Oracle® Enterprise Performance Management System

Guida alla configurazione della sicurezza

Release 11.2
F28811-22
Dicembre 2023

ORACLE

Oracle Enterprise Performance Management System Guida alla configurazione della sicurezza, Release 11.2

F28811-22

Autore principale: EPM Information Development Team

Sommario

3 Abilitazione dell'SSO con gli agenti di protezione

4 Configurazione delle directory utenti

5 Utilizzo di un modulo di autenticazione custom

6 Linee guida per la sicurezza di EPM System

A Codice campione di autenticazione customizzata

Accesso facilitato alla documentazione

Per informazioni sull'impegno di Oracle riguardo l'accesso facilitato, visitare il sito Web Oracle Accessibility Program all'indirizzo http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Accesso al Supporto Oracle

I clienti Oracle che hanno acquistato il servizio di supporto tecnico hanno accesso al supporto elettronico attraverso My Oracle Support. Per informazioni, visitare http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info oppure http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs per clienti non udenti.

Feedback relativi alla documentazione

Per fornire un feedback su questa documentazione, fare clic sul pulsante Feedback in fondo alla pagina in un qualsiasi argomento di Oracle Help Center. È anche possibile inviare un messaggio e-mail all'indirizzo epmdoc_ww@oracle.com.

1

Informazioni su EPM System Security

Vedere anche:

- Informazioni su EPM System
- Competenze presunte
- Componenti dell'infrastruttura di sicurezza
- Autenticazione degli utenti
- Assegnazione ruoli (autorizzazione basata sui ruoli)
- Avvio di Shared Services Console

Informazioni su EPM System

I prodotti Oracle Enterprise Performance Management System costituiscono un sistema aziendale globale che integra suite modulari di applicazioni per la gestione finanziaria e la pianificazione con le più complete funzionalità di business intelligence per il reporting e l'analisi. I componenti principali dei prodotti EPM System sono i seguenti:

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

Per informazioni sui prodotti e sui componenti di ognuna di queste famiglie di prodotti, fare riferimento alla *Guida introduttiva per l'installazione di Oracle Enterprise Performance Management*.

Competenze presunte

Questa guida si rivolge agli amministratori di sistema che configurano, proteggono e gestiscono i componenti di Oracle Enterprise Performance Management System. Si presume la conoscenza dei seguenti settori:

- Profonda conoscenza dell'infrastruttura di sicurezza dell'organizzazione, inclusi gli elementi seguenti.
  - Server directory, ad esempio Oracle Internet Directory, Sun Java System Directory Server e Microsoft Active Directory
  - Utilizzo di Secure Socket Layer (SSL) per la protezione dei canali di comunicazione
  - Sistemi di gestione dell'accesso, ad esempio Oracle Access Manager e SiteMinder
  - Infrastruttura Single Sign-On (SSO), ad esempio Kerberos
- Conoscenza dei concetti relativi alla sicurezza di EPM System rilevanti per l'organizzazione

Componenti dell'infrastruttura di sicurezza

In Oracle Enterprise Performance Management System sono integrati diversi componenti di sicurezza per garantire una sicurezza delle applicazioni avanzata. Se integrato in un'infrastruttura sicura, EPM System offre una suite di applicazioni sicure che garantisce la sicurezza dei dati e dell'accesso. Tra i componenti dell'infrastruttura che possono essere utilizzati per proteggere EPM System sono inclusi quelli elencati di seguito.

- Un sistema di gestione degli accessi facoltativo, ad esempio Oracle Access Manager, per garantire l'accesso SSO ai componenti di EPM System
- L'utilizzo di un'infrastruttura SSO integrata, ad esempio Kerberos

  È possibile utilizzare l'autenticazione Kerberos con il sistema di gestione degli accessi (SiteMinder) per consentire agli utenti Windows di accedere in modo trasparente a SiteMinder e ai componenti di EPM System.
- L'utilizzo di Secure Socket Layer (SSL) per proteggere i canali di comunicazione tra i componenti di EPM System e i client

Autenticazione degli utenti

L'autenticazione degli utenti consente di utilizzare la funzionalità Single Sign-On (SSO) nei componenti di Oracle Enterprise Performance Management System convalidando le informazioni di accesso di ogni utente per determinare gli utenti autenticati. L'autenticazione degli utenti, abbinata all'autorizzazione specifica di ogni componente, consente agli utenti l'accesso ai componenti di EPM System. Il processo di concessione dell'autorizzazione è denominato assegnazione ruoli.

Componenti di autenticazione

Nelle sessioni che seguono vengono descritti i componenti che supportano l'SSO:

- Directory nativa
- Directory utenti esterne

Directory nativa

Per directory nativa si intende il database relazionale utilizzato da Oracle Hyperion Shared Services per supportare l'assegnazione ruoli e memorizzare i seeddata, ad esempio gli account utente predefiniti.

Le funzioni della directory nativa sono le seguenti.

- Gestire gli account utente predefiniti di EPM System
- Memorizzare tutte le informazioni di assegnazione ruoli di EPM System (relazioni tra utenti, gruppi e ruoli)

L'accesso e la gestione della directory nativa vengono effettuati tramite Oracle Hyperion Shared Services Console. Fare riferimento alla sezione "Gestione della directory nativa" nella *Oracle Enterprise Performance Management System User Security Administration Guide (in lingua inglese)*.

Directory utenti esterne

Per directory utenti si intende qualsiasi sistema aziendale di gestione degli utenti e delle identità compatibile con i componenti di EPM System.

I componenti di EPM System sono supportati in numerose directory utenti, incluse directory utenti basate su LDAP, ad esempio Oracle Internet Directory, Sun Java System Directory Server (precedentemente noto come SunONE Directory Server) e Microsoft Active Directory. Come directory utente, sono inoltre supportati i database relazionali. In questo documento, per fare riferimento a directory utenti diverse dalla directory nativa viene utilizzato il termine directory utenti esterne.

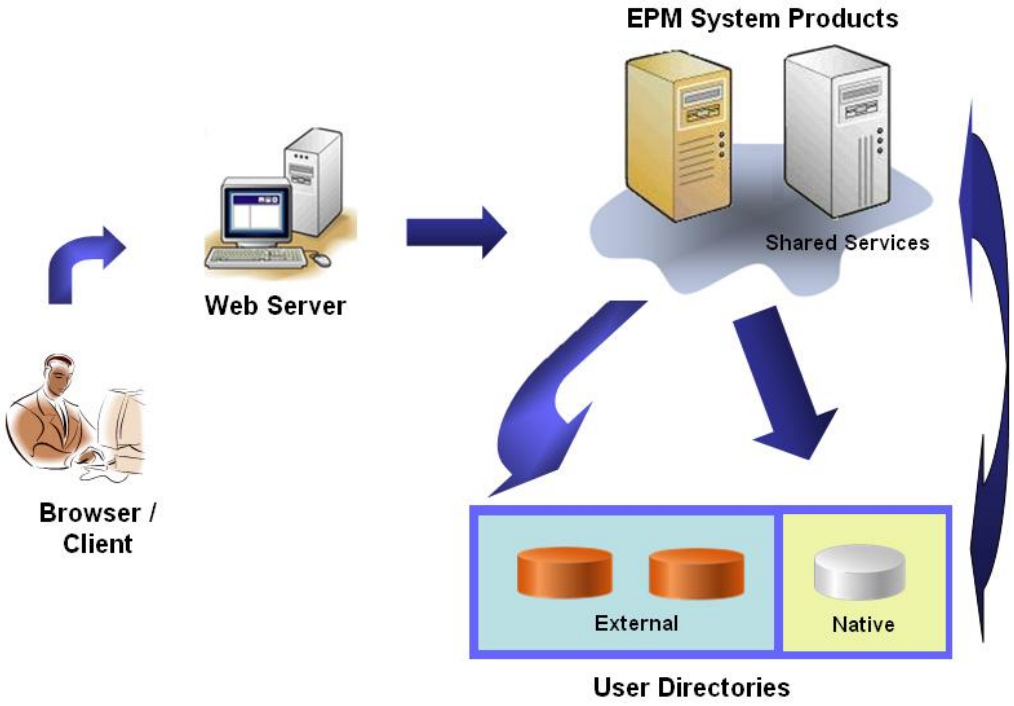
Per un elenco di directory utenti supportate, fare riferimento alla *Matrice per la certificazione di Oracle Enterprise Performance Management System* pubblicata nella pagina Configurazioni di sistema supportate da Oracle Fusion Middleware in Oracle Technology Network (OTN).

In Shared Services Console, è possibile configurare molte directory utenti esterne come origine di utenti e gruppi di EPM System. Ogni utente di EPM System deve disporre di un account univoco in una directory utenti configurata. In genere, gli utenti di EPM System sono assegnati a gruppi per facilitare l'assegnazione ruoli.

Single Sign-On di EPM System predefinito

EPM System supporta SSO tra le applicazioni Web di EPM System consentendo a utenti autenticati di un'applicazione di passare senza interruzioni ad altre applicazioni senza immettere di nuovo le credenziali. La funzionalità SSO è implementata integrando un ambiente di sicurezza comune che gestisce l'autenticazione degli utenti e l'assegnazione ruoli (autorizzazione basata sui ruoli) nei componenti di EPM System.

Nella figura riportata di seguito è descritto il processo SSO predefinito.



1. Mediante un browser, gli utenti accedono alla schermata di accesso di un componente di EPM System e immettono un nome utente e una password.

   Il componente di EPM System esegue una query sulle directory utenti configurate, compresa la directory nativa, per verificare le credenziali dell'utente. Quando viene identificato un account utente corrispondente in una directory utenti, la ricerca viene interrotta e le informazioni dell'utente vengono restituite al componente di EPM System.

   L'accesso viene invece negato se non viene individuato alcun account utente in alcuna directory utenti.

2. Utilizzando le informazioni dell'utente recuperate, il componente di EPM System esegue una query sulla directory nativa per ottenere i dettagli dell'assegnazione ruoli relativi a tale utente.

3. Il componente di EPM System controlla la lista di controllo dell'accesso (ACL) nel componente per determinare gli artifact dell'applicazione a cui può accedere l'utente.

Alla ricezione delle informazioni sull'assegnazione ruoli dalla directory nativa, il componente di EPM System viene reso disponibile per l'utente. A questo punto, viene abilitato l'accesso SSO per tutti i componenti di EPM System per cui sono stati assegnati ruoli all'utente.

Single Sign-On da sistemi di gestione degli accessi

Per proteggere ulteriormente i componenti di EPM System, è possibile implementare un sistema di gestione degli accessi supportato, ad esempio Oracle Access Manager o SiteMinder, in grado di fornire credenziali degli utenti autenticati ai componenti di EPM System e controllare l'accesso in base a privilegi di accesso predefiniti.

L'accesso SSO da agenti di sicurezza è disponibile solo per le applicazioni Web di EPM System. In questo scenario, i componenti di EPM System utilizzano le

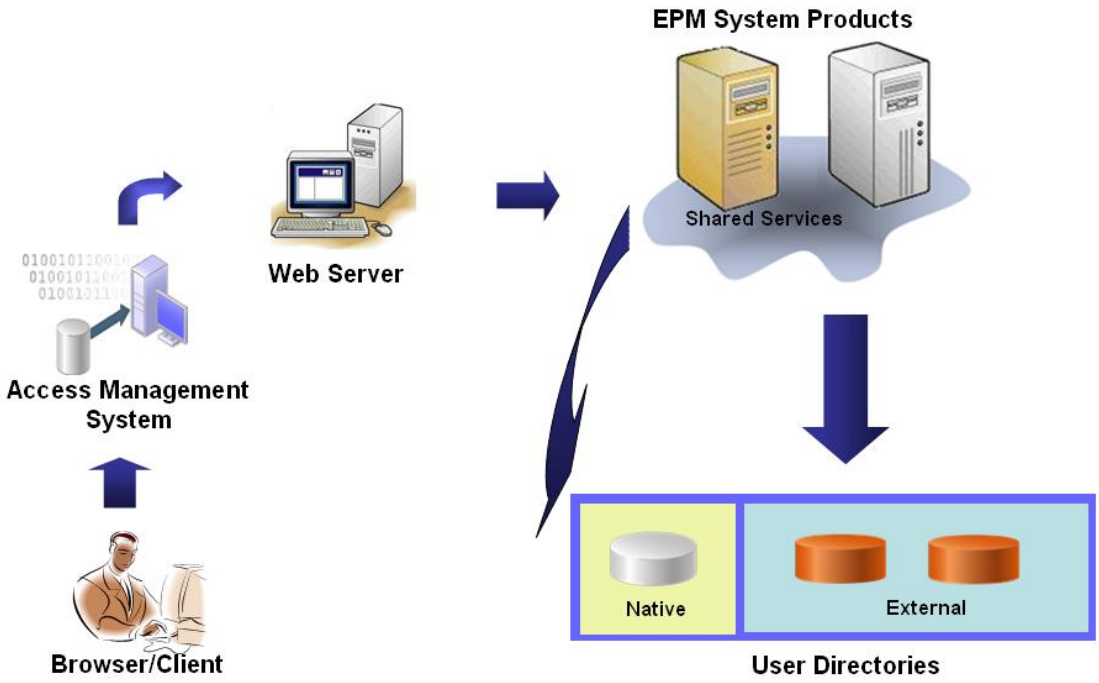
informazioni utente fornite dall'agente di sicurezza per determinare le autorizzazioni di accesso degli utenti. Per migliorare la sicurezza, Oracle consiglia di bloccare l'accesso diretto ai server tramite firewall in modo che tutte le richieste vengano indirizzate tramite un portale SSO.

L'accesso SSO da sistemi di gestione degli accessi è supportato mediante l'accettazione delle credenziali di utenti autenticati tramite un meccanismo SSO accettabile. Fare riferimento alla sezione Metodi SSO supportati. Il sistema di gestione degli accessi autentica gli utenti e passa il nome di accesso a EPM System. EPM System verifica il nome di accesso a fronte di directory utenti configurate.

Fare riferimento agli argomenti elencati di seguito.

- Single Sign-On da Oracle Access Manager
- OracleAS Single Sign-On
- SSO con SiteMinder
- Single Sign-On con Kerberos

Il concetto è illustrato di seguito.



1. Utilizzando un browser, gli utenti richiedono l'accesso a una risorsa protetta da un sistema di gestione degli accessi, ad esempio Oracle Access Manager o SiteMinder.

> **Nota:**
>
> I componenti di EPM System sono definiti come risorse protette dal sistema di gestione degli accessi.

Il sistema di gestione degli accessi intercetta la richiesta e visualizza una schermata di accesso. Gli utenti immettono un nome utente e una password, che vengono convalidati a fronte delle directory utenti configurate nel sistema di gestione degli accessi per la verifica dell'autenticità degli utenti. I componenti di EPM System vengono inoltre configurati per l'utilizzo di queste directory utenti.

Le informazioni sull'utente autenticato vengono passate al componente di EPM System, che le accetta come valide.

Il sistema di gestione degli accessi passa il nome di accesso dell'utente (valore di `Login Attribute`) al componente di EPM System con un meccanismo SSO accettabile. Fare riferimento alla sezione Metodi SSO supportati.

2. Per verificare le credenziali dell'utente, il componente di EPM System tenta di individuare l'utente all'interno di una directory utenti. Se viene rilevato un account utente corrispondente, le informazioni dell'utente vengono restituite al componente di EPM System. La funzionalità di sicurezza di EPM System imposta il token SSO che abilita l'accesso SSO nei componenti di EPM System.
3. Utilizzando le informazioni dell'utente recuperate, il componente di EPM System esegue una query sulla directory nativa per ottenere i dettagli dell'assegnazione ruoli relativi a tale utente.

   Alla ricezione delle informazioni di assegnazione ruoli dell'utente, il componente di EPM System viene reso disponibile per l'utente. L'accesso SSO viene abilitato per tutti i componenti di EPM System per cui sono stati assegnati ruoli all'utente.

