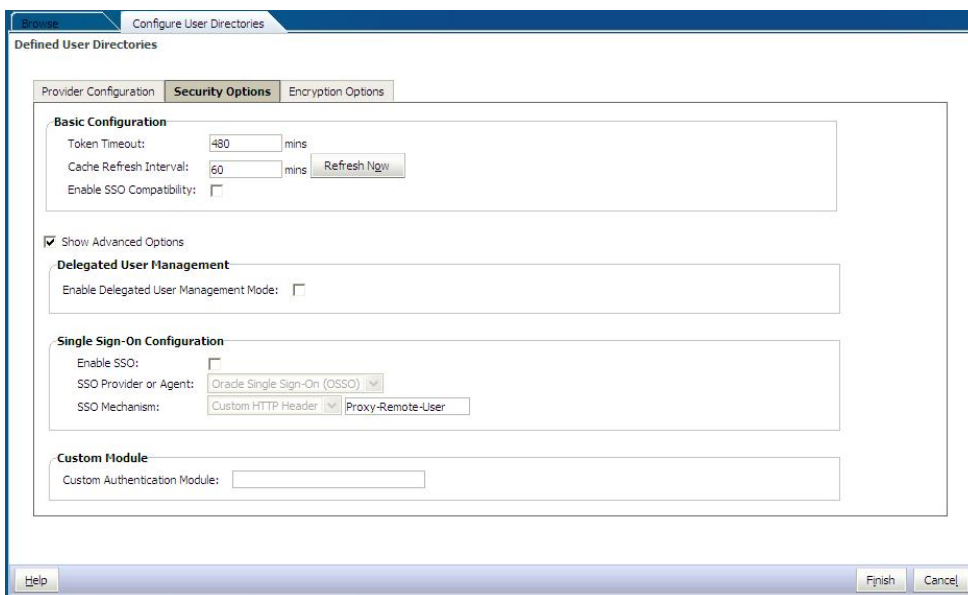
1. Accédez à Shared Services Console en tant qu'administrateur système. Reportez-vous à la section [Lancement de Shared Services Console](#).
2. Sélectionnez **Administration**, puis **Configurer les annuaires des utilisateurs**.
3. Sélectionnez l'annuaire dont vous voulez modifier l'ordre de recherche.
4. Cliquez sur **Déplacer vers le haut** ou **Déplacer vers le bas**.
5. Cliquez sur **OK**.
6. Redémarrez Foundation Services, d'autres composants EPM System et des applications personnalisées qui utilisent les API de sécurité Shared Services.

## Configuration des options de sécurité


Les options de sécurité comprennent les paramètres globaux applicables à tous les annuaires des utilisateurs inclus dans l'ordre de recherche.

Pour définir les options de sécurité :

1. Accédez à Oracle Hyperion Shared Services Console en tant qu'administrateur système. Reportez-vous à [Lancement de Shared Services Console](#).
2. Sélectionnez **Administration**, puis **Configurer les annuaires des utilisateurs**.
3. Sélectionnez **Options de sécurité**.
4. Dans **Options de sécurité**, définissez les paramètres globaux.




**Tableau 4-6 Définition des options pour les annuaires des utilisateurs**

Paramètre	Description
Délai d'expiration du jeton	Temps (en minutes) après lequel le jeton SSO délivré par les produits Oracle Enterprise Performance Management System ou la solution de gestion des identités Web expire. Les utilisateurs doivent se connecter à nouveau après cette période. Le Délai d'expiration du jeton est défini par rapport à l'horloge système du serveur. La valeur par défaut est de 480 minutes.
	<div style="border: 1px solid #0070C0; padding: 10px; background-color: #E6F2FF;"> <p> <b>Remarque :</b></p> <p>Le Délai d'expiration du jeton est différent du délai d'expiration de la session.</p> </div>
Intervalle d'actualisation du cache	Intervalle d'actualisation (en minutes) du cache Oracle Hyperion Shared Services qui contient les données de relation entre groupes et utilisateurs. La valeur par défaut est de 60 minutes. Shared Services met en mémoire cache les informations relatives aux nouveaux groupes des annuaires des utilisateurs externes et aux nouveaux utilisateurs ajoutés aux groupes existants uniquement après l'actualisation suivante du cache. Les utilisateurs auxquels des privilèges d'accès sont accordés via un groupe d'annuaires des utilisateurs externes nouvellement créé n'obtiennent pas les rôles correspondants avant l'actualisation du cache.
Actualiser maintenant	Cliquez sur ce bouton pour lancer manuellement l'actualisation du cache Shared Services qui contient les données de relation entre les groupes et les utilisateurs. Vous pouvez vouloir lancer une actualisation du cache après avoir créé et provisionné des groupes dans les annuaires des utilisateurs externes ou après avoir ajouté de nouveaux utilisateurs à des groupes existants. La mémoire cache est actualisée uniquement après un appel utilisant les données du cache de la part de Shared Services.
Activer la compatibilité SSO	Sélectionnez cette option si votre déploiement est intégré à Oracle Business Intelligence Enterprise Edition version 11.1.1.5 ou antérieure.
Activer le mode de gestion déléguée des utilisateurs	Option permettant d'activer la gestion déléguée des utilisateurs des produits EPM System pour prendre en charge la gestion distribuée des activités de provisionnement. Reportez-vous à la section "Gestion déléguée des utilisateurs" dans le <i>Guide d'administration de la sécurité utilisateur d'Oracle Enterprise Performance Management System</i> .
Activer l'authentification unique	Option permettant d'activer la prise en charge de l'authentification unique à partir d'agents de sécurité tels qu'Oracle Access Manager.



**Tableau 4-6 (suite) Définition des options pour les annuaires des utilisateurs**

Paramètre	Description
Fournisseur ou agent d'authentification unique	<p>Sélectionnez la solution de gestion des identités Web depuis laquelle les produits EPM System doivent accepter l'authentification unique. Sélectionnez <b>Autre</b> si votre solution de gestion des identités Web (par exemple, Kerberos) n'est pas répertoriée.</p> <p>Le mécanisme et le nom privilégiés de connexion unique sont automatiquement sélectionnés lorsque vous sélectionnez le fournisseur de connexion unique. Vous pouvez modifier le nom du mécanisme de connexion unique (en-tête HTTP ou classe de connexion personnalisée), si nécessaire.</p> <p>Si vous sélectionnez <b>Autre</b> comme fournisseur ou agent SSO, vous devez vous assurer qu'il prend en charge un mécanisme SSO pris en charge par EPM System. Reportez-vous à la section "Méthodes d'authentification unique prises en charge" du <i>Guide de configuration de la sécurité d'Oracle Enterprise Performance Management System</i>.</p>
Mécanisme SSO	<p>Méthode utilisée par la solution de gestion des identités Web sélectionnée pour attribuer un nom de connexion d'utilisateur aux produits EPM System. Pour obtenir une description des méthodes d'authentification unique possibles, reportez-vous à la section "Méthodes d'authentification unique prises en charge" du <i>Guide de configuration de la sécurité d'Oracle Enterprise Performance Management System</i>.</p> <ul style="list-style-type: none"> <li>• En-tête HTTP personnalisé : définissez le nom de l'en-tête que l'agent de sécurité transmet à EPM System.</li> <li>• Personnaliser la classe de connexion : indiquez la classe Java personnalisée gérant les demandes HTTP pour l'authentification. Reportez-vous à la section "Classe de connexion personnalisée" du <i>Guide de configuration de la sécurité d'Oracle Enterprise Performance Management System</i>.</li> </ul> <div style="border: 1px solid #0070C0; padding: 10px; margin: 10px 0;"> <p> <b>Remarque :</b></p> <p>Classe de connexion personnalisée et authentification personnalisée ne sont pas identiques.</p> </div> <ul style="list-style-type: none"> <li>• En-tête d'autorisation HTTP : mécanisme HTTP standard.</li> <li>• Obtenir les utilisateurs à distance à partir d'une requête HTTP : sélectionnez cette option si l'agent de sécurité renseigne l'utilisateur à distance dans la demande HTTP.</li> </ul>

**Tableau 4-6 (suite) Définition des options pour les annuaires des utilisateurs**

Paramètre	Description
Module d'authentification personnalisé	<p>Nom de classe Java qualifié complet du module d'authentification personnalisé (com.mycompany.epm.CustomAuthenticationImpl, par exemple) à utiliser pour authentifier les utilisateurs dans tous les annuaires des utilisateurs pour lesquels le module d'authentification personnalisé est sélectionné. Le module d'authentification n'est utilisé pour un annuaire d'utilisateurs que si la configuration d'annuaire a activé son utilisation (option par défaut).</p> <p>Oracle Hyperion Foundation Services exige que le fichier JAR d'authentification personnalisée soit nommé CustomAuth.jar. CustomAuth.jar doit être disponible dans MIDDLEWARE_HOME\user_projects\domains\WEBLOGIC_DOMAIN\lib, généralement, C:\Oracle\Middleware\user_projects\domains\EPMSysystem/lib.</p> <p>Dans toutes les installations client, CustomAuth.jar doit être présent dans EPM_ORACLE_HOME/common/jlib/11.1.2.0, généralement, C:\Oracle\Middleware\EPMSysystem11R1\common\jlib\11.1.2.0.</p> <p>Vous pouvez utiliser n'importe quelle structure de composant et nom de classe dans le fichier JAR.</p> <p>Pour plus d'informations, reportez-vous à la section "Utilisation d'un module d'authentification personnalisé" du <i>Guide de configuration de la sécurité d'Oracle Enterprise Performance Management System</i>.</p>

5. Cliquez sur **OK**.
6. Redémarrez Foundation Services et d'autres composants EPM System.

## Régénération des clés de cryptage

Oracle Enterprise Performance Management System utilise les clés suivantes pour garantir la sécurité :

- Clé de cryptage de jeton d'authentification unique, utilisée pour crypter et décrypter les jetons SSO EPM System. Cette clé est stockée dans le registre Oracle Hyperion Shared Services
- Clé de service sécurisée, utilisée par les composants EPM System pour vérifier l'authenticité du service qui demande un jeton SSO
- Clé de cryptage de la configuration du fournisseur, utilisée pour crypter le mot de passe (mot de passe associé au DN de l'utilisateur pour les annuaires d'utilisateurs compatibles LDAP) qui permet à la sécurité EPM System d'établir un lien avec un annuaire d'utilisateurs externes configuré. Ce mot de passe est défini lors de la configuration de l'annuaire.