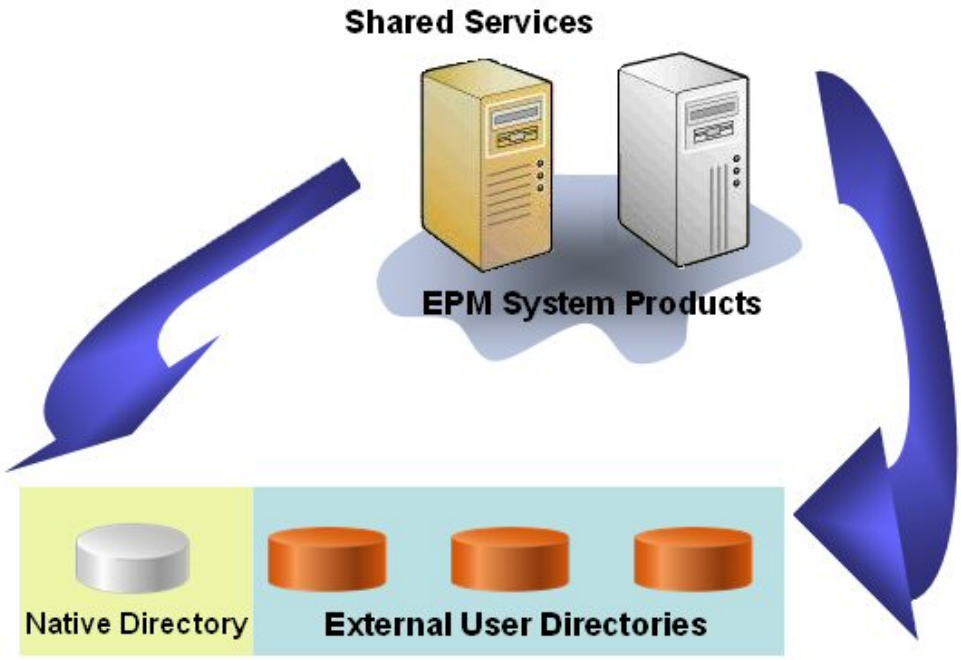
Assegnazione ruoli (autorizzazione basata sui ruoli)

La funzionalità di sicurezza di Oracle Enterprise Performance Management System determina l'accesso degli utenti alle applicazioni in base al concetto dei ruoli. I ruoli sono autorizzazioni che consentono agli utenti di accedere alle funzioni delle applicazioni. Alcuni componenti di EPM System applicano liste di controllo dell'accesso (ACL) a livello di oggetto per perfezionare il livello di accesso degli utenti agli artifact, ad esempio report e membri.

Ogni componente di EPM System offre ruoli predefiniti diversi, personalizzati in base a esigenze aziendali differenti. Questi ruoli vengono ereditati da tutte le applicazioni appartenenti a un componente di EPM System. Ruoli predefiniti delle applicazioni registrate in Oracle Hyperion Shared Services sono disponibili in Oracle Hyperion Shared Services Console. È inoltre possibile creare ulteriori ruoli in cui aggregare i ruoli predefiniti per soddisfare esigenze specifiche. Questi ruoli vengono utilizzati per l'assegnazione ruoli. Il processo durante il quale vengono concessi agli utenti e ai gruppi ruoli specifici appartenenti ad applicazioni EPM System e alle relative risorse è denominato *assegnazione ruoli*.

La directory nativa e le directory utenti configurate sono le origini delle informazioni su utenti e gruppi che vengono utilizzate per il processo di assegnazione ruoli. È possibile esplorare e assegnare ruoli a utenti e gruppi di tutte le directory utente configurate da Shared Services Console. È inoltre possibile utilizzare ruoli aggregati specifici di un'applicazione creati nella directory nativa durante il processo di assegnazione ruoli.

La figura che segue mostra una panoramica del processo di autorizzazione:



1. Dopo che un utente è stato autenticato, il componente di EPM System esegue una query sulle directory utenti per determinare i gruppi dell'utente.
2. Il componente di EPM System utilizza le informazioni sugli utenti e sui gruppi per recuperare i dati di assegnazione ruoli dell'utente da Shared Services e quindi utilizza tali dati per determinare le risorse a cui può accedere un utente.

   Vengono completati per ogni singolo prodotto task di assegnazione ruoli specifici del prodotto, ad esempio l'impostazione del controllo dell'accesso specifico di un prodotto. I dati ottenuti vengono combinati con i dati dell'assegnazione ruoli per determinare l'accesso al prodotto per l'utente.

L'assegnazione ruoli basata sui ruoli dei prodotti di EPM System viene eseguita in base a questi concetti.

Ruoli

Un ruolo è un costrutto, analogo a una lista di controllo dell'accesso (ACL), che definisce le autorizzazioni di accesso concesse a utenti e gruppi per l'esecuzione di funzioni sulle risorse di EPM System. Si tratta di una combinazione di una risorsa o di tipi di risorse (oggetti a cui gli utenti possono accedere, ad esempio un report) e di azioni che gli utenti possono eseguire sulla risorsa (ad esempio visualizzazione e modifica).

L'accesso alle risorse delle applicazioni EPM System è limitato. Un utente può accedervi solo dopo che è stato assegnato all'utente stesso o al gruppo di appartenenza un ruolo che fornisce l'accesso. Le limitazioni dell'accesso basate sui ruoli consentono agli amministratori di controllare e gestire l'accesso alle applicazioni.

Ruoli globali

I ruoli globali, ovvero ruoli di Shared Services che si estendono su più prodotti, consentono agli utenti di eseguire determinati task nei prodotti EPM System. L'amministratore di Shared Services ad esempio può assegnare ruoli agli utenti per tutte le applicazioni EPM System.

Ruoli predefiniti

I ruoli predefiniti sono ruoli built-in nei prodotti di EPM System. Non è possibile eliminarli. Ogni istanza di un'applicazione appartenente a un prodotto EPM System eredita i ruoli predefiniti del prodotto. Questi ruoli vengono registrati con Shared Services per ogni applicazione quando quest'ultima viene creata.

Ruoli aggregati

I ruoli aggregati, denominati anche ruoli custom, aggregano più ruoli predefiniti appartenenti a un'applicazione. Un ruolo aggregato può contenere altri ruoli aggregati. Ad esempio, un utente con il ruolo Gestione assegnazione ruoli o Amministratore di Shared Services può creare un ruolo aggregato che combina i ruoli Responsabile pianificazione e Utente visualizzazione di un'applicazione Oracle Hyperion Planning. L'aggregazione dei ruoli può semplificare l'amministrazione di applicazioni con vari ruoli granulari. I ruoli globali di Shared Services possono essere inclusi in ruoli aggregati. Non è possibile creare un ruolo aggregato che si estende a più applicazioni o prodotti.

Utenti

Nelle directory utente sono memorizzate informazioni sugli utenti che possono accedere ai prodotti di EPM System. Queste informazioni vengono utilizzate sia dal processo di autenticazione sia dal processo di autorizzazione. È possibile creare e gestire gli utenti della directory nativa solo da Shared Services Console.

Gli utenti di tutte le directory utente configurate possono essere visualizzati da Shared Services Console. Sebbene sia possibile assegnare ruoli a singoli utenti per concedere diritti di accesso alle applicazioni EPM System registrate con Shared Services, Oracle sconsiglia l'assegnazione individuale.

Amministratore di EPM System predefinito

Durante il processo di distribuzione viene creato un account amministratore, con nome predefinito `admin`, nella directory nativa. Si tratta dell'account di EPM System più potente e deve essere utilizzato solo per impostare un amministratore di sistema, ovvero l'esperto IT incaricato della gestione della sicurezza e dell'ambiente di EPM System.

Il nome utente e la password dell'amministratore di EPM System vengono impostati durante la distribuzione di Oracle Hyperion Foundation Services. Poiché questo account non può essere soggetto ai criteri delle password degli account aziendali, Oracle consiglia di disattivarlo dopo la creazione di un account amministratore di sistema.

In genere l'account amministratore di EPM System predefinito viene utilizzato per eseguire i task elencati di seguito.

- Configurare la directory aziendale come directory utenti esterna. Fare riferimento alla sezione Configurazione delle directory utenti.
- Creare un account amministratore di sistema assegnando a un esperto IT aziendale il ruolo di amministratore di Shared Services. Fare riferimento alla sezione "Assegnazione di ruoli a utenti e gruppi" nel manuale *Oracle Enterprise Performance Management System User Security Administration Guide (in lingua inglese)*.

Amministratore di sistema

L'amministratore di sistema è in genere un esperto IT aziendale con diritti di accesso in lettura, scrittura ed esecuzione per tutti i server interessati da una distribuzione di EPM System.

L'amministratore di sistema in genere esegue i task descritti di seguito.

- Disabilitare l'account amministratore di EPM System predefinito
- Creare almeno un amministratore funzionale
- Impostare la configurazione della sicurezza per EPM System utilizzando Shared Services Console
- Configurare facoltativamente le directory utenti come directory utenti esterne
- Monitorare EPM System eseguendo periodicamente lo strumento di analisi dei log

  I task eseguiti dagli amministratori funzionali sono descritti in questa guida.

Di seguito sono descritte le procedure per la creazione di un amministratore funzionale.

- Configurare la directory aziendale come directory utenti esterna. Fare riferimento alla sezione Configurazione delle directory utenti.
- Assegnare a un utente o un gruppo i ruoli necessari per la creazione di un amministratore funzionale. Fare riferimento alla sezione "Assegnazione di ruoli a utenti e gruppi" nel manuale *Oracle Enterprise Performance Management System User Security Administration Guide (in lingua inglese)*.

  All'amministratore funzionale devono essere assegnati i ruoli elencati di seguito.

  – Ruolo Amministratore LCM di Shared Services
  – Ruolo Amministratore e Gestione assegnazione ruoli di ogni componente di EPM System distribuito

Amministratori funzionali

L'amministrazione funzionale è un utente aziendale esperto di EPM System. In genere, questo utente è definito nella directory aziendale configurata in Shared Services come directory di utenti esterni.

L'amministratore funzionale esegue task di amministrazione di EPM System quali la creazione di altri amministratori funzionali, l'impostazione dell'amministrazione delegata, la creazione di applicazioni e artifact con relativa assegnazione ruoli, nonché la configurazione dell'auditing di EPM System. I task eseguiti dagli amministratori funzionali sono descritti nel manuale *Oracle Enterprise Performance Management System User Security Administration Guide (in lingua inglese)*.

Gruppi

I gruppi sono contenitori di utenti o di altri gruppi. È possibile creare e gestire gruppi della directory nativa da Shared Services Console. I gruppi di tutte le directory utente configurate sono visualizzati in Shared Services Console. È possibile assegnare ruoli a questi gruppi per concedere autorizzazioni per i prodotti EPM System registrati con Shared Services.

Avvio di Shared Services Console

Si utilizza un'opzione di menu in Oracle Hyperion Enterprise Performance Management Workspace per accedere a Oracle Hyperion Shared Services Console.

Per avviare Shared Services Console, procedere come segue:

1. Accedere all'indirizzo seguente:

   `http://web_server_name:port_number/workspace`

   Nell'URL, *web_server_name* indica il nome del computer su cui è in esecuzione il server Web utilizzato da Oracle Hyperion Foundation Services e *port_number* indica la porta del server Web, ad esempio `http://myWebserver:19000/workspace`.

   > **Nota:**
   >
   > Se si accede a EPM Workspace in ambienti protetti, utilizzare `https` come protocollo (anziché `http`) e il numero di porta del server Web protetto. ad esempio un URL simile a: `https://myserver:19043/easconsole/console.html`.

2. Fare clic su **Avvia applicazione**.

   > **Nota:**
   >
   > Un eventuale blocco dei popup può impedire l'apertura di EPM Workspace.

3. In **Accesso** immettere il nome utente e la password.

   Inizialmente, l'unico utente che può accedere a Shared Services Console è l'amministratore di Oracle Enterprise Performance Management System di cui nome utente e password sono stati specificati durante il processo di distribuzione.

4. Fare clic su **Accedi**.
5. Selezionare **Naviga**, quindi **Amministra** e infine **Shared Services Console**.

2

Abilitazione di SSL nei componenti di EPM System

Vedere anche:

- Presupposti
- Fonti di informazioni
- Riferimenti alle posizioni
- Informazioni sull'abilitazione per SSL dei prodotti EPM System
- Scenari SSL supportati
- Certificati richiesti
- Terminazione di SSL sull'offloader SSL
- Distribuzione di EPM System in modalità SSL completo
- Terminazione di SSL sul server Web
- SSL per Essbase 11.1.2.4
- SSL per Essbase 21c

Presupposti

- È stata determinata la topologia di distribuzione e sono stati identificati i collegamenti di comunicazione da proteggere tramite SSL.
- Sono stati ottenuti i certificati richiesti da un'Autorità di certificazione (CA, Certificate Authority), un'autorità di certificazione nota o personale, oppure sono stati creati certificati autofirmati. Fare riferimento alla sezione Certificati richiesti.
- È necessario avere familiarità con i concetti e le procedure di SSL, ad esempio l'importazione dei certificati.

  Per un elenco dei documenti di riferimento, fare riferimento alla sezione Fonti di informazioni.

Fonti di informazioni

Per abilitare per SSL Oracle Enterprise Performance Management System, è necessario preparare componenti come il server applicazioni, il server Web, i database e le directory utenti per comunicare tramite SSL. In questo documento si presuppone che si abbia familiarità con i task correlati all'abilitazione per SSL di tali componenti.

- **Oracle WebLogic Server**: fare riferimento alla sezione "Configurazione di SSL" nella *Guida alla protezione di WebLogic Server*.
- **Oracle HTTP Server:** fare riferimento agli argomenti seguenti nel manuale *Oracle HTTP Server Administrator's Guide* (in lingua inglese).

  - Gestione della sicurezza
  - Abilitazione di SSL per il server HTTP Oracle
- **Directory utenti**: fare riferimento alla documentazione del fornitore della directory utenti. Collegamenti utili:
  - **Oracle Internet Directory:** consultare la guida Oracle Internet Directory Administrator's Guide (in lingua inglese)
  - **Sun Java System Directory Server:** fare riferimento alla sezione "Sicurezza del server directory" nella *Guida all'amministrazione di Sun Java System Directory Server*
  - **Active Directory:** fare riferimento alla documentazione Microsoft.
- **Database**: fare riferimento alla documentazione del fornitore del database.

Riferimenti alle posizioni

In questo documento viene fatto riferimento alle posizioni di installazione e distribuzione elencate di seguito.

- *MIDDLEWARE_HOME* fa riferimento alla posizione dei componenti middleware, ad esempio Oracle WebLogic Server e, facoltativamente, a una o più directory *EPM_ORACLE_HOME*. La posizione *MIDDLEWARE_HOME* viene definita durante l'installazione del prodotto Oracle Enterprise Performance Management System. La directory *MIDDLEWARE_HOME* predefinita è `Oracle/Middleware`.
- *EPM_ORACLE_HOME* fa riferimento alla directory di installazione contenente i file necessari per supportare i prodotti EPM System. *EPM_ORACLE_HOME* si trova in *MIDDLEWARE_HOME*. La directory *EPM_ORACLE_HOME* predefinita è *MIDDLEWARE_HOME*`/EPMSystem11R1`, ad esempio `Oracle/Middleware/EPMSystem11R1`.

  I prodotti EPM System vengono installati nella directory *EPM_ORACLE_HOME*`/products`, ad esempio `Oracle/Middleware/EPMSystem11R1/products`.

  Inoltre, durante la configurazione dei prodotti EPM System, alcuni prodotti distribuiscono i componenti in *MIDDLEWARE_HOME*`/user_projects/epmsystem1`, ad esempio `Oracle/Middleware/user_projects/epmsystem1`.
- *EPM_ORACLE_INSTANCE* indica una posizione definita durante il processo di configurazione in cui vengono distribuiti i componenti di alcuni prodotti. La posizione predefinita di *EPM_ORACLE_INSTANCE* è *MIDDLEWARE_HOME*`/user_projects/epmsystem1`, ad esempio `Oracle/Middleware/user_projects/epmsystem1`.

Informazioni sull'abilitazione per SSL dei prodotti EPM System

Il processo di distribuzione di Oracle Enterprise Performance Management System consente di distribuire automaticamente i prodotti Oracle EPM System per il funzionamento sia in modalità SSL sia non SSL.