Modifiez ces clés régulièrement afin de renforcer la sécurité EPM System. Oracle Hyperion Shared Services et le sous-système de sécurité d'EPM System utilisent le cryptage AES avec une clé de 128 bits.

**▲ Attention :**

Les flux de tâches utilisés par Oracle Hyperion Financial Management et Oracle Hyperion Profitability and Cost Management sont invalidés lorsque vous régénérez la clé de cryptage d'authentification unique. Une fois la clé régénérée, ouvrez les flux de tâches, puis enregistrez-les pour les valider de nouveau.

Pour régénérer la clé de cryptage d'authentification unique, la clé de configuration du fournisseur ou la clé de service sécurisée, procédez comme suit :

1. Accédez à Oracle Hyperion Shared Services Console en tant qu'administrateur système. Reportez-vous à [Lancement de Shared Services Console](#).
2. Sélectionnez **Administration**, puis **Configurer les annuaires des utilisateurs**.
3. Sélectionnez **Options de cryptage**.
4. Dans **Options de cryptage**, sélectionnez la clé à régénérer.

**Tableau 4-7 Options de cryptage EPM System**

Option	Description
Jeton d'authentification unique	<p>Sélectionnez cette option pour régénérer la clé de cryptage qui permet de crypter et décrypter les jetons SSO EPM System.</p> <p>Sélectionnez l'un des boutons suivants si l'option <b>Activer la compatibilité SSO</b> est sélectionnée dans <b>Options de sécurité</b> :</p> <ul style="list-style-type: none"> <li>• <b>Générer une nouvelle clé</b> : permet de créer une clé de cryptage pour le jeton SSO</li> <li>• <b>Rétablir les valeurs par défaut</b> : permet de restaurer la clé de cryptage du jeton SSO par défaut</li> </ul>
Clé de service sécurisée	<p>Sélectionnez cette option pour régénérer la clé d'authentification sécurisée, utilisée par les composants EPM System pour vérifier l'authenticité du service qui demande un jeton SSO.</p>
Clé de configuration du fournisseur	<p>Sélectionnez cette option pour régénérer la clé utilisée pour crypter le mot de passe (mot de passe associé au DN de l'utilisateur pour les annuaires d'utilisateurs compatibles LDAP) qui permet à la sécurité EPM System d'établir un lien avec un annuaire des utilisateurs externe configuré. Ce mot de passe est défini lors de la configuration de l'annuaire.</p>

**✎ Remarque :**

Si vous rétablissez la clé de cryptage par défaut, vous devez supprimer le fichier de clés d'accès existant (`EPM_ORACLE_HOME/common/CSS/ssHandlerTK`) de tous les ordinateurs hôte EPM System.

5. Cliquez sur **OK**.
6. Si vous avez choisi de générer une nouvelle clé de cryptage SSO, effectuez cette étape.
  - a. Cliquez sur **Télécharger**.
  - b. Cliquez sur **OK** pour enregistrer `ssHandlerTK` (fichier de clés d'accès prenant en charge la nouvelle clé de cryptage SSO) dans un dossier du serveur qui héberge Oracle Hyperion Foundation Services.
  - c. Copiez `ssHandlerTK` dans `EPM_ORACLE_HOME/common/CSS` sur tous les ordinateurs hôte EPM System
7. Redémarrez Foundation Services et d'autres composants EPM System.

## Utilisation des caractères spéciaux

Active Directory et les autres annuaires des utilisateurs LDAP autorisent les caractères spéciaux dans les entités, telles que les DN, les noms d'utilisateur, les rôles et les noms de groupe. Un traitement spécial peut être nécessaire pour qu'Oracle Hyperion Shared Services comprenne ces caractères.

En général, vous devez utiliser des caractères d'échappement lorsque vous spécifiez des caractères spéciaux dans les paramètres de l'annuaire des utilisateurs (par exemple, les URL d'utilisateur et de groupe, et le DN de base). Le tableau suivant répertorie les caractères spéciaux autorisés dans les noms d'utilisateur, les noms de groupe, les URL d'utilisateur, les URL de groupe et la valeur OU du DN d'utilisateur.

**Tableau 4-8 Caractères spéciaux pris en charge**

Caractère	Nom ou signification	Caractère	Nom ou signification
(	parenthèse ouvrante	\$	dollar
)	parenthèse fermante	+	plus
"	guillemet	&	esperluette
'	guillemet simple	\	barre oblique inverse
,	virgule	^	caret
=	égal à	;	point-virgule
<	inférieur à	#	livre
>	supérieur à	@	at

### Remarque :

N'utilisez pas le caractère / (barre oblique) dans le nom d'unité organisationnelle indiqué dans le nom distinctif (DN) de base.

- Les caractères spéciaux ne sont pas autorisés dans la valeur de l'attribut Login User.
- L'astérisque (\*) n'est pas pris en charge dans les noms d'utilisateur et de groupe, les URL d'utilisateur et de groupe, ni dans le nom de l'OU dans le nom distinctif de l'utilisateur.
- Les valeurs d'attribut contenant une combinaison de caractères spéciaux ne sont pas prises en charge.

- L'esperluette (&) peut être utilisée sans caractère d'échappement. Pour les paramètres Active Directory, "&" doit être spécifié sous la forme &amp; ;.
- Les noms d'utilisateurs et de groupes ne peuvent pas contenir une barre oblique inverse (\) et une barre oblique (/). Par exemple, les noms tels que `test/  
\utilisateur` et `nouveau\test/utilisateur` ne sont pas pris en charge.

**Tableau 4-9 Caractères qui ne doivent pas être remplacés par des caractères d'échappement**

Caractère	Nom ou signification	Caractère	Nom ou signification
(	parenthèse ouvrante	'	guillemet simple
)	parenthèse fermante	^	caret
\$	dollar	@	at
&	Esperluette		



**Remarque :**

& doit être indiqué sous la forme &amp; ;.

Ces caractères doivent être remplacés par des caractères d'échappement si vous les utilisez dans les paramètres d'annuaire des utilisateurs (noms d'utilisateurs, noms de groupes, URL d'utilisateurs, URL de groupes et DN de l'utilisateur).

**Tableau 4-10 Echappement pour caractères spéciaux dans les paramètres de configuration de l'annuaire des utilisateurs**

Caractère spécial	Caractère d'échappement	Exemple de paramètre	Exemple de caractère avec caractère d'échappement
virgule (,)	barre oblique inverse (\)	<code>ou=test,ou</code>	<code>ou=test\,ou</code>
signe plus (+)	barre oblique inverse (\)	<code>ou=test+ou</code>	<code>ou=test\+ou</code>
égal à (=)	barre oblique inverse (\)	<code>ou=test=ou</code>	<code>ou=test\=ou</code>
livre (#)	barre oblique inverse (\)	<code>ou=test#ou</code>	<code>ou=test\#ou</code>
point-virgule (;)	barre oblique inverse (\)	<code>ou=test;ou</code>	<code>ou=test\;ou</code>
inférieur à (<)	barre oblique inverse (\)	<code>ou=test&lt;ou</code>	<code>ou=test\&lt;&lt;ou</code>
supérieur à (>)	barre oblique inverse (\)	<code>ou=test&gt;ou</code>	<code>ou=test\&gt;ou</code>
guillemet (")	deux barres obliques inverses (\)	<code>ou=test"ou</code>	<code>ou=test\\"ou</code>
barre oblique inverse (\)	trois barres obliques inverses (\)	<code>ou=test\ou</code>	<code>ou=test\\ou</code>

 **Remarque :**

- Dans les noms distinctifs d'utilisateur, les guillemets (") doivent être précédés d'une autre barre oblique inverse. Par exemple, `ou=test"ou` doit être spécifié sous la forme `ou=test\"ou`.
- Dans les DN d'utilisateur, la barre oblique inverse (\) doit être précédée d'une barre oblique inverse simple. Par exemple, `ou=test\ou` doit être spécifié sous la forme `ou=test\\ou`.

 **Attention :**

Si l'URL d'utilisateur n'est pas spécifiée, les utilisateurs créés dans la racine RDN ne doivent pas contenir de barre oblique (/) ni de barre oblique inverse (\). De même, ces caractères ne doivent pas être utilisés dans les noms de groupes créés dans la racine RDN si l'URL d'un groupe n'est pas spécifiée. Par exemple, les noms de groupe tels que `OU=child\ou`, `OU=parent/ou` ou `OU=child/ou`, `OU=parent\ou` ne sont pas pris en charge. Ce problème ne se pose pas si vous utilisez un attribut unique comme `attribut d'ID` dans la configuration de l'annuaire des utilisateurs.

### Caractères spéciaux dans l'annuaire natif

Les caractères spéciaux sont pris en charge dans les noms d'utilisateur et de groupe dans l'annuaire natif.