Nota:

- EPM System supporta solo SSL su HTTP e JDBC. Non sono supportati altri standard per la comunicazione sicura, ad esempio Thrift e ODBC.
- Per proteggersi dalla vulnerabilità nota come POODLE (Padding Oracle On Downgraded Legacy Encryption), un attacco che interessa il protocollo SSLv3, è necessario disabilitare il supporto di SSLv3 nei server e nei browser utilizzati per accedere ai componenti di EPM System. Per informazioni su come disabilitare il supporto di SSLv3, fare riferimento alla documentazione dei server e dei browser.
- I server EPM System potrebbero non avviarsi se si disabilita la modalità non SSL dopo la configurazione di SSL.
  Abilitare la replica sicura per tutti i server EPM System presenti nel dominio in modo che si avviino quando viene disabilitata la modalità non SSL.

Quando si specificano le impostazioni comuni per EPM System, si specifica se abilitare per SSL tutte le comunicazioni da server a server nella distribuzione.

Se si selezionano le impostazioni SSL durante il processo di distribuzione, l'ambiente non viene configurato automaticamente per SSL. Infatti, viene unicamente impostato un flag in Registro di Oracle Hyperion Shared Services per indicare che tutti i componenti di EPM System che utilizzano tale Registro devono utilizzare il protocollo sicuro (HTTPS) per le comunicazioni da server a server. Per abilitare per SSL l'ambiente, è necessario completare procedure aggiuntive. Tali procedure sono illustrate nel presente documento.

Nota:

Se si ridistribuiscono le applicazioni, si cancellano le impostazioni customizzate del server applicazioni e del server Web specificate per abilitare SSL.

Nota:

Nell'utility RCU (Repository Creation Utility) di Enterprise Performance Management System Release 11.2.x non è supportato SSL (Secure Sockets Layer) per MS SQL Server.

Scenari SSL supportati

Sono supportati gli scenari SSL descritti di seguito.

- Terminazione di SSL sull'offloader SSL. Fare riferimento alla sezione Terminazione di SSL sull'offloader SSL.
- Distribuzione in modalità SSL completo. Fare riferimento alla sezione Distribuzione di EPM System in modalità SSL completo.

Certificati richiesti

Le comunicazioni SSL utilizzano i certificati per stabilire una relazione di attendibilità tra i componenti. Oracle consiglia di utilizzare certificati di CA di terze parti note per abilitare il protocollo SSL per Oracle Enterprise Performance Management System in un ambiente di produzione.

> **Nota:**
>
> EPM System supporta l'utilizzo di certificati con caratteri jolly, che possono proteggere più sottodomini con un certificato SSL. Utilizzando un certificato con caratteri jolly è possibile ridurre i tempi e i costi di gestione.
>
> Se si utilizzano certificati con caratteri jolly per cifrare le comunicazioni, è necessario disabilitare la verifica del nome host in Oracle WebLogic Server.

Per ogni server che ospita componenti di EPM System sono necessari i certificati elencati di seguito.

- Un certificato CA radice.

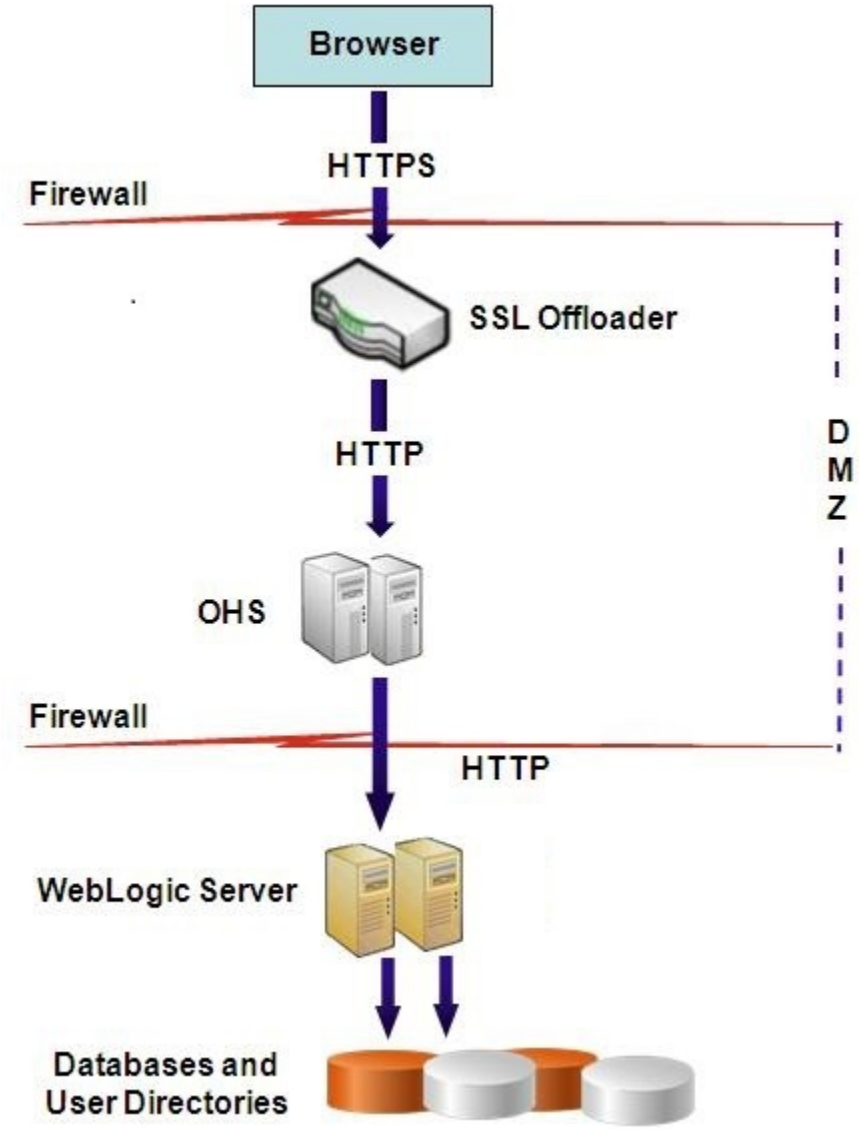
  > **Nota:**
  >
  > Non è necessario installare un certificato CA radice nel keystore Java se si utilizzano certificati di CA di terze parti note il cui certificato radice è già installato nel keystore Java.
  >
  > In Firefox e Internet Explorer sono precaricati certificati di CA di terze parti note. Se si agisce come CA, è necessario importare il proprio certificato CA radice nel keystore utilizzato dai client a cui accedono questi browser. Se si agisce come CA, i client Web non possono stabilire un handshake SSL con il server se il certificato CA radice non è disponibile per il browser da cui si accede al client.

- Certificati firmati per ogni istanza di Oracle HTTP Server nella distribuzione.
- Un certificato firmato per il computer host WebLogic Server. Anche i server gestiti presenti in tale computer possono utilizzare questo certificato.
- Due certificati per l'offloader/load balancer SSL. Uno di questi certificati è per le comunicazioni esterne e l'altro per quelle interne.

Terminazione di SSL sull'offloader SSL

Architettura di distribuzione

In questo scenario, l'autenticazione SSL viene utilizzata per proteggere il collegamento di comunicazione tra i client Oracle Enterprise Performance Management System (ad esempio un browser) e un offloader SSL. Il concetto è illustrato di seguito.



Presupposti

Offloader SSL e load balancer

Nell'ambiente di distribuzione deve essere presente un offloader SSL completamente configurato con un load balancer.

Il load balancer deve essere configurato per inoltrare tutte le richieste ricevute dagli host virtuali alle istanze di Oracle HTTP Server.

Quando SSL viene arrestato su Oracle HTTP Server (OHS) o sul load balancer, è necessario:

- Impostare ogni Applicazione Web logica su host virtuale non SSL del load balancer o di Oracle HTTP Server (ad esempio, `empinternal.myCompany.com:80` dove 80 è la porta non SSL). Aprire la schermata di configurazione e procedere come segue:
  1. Espandere il task di configurazione **Hyperion Foundation**.
  2. Selezionare **Configurazione indirizzo logico per applicazioni Web**.

3. Specificare un valore per *Nome host*, numero di porta non SSL e numero di porta SSL.

- Impostare l'URL esterno su host virtuale abilitato per SSL del load balancer o di Oracle HTTP Server (ad esempio, `empexternal.myCompany.com:443` dove 443 è la porta SSL). Aprire la schermata di configurazione e procedere come segue:
  1. Espandere il task di configurazione **Hyperion Foundation**.
  2. Selezionare **Configura impostazioni comuni**.
  3. Selezionare **Abilita offloading SSL** in Dettagli URL esterno.
  4. Specificare *Host URL esterno* e *Porta URL esterno*.

> **Nota:**
>
> Se si ridistribuiscono le applicazioni Web o si riconfigura il server Web con **ConfigTool**, le impostazioni dell'Applicazione Web logica e degli URL esterni verranno sostituite.

Host virtuali

La configurazione con autenticazione SSL terminata sull'offloader SSL utilizza due alias di server, ad esempio `epm.myCompany.com` ed `empinternal.myCompany.com`, nell'offloader/load balancer SSL, uno per le comunicazioni esterne tra l'offloader e i browser e l'altro per le comunicazioni interne tra server EPM System. Assicurarsi che gli alias dei server puntino all'indirizzo IP del computer e che siano risolvibili tramite DNS.

Un certificato firmato che supporta le comunicazioni esterne tra l'offloader e i browser (tramite `epm.myCompany.com`) deve essere installato nell'offloader/load balancer.

Configurazione di EPM System

La distribuzione predefinita dei componenti di EPM System supporta la terminazione di SSL sull'offloader SSL. Non sono richieste azioni aggiuntive.

Durante la configurazione di EPM System, assicurarsi che l'indirizzo logico delle applicazioni Web punti all'alias (ad esempio `empinternal.myCompany.com`) creato per le comunicazioni interne. Per installare e configurare EPM System, fare riferimento alle fonti di informazioni elencate di seguito.

- *Guida di installazione e configurazione di Oracle Enterprise Performance Management System*
- *Guida introduttiva per l'installazione di Oracle Enterprise Performance Management*
- *Guida per la risoluzione dei problemi di installazione e configurazione di Oracle Enterprise Performance Management System*

Test della distribuzione

Al termine del processo di distribuzione, verificare che sia tutto funzionante effettuando una connessione all'URL di Oracle Hyperion Enterprise Performance Management Workspace sicuro:

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

Ad esempio, `https://epm.myCompany.com:443/workspace/index.jsp`, dove 443 è la porta SSL.

Distribuzione di EPM System in modalità SSL completo

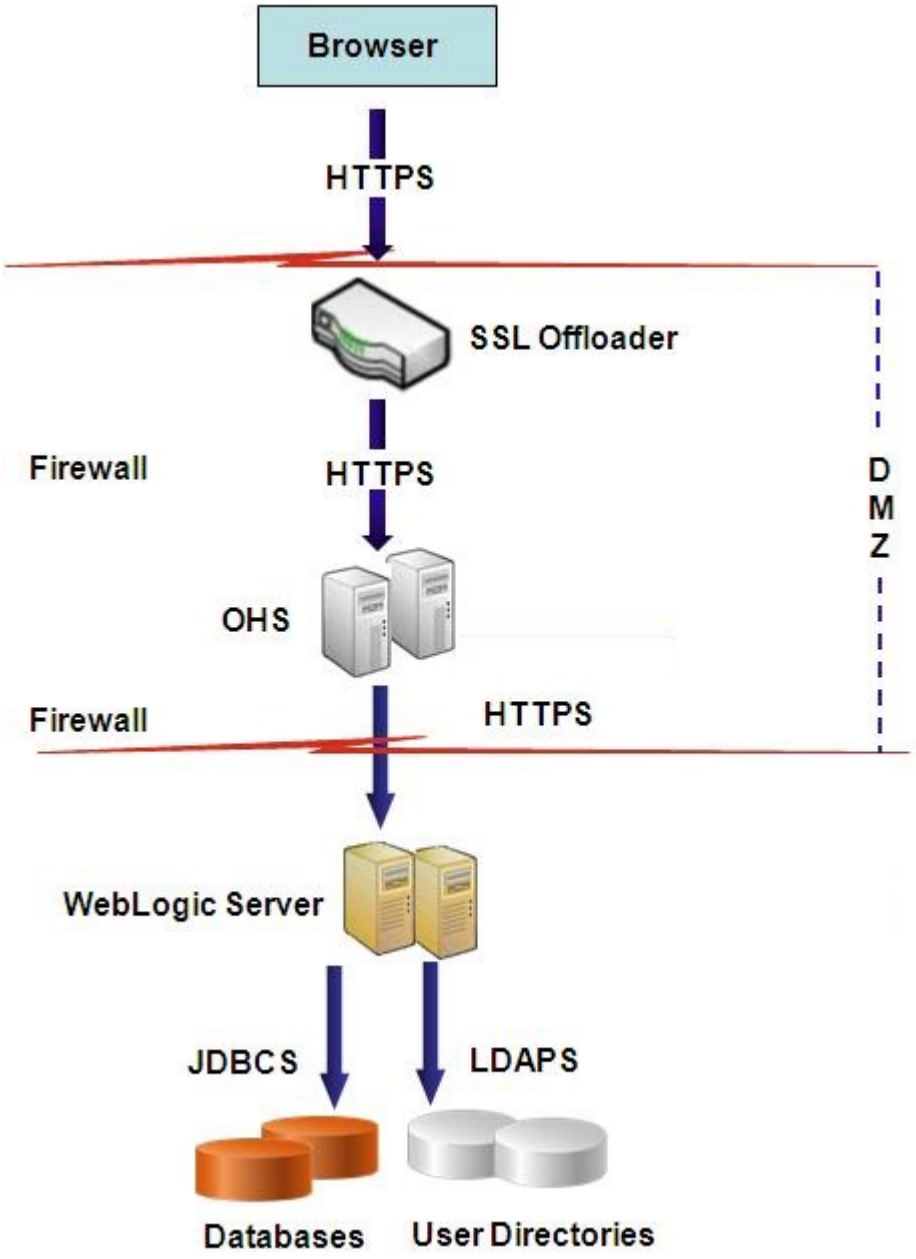
Vedere anche:

- Architettura di distribuzione
- Presupposti
- Configurazione di EPM System per SSL completo

Architettura di distribuzione

In modalità SSL completo, la comunicazione fra tutti i canali che è possibile proteggere viene protetta tramite SSL. Questo scenario di distribuzione di Oracle Enterprise Performance Management System è il più sicuro.

Il concetto è illustrato di seguito.



Presupposti

Database

I database server e i client sono abilitati per SSL. Per informazioni su come abilitare per SSL il database server e il client, fare riferimento alla documentazione relativa al database.

EPM System

È necessario che i componenti di Oracle Enterprise Performance Management System, inclusi Oracle WebLogic Server e Oracle HTTP Server, siano stati installati e distribuiti. È inoltre necessario che l'ambiente EPM System sia stato testato per

verificare che tutti gli elementi funzionino in modalità non SSL. Fare riferimento alle fonti di informazione seguenti.

- *Guida di installazione e configurazione di Oracle Enterprise Performance Management System*
- *Guida introduttiva per l'installazione di Oracle Enterprise Performance Management*
- *Guida per la risoluzione dei problemi di installazione e configurazione di Oracle Enterprise Performance Management System*

Se si intende abilitare per SSL le connessioni a database, durante il processo di configurazione è necessario selezionare il collegamento **Opzioni avanzate** in ogni schermata di configurazione del database e quindi specificare le impostazioni richieste, riportate di seguito.

- Selezionare **Usa connessione sicura al database (SSL)** e immettere un URL di database sicuro. Ad esempio,
  `jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCPS)(HOST=`*`myDBhost`*`)(PORT=1529)(CONNECT_DATA=(SERVICE NAME=`*`myDBhost.myCompany.com`*`)))`
- **Keystore di accesso sicuro**
- **Password keystore di accesso sicuro**

Per informazioni dettagliate, fare riferimento al manuale *Guida di installazione e configurazione di Oracle Enterprise Performance Management System*.

Offloader SSL e load balancer

Nell'ambiente di distribuzione deve essere presente un offloader SSL completamente configurato con un load balancer.