**Tableau 4-11** Caractères spéciaux pris en charge : annuaire natif

Caractère	Nom ou signification	Caractère	Nom ou signification
@	at	,	virgule
#	livre	=	égal à
\$	dollar	+	plus
^	caret	;	point-virgule
(	parenthèse ouvrante	!	point d'exclamation
)	parenthèse fermante	%	pourcentage
'	guillemet simple		

# 5

## Utilisation d'un module d'authentification personnalisé

### Voir aussi :

- [Présentation](#)
- [Exemples de cas d'utilisation et limitation](#)
- [Prérequis](#)
- [Remarques concernant la conception et le codage](#)
- [Déploiement du module d'authentification personnalisé](#)

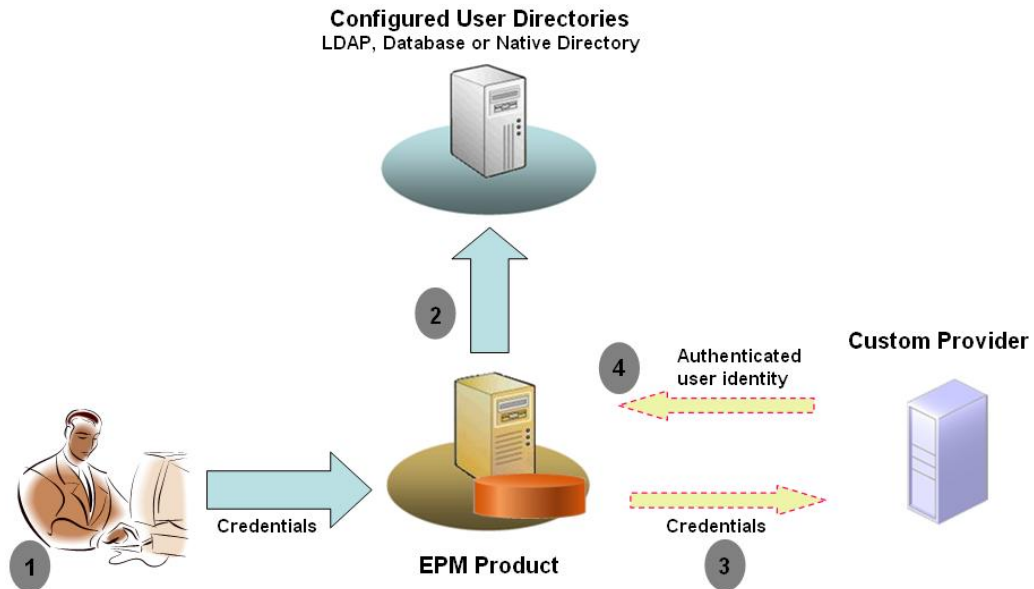
### Présentation

Un module d'authentification personnalisée est un module Java développé et implémenté par les clients pour authentifier les utilisateurs Oracle Enterprise Performance Management System. En règle générale, les produits EPM System utilisent un écran de connexion pour capturer le nom d'utilisateur et le mot de passe, qui servent à authentifier les utilisateurs. Plutôt que l'authentification EPM System, vous pouvez utiliser un module d'authentification personnalisée pour authentifier les utilisateurs et transmettre les informations d'identification validées à EPM System en vue d'un traitement. L'implémentation d'un module d'authentification personnalisée n'implique pas de modifier les produits EPM System.

Vous pouvez utiliser un module d'authentification personnalisée aussi bien avec des clients lourds (par exemple, Oracle Smart View for Office et Oracle Essbase Studio) qu'avec des clients légers (par exemple, Oracle Hyperion Enterprise Performance Management Workspace).

Le module d'authentification personnalisée se sert des informations saisies par l'utilisateur lors de la connexion à un produit EPM System. S'il est activé pour un annuaire des utilisateurs, c'est à travers lui que sont authentifiés les utilisateurs. Une fois l'utilisateur authentifié, le module d'authentification personnalisée renvoie le nom d'utilisateur à EPM System.

L'illustration suivante présente un exemple de scénario d'authentification personnalisée :



Par exemple, vous pouvez utiliser l'infrastructure SecurID RSA comme fournisseur personnalisé pour veiller à ce que l'authentification auprès d'EPM System soit sécurisée et transparente. Présentation :

1. L'utilisateur saisit des informations d'identification (généralement un nom d'utilisateur et un mot de passe) pour accéder à un produit EPM System. Ces informations servent à identifier l'utilisateur de façon unique auprès du fournisseur sollicité par le module d'authentification personnalisée. Par exemple, si vous utilisez une infrastructure SecurID RSA pour l'authentification, l'utilisateur saisit un ID d'utilisateur et un code PIN RSA (et non un ID d'utilisateur et un mot de passe EPM System).
2. En suivant l'ordre de recherche (voir [Ordre de recherche](#)), EPM System parcourt tous les annuaires des utilisateurs configurés afin de localiser cet utilisateur.
  - Si l'annuaire d'utilisateur en cours n'est pas configuré dans le module d'authentification personnalisée, EPM System tente de localiser et d'authentifier l'utilisateur via l'authentification EPM System.
  - Si l'annuaire d'utilisateur est configuré dans le module d'authentification personnalisée, EPM System délègue le processus d'authentification au module personnalisé.
3. Si EPM System délègue l'authentification au module personnalisé, ce dernier accepte les informations d'identification et utilise sa propre logique pour diriger l'authentification de l'utilisateur vers un fournisseur personnalisé (par exemple, l'infrastructure SecurID RSA).
4. Si le module d'authentification personnalisée authentifie l'utilisateur auprès de son fournisseur, il renvoie le nom d'utilisateur à EPM System ou il renvoie une exception Java.

Le nom d'utilisateur renvoyé par le module d'authentification personnalisée doit être identique à un nom d'utilisateur qui figure dans un annuaire pour lequel l'authentification personnalisée est activée.

- Si le module d'authentification personnalisée renvoie un nom d'utilisateur, EPM System localise cet utilisateur dans un annuaire pour lequel l'authentification personnalisée est activée. A ce stade, EPM System ne



consulte pas les annuaires des utilisateurs qui ne sont pas configurés pour l'authentification personnalisée.

- Si le module d'authentification personnalisée génère une exception ou renvoie un utilisateur NULL, EPM System consulte les annuaires des utilisateurs restants pour lesquels l'authentification personnalisée n'est pas activée en respectant l'ordre de recherche. En l'absence d'utilisateur correspondant aux informations d'identification, EPM System affiche une erreur.

## Exemples de cas d'utilisation et limitation

Les scénarios d'implémentation d'authentification personnalisée incluent :

- l'ajout de la prise en charge des mots de passe à usage unique ;
- la réalisation de l'authentification avec la fonction [Resource Access Control Facility \(RACF\)](#) ;
- l'ajout d'une liaison SASL (Simple Authentication and Security Layer) aux annuaires des utilisateurs LDAP au lieu de liaisons LDAP simples.

Il se peut que l'authentification avec mécanisme de question/réponse de vérification ne fonctionne pas correctement si vous implémentez un module d'authentification personnalisé. Les messages générés par le module d'authentification personnalisé ne sont pas propagés aux clients. Etant donné que les clients (par exemple, Oracle Hyperion Enterprise Performance Management Workspace) remplacent le message d'erreur pour afficher un message générique, les scénarios suivants ne sont pas valides :

- deux codes PIN consécutifs RSA SecurID ;
- une variante de mot de passe avec question de vérification, comme la saisie du premier, du dernier et du troisième caractères du mot de passe.

## Prérequis

- Une archive Java entièrement testée nommée `CustomAuth.jar` qui contient des bibliothèques de modules d'authentification personnalisée. `CustomAuth.jar` doit implémenter l'interface publique `CSSCustomAuthenticationIF`, définie dans le package `com.hyperion.css` comme partie intégrante des API standard Oracle Hyperion Shared Services. Reportez-vous à [http://download.oracle.com/docs/cd/E12825\\_01/epm.111/epm\\_security\\_api\\_11111/client/com/hyperion/css/CSSCustomAuthenticationIF.html](http://download.oracle.com/docs/cd/E12825_01/epm.111/epm_security_api_11111/client/com/hyperion/css/CSSCustomAuthenticationIF.html).
- Un accès à Shared Services en tant qu'administrateur Shared Services

## Remarques concernant la conception et le codage

### Ordre de recherche

En plus de l'annuaire natif, il est possible de configurer plusieurs annuaires des utilisateurs dans Oracle Hyperion Shared Services. Une position d'ordre de recherche par défaut est attribuée à tous les annuaires des utilisateurs configurés. Vous pouvez modifier l'ordre de recherche dans Oracle Hyperion Shared Services Console. A l'exception de l'annuaire natif, vous pouvez enlever les annuaires des utilisateurs configurés de l'ordre de recherche. Oracle Enterprise Performance Management System ne tient pas compte des annuaires des utilisateurs qui ne sont pas inclus dans l'ordre de recherche. Reportez-vous au *Guide*

*d'administration de la sécurité utilisateur d'Oracle Enterprise Performance Management System.*

L'ordre de recherche détermine l'ordre dans lequel EPM System parcourt les annuaires des utilisateurs pour authentifier ces derniers. Si l'utilisateur est authentifié dans un annuaire, EPM System cesse la recherche et renvoie cet utilisateur. EPM System refuse l'authentification et renvoie une erreur s'il ne parvient pas à authentifier l'utilisateur à l'aide des annuaires inclus dans l'ordre de recherche.

### Impact de l'authentification personnalisée sur l'ordre de recherche

L'authentification personnalisée influe sur la façon dont la sécurité d'EPM System interprète l'ordre de recherche.

Si le module d'authentification personnalisée renvoie un nom d'utilisateur, EPM System localise cet utilisateur uniquement dans un annuaire pour lequel l'authentification personnalisée est activée. A ce stade, EPM System ignore les annuaires des utilisateurs qui ne sont pas configurés pour l'authentification personnalisée.

### Fonctionnement du flux d'authentification personnalisée

Les scénarios suivants servent à explorer le flux d'authentification personnalisée :

- [Scénario 1](#)
- [Scénario 2](#)
- [Scénario 3](#)

#### Scénario 1

Le tableau suivant montre en détail la configuration des annuaires des utilisateurs d'EPM System et l'ordre de recherche utilisés dans ce scénario. On suppose ici que le module d'authentification personnalisée a recours à une infrastructure RSA pour authentifier les utilisateurs.

**Tableau 5-1 Configuration du scénario 1**

Type et nom des annuaires des utilisateurs	Ordre de recherche	Authentification personnalisée	Exemples de noms d'utilisateur	Mot de passe <sup>1</sup>
Annuaire natif	1	Désactivé	test_user_1 test_user_2 test_user_3	password
Activé via LDAP SunONE_West	2	Désactivé	test_ldap1 test_ldap_2 test_user_3 test_ldap_4	ldappassword
Activé via LDAP SunONE_East	3	Activé	test_ldap1 test_ldap_2 test_user_3	ldappassword sur SunONE et RSA PIN dans le module personnalisé

<sup>1</sup> Par souci de simplification, on suppose que le mot de passe des annuaires des utilisateurs est le même pour tous les utilisateurs.

Pour lancer le processus d'authentification, un utilisateur saisit son nom et son mot de passe dans l'écran de connexion d'un produit EPM System. Dans ce scénario, le module d'authentification personnalisée effectue les actions suivantes :

- Il accepte un nom d'utilisateur et code PIN RSA comme informations d'identification de l'utilisateur.
- Il renvoie un nom d'utilisateur au format *username@providername* (par exemple, `test_ldap_2@SunONE_East`) à la sécurité d'EPM System.

**Tableau 5-2 Interaction utilisateur et résultats**

Nom d'utilisateur et mot de passe	Résultat de l'authentification	Annuaire des utilisateurs de connexion
<code>test_user_1/password</code>	Succès	Annuaire natif
<code>test_user_3/password</code>	Succès	Annuaire natif
<code>test_user_3/ ldappassword</code>	Succès	SunONE_West (n°2 dans l'ordre de recherche) <sup>1</sup>
<code>test_user_3/RSA PIN</code>	Succès	SunONE_East (n°3 dans l'ordre de recherche) <sup>2</sup>
<code>test_ldap_2/ ldappassword</code>	Succès	SunONE_West (n°2 dans l'ordre de recherche)
<code>test_ldap_4/RSA PIN</code>	Echec EPM System affiche une erreur d'authentification. <sup>3</sup>	

<sup>1</sup> L'authentification personnalisée ne parvient pas à authentifier cet utilisateur, car ce dernier a saisi des informations d'identification EPM System. EPM System peut identifier cet utilisateur uniquement dans un annuaire qui n'est pas activé pour l'authentification personnalisée. L'utilisateur ne figure pas dans l'annuaire natif (n°1 dans l'ordre de recherche), mais dans SunONE West (n°2 dans l'ordre de recherche).

<sup>2</sup> EPM System ne parvient pas à trouver cet utilisateur dans l'annuaire natif (n°1 dans l'ordre de recherche) ni dans SunONE West (n°2 dans l'ordre de recherche). Le module d'authentification personnalisée valide l'utilisateur via le serveur RSA et renvoie `test_user_3@SunONE_EAST` à EPM System. EPM System localise l'utilisateur dans SunONE East (n°3 dans l'ordre de recherche), un annuaire des utilisateurs activé pour l'authentification personnalisée.

<sup>3</sup> Oracle recommande de faire figurer tous les utilisateurs authentifiés par le module personnalisé dans un annuaire activé pour l'authentification personnalisée et inclus dans l'ordre de recherche. La connexion échoue si le nom d'utilisateur renvoyé par le module d'authentification personnalisée ne figure pas dans un annuaire activé pour l'authentification personnalisée et inclus dans l'ordre de recherche.

## Scénario 2

Le tableau suivant montre en détail la configuration des annuaires des utilisateurs d'EPM System et l'ordre de recherche utilisés dans ce scénario. On suppose ici que le module d'authentification personnalisée a recours à une infrastructure RSA pour authentifier les utilisateurs.

Dans ce scénario, le module d'authentification personnalisée effectue les actions suivantes :

- Il accepte un nom d'utilisateur et code PIN RSA comme informations d'identification de l'utilisateur.
- Il renvoie un nom d'utilisateur (par exemple, `test_ldap_2`) à la sécurité d'EPM System.

**Tableau 5-3 Exemple d'ordre de recherche**

Annuaire des utilisateurs	Ordre de recherche	Authentification personnalisée	Exemples de noms d'utilisateur	Mot de passe <sup>1</sup>
Annuaire natif	1	Désactivé	test_user_1 test_user_2 test_user_3	password
Activé pour LDAP (par exemple, SunONE)	2	Activé	test_ldap1 test_ldap2 test_user_3	ldappassword sur SunONE et RSA PIN dans le module personnalisé

<sup>1</sup> Par souci de simplification, on suppose que le mot de passe des annuaires des utilisateurs est le même pour tous les utilisateurs.

Pour lancer le processus d'authentification, un utilisateur saisit son nom et son mot de passe dans l'écran de connexion d'un produit EPM System.

**Tableau 5-4 Interaction utilisateur et résultats**

Nom d'utilisateur et mot de passe	Résultat de la connexion	Annuaire des utilisateurs de connexion
test_user_1/password	Succès	Annuaire natif
test_user_3/password	Succès	Annuaire natif
test_user_3/ldappassword	Echec	SunONE <sup>1</sup>
test_user_3/RSA PIN	Succès	SunONE <sup>2</sup>

<sup>1</sup> L'authentification de l'utilisateur avec l'annuaire natif échoue, car le mot de passe ne correspond pas. L'authentification de l'utilisateur à l'aide du module d'authentification personnalisée échoue, car le mot de passe utilisé n'est pas un code PIN RSA valide. EPM System n'essaie pas d'authentifier cet utilisateur dans SunONE (n°2 dans l'ordre de recherche), car les paramètres d'authentification personnalisée prévalent sur l'authentification EPM System dans cet annuaire.

<sup>2</sup> L'authentification de l'utilisateur avec l'annuaire natif échoue, car le mot de passe ne correspond pas. Le module d'authentification personnalisée authentifie l'utilisateur et renvoie le nom test\_user\_3 à EPM System.

### Scénario 3

Le tableau suivant montre en détail la configuration des annuaires des utilisateurs d'EPM System et l'ordre de recherche utilisés dans ce scénario. On suppose ici que le module d'authentification personnalisée a recours à une infrastructure RSA pour authentifier les utilisateurs.

Afin de clarifier ces scénarios, Oracle recommande de faire en sorte que le module d'authentification personnalisée renvoie le nom d'utilisateur au format `username@providername` (par exemple, `test_ldap_4@SunONE`).

**Tableau 5-5 Exemple d'ordre de recherche**

Annuaire des utilisateurs	Ordre de recherche	Authentification personnalisée	Exemples de noms d'utilisateur	Mot de passe <sup>1</sup>
Annuaire natif	1	Activé	test_user_1 test_user_2 test_user_3	RSA_PIN
Activé pour LDAP (par exemple, MSAD)	2	Désactivé	test_ldap1 test_ldap4 test_user_3	ldappassword
Activé pour LDAP (par exemple, SunONE)	3	Activé	test_ldap1 test_ldap4 test_user_3	ldappassword sur SunONE et RSA PIN dans le module personnalisé

<sup>1</sup> Par souci de simplification, on suppose que le mot de passe des annuaires des utilisateurs est le même pour tous les utilisateurs.

Pour lancer le processus d'authentification, un utilisateur saisit son nom et son mot de passe dans l'écran de connexion d'un produit EPM System.

**Tableau 5-6 Interaction utilisateur et résultats**

Nom d'utilisateur et mot de passe	Résultat de l'authentification	Annuaire des utilisateurs de connexion
test_user_1/password	Succès	Annuaire natif
test_user_3/RSA_PIN	Succès	Annuaire natif
test_user_3/ldappassword	Succès	MSAD (n°2 dans l'ordre de recherche)
test_ldap_4/ldappassword	Succès	MSAD (n°2 dans l'ordre de recherche)
test_ldap_4/RSA PIN	Succès	SunONE (n°3 dans l'ordre de recherche)

### Annuaire des utilisateurs et module d'authentification personnalisée

Pour utiliser le module d'authentification personnalisée, il est possible de configurer individuellement les annuaires des utilisateurs qui contiennent les informations sur les utilisateurs et les groupes EPM System afin de déléguer l'authentification au module personnalisé.

Les utilisateurs EPM System authentifiés à l'aide du module personnalisé doivent figurer dans l'un des annuaires des utilisateurs inclus dans l'ordre de recherche (voir [Ordre de recherche](#)). Par ailleurs, l'annuaire des utilisateurs doit être configuré pour déléguer l'authentification au module personnalisé.

L'identité de l'utilisateur dans le fournisseur personnalisé (par exemple, 1357642 dans l'infrastructure SecurID RSA) peut différer du nom d'utilisateur présent dans l'annuaire (par exemple, jDoe dans Oracle Internet Directory) configuré dans Shared Services. Une fois

l'utilisateur authentifié, le module d'authentification personnalisé doit renvoyer le nom d'utilisateur `jDoe` à EPM System.

 **Remarque :**

Comme bonne pratique, Oracle recommande de faire en sorte que le nom d'utilisateur figurant dans les annuaires configurés dans EPM System soit identique à celui disponible dans l'annuaire utilisé par le module d'authentification personnalisée.