Nella configurazione in modalità SSL completo vengono utilizzati due alias server, ad esempio `epm.myCompany.com` ed `empinternal.myCompany.com` nell'offloader SSL. Uno è per la comunicazione esterna tra l'offloader e i browser, mentre l'altro è per la comunicazione interna tra i server EPM System. Assicurarsi che gli alias server puntino all'indirizzo IP del computer e che possano essere risolti tramite DNS.

Il load balancer deve essere configurato per inoltrare tutte le richieste ricevute dagli host virtuali alle istanze di Oracle HTTP Server.

I due certificati firmati, uno per supportare la comunicazione esterna tra l'offloader e i browser (tramite `epm.myCompany.com`) e l'altro per supportare la comunicazione interna (tramite `empinternal.myCompany.com`) tra le applicazioni, devono essere installati nell'offloader/load balancer. Oracle consiglia di associare tali certificati agli alias server per impedire l'esposizione dei nomi dei server e per migliorare la sicurezza.

Configurazione di EPM System per SSL completo

Vedere anche:

- Riconfigurazione delle impostazioni comuni di EPM System
- Facoltativo: Installazione del certificato CA radice per WebLogic Server
- Installazione del certificato in WebLogic Server
- Configurazione di WebLogic Server
- Abilitazione della connessione di un server HFM con Oracle Database abilitato per SSL

- Procedure di Oracle HTTP Server
- Configurazione dei componenti Web di EPM System distribuiti in WebLogic Server
- Aggiornamento della configurazione del dominio
- Riavvio dei server e di EPM System
- Test della distribuzione
- Configurazione delle directory utenti esterne abilitate per SSL

Riconfigurazione delle impostazioni comuni di EPM System

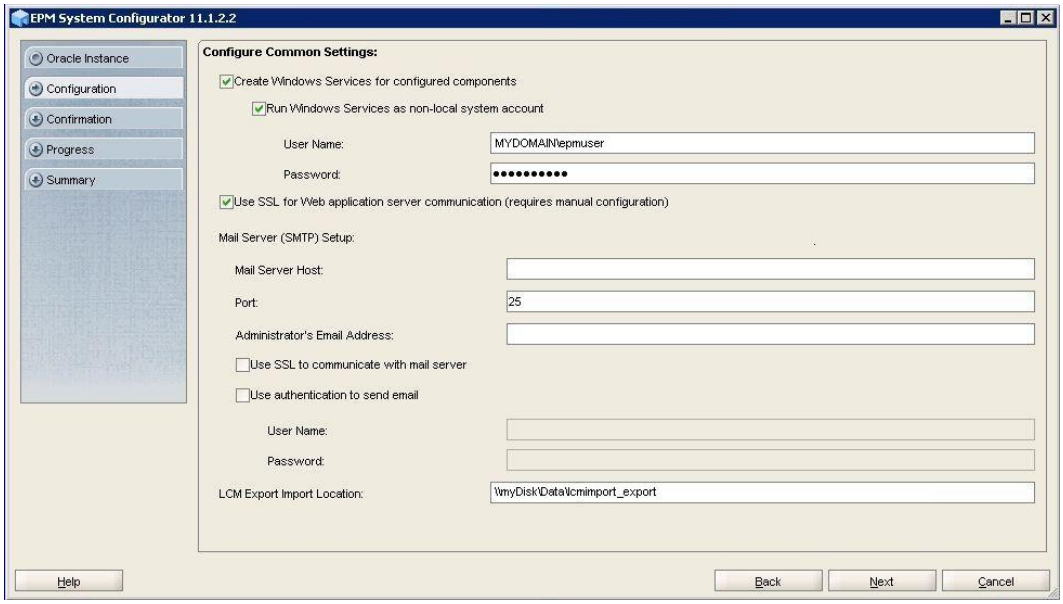
Durante questo processo, si selezionano le impostazioni che forzano i componenti di Oracle Enterprise Performance Management System a utilizzare le comunicazioni SSL.

> **Nota:**
>
> **Se si sta abilitando il protocollo SSL per il server Web Oracle Hyperion Financial Management:** prima di configurare Financial Management, è necessario proteggere il cookie modificando il descrittore sessione di HFM WebApp in `weblogic.xml`.
>
> 1. Espandere l'archivio Web di Financial Management utilizzando uno strumento come 7 Zip. La posizione di `weblogic.xml` nell'archivio è *`EPM_ORACLE_HOME`*`\products\FinancialManagement\AppServer\InstallableApps\HFMWebApplication.ear\HFMWeb.war\WEB-INF\weblogic.xml`.
> 2. Includere la direttiva seguente nel descrittore sessione di HFM WebApp in `weblogic.xml`:
> `<cookie-secure>true</cookie-secure>`
> 3. Salvare `weblogic.xml`
> 4. Quando 7-Zip richiede se si desidera aggiornare l'archivio, fare clic su **Yes**.

Per riconfigurare EPM System per SSL, procedere come segue.

1. Avviare EPM System Configurator.
2. In **Selezionare l'istanza di Oracle EPM a cui la configurazione verrà applicata**, procedere come segue.
   a. In **Nome istanza Oracle EPM**, immettere il nome dell'istanza utilizzato durante la configurazione iniziale dei componenti di EPM System.
   b. Fare clic su **Avanti**.
3. Nella schermata di configurazione, procedere come segue.
   a. Deselezionare **Deseleziona tutto**.
   b. Espandere il task di configurazione **Hyperion Foundation** e quindi selezionare **Configura impostazioni comuni**.
   c. Fare clic su **Avanti**.
4. In **Configura impostazioni comuni**, procedere come segue.

> **Attenzione:**
>
> Prima di selezionare le impostazioni per l'utilizzo di SSL per comunicare con il server di e-mail, assicurarsi che il server di e-mail sia configurato per SSL.



a. Selezionare **Utilizzare SSL per le comunicazioni del server applicazioni Web Java (richiede la configurazione manuale)** per specificare che in EPM System deve essere utilizzato il protocollo SSL per le comunicazioni.

b. **Facoltativo:** immettere le informazioni in **Host server di posta** e **Porta**. Per supportare le comunicazioni SSL, è necessario specificare la porta sicura utilizzata dal server di posta SMTP.

c. **Facoltativo:** per supportare le comunicazioni SSL con il server di posta SMTP, selezionare **Usa SSL per comunicare con il server di posta**.

d. Selezionare o immettere impostazioni nei campi restanti.

e. Fare clic su **Avanti**.

5. Fare clic su **Avanti** nelle schermate successive di EPM System Configurator.
6. Al termine del processo di distribuzione, viene visualizzata la schermata di riepilogo. Fare clic su **Fine**.

Facoltativo - Installazione del certificato CA radice per WebLogic Server

I certificati radice della maggior parte delle CA di terze parti note sono già installati nel keystore JVM. Completare le procedure descritte in questa sezione se non si utilizzano certificati di una CA di terze parti nota (non consigliato). La posizione predefinita del keystore JVM è *MIDDLEWARE_HOME*`/jdk/jre/lib/security/cacerts`.

> **Nota:**
>
> Eseguire questa procedura in ogni server Oracle Enterprise Performance Management System.

Per installare il certificato CA radice, procedere come segue.

1. Copiare il certificato CA radice nella directory locale nel computer in cui è installato Oracle WebLogic Server.
2. Da una console, cambiare directory passando a *MIDDLEWARE_HOME*/jdk/jre/bin.
3. Eseguire un comando keytool come quello riportato di seguito per installare il certificato CA radice nel keystore JVM:

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

   È ad esempio possibile utilizzare il comando riportato di seguito per aggiungere un certificato `CAcert.crt` memorizzato nella directory corrente al keystore JVM con `Blister` come alias del certificato nel keystore. Si presuppone l'utilizzo di `example_pwd` di storepass.

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

   > **Nota:**
   >
   > Il comando e l'esempio precedenti utilizzano parte della sintassi per l'importazione dei certificati tramite keytool. Per un elenco completo della sintassi di importazione, fare riferimento alla documentazione relativa al keytool.

Installazione del certificato in WebLogic Server

L'installazione predefinita di Oracle WebLogic Server utilizza un certificato demo per supportare SSL. Oracle consiglia di installare un certificato di terze parti note per aumentare la sicurezza dell'ambiente in uso.

In ogni computer che ospita WebLogic Server, utilizzare uno strumento (ad esempio, keytool) per creare un keystore customizzato in cui memorizzare il certificato firmato per WebLogic Server e i componenti Web di Oracle Enterprise Performance Management System.

Per creare un keystore customizzato e importare il certificato, procedere come segue.

1. Da una console, cambiare directory passando a *MIDDLEWARE_HOME*/jdk/jre/bin.

2. Eseguire un comando keytool come il seguente per creare il keystore customizzato (identificato dalla direttiva `-keystore` nel comando) in una directory esistente:

   ```
   keytool -genkey -dname "cn=myserver, ou=EPM, o=myCompany, c=US" -alias
   epm_ssl -keypass password -keystore
   C:\oracle\Middleware\EPMSystem11R1\ssl\keystore -storepass password -
   validity 365 -keyalg RSA
   ```

   > **Nota:**
   >
   > Il nome comune (cn) impostato deve corrispondere al nome del server. Se si utilizza un nome dominio completamente qualificato (FQDN) come cn, è necessario utilizzare tale nome durante la distribuzione dei componenti Web.

3. Generare la richiesta di un certificato.

   ```
   keytool -certreq -alias epm_ssl -file C:/certs/epmssl_csr -keypass
   password -storetype jks -keystore
   C:\oracle\Middleware\EPMSystem11R1\ssl\keystore -storepass password
   ```

4. Ottenere un certificato firmato per il computer WebLogic Server.
5. Importare nel keystore il certificato firmato:

   ```
   keytool -import -alias epm_ssl -file C:/certs/epmssl_crt -keypass
   password -keystore C:\Oracle\Middleware\EPMSystem11R1\ssl\keystore -
   storepass password
   ```

Configurazione di WebLogic Server

Dopo aver distribuito i componenti Web di Oracle Enterprise Performance Management System, è necessario configurarli per la comunicazione SSL.

Per configurare i componenti Web per SSL, procedere come segue.

1. Avviare Oracle WebLogic Server eseguendo *MIDDLEWARE_HOME*`/user_projects/domains/EPMSystem/bin/startWebLogic.cmd`:
2. Avviare la console di amministrazione di WebLogic Server accedendo all'URL seguente:

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

   Ad esempio, per accedere alla console di WebLogic Server distribuita sulla porta predefinita in `myServer`, è necessario utilizzare `http://myServer:7001/console`.
3. Nella schermata di benvenuto immettere il nome utente e la password di amministratore di WebLogic Server specificati in EPM System Configurator.
4. Nel **Centro modifiche**, fare clic su **Blocca e modifica**.
5. Nel riquadro sinistro della console, espandere **Ambiente** e selezionare **Server**.
6. Nella schermata Riepilogo dei server, fare clic sul nome del server che si desidera abilitare per SSL.

Ad esempio, per abilitare per SSL i componenti Oracle Hyperion Foundation Services, è necessario utilizzare il server `EPMServer0`.

7. Deselezionare **Porta di ascolto abilitata** per disabilitare la porta di ascolto HTTP.
8. Assicurarsi che l'opzione **Porta di ascolto SSL abilitata** sia selezionata.
9. In **Porta di ascolto SSL**, immettere la porta di ascolto SSL su cui questo server deve restare in ascolto delle richieste.
10. Per specificare il keystore identità e il keystore sicuro da utilizzare, selezionare **Keystore** per aprire la scheda corrispondente.
11. Fare clic su **Modifica**.
12. Selezionare un'opzione.
    - **Identità personalizzata e sicurezza personalizzata** se non si utilizza un certificato server proveniente da una CA di terze parti nota
    - **Identità personalizzata e sicurezza standard Java** se si utilizza un certificato server proveniente da una CA di terze parti nota
13. Fare clic su **Salva**.
14. In **Keystore identità personalizzato**, immettere il percorso del keystore in cui è installato il certificato firmato di WebLogic Server.
15. In **Tipo di keystore identità personalizzato**, immettere `jks`.
16. In **Passphrase keystore identità personalizzato** e **Conferma passphrase keystore identità personalizzato**, immettere la password del keystore.
17. Se in **Keystore** è stata selezionata l'opzione **Identità personalizzata e sicurezza personalizzata**, procedere come segue.
    - In **Keystore sicuro personalizzato**, immettere il percorso del keystore customizzato in cui è disponibile il certificato radice della CA che ha firmato il certificato server.
    - In **Tipo di keystore sicuro personalizzato**, immettere `jks`.
    - In **Passphrase keystore sicuro personalizzato** e **Conferma passphrase keystore sicuro personalizzato**, immettere la password del keystore.
18. Fare clic su **Salva**.
19. Specificare le impostazioni SSL.
    - Selezionare **SSL**.
    - In **Alias chiave privata**, immettere l'alias specificato durante l'importazione del certificato firmato di WebLogic Server.
    - In **Passphrase chiave privata** e **Conferma passphrase chiave privata**, immettere la password da utilizzare per recuperare la chiave privata.
    - Fare clic su **Salva**.

> **Nota:**
>
> Se si stanno utilizzando certificati SHA-2, è necessario selezionare l'impostazione **Usa SSL JSSE** per ogni server gestito utilizzato per supportare EPM System. Questa impostazione è disponibile nella scheda Avanzate della pagina SSL. Per rendere effettiva tale modifica, è necessario riavviare WebLogic Server.

20. Abilitare la replica sicura per il server procedendo come segue.
    a. Nel riquadro sinistro della console, espandere **Ambiente** e fare clic su **Cluster**.
    b. In Riepilogo dei cluster, fare clic sul nome del server, ad esempio `Foundation Services`, per il quale si desidera abilitare la replica sicura.

       Viene visualizzata la scheda Configurazione della schermata Impostazioni per il server selezionato.
    c. Fare clic su **Replica** per aprire la scheda corrispondente.
    d. Selezionare **Replica protetta abilitata**. Prima di selezionare questa opzione, potrebbe essere necessario fare clic su **Blocca e modifica**.
    e. Fare clic su **Salva**.
21. Completare i passi 6 - 20 per ogni server gestito appartenente a questo host.
22. Abilitare la replica sicura per fornire il canale per le chiamate di replica per il cluster.

    Per informazioni dettagliate, fare riferimento al documento Oracle metalink 1319381.1.
    - Nella console di amministrazione, espandere **Ambiente** e selezionare **Cluster**.
    - Selezionare **Replica**.
    - In **Replica**, selezionare **Replica protetta abilitata**.
    - Fare clic su **Salva**.
23. Nel **Centro modifiche**, fare clic su **Attiva modifiche**.

Abilitazione della connessione di un server HFM con Oracle Database abilitato per SSL

La connessione di rete tra l'origine dati HFM e il database Oracle può essere cifrata utilizzando SSL. Affinché questo funzioni, è necessario che Oracle Wallet sia configurato come indicato nella documentazione di Oracle. È necessario che anche il listener TNS sia configurato per l'ascolto su una nuova porta per le connessioni cifrate SSL. Infine, è necessario che i certificati appropriati siano stati caricati nel keystore e nel truststore sul server che ospita l'origine dati HFM. Le istruzioni fornite di seguito sono riportate nella documentazione di Oracle Database.

Prerequisiti

Prima di procedere con i passi riportati in basso, verificare che siano soddisfatti i seguenti prerequisiti:

- Un server database che funzioni correttamente.
- Verificare che nessun firewall locale o di rete blocchi la comunicazione con il server sulla porta su cui è in esecuzione il listener TNS abilitato per SSL.

Negli esempi che seguono, è stata utilizzata la versione Oracle 12c (12.1.0.2) in esecuzione su MS Windows Server 2016. Queste istruzioni saranno utilizzabili in un'installazione su Linux se i percorsi specificati per i file del wallet sono percorsi del file system Linux e le sostituzioni per le variabili di ambiente corrispondono alla shell utilizzata nel server database. Queste stesse istruzioni sono state utilizzate nelle istanze di sviluppo e supporto 19c.

Negli esempi riportati in questo articolo vengono utilizzati certificati autofirmati, ma è possibile utilizzare qualunque certificato CA appropriato. Per la procedura esatta da seguire quando si installa un certificato emesso da un'autorità di certificazione, fare riferimento alla documentazione di Oracle Database.

Configurazione di Oracle Database

Per configurare Oracle Database, procedere come segue.

1. Creare un nuovo wallet di login automatico sul server database.

> **Nota:**
>
> Queste operazioni sono necessarie solo se non è già stato creato un Oracle Wallet in precedenza. I passi riportati di seguito non sono necessari se sul server database viene utilizzato lo strumento relativo all'interfaccia utente grafica di Oracle Wallet.

```
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
```

È possibile ignorare i messaggi che richiedono l'utilizzo di `-auto_login_local` sulla riga di comando `orapki`. Se si verifica un errore di autenticazione SSL, fare riferimento a ID documento 2238096.1 per risolvere il problema.
Inoltre, verificare le autorizzazioni di sicurezza del file `cwallet.sso` (nella directory wallet) e controllare che l'utente del servizio listener Oracle disponga delle autorizzazioni di lettura per il file. Se non si dispone delle autorizzazioni di lettura, l'handshake SSL avrà esito negativo più avanti. Questa situazione si verifica se il database Oracle è stato installato senza che l'utente Oracle suggerito fosse autorizzato a eseguire l'accesso. Se il database Oracle è stato installato con l'utente Oracle, è necessario che il listener TNS venga eseguito come utente differente.

2. Creare un certificato autofirmato e caricarlo nel wallet

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

La password `password1` specificata nell'esempio sopra deve essere uguale alla password specificata nel *Passo 1*.

3. Esportare il certificato autofirmato appena creato

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

4. Copiare il file di certificato Base64 esportato sul server o sui server HFM.
5. Configurare SQL*NET e il listener TNS procedendo come segue.
   a. Individuare sul server database una porta non utilizzata. Nell'esempio che segue il nuovo listener viene creato sulla porta `1522`. In genere, per le connessioni SSL viene utilizzata la porta `2484` ed è possibile utilizzare qualsiasi porta disponibile. Prima di procedere apportando le modifiche necessarie, verificare che la porta che si desidera utilizzare sia disponibile sul server database.
   b. Aggiornare `SQLNET.ORA`. L'elemento DIRECTORY nella dichiarazione WALLET_LOCATION deve puntare al wallet creato nel precedente *Passo 1*.

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

   c. Aggiornare LISTENER.ORA per definire un nuovo listener. Utilizzare la porta individuata nel precedente *Passo 5a*.

```
SID_LIST_LISTENER =
(SID_LIST =
(SID_DESC =
(SID_NAME = CLRExtProc)
(ORACLE_HOME = C:\oracledb\12.1.0\home)
(PROGRAM = extproc)
(ENVS = "EXTPROC_DLLS=ONLY:C:\oracledb\12.1.0\home\bin\oraclr12.dll")
)
)
SSL_CLIENT_AUTHENTICATION = FALSE
WALLET_LOCATION=
(SOURCE =
(METHOD = FILE)
(METHOD_DATA =
(DIRECTORY = C:\oracledb\12.1.0\home\wallet)
)
)
LISTENER =
(DESCRIPTION_LIST =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = myServer)(PORT = 1521))
)
(DESCRIPTION =
```

```
(ADDRESS = (PROTOCOL = TCPS)(HOST = myServer)(PORT = 1522))
)
(DESCRIPTION =
(ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC1521))
)
)
ADR_BASE_LISTENER = C:\oracledb
```

d. Creare una nuova voce in `TNSNAMES.ORA` per la nuova porta.

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

Specificare la stessa porta individuata nel precedente *Passo 5a* e utilizzata nel *Passo 5c*.

e. Avviare il listener TNS.

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

f. Verificare che il nuovo listener TNS funzioni correttamente

```
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)
```

Configurazione del server HFM per l'utilizzo delle connessioni al database SSL

Aggiunta del certificato del database al truststore sul server o sui server HFM

È necessario effettuare le operazioni riportate di seguito su ogni singolo server EPM su cui viene eseguita l'origine dati HFM. La variabile di ambiente `%MW_HOME%` utilizzata di seguito corrisponde al percorso di installazione di Oracle Middleware. Questa variabile di ambiente non viene creata per impostazione predefinita durante l'installazione EPM e viene utilizzata qui per indicare la directory padre dell'installazione EPM.

La variabile di ambiente `EMP_ORACLE_HOME` indica la posizione dell'installazione EPM. Nell'esempio che segue, il keystore e i truststore sono in una directory che si trova nella stessa posizione dell'installazione EPM. I file keystore e truststore possono trovarsi in qualunque posizione nel file system del server HFM.

1. Creare una nuova directory in `%MW_HOME%` dove memorizzare il keystore Java e il truststore PKCS12.
   a. cd `%MW_HOME%`
   b. mkdir `certs`
2. Copiare il file keystore Java cacerts dal JDK.
   a. cd `%MW_HOME%\certs`
   b. copy `%MW_HOME%\jdk1.8.0_181\jre\lib\security\cacerts testing_cacerts`
   È opportuno copiare e utilizzare il keystore del JDK piuttosto che il keystore predefinito del JDK perché se il JDK viene aggiornato e il precedente JDK viene eliminato, le chiavi e i certificati inseriti nel keystore predefinito andranno persi.
3. Copiare il certificato Base64 in `%MW_HOME%\certs`.
4. Importare il certificato nel file keystore Java `testing_cacerts`.
   a. Ad esempio, `keytool -importcert -file bur00cbb-certificate.crt -keystore testing_cacerts -alias "myserver"`
      i. Sarà necessario specificare la password per il keystore.
      ii. Sostituire "myserver" con il dominio completamente qualificato del server database.
   b. Quando viene chiesto di indicare se il certificato deve essere ritenuto sicuro, specificare **y**.
5. Creare il truststore in formato PKCS12 dal file keystore Java del JDK. Ad esempio:

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

Aggiornamento delle connessioni JDBC di HFM per l'utilizzo di SSL

1. Riconfigurare la connessione JDBC del database HFM per l'utilizzo di SSL.
   a. Avviare lo strumento di configurazione EPM.
      i. Selezionare i nodi **Configura database** e **Distribuisci su server applicazioni** nel nodo **Financial Management**.
      ii. Fare clic su **Avanti**.
      iii. Effettuare ognuna di queste operazioni per la connessione JDBC di HFM
         i. Nelle colonne Porta, Nome servizio, Nome utente e Password, specificare la porta SSL, il nome del servizio, il nome utente e la password della connessione.
         ii. Fare clic su **(+)** per aprire le **opzioni database avanzate.**
         iii. Selezionare la casella di controllo **Usa connessioni sicure**.
         iv. Specificare la posizione del keystore Java creato nel *Passo 2*.
         v. Fare clic su **Applica**.

vi. Fare clic su **(+)** per aprire le **opzioni database avanzate.**

vii. Fare clic su **Modifica e usa URL JDBC modificato**. Non apportare modifiche all'URL JDBC visualizzato.

viii. Fare clic su **Applica**.

ix. Fare clic su **Avanti**.

b. Completare la procedura necessaria per distribuire l'applicazione HFM come descritto nella documentazione EPM.

2. Aprire una finestra dei comandi o una shell per aggiornare manualmente il registro EPM in modo che la connessione ODBC utilizzata dall'origine dati possa essere abilitata per SSL.
Eseguire ognuno dei comandi riportati in basso:

```
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
```

Negli esempi riportati sopra, il percorso `C:\Oracle\Middleware` è il valore di `%MW_HOME%` nei passi 1, 2 e 3.

Se si utilizza un certificato autofirmato, impostare la proprietà `FINANCIAL_MANAGEMENT_PRODUCT/DATABASE_CONN/@ODBC_VALIDATESERVERCERTIFICATE` su False. Il valore di `FINANCIAL_MANAGEMENT_PRODUCT/DATABASE_CONN/@ODBC_TRUSTSTOREPASSWORD` deve essere la password del keystore Java originale copiato nel *Passo 2*.

Aggiornare la voce relativa ai nomi TNS utilizzata da HFM

Modificare `TNSNAMES.ORA` per creare una nuova voce e assegnare un nuovo nome alla voce precedente. Nell'esempio che segue viene riportata la versione aggiornata del file `TNSNAMES.ORA` presente sul server HFM a cui sono state applicate le modifiche necessarie. Sono state apportate queste modifiche perché HFM cerca e utilizza una voce relativa ai nomi TNS che si chiama `HFMTNS`. Affinché `XFMDataSource` possa funzionare correttamente, è necessario modificare il protocollo e la porta della voce.

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

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

La versione originale della voce `HFMTNS` è stata rinominata `HFMTNS_UNENC`. La nuova versione della voce `HFMTNS` è stata creata copiando la voce `HFMTNS_UNENC` e rinominandola `HFMTNS`. A questo punto, il protocollo è stato aggiornato in TCPS e la porta è stata modificata in `1522`. È necessario che la porta specificata sia la stessa porta specificata nel file `TNS LISTENER.ORA`.

Procedure di Oracle HTTP Server

Creazione di un wallet e installazione del certificato per Oracle HTTP Server

Con Oracle HTTP Server viene installato automaticamente un wallet predefinito. È necessario configurare un vero wallet per ciascuna istanza di Oracle HTTP Server nella propria distribuzione.

Nota: a partire dalla versione 11.2.x, Oracle Wallet Manager non viene installato con Oracle HTTP Server. Oracle Wallet Manager viene installato solo se si installa il client di Oracle Database. È necessario utilizzare Wallet Manager disponibile con il client di Database per creare il wallet e importare il certificato. Se si sta configurando Oracle HTTP Server per SSL, installare sempre il client di Oracle Database a 64 bit come parte dell'installazione dei prodotti di EPM System.

Per creare e installare il certificato di Oracle HTTP Server, procedere come segue.

1. In ogni computer che ospita Oracle HTTP Server, avviare Wallet Manager.

   Fare clic su **Start**, quindi scegliere **Tutti i programmi**, **Oracle-OHxxxxxx**, **Strumenti di gestione integrata** e infine **Wallet Manager**.

   `xxxxxx` è il numero di istanza di Oracle HTTP Server.

2. Creare un nuovo wallet vuoto.
   a. In Oracle Wallet Manager, selezionare **Wallet** e quindi **Nuovo**.
   b. Fare clic su **Sì** per creare una directory wallet predefinita oppure su **No** per creare il file wallet in una posizione a propria scelta.
   c. In **Password wallet** e **Conferma password** nella schermata Nuovo wallet immettere la password che si desidera utilizzare.
   d. Fare clic su **OK**.
   e. Nella finestra di dialogo di conferma, fare clic su **No**.
3. **Facoltativo:** se non si utilizza una CA nota a Oracle HTTP Server, importare il certificato CA radice nel wallet.
   a. In Oracle Wallet Manager, fare clic con il pulsante destro del mouse su **Certificati protetti** e scegliere **Importa certificato protetto**.

b. Sfogliare e selezionare il certificato CA radice.

c. Selezionare **Apri**.

4. Creare una richiesta di certificato.

   a. In Oracle Wallet Manager, fare clic con il pulsante destro del mouse su **Certificato: [Vuoto]** e scegliere **Aggiungi richiesta certificato**.

   b. In Crea richiesta di certificato, immettere le informazioni richieste.

      Come nome comune, immettere l'alias di server completo, ad esempio `epm.myCompany.com` oppure `epminternal.myCompany.com`, disponibile nel file `hosts` nel sistema.

   c. Fare clic su **OK**.

   d. Nella finestra di dialogo di conferma, fare clic su **OK**.

   e. Fare clic con il pulsante destro del mouse sulla richiesta di certificato creata e quindi scegliere **Esporta richiesta certificato**.

   f. Specificare un nome per il file di richiesta di certificato.

5. Utilizzando i file di richiesta di certificato, ottenere dalla CA i certificati firmati.

6. Importare i certificati firmati.

   a. In Oracle Wallet Manager, fare clic con il pulsante destro del mouse sulla richiesta di certificato utilizzata per ottenere il certificato firmato e quindi scegliere **Importa certificato utente**.

   b. In Importa certificato, fare clic su **OK** per importare il certificato da un file.

   c. In Importa certificato, selezionare il file di certificato e quindi fare clic su **Apri**.

7. Salvare il wallet in una posizione appropriata, ad esempio *EPM_ORACLE_INSTANCE*`/httpConfig/ohs/config/OHS/ohs_component/keystores/epmsystem`.

8. Selezionare **Wallet** e quindi **Login automatico** per attivare l'accesso automatico.

Impostazione di Oracle Wallet utilizzando ORAPKI (su Linux)

Per configurare Oracle Wallet utilizzando la riga di comando ORAPKI, completare i passi riportati di seguito.

1. Creare una cartella per il wallet.

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

2. Aggiungere la posizione dell'utilità orapki al percorso.

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

3. Creare un wallet per conservare il certificato.

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

Se non è stata specificata alcuna password nella riga di comando, questo comando richiede di inserire e reinserire una password per il wallet. Crea un wallet nella posizione specificata per `-wallet`.