### Interface Java `CSSCustomAuthenticationIF`

Le module d'authentification personnalisée doit utiliser l'interface Java `CSSCustomAuthenticationIF` dans le cadre d'une intégration à la structure de sécurité d'EPM System. Si l'authentification personnalisée aboutit, il doit renvoyer une chaîne de nom d'utilisateur. Dans le cas contraire, il renvoie un message d'erreur. Pour que le processus d'authentification aboutisse, le nom d'utilisateur renvoyé par le module d'authentification personnalisée doit figurer dans l'un des annuaires inclus dans l'ordre de recherche de Shared Services. La structure de sécurité d'EPM System prend en charge le format `username@providerName`.

 **Remarque :**

Vérifiez que le nom d'utilisateur renvoyé par le module d'authentification personnalisée ne contient pas le symbole `*` (astérisque), car la structure de sécurité d'EPM System l'interprète comme un caractère générique lors de la recherche d'utilisateurs.

Reportez-vous à la section [Exemple de code 1](#) sur la signature d'interface `CSSCustomAuthenticationIF`.

Le module d'authentification personnalisée (potentiellement un fichier de classe) doit être inclus dans `CustomAuth.jar`. La structure du package est sans importance.

Pour plus d'informations sur l'interface `CSSCustomAuthenticationIF`, reportez-vous à la section [Documentation sur l'API de sécurité](#).

La méthode `authenticate` de `CSSCustomAuthenticationIF` prend en charge l'authentification personnalisée. La méthode `authenticate` accepte les informations d'identification (nom d'utilisateur et mot de passe) saisies par l'utilisateur comme paramètres d'entrée lors de la tentative d'accès à EPM System. Si l'authentification aboutit, cette méthode renvoie une chaîne (nom d'utilisateur). Si l'authentification échoue, elle génère une exception `java.lang.Exception`. Le nom d'utilisateur renvoyé par la méthode doit identifier de façon unique un utilisateur figurant dans l'un des annuaires inclus dans l'ordre de recherche de Shared Services. La structure de sécurité d'EPM System prend en charge le format `username@providerName`.

 **Remarque :**

Pour initialiser les ressources (par exemple, un pool de connexions JDBC), utilisez le constructeur de classe. Cela permet d'améliorer les performances, en évitant de charger les ressources pour chaque authentification.

## Déploiement du module d'authentification personnalisé

Un déploiement Oracle Enterprise Performance Management System ne prend en charge qu'un seul module personnalisé. Vous pouvez activer l'authentification personnalisée pour au moins un annuaire des utilisateurs dans l'ordre de recherche.

Le module d'authentification personnalisé doit implémenter l'interface publique `CSSCustomAuthenticationIF`, définie dans le package `com.hyperion.css`. Ce document suppose que vous disposez d'un module personnalisé entièrement fonctionnel qui définit la logique pour l'authentification des utilisateurs par rapport au fournisseur d'utilisateurs de votre choix. Après avoir développé et testé un module d'authentification personnalisé, vous devez l'implémenter dans l'environnement EPM System.

### Présentation des étapes

Votre code d'authentification personnalisée ne doit pas utiliser `log4j` pour la journalisation des erreurs. Si le code utilisé dans une version précédente utilise `log4j`, vous devez l'enlever du code avant de l'utiliser avec cette version.

Pour implémenter le module d'authentification personnalisé, effectuez les étapes suivantes :

- Arrêtez les produits EPM System, y compris Oracle Hyperion Shared Services et les systèmes qui utilisent les API Shared Services.
- Copiez l'archive Java du module d'authentification personnalisé `CustomAuth.jar` dans le déploiement :

- **WebLogic :** copiez `CustomAuth.jar` dans `MIDDLEWARE_HOME/user_projects/domains/WEBLOGIC_DOMAIN/lib`, en règle générale, `C:/Oracle/Middleware/user_projects/domains/EPMSysstem/lib`.

Si vous effectuez une mise à niveau depuis la version 11.1.2.0 ou 11.1.2.1, qui comportait une implémentation de module d'authentification personnalisé, déplacez `CustomAuth.jar` depuis `EPM_ORACLE_HOME/common/jlib/11.1.2.0` vers `MIDDLEWARE_HOME/user_projects/domains/WEBLOGIC_DOMAIN/lib`.

- **Tous les déploiements client :** copiez `CustomAuth.jar` dans tous les déploiements client EPM System, à l'emplacement suivant :

`EPM_ORACLE_HOME/common/jlib/11.1.2.0`, en règle générale, `Oracle/Middleware/common/jlib/11.1.2.0`. Assurez-vous que le fichier `CustomAuth.jar` se trouve toujours dans l'annuaire `EPM_ORACLE_HOME/common/jlib/11.1.2.0`.

Pour que tous les serveurs et les clients puissent fonctionner avec l'authentification personnalisée, le fichier `CustomAuth.jar` doit se trouver dans les deux emplacements suivants :

- \* `MIDDLEWARE_HOME/user_projects/domains/WEBLOGIC_DOMAIN/lib`
- \* `EPM_ORACLE_HOME/common/jlib/11.1.2.0`

- Mettez à jour les paramètres d'annuaire des utilisateurs dans Shared Services. Reportez-vous à [Mise à jour des paramètres dans Shared Services](#).
- Démarrez Shared Services,, puis les autres produits EPM System.
- Testez votre implémentation. Reportez-vous à [Test de votre déploiement](#).

### Mise à jour des paramètres dans Shared Services

Par défaut, l'authentification personnalisée est désactivée pour tous les annuaires des utilisateurs. Vous pouvez remplacer le comportement par défaut pour activer l'authentification personnalisée pour un annuaire des utilisateurs externe spécifique ou pour l'annuaire natif.

### Mise à jour des configurations d'annuaire des utilisateurs

Vous devez mettre à jour la configuration de l'annuaire des utilisateurs pour lequel l'authentification personnalisée doit être activée.

Pour mettre à jour la configuration de l'annuaire des utilisateurs :

1. Démarrez Oracle Hyperion Foundation Services.
2. Accédez à Oracle Hyperion Shared Services Console en tant qu'administrateur système.
3. Sélectionnez **Administration**, puis **Configurer les annuaires des utilisateurs**.
4. Dans l'écran Annuaires des utilisateurs définis, sélectionnez l'annuaire des utilisateurs dont vous voulez modifier le paramètre d'authentification personnalisée.

#### Remarque :

EPM System utilise uniquement les annuaires des utilisateurs inclus dans l'ordre de recherche.

5. Cliquez sur **Modifier**.
6. Sélectionnez **Afficher les options avancées**.
7. Dans **Module personnalisé**, sélectionnez **Module d'authentification** afin d'activer le module personnalisé pour l'annuaire des utilisateurs en cours.
8. Cliquez sur **Terminer**.
9. Répétez cette procédure pour mettre à jour la configuration d'autres annuaires des utilisateurs dans l'ordre de recherche.

### Mise à jour des options de sécurité

Assurez-vous que `CustomAuth.jar` est disponible dans `EPM_ORACLE_HOME/user_projects/domains/WEBLOGIC_DOMAIN/lib` avant de démarrer la procédure suivante.

Pour mettre à jour les options de sécurité :

1. Accédez à Shared Services Console en tant qu'administrateur système.
2. Sélectionnez **Administration**, puis **Configurer les annuaires des utilisateurs**.



3. Sélectionnez **Options de sécurité**.
4. Sélectionnez **Afficher les options avancées**.
5. Dans **Module d'authentification**, entrez le nom de classe complet du module d'authentification personnalisé à utiliser pour authentifier les utilisateurs dans tous les annuaires des utilisateurs pour lesquels le module d'authentification personnalisé est sélectionné. Par exemple, `com.mycompany.epm.CustomAuthenticationImpl`.
6. Cliquez sur **OK**.

### Test de votre déploiement

Si l'annuaire natif n'est pas configuré pour l'authentification personnalisée, n'employez pas les utilisateurs de l'annuaire natif pour tester l'authentification personnalisée.

#### Remarque :

Il vous incombe d'identifier et de corriger tout problème lié au module d'authentification personnalisé. Oracle suppose que votre module personnalisé fonctionne parfaitement pour le mapping d'un utilisateur de l'annuaire des utilisateurs utilisé par le module personnalisé avec un utilisateur d'un annuaire des utilisateurs pour lequel l'authentification personnalisée est activée dans l'ordre de recherche EPM System.

Pour tester votre déploiement, connectez-vous à EPM System à l'aide des informations d'identification de l'utilisateur provenant de l'annuaire des utilisateurs, par exemple, une infrastructure RSA SecurID, utilisé par le module personnalisé. Ces informations d'identification peuvent être différentes des informations d'identification EPM System.

Votre implémentation a été effectuée correctement si les produits EPM System vous autorisent à accéder à leurs ressources. Une erreur indiquant que l'utilisateur est introuvable n'est pas toujours le signe d'un échec de l'implémentation. Dans un tel cas, vérifiez que les informations d'identification que vous avez entrées sont présentes dans le magasin d'utilisateurs personnalisé et qu'un utilisateur correspondant est présent dans l'un des annuaires des utilisateurs pour lesquels l'authentification personnalisée est activée dans l'ordre de recherche EPM System.

Pour tester l'authentification personnalisée, procédez comme suit :

1. Assurez-vous que les produits EPM System sont en cours d'exécution.
2. Accédez à un composant EPM System, par exemple, Oracle Hyperion Enterprise Performance Management Workspace.
3. Connectez-vous en tant qu'utilisateur défini dans un annuaire des utilisateurs pour lequel l'authentification personnalisée est activée.
  - a. Dans **Nom d'utilisateur**, entrez votre ID utilisateur, par exemple, un ID utilisateur RSA.
  - b. Dans **Mot de passe**, entrez un mot de passe, par exemple un code PIN RSA.
  - c. Cliquez sur **Connexion**.
4. Vérifiez que vous avez accès aux ressources des produits EPM System.