4. Generare una richiesta di firma di certificato (CSR) e aggiungerla al wallet.

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

5. Aggiungere un certificato radice e intermedio nel keystore attendibile

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

6. Utilizzare la CA (Autorità di certificazione) per firmare la CSR (Richiesta di firma del certificato). Per esportare la richiesta di certificato da un Oracle Wallet procedere come riportato di seguito.

```
$ 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. Importare la CSR firmata nel wallet.

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

8. Per visualizzare i contenuti del wallet procedere come riportato di seguito.

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

Abilitazione del protocollo SSL per Oracle HTTP Server

Dopo aver riconfigurato il server Web in ogni computer che ospita Oracle HTTP Server, aggiornare il file di configurazione di Oracle HTTP Server sostituendo la posizione del wallet predefinito con la posizione del wallet creato.

Per configurare Oracle HTTP Server per SSL, procedere come segue.

1. Riconfigurare il server Web in ogni computer host Oracle HTTP Server presente nella distribuzione.
2. Avviare EPM System Configurator per l'istanza.
3. Nella schermata di selezione dei task di configurazione, eseguire questi passi e quindi fare clic su **Avanti**.
   a. Rimuovere il segno di spunta da **Deseleziona tutto**.
   b. Espandere il gruppo di task **Hyperion Foundation** e quindi selezionare **Configura Web server**.
4. In **Configura Web server**, fare clic su **Avanti**.

5. In **Conferma**, fare clic su **Avanti**.
6. In **Riepilogo**, fare clic su **Fine**.
7. Aprire *EPM_ORACLE_INSTANCE*`/httpConfig/ohs/config/fmwconfig/components/OHS/ohs_component/ssl.conf` con un editor di testo.
8. Assicurarsi che la porta SSL in uso sia elencata sotto `OHS Listen port`, come indicato di seguito.

   Se si utilizza `19443` come porta di comunicazione SSL, dovrebbe venire visualizzato quanto segue:

   ```
   Listen 19443
   ```

9. Impostare il valore del parametro `SSLSessionCache` su `none`.
10. Aggiornare le impostazioni di configurazione di ogni istanza di Oracle HTTP Server nella distribuzione.
    a. Aprire *EPM_ORACLE_INSTANCE*`/httpConfig//ohs/config/fmwconfig/components/OHS/ohs_component/ssl.conf` con un editor di testo.
    b. Individuare la direttiva `SSLWallet` e modificarne il valore in modo che punti al wallet in cui è stato installato il certificato. Se il wallet è stato creato in *EPM_ORACLE_INSTANCE*`httpConfig/ohs/config/OHS/ohs_component/keystores/epmsystem`, la direttiva `SSLWallet` potrebbe essere simile alla seguente:

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

    c. Salvare e chiudere `ssl.conf`.
11. Aggiornare `mod_wl_ohs.conf` in ogni istanza di Oracle HTTP Server nella distribuzione.
    a. Aprire *EPM_ORACLE_INSTANCE*`/httpConfig//ohs/config/fmwconfig/components/OHS/ohs_component/mod_wl_ohs.conf` con un editor di testo.
    b. Assicurarsi che la direttiva `WLSSLWallet` punti all'Oracle Wallet in cui è memorizzato il certificato SSL.

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

       Ad esempio, `C:/Oracle/Middleware/ohs/bin/wallets/myWallet`
    c. Impostare il valore della direttiva `SecureProxy` su `ON`.

       ```
       SecureProxy ON
       ```

    d. Assicurarsi che le definizioni `LocationMatch` dei componenti di Oracle Enterprise Performance Management System distribuiti siano simili all'esempio di Oracle Hyperion Shared Services riportato di seguito, in cui si

presuppone l'esistenza di un cluster Oracle WebLogic Server (in `myserver1` e `myserver2` con la porta SSL 28443):

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

e. Salvare e chiudere `mod_wl_ohs.conf`.

Configurazione dei componenti Web di EPM System distribuiti in WebLogic Server

Dopo aver distribuito i componenti Web di Oracle Enterprise Performance Management System, è necessario configurarli per la comunicazione SSL.

Per configurare i componenti Web per SSL, procedere come segue.

1. Avviare Oracle WebLogic Server eseguendo un file memorizzato in *EPM_ORACLE_INSTANCE*`/domains/EPMSystem/bin/startWebLogic.cmd`:
2. Avviare la console di amministrazione di WebLogic Server accedendo all'URL seguente:

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

   Ad esempio, per accedere alla console di WebLogic Server distribuita sulla porta predefinita in `myServer`, è necessario utilizzare `http://myServer:7001/console`.
3. Nella schermata di benvenuto, immettere il nome utente e la password per accedere a `EPMSystem`. Il nome utente e la password vengono specificati in EPM System Configurator durante il processo di configurazione.
4. Nel **Centro modifiche**, fare clic su **Blocca e modifica**.
5. Nel riquadro sinistro della console, espandere **Ambiente** e selezionare **Server**.
6. Nella schermata Riepilogo dei server, fare clic sul nome del server che si desidera abilitare per SSL.

   Ad esempio, se sono stati installati tutti i componenti Oracle Hyperion Foundation Services, è possibile abilitare per SSL tutti i server seguenti.

   - `CalcManager`
   - `FoundationServices`
7. Deselezionare **Porta di ascolto abilitata** per disabilitare la porta di ascolto HTTP.
8. Assicurarsi che l'opzione **Porta di ascolto SSL abilitata** sia selezionata.
9. In **Porta di ascolto SSL**, immettere la porta di ascolto SSL di WebLogic Server.
10. Specificare il keystore identità e il keystore sicuro da utilizzare.
    - Selezionare **Keystore** per aprire la scheda corrispondente.
    - In **Keystore**, selezionare una delle opzioni riportate di seguito.

    a. Selezionare **Keystore** per aprire la scheda corrispondente.

    b. In **Keystore**, selezionare una delle opzioni riportate di seguito.

- **Identità personalizzata e sicurezza personalizzata** se non si utilizza un certificato server proveniente da una CA di terze parti nota
- **Identità personalizzata e sicurezza standard Java** se si utilizza un certificato server proveniente da una CA di terze parti nota

c. In **Keystore identità personalizzato**, immettere il percorso del keystore in cui è installato il certificato firmato di WebLogic Server.

d. In **Tipo di keystore identità personalizzato**, immettere `jks`.

e. In **Passphrase keystore identità personalizzato** e **Conferma passphrase keystore identità personalizzato**, immettere la password del keystore.

f. Se in **Keystore** è stata selezionata l'opzione **Identità personalizzata e sicurezza personalizzata**, procedere come segue.

- In **Keystore sicuro personalizzato**, immettere il percorso del keystore customizzato in cui è disponibile il certificato radice della CA che ha firmato il certificato server.
- In **Tipo di keystore sicuro personalizzato**, immettere `jks`.
- In **Passphrase keystore sicuro personalizzato** e **Conferma passphrase keystore sicuro personalizzato**, immettere la password del keystore.

g. Fare clic su **Salva**.

11. Specificare le impostazioni SSL.

- Selezionare **SSL**.
- In **Alias chiave privata**, immettere l'alias specificato durante l'importazione del certificato firmato di WebLogic Server.
- In **Passphrase chiave privata** e **Conferma passphrase chiave privata**, immettere la password da utilizzare per recuperare la chiave privata.
- **Solo applicazione Web Oracle Hyperion Provider Services:** se si utilizzano certificati con caratteri jolly per cifrare la comunicazione tra WebLogic Server e altri componenti server di EPM System, disabilitare la verifica del nome host per l'applicazione Web Provider Services.
  - Selezionare **Avanzate**.
  - In **Verifica nome host**, selezionare **Nessuna**.
- Fare clic su **Salva**.

12. Nel **Centro modifiche**, fare clic su **Attiva modifiche**.

Aggiornamento della configurazione del dominio

Questo processo consente di aggiornare la configurazione del dominio. Prima di iniziare la procedura, creare un backup completo della distribuzione. Oracle consiglia di eseguire il test di questa procedura con una distribuzione di prova prima di apportare modifiche a una distribuzione di produzione.

Per aggiornare la configurazione del dominio:

1. Passare alla directory `MIDDLEWARE_HOME/oracle_common/bin directory`:
   `cd MIDDLEWARE_HOME/oracle_common/bin`
2. Impostare *`ORACLE_HOME`*, *`WL_HOME`* e *`JAVA_HOME`*.