# 6

## Consignes générales de sécurité pour EPM System

### Voir aussi :

- [Implémentation du protocole SSL](#)
- [Modification du mot de passe d'administration](#)
- [Régénération des clés de cryptage](#)
- [Modification des mots de passe de base de données](#)
- [Sécurité des cookies](#)
- [Réduction du délai d'expiration du jeton SSO](#)
- [Vérification des rapports de sécurité](#)
- [Personnalisation du système d'authentification pour une authentification forte](#)
- [Désactivation des utilitaires de débogage d'EPM Workspace](#)
- [Modification des pages d'erreur par défaut du serveur Web](#)
- [Prise en charge des logiciels tiers](#)

## Implémentation du protocole SSL

SSL utilise un système cryptographique qui crypte les données. SSL crée une connexion sécurisée entre un client et un serveur, par laquelle des données peuvent être envoyées en toute sécurité.

Pour sécuriser votre environnement Oracle Enterprise Performance Management System, sécurisez tous les canaux de communication utilisés par vos applications Web et les connexions à l'annuaire des utilisateurs utilisant SSL. Reportez-vous à [Activation SSL des composants EPM System](#).

En outre, protégez tous les ports d'agent à l'aide d'un pare-feu, par exemple, le port 6861, qui est le port d'agent Oracle Hyperion Reporting and Analysis. Les utilisateurs finals n'ont pas besoin d'accéder aux ports d'agent EPM System.

## Modification du mot de passe d'administration

Le compte utilisateur admin par défaut de l'annuaire natif fournit l'accès à toutes les fonctions Oracle Hyperion Shared Services. Le mot de passe est défini lorsque vous déployez Oracle Hyperion Foundation Services. Vous devez modifier régulièrement le mot de passe de ce compte.

Modifiez le compte utilisateur *Admin* pour changer le mot de passe. Reportez-vous à la section "Modification des comptes utilisateur" du *Guide d'administration de la sécurité utilisateur d'Oracle Enterprise Performance Management System*.

## Régénération des clés de cryptage

Utilisez Oracle Hyperion Shared Services Console pour régénérer régulièrement les éléments suivants :

- Jeton d'authentification unique

### ▲ Attention :

Les flux de tâches utilisés par Oracle Hyperion Financial Management et Oracle Hyperion Profitability and Cost Management sont invalidés lorsque vous générez un nouveau fichier de clés d'accès. Après la nouvelle génération du fichier de clés d'accès, ouvrez les flux de tâches, puis enregistrez-les pour les valider de nouveau.

- Clé de service sécurisée
- Clé de configuration du fournisseur

Reportez-vous à [Régénération des clés de cryptage](#).

### ✎ Remarque :

Oracle Hyperion Shared Services et le sous-système de sécurité d'Oracle Enterprise Performance Management System utilisent le cryptage AES avec une clé de 128 bits.

## Modification des mots de passe de base de données

Modifiez régulièrement le mot de passe pour toutes les bases de données produit Oracle Enterprise Performance Management System. La procédure de modification du mot de passe d'une base de données dans le registre Oracle Hyperion Shared Services est détaillée dans cette section.

Pour obtenir la procédure détaillée de modification d'un mot de passe de base de données produit EPM System, reportez-vous au *Guide d'installation et de configuration d'Oracle Enterprise Performance Management System*.

Pour modifier les mots de passe des bases de données des produits EPM System dans le registre Shared Services :

1. A l'aide de la console d'administration de la base de données, modifiez le mot de passe du compte utilisateur utilisé pour configurer la base de données des produits EPM System.
2. Arrêtez les produits EPM System (applications Web, services et processus).
3. A l'aide du configurateur EPM System, reconfigurez la base de données en suivant l'une des procédures ci-dessous.

**Oracle Hyperion Shared Services uniquement :**

 **Remarque :**

Dans les environnements distribués où les produits EPM System se trouvent sur des machines autres que Shared Services, vous devez suivre cette procédure sur tous les serveurs.

- a. Dans les tâches Foundation du configurateur EPM System, sélectionnez **Configurer la base de données**.
- b. Dans la page Configuration de la base de données Shared Services et du registre, sélectionnez **Se connecter à une base de données Shared Services configurée précédemment**.
- c. Spécifiez le nouveau mot de passe de l'utilisateur dont le compte a été utilisé pour configurer la base de données Shared Services. Ne modifiez aucun autre paramètre.
- d. Continuez la configuration puis cliquez sur **Terminer** une fois toutes les tâches terminées.

**Pour modifier le mot de passe des produits EPM System autres que Shared Services :**

 **Remarque :**

Suivez les mêmes étapes pour les produits EPM System déployés sur le serveur en cours d'exécution uniquement.

Reportez-vous au *Guide d'installation et de configuration d'Oracle Enterprise Performance Management System* pour obtenir des instructions détaillées.

4. Démarrez les produits et services EPM System.

## Sécurité des cookies

L'application Web Oracle Enterprise Performance Management System définit un cookie pour effectuer le suivi de la session. Au cours de la définition d'un cookie, en particulier un cookie de session, le serveur peut définir l'indicateur de sécurité, qui force le navigateur à envoyer le cookie par l'intermédiaire d'un canal sécurisé. Le risque de détournement de la session est ainsi réduit.

 **Remarque :**

Sécurisez les cookies uniquement si les produits EPM System sont déployés dans un environnement SSL.

Modifiez le descripteur de session Oracle WebLogic Server pour sécuriser les cookies WebLogic Server. Attribuez la valeur `true` à l'attribut `cookieSecure` dans l'élément `session-param`. Reportez-vous la section "Sécurisation des applications Web" dans le guide [Sécurité de la programmation d'Oracle Fusion Middleware pour Oracle WebLogic Server 11g](#).

## Réduction du délai d'expiration du jeton SSO

Par défaut, le délai d'expiration du jeton SSP est de 480 minutes. Il est recommandé de le réduire à 60 minutes, par exemple, pour réduire la réutilisation du jeton s'il est exposé. Reportez-vous à "Configuration des options de sécurité" dans le *Guide d'administration de la sécurité utilisateur d'Oracle Enterprise Performance Management System*.

## Vérification des rapports de sécurité

Le rapport de sécurité contient les informations d'audit associées aux tâches de sécurité pour lesquelles l'audit est configuré. Générez ce rapport à partir d'Oracle Hyperion Shared Services Console et examinez-le régulièrement, en particulier pour identifier les échecs de connexion entre les produits Oracle Enterprise Performance Management System et les modifications de provisionnement. Sélectionnez **Vue détaillée** comme option de génération de rapport pour regrouper les données de rapport en se basant sur les attributs modifiés et les nouvelles valeurs des attributs. Reportez-vous à la section "Génération de rapports" du *Guide d'administration de la sécurité utilisateur d'Oracle Enterprise Performance Management System*.

## Personnalisation du système d'authentification pour une authentification forte

Vous pouvez utiliser un module d'authentification personnalisé pour ajouter une authentification forte à EPM System. Vous pouvez, par exemple, utiliser l'authentification à double facteur RSA SecurID dans un mode autre qu'avec mécanisme de question/réponse de vérification. Le module d'authentification personnalisé est transparent pour les clients lourds et légers et ne requiert pas de modification du déploiement côté client. Reportez-vous à [Utilisation d'un module d'authentification personnalisé](#).

## Désactivation des utilitaires de débogage d'EPM Workspace

- Oracle Hyperion Enterprise Performance Management Workspace est livré avec des fichiers JavaScript décompressés destinés à résoudre des problèmes. A des fins de sécurité, vous devez enlever ces fichiers JavaScript décompressés de votre environnement de production :

- Créez une copie de sauvegarde du répertoire `EPM_ORACLE_HOME/common/epmstatic/wspace/js/`.
- A l'exception du fichier `DIRECTORY_NAME.js`, supprimez les fichiers `.js` de chaque sous-répertoire dans `EPM_ORACLE_HOME/common/epmstatic/wspace/js/`.

Chaque sous-répertoire contient un fichier `.js` qui comporte le nom du répertoire. Par exemple, `EPM_ORACLE_HOME/common/epmstatic/wspace/js/com/hyperion/bpm/web/common` contient `Common.js`. Supprimez tous les fichiers `.js` à l'exception de celui qui porte le nom du répertoire. Dans ce cas, il s'agit de `Common.js`.

- EPM Workspace fournit des utilitaires de débogage et des applications de test, qui sont accessibles si EPM Workspace est déployé en mode de débogage. A des fins de sécurité, les administrateurs doivent désactiver le débogage côté client dans EPM Workspace.

Pour désactiver le mode de débogage, procédez comme suit :

1. Connectez-vous à EPM Workspace en tant qu'administrateur.
2. Sélectionnez **Naviguer, Administrer**, puis **Paramètres du serveur Workspace**.
3. Dans **Débogage du client activé** dans Paramètres du serveur Workspace, sélectionnez **Non**.
4. Cliquez sur **OK**.

## Modification des pages d'erreur par défaut du serveur Web

Lorsque les serveurs d'applications ne sont pas disponibles pour accepter les demandes, le plug-in de serveur Web pour le serveur d'applications back-end (par exemple, le plug-in Oracle HTTP Server pour Oracle WebLogic Server) renvoie une page d'erreur par défaut affichant des informations sur la version du plug-in. Les serveurs Web peuvent également afficher leur page d'erreur par défaut à d'autres occasions. Les pirates informatiques peuvent utiliser ces informations pour détecter les vulnérabilités connues de certains sites Web publics.

Personnalisez les pages d'erreur (du plug-in de serveur d'applications Web et du serveur Web) afin qu'elles ne contiennent pas d'informations sur les composants système de production, par exemple, la version du serveur, le type du serveur, la date de la version du plug-in et le type du plug-in. Consultez la documentation de votre serveur d'applications et du fournisseur de votre serveur Web pour plus d'informations.

## Prise en charge des logiciels tiers

Oracle reconnaît et prend en charge les garanties de compatibilité ascendante de fournisseurs tiers. Par conséquent, lorsque les fournisseurs garantissent la compatibilité ascendante, des versions de maintenance et service packs ultérieurs peuvent être utilisés. Si une incompatibilité est identifiée, Oracle indique une version de correctif à partir de laquelle le produit doit être déployé (et supprime la version incompatible de la matrice de prise en charge) ou fournit une version de maintenance et un service pack pour le produit Oracle.

**Mises à niveau du côté des serveurs** : l'assistance relative aux mises à niveau des composants des serveurs tiers est régie par la Subsequent Maintenance Release Policy (Politique relative aux versions de maintenance ultérieures). En général, Oracle prend en charge la mise à niveau des composants des serveurs tiers jusqu'à la prochaine version de maintenance du service pack de la version actuellement prise en charge. Les mises à niveau vers la prochaine version principale ne sont pas prises en charge.

**Mises à jour côté client** : Oracle prend en charge les mises à jour automatiques vers les composants client, y compris les mises à jour vers la prochaine version principale des composants client tiers. Par exemple, vous pouvez effectuer une mise à jour du navigateur JRE pour passer à la version actuellement prise en charge.

# A

## Exemple de code d'authentification personnalisé

### Exemple de code 1

#### Remarque :

Votre code d'authentification personnalisée ne doit pas utiliser log4j pour la journalisation des erreurs. Si le code d'authentification personnalisée que vous avez utilisé dans une version précédente utilise log4j, vous devez l'enlever du code avant de l'utiliser avec cette version.

Le fragment de code suivant est une implémentation vide du module personnalisé :

```
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;
 }
}
```

Paramètres d'entrée :

- Contexte : un mapping contenant une paire clé/valeur de paramètres régionaux
- Nom d'utilisateur : identificateur qui identifie de manière unique l'utilisateur dans l'annuaire des utilisateurs dans lequel le module personnalisé authentifie l'utilisateur. L'utilisateur entre la valeur de ce paramètre lorsqu'il se connecte à un composant Oracle Enterprise Performance Management System.
- Mot de passe : mot de passe défini par l'utilisateur dans l'annuaire des utilisateurs dans lequel le module personnalisé authentifie l'utilisateur. L'utilisateur entre la valeur de ce paramètre lorsqu'il se connecte à un composant EPM System.

## Exemple de code 2

L'exemple de code suivant illustre l'authentification personnalisée des utilisateurs à l'aide d'un nom d'utilisateur et d'un mot de passe contenus dans un fichier plat. Vous devez initialiser les listes de mots de passe et d'utilisateurs dans le constructeur de classe pour que l'authentification personnalisée fonctionne.

```
package com.hyperion.css.security;

import java.util.Map;
import java.util.HashMap;
import com.hyperion.css.CSSCustomAuthenticationIF;
import java.io.*;

public class CSSCustomAuthenticationImpl implements
CSSCustomAuthenticationIF{
 static final String DATA_FILE = "datafile.txt";

 /**
 * authenticate method includes the core implementation of the
 * Custom Authentication Mechanism. If custom authentication is
 * enabled for the provider, authentication operations
 * are delegated to this method. Upon successful authentication,
 * this method returns a valid user name, using which EPM System
 * retrieves the user from a custom authentication enabled provider.
 * User name can be returned in the format username@providerName,
 * where providerName indicates the name of the underlying provider
 * where the user is available. authenticate method can use other
 * private methods to access various core components of the
 * custom authentication module.

 * @param context
 * @param userName
 * @param password
 * @return
 * @throws Exception
 */

 Map users = null;

 public CSSCustomAuthenticationImpl(){
 users = new HashMap();
 }
}
```



```
InputStream is = null;
BufferedReader br = null;
String line;
String[] userDetails = null;
String userKey = null;
try{
 is = CSSCustomAuthenticationImpl.class.getResourceAsStream(DATA_FILE);
 br = new BufferedReader(new InputStreamReader(is));
 while(null != (line = br.readLine())){
 userDetails = line.split(":");
 if(userDetails != null && userDetails.length==3){
 userKey = userDetails[0]+ ":" + userDetails[1];
 users.put(userKey, userDetails[2]);
 }
 }
}
catch(Exception e){
 // log a message
}
finally{
 try{
 if(br != null) br.close();
 if(is != null) is.close();
 }
 catch(IOException ioe){
 ioe.printStackTrace();
 }
}
}

/* Use this authenticate method snippet to return username from a flat file
*/

public String authenticate(Map context, String userName, String password)
throws Exception{
 //userName : user input for the userName
 //password : user input for password
 //context : Map, can be used to additional information required by
 // the custom authentication module.

 String authenticatedUserKey = userName + ":" + password;

 if(users.get(authenticatedUserKey)!=null)
 return (String)users.get(authenticatedUserKey);
 else throw new Exception("Invalid User Credentials");
}

/* Refer to this authenticate method snippet to return username in
 username@providername format */

public String authenticate(Map context, String userName, String password)
throws Exception{

 //userName : user input for userName
 //password : user input for password
```

```
//context : Map can be used to additional information required by
// the custom authentication module.

//Your code should uniquely identify the user in a custom provider
and in a configured
//user directory in Shared Services. EPM Security expects you to
append the provider
//name to the user name. Provider name must be identical to the name
of a custom
//authentication-enabled user directory specified in Shared Services.

//If invalid arguments, return null or throw exception with
appropriate message
//set authenticationSuccessFlag = false

String authenticatedUserKey = userName + ":" + password;
if(users.get(authenticatedUserKey)!=null)
 String userNameStr = (new StringBuffer()
 .append((String)users.get(authenticatedUserKey))
 .append("@").append(PROVIDER_NAME).toString(
);
 return userNameStr;
else throw new Exception("Invalid User Credentials");
 }
}
```

## Fichier de données pour l'exemple de code 2

Assurez-vous que le fichier de données est nommé `datafile.txt`, conformément au nom utilisé dans l'exemple de code, et qu'il est inclus dans l'archive Java que vous créez.

Utilisez ce qui suit comme contenu du fichier plat utilisé en tant qu'annuaire des utilisateurs personnalisé pour prendre en charge le module d'authentification personnalisé implémenté par l'exemple de code 2 (reportez-vous à la section [Exemple de code 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
```

Utilisez ce qui suit comme contenu du fichier plat utilisé en tant qu'annuaire des utilisateurs personnalisé si vous prévoyez de revenir au format `username@providername` pour le nom d'utilisateur :

```
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

## Implémentation d'une classe de connexion personnalisée

Oracle Enterprise Performance Management System fournit `com.hyperion.css.sso.agent.X509CertificateSecurityAgentImpl` pour extraire l'identité de l'utilisateur (DN) des certificats X509.

Si vous devez dériver l'identité de l'utilisateur à partir d'un attribut du certificat autre que le DN, vous devez développer et implémenter une classe de connexion personnalisée semblable à `com.hyperion.css.sso.agent.X509CertificateSecurityAgentImpl`, tel que décrit dans cette annexe.

### Exemple de code de classe de connexion personnalisée

Cet exemple de code illustre l'implémentation de l'élément `com.hyperion.css.sso.agent.X509CertificateSecurityAgentImpl` par défaut. En règle générale, vous devez personnaliser la méthode `parseCertificate(String sCertificate)` de cette implémentation pour dériver le nom d'utilisateur à partir d'un attribut de certificat autre que le 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
```

## Déploiement d'une classe de connexion personnalisée

Pour implémenter la classe de connexion personnalisée, effectuez les étapes suivantes :

1. Créez et testez la classe de connexion personnalisée. Assurez-vous que votre code ne comporte aucune référence à `log4j`. Reportez-vous à [Exemple de code de classe de connexion personnalisée](#).

Vous pouvez utiliser n'importe quel nom pour votre classe personnalisée.

2. Packagez la classe de connexion personnalisée dans un fichier `CustomAuth.jar`.
3. Copiez le fichier `CustomAuth.jar` dans le déploiement :
  - **WebLogic** : copiez `CustomAuth.jar` dans `MIDDLEWARE_HOME/user_projects/domains/WEBLOGIC_DOMAIN/lib`, en règle générale, `Oracle/Middleware/user_projects/domains/EPMSysstem/lib`.

### Remarque :

Si vous effectuez une mise à niveau depuis la version 11.1.2.0 ou 11.1.2.1, qui comportait une implémentation de classe de connexion personnalisée, déplacez `CustomAuth.jar` depuis `EPM_ORACLE_HOME/common/jlib/11.1.2.0` vers `MIDDLEWARE_HOME/user_projects/domains/WEBLOGIC_DOMAIN/lib`.

- **Déploiements client** : copiez `CustomAuth.jar` dans tous les déploiements client Oracle Enterprise Performance Management System, à l'emplacement suivant :

`EPM_ORACLE_HOME/common/jlib/11.1.2.0`, en règle générale, `Oracle/Middleware/common/jlib/11.1.2.0`

Oracle recommande d'activer l'authentification par certificat client si vous utilisez une classe de connexion personnalisée.

# C

## Migration d'utilisateurs et de groupes entre les annuaires des utilisateurs

### Présentation

De nombreux scénarios peuvent expliquer que les identités d'utilisateur et de groupe d'utilisateurs Oracle Enterprise Performance Management System provisionnés deviennent obsolètes. Les composants EPM System deviennent inaccessibles si les informations sur le provisionnement à leur disposition sont obsolètes. Les scénarios susceptibles de créer des données de provisionnement obsolètes comprennent les cas suivants :

- Mise hors service d'un annuaire des utilisateurs : les organisations peuvent mettre hors service un annuaire des utilisateurs après avoir déplacé les utilisateurs vers un autre annuaire.
- Mise à niveau de version : les mises à niveau de version peuvent impliquer des changements dans le nom de l'ordinateur hôte ou les environnements de système d'exploitation requis.
- Changement de fournisseur : les organisations peuvent remplacer un annuaire des utilisateurs par celui d'un autre fournisseur. Par exemple, une organisation pourrait remplacer son annuaire Oracle Internet Directory par un serveur d'annuaire SunONE.



#### Remarque :

- Dans l'annexe, l'annuaire des utilisateurs que vous cessez d'utiliser est appelé l'annuaire des utilisateurs *source* et celui vers lequel vous déplacez les comptes utilisateur est appelé l'annuaire des utilisateurs *cible*.
- Cette procédure de migration ne prend pas en charge la migration de comptes utilisateur d'un annuaire d'utilisateurs source vers un annuaire d'utilisateurs cible, mais uniquement leur association dans les applications EPM. Vous devez créer les utilisateurs manuellement dans l'annuaire des utilisateurs cible. Ce processus s'applique aux utilisateurs de n'importe quel annuaire source, notamment l'annuaire natif.

Si un annuaire des utilisateurs source configuré avec Hyperion Shared Services comporte des groupes, à l'exception des groupes de l'annuaire natif, ces groupes doivent également être créés dans l'annuaire des utilisateurs cible.

### Prérequis

- Les utilisateurs et les groupes Oracle Enterprise Performance Management System dont les données de provisionnement sont migrées d'un annuaire des utilisateurs à l'autre doivent être disponibles dans l'annuaire des utilisateurs cible.



Les relations de groupe qui existent dans l'annuaire des utilisateurs source doivent être conservées dans l'annuaire des utilisateurs cible.

- Les noms des utilisateurs d'EPM System doivent être identiques entre les annuaires des utilisateurs source et cible.

## Procédure de migration

### Exporter les données de l'annuaire natif

Exécutez les étapes suivantes dans l'environnement source :

Utilisez la gestion du cycle de vie Oracle Hyperion Enterprise Performance Management System pour exporter uniquement les artefacts Shared Services suivants de l'annuaire natif :

- Groupes de l'annuaire natif
- Rôles affectés
- Listes déléguées

La gestion du cycle de vie crée plusieurs fichiers d'export, généralement dans `EPM_ORACLE_INSTANCE/import_export/USER_NAME/EXPORT_DIR/resource/` Native Directory, où `USER_NAME` correspond à l'identité de l'utilisateur (par exemple, admin) qui a effectué l'opération d'export, et `EXPORT_DIR` est le nom du répertoire d'export. Dans la plupart des cas, les fichiers suivants sont créés :

- `Groups.csv`
- `Assigned Roles.csv`
- `Delegated Lists.csv`
- `Assigned Roles/PROD_NAME.csv` pour chaque application déployée, où `PROD_NAME` est le nom d'un composant Oracle Enterprise Performance Management System (par exemple, Shared Services).

#### Remarque :

- Reportez-vous au *Guide de gestion du cycle de vie d'Oracle Enterprise Performance Management System* pour obtenir des instructions détaillées sur l'export de données à l'aide de la gestion du cycle de vie.
- Assurez-vous que le fichier `Users.csv` n'est pas exporté.

Après avoir exporté les artefacts, vérifiez que le rapport de statut de migration indique la dernière opération d'export comme étant terminée.

Pour exporter les données de l'annuaire natif, procédez comme suit :

1. Dans le volet d'affichage d'Oracle Hyperion Shared Services Console, accédez au groupe d'applications **Foundation**, puis sélectionnez l'application **Shared Services**.
2. Pour la migration, sélectionnez uniquement les artefacts requis dans la liste ci-dessous :

- Groupes de l'annuaire natif
  - Rôles affectés
  - Listes déléguées
3. Cliquez sur **Exporter**.
  4. Saisissez le nom de l'archive d'export. La valeur par défaut est `admin DATE` (par exemple, `admin 13-03-18`).
  5. Cliquez sur **Exporter**.

### Importer les données de l'annuaire natif

Exécutez les étapes suivantes dans l'environnement cible :

1. Créez manuellement les éléments suivants :
  - a. Utilisateurs dans l'annuaire des utilisateurs externes cible, comme dans l'annuaire des utilisateurs source
  - b. Groupes dans l'annuaire des utilisateurs externes cible, comme dans l'annuaire des utilisateurs source, à l'exception des groupes de l'annuaire natif
2. Configurez l'annuaire des utilisateurs cible.

Ajoutez l'annuaire des utilisateurs cible en tant qu'annuaire des utilisateurs externe dans EPM System si vous avez déplacés les comptes utilisateur de l'annuaire source vers un autre annuaire. Par exemple, si vous avez déplacé les comptes utilisateur d'Oracle Internet Directory vers SunONE Directory Server, ajoutez SunONE Directory Server en tant qu'annuaire des utilisateurs externe. Reportez-vous au chapitre 3, "Configuration des annuaires des utilisateurs", du *Guide d'administration de la sécurité utilisateur d'Oracle Enterprise Performance Management System*.

#### Remarque :

Vérifiez que l'annuaire des utilisateurs cible contient les comptes utilisateur et les groupes de tous les utilisateurs EPM System dont les données sont migrées depuis l'annuaire source.

Si vous avez déplacé les utilisateurs dans un annuaire déjà défini comme annuaire des utilisateurs externe, vérifiez que les comptes utilisateur sont visibles pour Oracle Hyperion Shared Services. Pour ce faire, recherchez des utilisateurs à partir de Shared Services Console. Reportez-vous à la section "Recherche d'utilisateurs, groupes, rôles et listes déléguées" dans le *Guide d'administration de la sécurité utilisateur d'Oracle Enterprise Performance Management System*.

Lors de la configuration de l'annuaire des utilisateurs cible en tant qu'annuaire des utilisateurs externe, vérifiez que la propriété `Attribut de connexion` pointe vers l'attribut dont la valeur était initialement employée comme nom d'utilisateur dans l'annuaire source. Reportez-vous à la section [Prérequis](#).

3. Déplacez l'annuaire des utilisateurs cible en haut de l'ordre de recherche.

 **Remarque :**

Si le nom de l'annuaire des utilisateurs cible est identique à celui de l'annuaire source, vous devez supprimer l'annuaire des utilisateurs source de la configuration EPM System.

Shared Services affecte une priorité d'ordre de recherche inférieure à l'annuaire des utilisateurs que vous venez d'ajouter par rapport à l'ordre de recherche des annuaires existants. Modifiez l'ordre de recherche de sorte que l'annuaire des utilisateurs cible ait une priorité supérieure à l'annuaire des utilisateurs source. Cet ordre permet à Shared Services de détecter les utilisateurs dans l'annuaire cible avant de chercher dans l'annuaire source. Reportez-vous à la section "Gestion de l'ordre de recherche de l'annuaire des utilisateurs" dans le *Guide d'administration de la sécurité utilisateur d'Oracle Enterprise Performance Management System*.

4. Redémarrez Oracle Hyperion Foundation Services et les autres composants EPM System pour appliquer les modifications apportées.
5. Importez les données de l'annuaire natif (exportées à partir de l'environnement source) :  
Exécutez la gestion du cycle de vie avec l'option `créer/mettre à jour` pour importer les données précédemment exportées (figurant dans la liste ci-dessous) depuis l'annuaire natif.

- `Groups.csv`
- `Assigned Roles.csv`
- `Delegated Lists.csv`

 **Remarque :**

- Reportez-vous au *Guide de gestion du cycle de vie d'Oracle Enterprise Performance Management System* pour obtenir des instructions détaillées sur l'import de données à l'aide de la gestion du cycle de vie.
- Assurez-vous que le fichier `Users.csv` n'est pas importé.

Après avoir importé les données, vérifiez que le rapport de statut de migration indique la dernière opération d'import comme étant terminée.

Pour importer les données de l'annuaire natif, procédez comme suit :

- a. Dans le volet d'affichage de Shared Services Console, développez **Système de fichiers**.
- b. Sélectionnez l'emplacement du système de fichiers pour les fichiers d'import.
- c. Sélectionnez le type d'artefact dont vous souhaitez importer les informations de provisionnement.
- d. Cliquez sur **Importer**.
- e. Cliquez sur **OK**.

## Mises à jour spécifiques du produit

### ▲ Attention :

Oracle recommande de sauvegarder les données d'utilisateur et de groupe dans le référentiel utilisé par le composant Oracle Enterprise Performance Management System avant de lancer les mises à jour propres au produit. Après avoir mis à jour les informations dans le référentiel du produit local, vous pouvez revenir aux anciennes données d'utilisateur et de groupe dans le référentiel du produit local à partir des sauvegardes uniquement.

### Planning

Oracle Hyperion Planning stocke les informations sur les utilisateurs et groupes provisionnés dans le référentiel Planning. Si une identité d'utilisateur est modifiée dans l'annuaire natif à la suite de la migration d'utilisateurs et de groupes d'un annuaire des utilisateurs à l'autre, vous devez synchroniser les informations dans le référentiel Planning avec celles de l'annuaire natif en sélectionnant Migrer des utilisateurs/groupe. Ce bouton est disponible dans Planning lorsque vous affectez l'accès aux formulaires , aux membres et aux listes de tâches.

### Financial Management

Oracle Hyperion Financial Management enregistre les informations sur les utilisateurs et les groupes provisionnés pour accéder aux objets dans un référentiel local Financial Management. Si les informations sur les utilisateurs et les groupes dans l'annuaire natif sont modifiées à la suite de la migration d'utilisateurs et de groupes d'un annuaire des utilisateurs à l'autre, vous devez synchroniser les informations dans le référentiel Financial Management avec celles de l'annuaire natif.