```
impostare ORACLE_HOME= /Oracle/Middleware

impostare WL_HOME= /Oracle/Middleware/wlserver

impostare JAVA_HOME= /Oracle/Middleware/jdk
```

3. Nella console di WebLogic, abilitare la porta HTTP per il server di amministrazione.
4. Creare un keystore utilizzando un comando simile al seguente:
   `libovdconfig.bat -host HOSTNAME -port 7001 -userName USERNAME -domainPath %MWH%\user_projects\domains\EPMSystem -createKeystore`

   Nel comando, sostituire *HOSTNAME* e *USERNAME* rispettivamente con il nome host del server WebLogic e il nome utente dell'amministratore. Assicurarsi che l'output segnali la riuscita della creazione del keystore OVD.
5. Esportare il certificato SSL da AdminServer.

   > **Note:**
   >
   > Questa fase è applicabile solo per LDAP incorporato (autenticatore predefinito). Per altri LDAP, il certificato deve essere esportato utilizzando i comandi appropriati specifici del LDAP. Il formato del file del certificato deve essere **X.509** con codifica Base64

   a. Utilizzando Internet Explorer, accedere alla console di amministrazione di WebLogic all'indirizzo `https://NOMEHOST:7002/console`
   b. Fare clic su **Visualizza certificato**, quindi **Dettagli**, e seleziona **Copia in un file** per esportare il certificato SSL.
   c. Salvare il certificato come file di certificato **X.509** con codifica Base64 in una directory locale, ad esempio `C:\certificate\slc17rby.cer`.
   d. Spostare il certificato sul server.
6. Utilizzando lo strumento keytool, importare nel keystore il certificato creato nel passo 4. Utilizzare comandi simili ai seguenti presupponendo che *JAVA_HOME*, e l'eseguibile keytool, si trovino nel percorso:
   `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`, ad esempio:

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

> **Note:**
>
> - La password utilizzata in questo comando deve corrispondere alla password utilizzata durante la generazione del keystore nel passo 4.
> - *CERTIFICATE_PATH* corrisponde alla posizione e al nome del certificato
> - alias può corrispondere a qualsiasi alias di propria scelta.

Al termine dell'importazione del certificato, keytool visualizza il messaggio `Certificate was added to keystore`.

7. Nella console di WebLogic abilitare la porta SSL per il server di amministrazione oltre alla porta HTTP.
8. Riavviare il server di amministrazione WebLogic e i server gestiti.
9. Eseguire l'accesso a Oracle Hyperion Enterprise Performance Management Workspace utilizzando una connessione sicura per verificare che tutto funzioni.

Riavvio di server ed EPM System

Riavviare tutti i server nella distribuzione e quindi avviare Oracle Enterprise Performance Management System in ciascun server.

Test della distribuzione

Al termine della distribuzione dell'autenticazione SSL, verificare che funzioni tutto.

Per testare la distribuzione, procedere come segue.

1. Accedere con un browser all'URL sicuro di Oracle Hyperion Enterprise Performance Management Workspace riportato di seguito.

   Se si è utilizzato `epm.myCompany.com` come alias del server per le comunicazioni esterne e `4443` come porta SSL, l'URL di EPM Workspace è

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

2. Immettere il nome utente e la password nella schermata di accesso.
3. Fare clic su **Accedi**.
4. Verificare di poter accedere in modo sicuro ai componenti di Oracle Enterprise Performance Management System distribuiti.

Configurazione delle directory utenti esterne abilitate per SSL

Presupposti

- Le directory utenti esterne che si prevede di configurare in Oracle Hyperion Shared Services Console sono abilitate per SSL.

- Se non è stato utilizzato un certificato proveniente da una CA di terze parti nota per abilitare per SSL la directory utenti, si dispone di una copia del certificato radice della CA che ha firmato il certificato server.

Importazione del certificato CA radice

Se non è stato utilizzato un certificato proveniente da una CA di terze parti nota per abilitare per SSL la directory utenti, è necessario importare il certificato radice della CA che ha firmato il certificato server nei keystore riportati di seguito.

> **Nota:**
>
> Durante la distribuzione dell'applicazione, WebLogic aggiunge la direttiva `-Djavax.net.ssl.trustStore` che punta a `DemoTrust.jks` in `setDomainEnv.sh` o `setDomainEnv.cmd`. Se non si utilizza il certificato WebLogic predefinito, rimuovere `-Djavax.net.ssl.trustStore` da `setDomainEnv.sh` o `setDomainEnv.cmd`.

Utilizzare uno strumento come keytool per importare il certificato CA radice.

- Tutti i server Oracle Enterprise Performance Management System:

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

- Il keystore utilizzato da JVM in ogni computer host dei componenti di EPM System. Per impostazione predefinita, i componenti di EPM System utilizzano il keystore seguente:

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

Configurazione delle directory utenti esterne

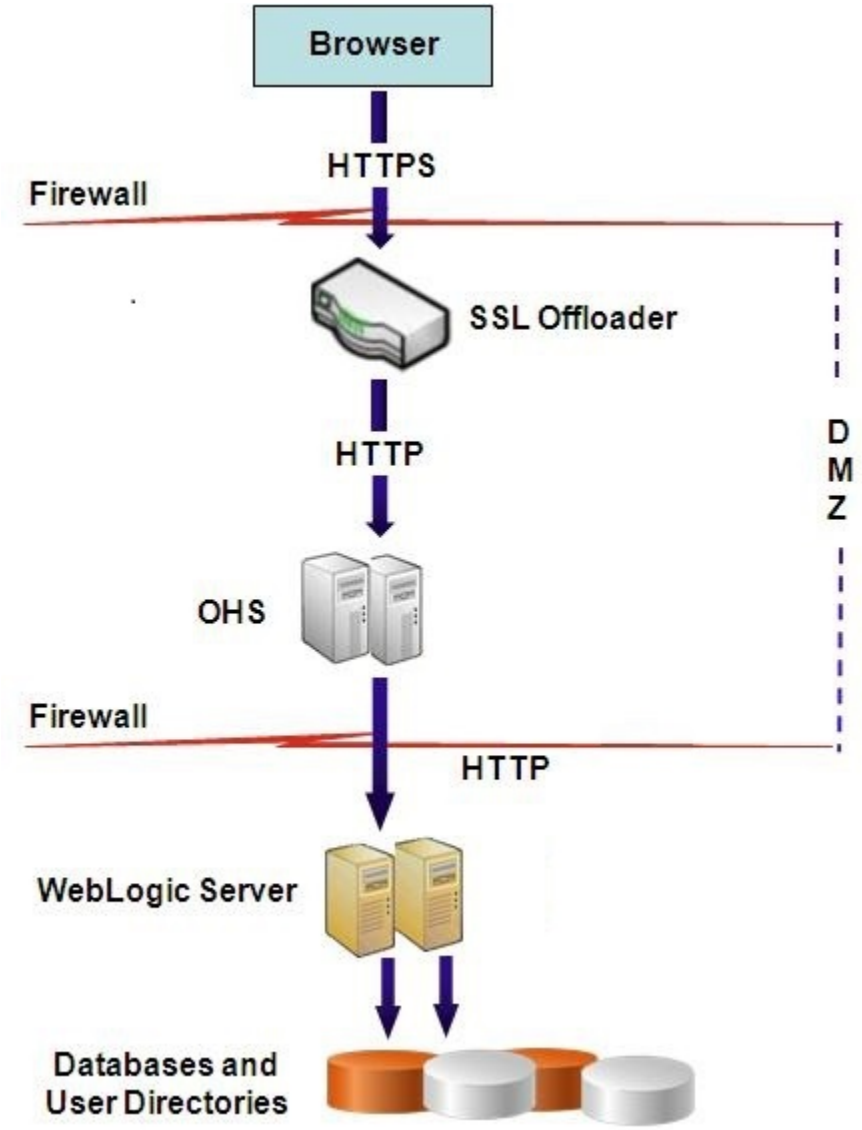
Per configurare le directory utenti, è possibile utilizzare Shared Services Console. Durante la configurazione delle directory utenti, è necessario selezionare l'opzione `SSL Enabled`, che indica alla funzionalità di sicurezza di EPM System di utilizzare il protocollo sicuro per comunicare con la directory utenti. È possibile abilitare per SSL una connessione tra la funzionalità di sicurezza di EPM System e le directory utenti abilitate per LDAP, ad esempio Oracle Internet Directory e Microsoft Active Directory.

Fare riferimento alla sezione "Configurazione delle directory utente" nel manuale *Oracle Enterprise Performance Management System User Security Administration Guide (in lingua inglese)*.

Terminazione di SSL sul server Web

Architettura di distribuzione

In questo scenario, l'autenticazione SSL viene utilizzata per proteggere il collegamento di comunicazione tra i client Oracle Enterprise Performance Management System (ad esempio un browser) e Oracle HTTP Server. Il concetto è illustrato di seguito.



Presupposti

Questa configurazione utilizza due alias di server, ad esempio `epm.myCompany.com` ed `empinternal.myCompany.com`, nel server Web, uno per le comunicazioni esterne tra il server Web e i browser e l'altro per le comunicazioni interne tra server EPM System. Assicurarsi che gli alias dei server puntino all'indirizzo IP del computer e che siano risolvibili tramite DNS.

Un certificato firmato che supporta le comunicazioni esterne tra i browser (ad esempio tramite `epm.myCompany.com`) deve essere installato nel server Web (dove è definito l'host virtuale che supporta le comunicazioni esterne sicure). Questo host virtuale deve terminare SSL e inoltrare le richieste HTTP a Oracle HTTP Server.

Quando SSL viene arrestato su Oracle HTTP Server (OHS) o sul load balancer, è necessario:

- Impostare ogni Applicazione Web logica su host virtuale non SSL del load balancer o di Oracle HTTP Server (ad esempio, `empinternal.myCompany.com:80`

dove 80 è la porta non SSL). Aprire la schermata di configurazione e procedere come segue:

1. Espandere il task di configurazione **Hyperion Foundation**.
2. Selezionare **Configurazione indirizzo logico per applicazioni Web**.
3. Specificare un valore per *Nome host*, numero di porta non SSL e numero di porta SSL.

- Impostare l'URL esterno su host virtuale abilitato per SSL del load balancer o di Oracle HTTP Server (ad esempio, `empexternal.myCompany.com:443` dove 443 è la porta SSL). Aprire la schermata di configurazione e procedere come segue:
  1. Espandere il task di configurazione **Hyperion Foundation**.
  2. Selezionare **Configura impostazioni comuni**.
  3. Selezionare **Abilita offloading SSL** in Dettagli URL esterno.
  4. Specificare *Host URL esterno* e *Porta URL esterno*.

> **Nota:**
>
> Se si ridistribuiscono le applicazioni Web o si riconfigura il server Web con **ConfigTool**, le impostazioni dell'Applicazione Web logica e degli URL esterni verranno sostituite.

Configurazione di EPM System

La distribuzione predefinita dei componenti di EPM System supporta la terminazione di SSL sul server Web. Non sono richieste azioni aggiuntive.

Durante la configurazione di EPM System, assicurarsi che le applicazioni Web logiche puntino all'host virtuale (ad esempio `empinternal.myCompany.com`) creato per le comunicazioni interne. Per installare e configurare EPM System, fare riferimento alle fonti di informazioni elencate di seguito.

- *Guida di installazione e configurazione di Oracle Enterprise Performance Management System*
- *Guida introduttiva per l'installazione di Oracle Enterprise Performance Management*

Test della distribuzione

Al termine del processo di distribuzione, verificare che sia tutto funzionante effettuando una connessione all'URL di Oracle Hyperion Enterprise Performance Management Workspace sicuro:

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

Ad esempio, `https://epm.myCompany.com:443/workspace/index.jsp`, dove 443 è la porta SSL.

SSL per Essbase 11.1.2.4

Panoramica

In questa sezione vengono illustrate le procedure per la sostituzione dei certificati predefiniti utilizzati per proteggere le comunicazioni tra un'istanza di Oracle Essbase e componenti quali MaxL, il server Oracle Essbase Administration Services, il server Oracle Essbase Studio, Oracle Hyperion Provider Services, Oracle Hyperion Foundation Services, Oracle Hyperion Planning, Oracle Hyperion Financial Management e Oracle Hyperion Shared Services Registry.

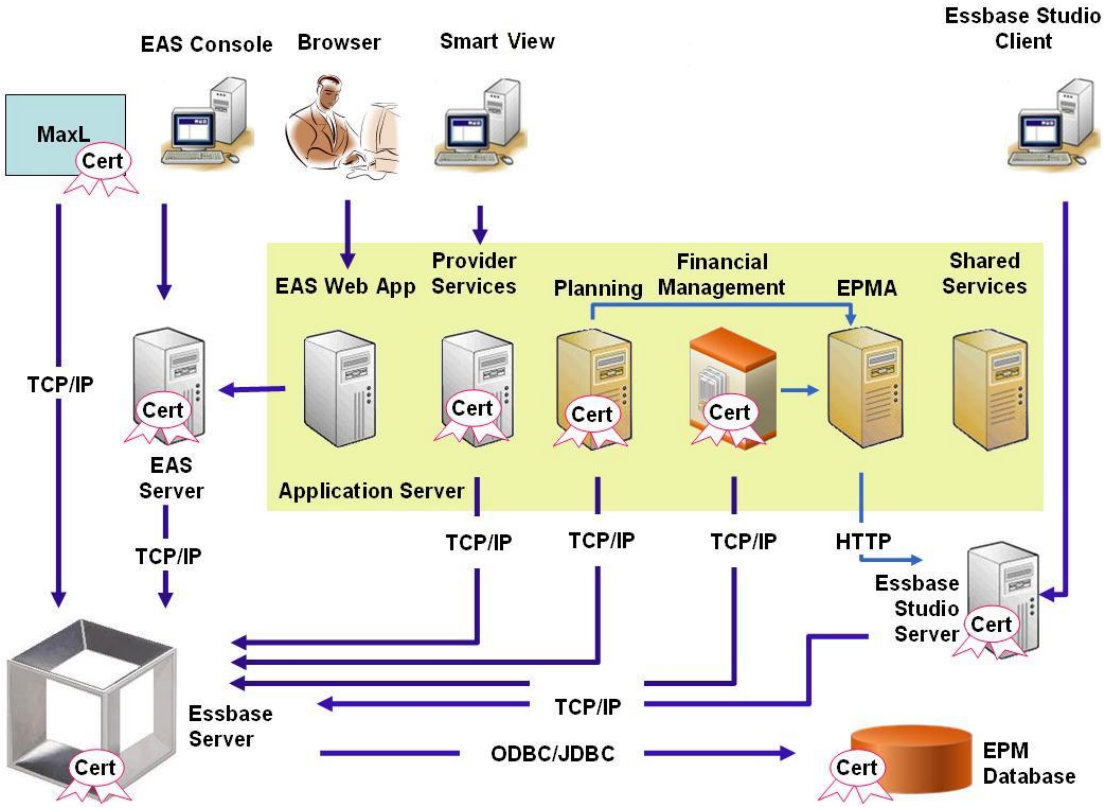
Distribuzione predefinita

È possibile distribuire Essbase in modo che funzioni in modalità SSL e non SSL. L'agente Essbase rimane in ascolto su una porta non sicura. Può essere configurato anche per rimanere in ascolto su una porta sicura. Tutte le connessioni che accedono alla porta sicura vengono gestite come connessioni SSL. Se un client si connette all'agente Essbase sulla porta non SSL, la connessione viene gestita come connessione non SSL. I componenti possono stabilire connessioni contemporanee non SSL e SSL con un agenteEssbase.

È possibile controllare SSL per ogni singola sessione specificando al momento dell'accesso il protocollo e la porta sicuri. Fare riferimento alla sezione Attivazione di una connessione SSL per la singola sessione.

Se è abilitata l'autenticazione SSL, tutte le comunicazioni nell'ambito di un'istanza Essbase vengono cifrate per garantire la sicurezza dei dati.

Nelle distribuzioni predefinite dei componenti di Essbase in modalità sicura vengono utilizzati certificati con firma automatica per abilitare le comunicazioni SSL, principalmente a scopo di test. Oracle consiglia di utilizzare certificati di CA di terze parti note per abilitare per SSL Essbase in ambienti di produzione.



In genere, in un Oracle Wallet viene memorizzato il certificato che abilita le comunicazioni SSL con i client che utilizzano Essbase RTC, mentre in un keystore Java viene memorizzato il certificato che abilita le comunicazioni SSL con componenti che utilizzano JAPI per le comunicazioni. Per stabilire comunicazioni SSL, i client e gli strumenti Essbase memorizzano il certificato radice della CA che ha firmato i certificati del server e dell'agente Essbase. Fare riferimento alla sezione Certificati richiesti e relativa posizione.

Certificati richiesti e relativa posizione

Oracle consiglia di utilizzare certificati di CA di terze parti note per abilitare per SSL Essbase in un ambiente di produzione. È possibile utilizzare i certificati con firma automatica predefiniti a scopo di test.

> **Nota:**
>
> Essbase supporta l'utilizzo di certificati con caratteri jolly, che possono proteggere più sottodomini con un certificato SSL. Utilizzando un certificato con caratteri jolly è possibile ridurre i tempi e i costi di gestione.
>
> Non è possibile utilizzare i certificati con caratteri jolly se è abilitata la verifica del nome host.

Sono necessari i certificati elencati di seguito.

- Un certificato CA radice.
  Per i componenti che utilizzano Essbase RTC per stabilire una connessione a Essbase, il certificato CA radice deve essere memorizzato nell'Oracle Wallet. Per i componenti che

utilizzano JAPI per stabilire una connessione, il certificato CA radice deve essere memorizzato in un keystore Java. I certificati richiesti e le relative posizioni sono indicati nella tabella riportata di seguito.

> **Nota:**
>
> Potrebbe non essere necessario installare un certificato CA radice se si utilizzano certificati di una CA di terze parti nota il cui certificato radice è già installato nell'Oracle Wallet.

- Certificato firmato per il server Essbase e l'agente Essbase.

Tabella 2-1 Certificati richiesti e relative posizioni

Componente[1]	Keystore	Certificato [2]
MaxL	Oracle Wallet	Certificato CA radice
Server Administration Services	Oracle Wallet	Certificato CA radice
Provider Services	Oracle Wallet	Certificato CA radice
Database Oracle Enterprise Performance Management System	Oracle Wallet	Certificato CA radice
Server Essbase Studio	Keystore Java	Certificato CA radice
Planning	• Oracle Wallet • Keystore Java	Certificato CA radice
Financial Management	Keystore Java	Certificato CA radice
Essbase (server e agente) [3]	• Oracle Wallet • Keystore Java	• Certificato CA radice • Certificato firmato per server e agente Essbase
Repository Oracle Hyperion Shared Services		

[1] È sufficiente una sola istanza del keystore per supportare più componenti che utilizzano un keystore simile.

[2] Più componenti possono utilizzare un certificato radice installato in un keystore.

[3] I certificati devono essere installati nell'Oracle Wallet predefinito e nel keystore Java.

Installazione e distribuzione dei componenti Essbase

Il processo di configurazione consente di selezionare una porta sicura dell'agente (la porta predefinita è la 6423), che può essere modificata durante la configurazione di Oracle Essbase. Per impostazione predefinita, il processo di distribuzione installa i certificati autofirmati necessari per creare una distribuzione sicura funzionante a fini di test.

Il programma di installazione di EPM System installa un certificato Oracle Wallet autofirmato all'interno di *ARBOR_PATH* nel computer che ospita l'istanza di Essbase se è installato Oracle HTTP Server. Nelle distribuzioni con host singolo, tutti i componenti Essbase condividono tale certificato.

Utilizzo di certificati CA di terze parti sicuri per Essbase

Creazione di richieste di certificati e ottenimento di certificati

Generare una richiesta di certificato per ottenere un certificato per il server che ospita il server Oracle Essbase e l'agente Essbase. Una richiesta di certificato contiene informazioni cifrate specifiche del proprio nome distinto (DN). La richiesta di certificato viene sottomessa a un'autorità di certificazione per ottenere un certificato SSL.

Per creare una richiesta di certificato viene utilizzato un keytool oppure Oracle Wallet Manager. Per informazioni dettagliate sulla creazione di una richiesta di certificato, fare riferimento alla documentazione relativa allo strumento in uso.

Se si utilizza un keytool, eseguire un comando simile al seguente per creare una richiesta di certificato:

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

Ottenimento e installazione del certificato CA radice

Il certificato CA radice verifica la validità del certificato utilizzato per supportare SSL. Contiene la chiave pubblica a fronte della quale viene confrontata per una corrispondenza la chiave privata utilizzata per firmare il certificato in modo da verificarlo. È possibile ottenere il certificato CA radice dall'autorità di certificazione che ha firmato i certificati SSL.

Installare il certificato radice dell'autorità CA che ha firmato il certificato del server Essbase nei client che si connettono al server o all'agente Essbase. Assicurarsi che il certificato radice sia installato nel keystore appropriato per il client. Fare riferimento alla sezione Certificati richiesti e relativa posizione .

> **Nota:**
>
> Un certificato CA radice installato in un server può essere utilizzato da più componenti.

Oracle Wallet

Fare riferimento alla Certificati richiesti e relativa posizione per un elenco dei componenti che richiedono il certificato CA radice in un Oracle Wallet. È possibile creare un wallet o installare il certificato nel wallet demo in cui è installato il certificato con firma automatica predefinito.

Fare riferimento alla documentazione di Oracle Wallet Manager per le procedure dettagliate per la creazione di wallet e l'importazione del certificato CA radice.

Keystore Java

Fare riferimento alla Certificati richiesti e relativa posizione per un elenco dei componenti che richiedono il certificato CA radice in un keystore Java. È possibile aggiungere il certificato nel keystore in cui è installato il certificato con firma automatica predefinito oppure creare un keystore per la memorizzazione del certificato.

> **Nota:**
>
> I certificati CA radice di molte CA di terze parti note sono già installati nel keystore Java.

Per istruzioni dettagliate, fare riferimento alla documentazione dello strumento in uso. Se si utilizza il keytool, eseguire un comando simile al seguente per importare il certificato radice:

```
keytool -import -alias blister_CA -file c:/certs/CA.crt -keypass
password -trustcacerts -keystore
C:\Oracle\Middleware\EPMSystem11R1\Essbase_ssl
\keystore -storepass password
```

Installazione di certificati firmati

I certificati SSL firmati vengono installati nel server che ospita il server Essbase e l'agente Essbase. Per i componenti che utilizzano Essbase RTC (API C) per stabilire una connessione al server o all'agente Essbase, il certificato deve essere memorizzato in un Oracle Wallet con il certificato CA radice. Per i componenti che utilizzano JAPI per stabilire una connessione al server o all'agente Essbase, il certificato CA radice e il certificato SSL firmato devono essere memorizzati in un keystore Java. Per le procedure dettagliate, fare riferimento alle fonti di informazioni elencate di seguito.

- Documentazione di Oracle Wallet Manager
- Documentazione o Guida in linea relativa allo strumento, ad esempio il keytool, utilizzato per importare il certificato

Se si utilizza il keytool, eseguire un comando simile al seguente per importare il certificato:

```
keytool -import -alias essbase_ssl -file C:/certs/essbase_ssl_crt -
keypass password -keystore
 C:\Oracle\Middleware\EPMSystem11R1\Essbase_ssl\keystore -storepass
password
```

Aggiornamento dei valori di registro del server Essbase

Windows

1. In un prompt dei comandi, passare alla directory *EPM_ORACLE_INSTANCE*/epmsystem1/bin.
2. Per aggiornare il Registro di sistema di Windows, eseguire i comandi riportati in basso.

   ```
   epmsys_registry.bat updateproperty "#<ID oggetto>/@EnableSecureMode"
   true
   ```

   ```
   epmsys_registry.bat updateproperty "#<ID oggetto>/@EnableClearMode"
   false
   ```

Sostituire `<ID oggetto>` con l'ID del componente server Essbase, disponibile nel report del registro generato dopo il completamento del processo di configurazione del server Essbase.

Linux

1. In una console, passare alla directory *EPM_ORACLE_INSTANCE*/epmsystem1/bin.
2. Per aggiornare il registro, eseguire i comandi riportati in basso.

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

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

   Sostituire `<ID oggetto>` con l'ID del componente server Essbase, disponibile nel report del registro generato dopo il completamento del processo di configurazione del server Essbase.

Aggiornamento delle impostazioni SSL di Essbase

Customizzare le impostazioni SSL dei client e del server Essbase specificando i valori dei seguenti elementi in `essbase.cfg`.

- L'impostazione per abilitare la modalità sicura
- L'impostazione per abilitare la modalità non cifrata
- La modalità preferita per comunicare con i client (utilizzata solo dai client)
- La porta sicura
- Le suite di cifratura
- Il percorso dell'Oracle Wallet

> **Nota:**
>
> In `essbase.cfg`, aggiungere gli eventuali parametri obbligatori mancanti, in particolare `EnableSecureMode`, `AgentSecurePort` e impostare i relativi valori.

Per aggiornare `essbase.cfg`, procedere come segue.

1. Copiare l'Oracle Wallet con i certificati per il server Essbase in *EPM_ORACLE_INSTANCE*/EssbaseServer/essbaseserver1/bin/wallet.
   Questa è l'unica ubicazione dell'Oracle Wallet accettabile per il server Essbase.
2. Aprire *EPM_ORACLE_INSTANCE*/EssbaseServer/essbaseserver1/bin/essbase.cfg con un editor di testo.
3. Specificare le impostazioni in base alle esigenze. È implicito l'utilizzo delle impostazioni di Essbase predefinite. Se si desidera modificare il comportamento predefinito, aggiungere le impostazioni per il comportamento customizzato in `essbase.cfg`. Ad esempio, l'impostazione `EnableClearMode` è applicata per impostazione predefinita e in base a essa il server Essbase è abilitato a comunicare su un canale non cifrato. Per disattivare la capacità del server Essbase di comunicare su un canale non cifrato, specificare `EnableClearMode FALSE` in `essbase.cfg`. Fare riferimento alla tabella riportata di seguito.

Tabella 2-2 Impostazioni SSL di Essbase

Impostazione	Descrizione[1]
`EnableClearMode`[2]	Abilita le comunicazioni non cifrate tra le applicazioni Essbase e l'agente Essbase. Se questa proprietà è impostata su `FALSE`, Essbase non gestisce le richieste non SSL. **Valore predefinito:** `EnableClearMode TRUE` **Esempio:** `EnableClearMode FALSE`
`EnableSecureMode`	Abilita le comunicazioni cifrate SSL tra i client Essbase e l'agente Essbase. Questa proprietà deve essere impostata su `TRUE` per supportare SSL. **Valore predefinito:** `FALSE` **Esempio:** `EnableSecureMode TRUE`
`SSLCipherSuites`	Elenco di suite di cifratura, in ordine di preferenza, da utilizzare per le comunicazioni SSL. L'agente Essbase utilizza una di queste suite di cifratura per le comunicazioni SSL. Alla prima suite di cifratura nell'elenco è assegnata la priorità più alta quando l'agente sceglie una suite di cifratura. **Valore predefinito:** `SSL_RSA_WITH_RC4_128_MD5` **Esempio:** `SSLCipherSuites SSL_RSA_WITH_AES_256_CBC_SHA256,SSL_RSA_WITH_AES_256_GCM_SHA384`
`APSRESOLVER`	URL di Oracle Hyperion Provider Services. Se si utilizzano più server Provider Services, separare i singoli URL utilizzando il punto e virgola. **Esempio:** `APSRESOLVER https://exampleAPShost1:`*`PORT`*`/aps;https://exampleAPShost2:`*`PORT`*`/aps`
`AgentSecurePort`	Porta sicura su cui è in ascolto l'agente. **Valore predefinito:** `6423` **Esempio:** `AgentSecurePort 16001`
`WalletPath`	Posizione dell'Oracle Wallet (meno di 1024 caratteri) in cui sono memorizzati il certificato CA radice e il certificato firmato. **Valore predefinito:** *`ARBORPATH`*`/bin/wallet` **Esempio:** `WalletPath/usr/local/wallet`
`ClientPreferredMode`[3]	Modalità (Secure o Clear) per la sessione client. Se questa proprietà è impostata su Secure, viene utilizzata la modalità SSL per tutte le sessioni. Se questa proprietà è impostata su Clear, il trasporto viene scelto a seconda che nella richiesta di accesso client sia contenuta la parola chiave di trasporto sicuro. Fare riferimento alla sezione Attivazione di una connessione SSL per la singola sessione. **Valore predefinito:** `CLEAR` **Esempio:** `ClientPreferredMode SECURE`

Tabella 2-2 (Cont.) Impostazioni SSL di Essbase

Impostazione	Descrizione[1]

[1] Il valore predefinito viene applicato se le proprietà non sono disponibili in `essbase.cfg`.

[2] Essbase diventa non operativo se `EnableClearMode` e `EnableSecureMode` sono entrambi impostati su `FALSE`.

[3] I client utilizzano questa impostazione per determinare se devono stabilire una connessione sicura o non sicura con Essbase.

4. Salvare e chiudere `essbase.cfg`.

Aggiornamento dei nodi Essbase distribuiti per SSL

> **Nota:**
>
> Questa sezione è valida solo per la distribuzione distribuita di Essbase

Verificare che la cartella del wallet (ad esempio, `WalletPath/usr/local/wallet`) contenga il certificato CA radice e che il certificato firmato si trovi nella posizione richiesta in ogni nodo distribuito.

1. Copiare la cartella del wallet nelle posizioni indicate in ogni nodo distribuito.
   - *EPM_ORACLE_HOME*`/common/EssbaseRTC/11.1.2.0/bin`
   - *EPM_ORACLE_HOME*`/common/EssbaseRTC-64/11.1.2.0/bin`
2. Copiare la cartella del wallet nelle posizioni indicate, se presenti, in ogni nodo distribuito.
   - *EPM_ORACLE_HOME*`/products/Essbase/EssbaseServer/bin`
   - *EPM_ORACLE_HOME*`/products/Essbase/EssbaseServer-32/bin`
   - *EPM_ORACLE_INSTANCE*`/EssbaseServer/essbaseserver1/bin`
3. Copiare *EPM_ORACLE_INSTANCE*`/EssbaseServer/essbaseserver1/bin/essbase.cfg` nelle posizioni indicate in ogni nodo distribuito.
   - *EPM_ORACLE_HOME*`/common/EssbaseRTC/11.1.2.0/bin`
   - *EPM_ORACLE_HOME*`/common/EssbaseRTC-64/11.1.2.0/bin`
4. Copiare *EPM_ORACLE_INSTANCE*`/EssbaseServer/essbaseserver1/bin/essbase.cfg` nelle posizioni indicate, se presenti, in ogni nodo distribuito.
   - *EPM_ORACLE_HOME*`/products/Essbase/EssbaseServer/bin`
   - *EPM_ORACLE_HOME*`/products/Essbase/EssbaseServer-32/bin`
   - *EPM_ORACLE_INSTANCE*`/EssbaseServer/essbaseserver1/bin`
5. Copiare la cartella del wallet nelle posizioni di installazione dei client Essbase indicate in ogni nodo distribuito.
   - *EPM_ORACLE_HOME*`/products/Essbase/EssbaseClient/bin`
   - *EPM_ORACLE_HOME*`/products/Essbase/EssbaseClient-32/bin`

6. Copiare *EPM_ORACLE_INSTANCE*/EssbaseServer/essbaseserver1/bin/essbase.cfg nelle posizioni di installazione dei client Essbase indicate in ogni nodo distribuito.
   - *EPM_ORACLE_HOME*/products/Essbase/EssbaseClient/bin
   - *EPM_ORACLE_HOME*/products/Essbase/EssbaseClient-32/bin
7. Aggiungere al file essbase.properties le proprietà indicate di seguito.
   - essbase.ssleverywhere=true
   - olap.server.ssl.alwaysSecure=true
   - APSRESOLVER=*http[s]://host:httpsPort/aps*
     Sostituire questo valore con l'URL appropriato.

   Aggiornare il file essbase.properties nelle posizioni indicate, se presenti, in ogni nodo distribuito.
   - *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. Copiare la directory *EPM_ORACLE_HOME*/products/Essbase/aps/bin/essbase.properties in *EPM_ORACLE_HOME*/products/Essbase/eas, se disponibile, in ogni nodo distribuito.
9. **Solo per Oracle Hyperion Planning:** aggiungere al file essbase.properties le tre proprietà indicate di seguito.
   - essbase.ssleverywhere=true
   - olap.server.ssl.alwaysSecure=true
   - APSRESOLVER=*APS_URL*
     Sostituire *APS_URL* con l'URL di Provider Services. Se si utilizzano più server Provider Services, separare i singoli URL utilizzando il punto e virgola. Ad esempio, https://exampleAPShost1:*PORT*/aps;https://exampleAPShost2:*PORT*/aps.

     Aggiornare il file essbase.properties nelle posizioni indicate in ogni nodo distribuito.
     - *EPM_ORACLE_HOME*/products/Planning/config/essbase.properties
     - *EPM_ORACLE_HOME*/products/Planning/lib/essbase.properties
10. **Solo per Oracle Hyperion Financial Reporting:** aggiungere al file *EPM_ORACLE_HOME*/products/financialreporting/bin/EssbaseJAPI/bin/essbase.properties le tre proprietà indicate di seguito.
    - essbase.ssleverywhere=true
    - olap.server.ssl.alwaysSecure=true
    - APSRESOLVER=*APS_URL*
      Sostituire *APS_URL* con l'URL di Provider Services. Se si utilizzano più server Provider Services, separare i singoli URL utilizzando il punto e virgola. Ad esempio, https://exampleAPShost1:*PORT*/aps;https://exampleAPShost2:*PORT*/aps.

> **Nota:**
>
> Negli ambienti SSL completi, Financial Reporting necessita del nome del cluster Essbase per stabilire una connessione. Le connessioni hanno esito negativo se il nome host viene utilizzato per la connessione.

11. a. Impostare le variabili di ambiente.
    - **Windows:** creare una nuova variabile di ambiente con nome `API_DISABLE_PEER_VERIFICATION` e impostarla su `1`.
    - **Linux:** aggiungere la direttiva `API_DISABLE_PEER_VERIFICATION=1` in `setCustomParamsPlanning.sh`.

    b. Aggiungere la direttiva `API_DISABLE_PEER_VERIFICATION=1` in *`EPM_ORACLE_INSTANCE`*`/EssbaseServer/essbaseserver1/bin/setEssbaseenv.bat` oppure *`EPM_ORACLE_INSTANCE`*`/EssbaseServer/essbaseserver1/bin/setEssbaseenv.sh`.

    Impostare le variabili di ambiente.

Customizzazione delle proprietà SSL dei client JAPI

Sono presenti diverse proprietà predefinite per i componenti Essbase che si basano su JAPI. Le proprietà predefinite possono essere sostituite includendo le proprietà in `essbase.properties`.

> **Nota:**
>
> Solo alcune delle proprietà SSL identificate nella tabella che segue sono esternalizzate in `essbase.properties`. Devono essere aggiunte le proprietà che non sono esternalizzate.

Per aggiornare le proprietà SSL dei client JAPI, procedere come segue.

1. Aprire *`EPM_ORACLE_HOME`*`/common/EssbaseJavaAPI/11.1.2.0/bin/essbase.properties` con un editor di testo.
2. Aggiornare le proprietà in base alle esigenze. Fare riferimento alla tabella che segue per una descrizione delle proprietà client JAPI customizzabili.
   Se una proprietà desiderata non è inclusa in `essbase.properties`, aggiungerla.

Tabella 2-3 Proprietà SSL predefinite per i client JAPI

Proprietà	Descrizione
`olap.server.ssl.alwaysSecure`	Imposta la modalità che deve essere utilizzata dai client in tutte le istanze di Essbase. Modificare il valore di questa proprietà impostandolo su `true` per applicare la modalità SSL. **Valore predefinito:** `false`

Tabella 2-3 (Cont.) Proprietà SSL predefinite per i client JAPI

Proprietà	Descrizione
`olap.server.ssl.securityHandler`	Nome del package per la gestione del protocollo. È possibile modificare questo valore per indicare un altro handler. **Valore predefinito:** `java.protocol.handler.pkgs`
`olap.server.ssl.securityProvider`	Oracle utilizza l'implementazione del protocollo Sun SSL. È possibile modificare questo valore per indicare un altro provider. **Valore predefinito:** `com.sun.net.ssl.internal.www.protocol`
`olap.server.ssl.supportedCiphers`	Elenco di voci separate da virgole contenente cifrature aggiuntive da abilitare per le comunicazioni sicure. È necessario specificare solo le cifrature supportate da Essbase. **Esempio**: `SSL_RSA_WITH_AES_256_CBC_SHA256,SSL_RSA_WITH_AES_256_GCM_SHA384`
`olap.server.ssl.trustManagerClass`	Classe TrustManager da utilizzare per convalidare il certificato SSL verificando la firma e controllando la data di scadenza del certificato. Per impostazione predefinita, questa proprietà non è impostata per applicare tutti i controlli di verifica. Per non applicare i controlli di verifica, impostare il valore di questo parametro su `com.essbase.services.olap.security.EssDefaultTrustManager`, ovvero la classe TrustManager predefinita che consente di superare tutti i controlli di verifica. Per implementare una classe TrustManager customizzata, specificare un nome di classe completo della classe TrustManager che implementi l'interfaccia `javax.net.ssl.X509TrustManager`. **Esempio**: `com.essbase.services.olap.security.EssDefaultTrustManager`

3. Salvare e chiudere `essbase.properties`.
4. Riavviare tutti i componenti di Essbase.

Attivazione di una connessione SSL per la singola sessione

I componenti Oracle Essbase, ad esempio MaxL, sono in grado di controllare SSL a livello di sessione mediante la connessione all'agente Essbase con `secure` come parola chiave per il trasporto. Ad esempio, è possibile stabilire una connessione sicura

tra MaxL e l'agente Essbase eseguendo da una console MaxL uno dei comandi riportati di seguito:

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

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

Il controllo a livello di singola sessione ha la priorità sulle impostazioni di configurazione specificate nel file `essbase.cfg`. Se non viene specificata alcuna parola chiave per il trasporto, i client Essbase utilizzano il valore impostato per `ClientPreferredMode` per stabilire se avviare una connessione sicura a Essbase. Se l'impostazione `ClientPreferredMode` non è configurata su secure, la comunicazione avviene su un canale non sicuro.

SSL per Essbase 21c

Panoramica

In questa sezione vengono illustrate le procedure per sostituire i certificati predefiniti utilizzati per proteggere le comunicazioni tra un'istanza di Oracle Essbase e componenti quali MaxL, il server Oracle Essbase Administration Services, Oracle Hyperion Provider Services, Oracle Hyperion Foundation Services, Oracle Hyperion Planning, Oracle Hyperion Financial Management e Oracle Hyperion Shared Services Registry.

> **Nota:**
>
> In Essbase Administration Services (EAS) Lite non viene utilizzata la porta SSL del server HTTP (ad esempio la 443) configurata utilizzando EPM Configurator. L'URL protetto nel file `easconsole.jnlp` rimanda per impostazione predefinita alla porta non SSL (80).
>
> **Soluzione alternativa:** sostituire la porta non SSL predefinita nell'URL protetto identificato in `easconsole.jnlp`con l'URL protetto aggiornato:
>
> URL protetto predefinito: `https://myserver:SECURE_PORT/easconsole/console.html`. Esempio, `https://myserver:80/easconsole/console.html`
>
> URL protetto aggiornato: `https://myserver:SECURE_PORT/easconsole/console.html`. Esempio, `https://myserver:443/easconsole/console.html`
>
> Per ulteriori informazioni, consultare l'articolo di My Oracle Support (MOS) - ID documento 1926558.1 - Porta SSL non inclusa nel file easconsole.jnlp di EAS Web Console .

Distribuzione predefinita

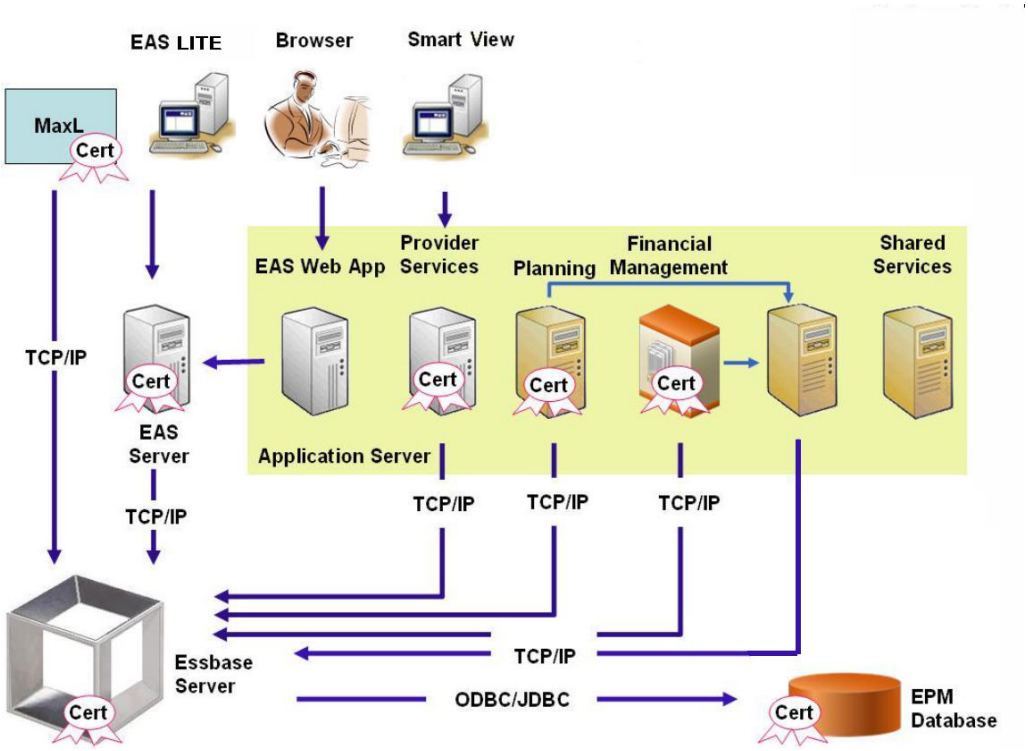
È possibile distribuire Essbase in modo che funzioni in modalità SSL e non SSL. L'agente Essbase rimane in ascolto su una porta non sicura. Può essere configurato anche per rimanere in ascolto su una porta sicura. Tutte le connessioni che accedono alla porta sicura vengono gestite come connessioni SSL. Se un client si connette all'agente Essbase sulla

porta non SSL, la connessione viene gestita come connessione non SSL. I componenti possono stabilire connessioni contemporanee non SSL e SSL con un agenteEssbase.

È possibile controllare SSL per ogni singola sessione specificando al momento dell'accesso il protocollo e la porta sicuri. Fare riferimento alla sezione Attivazione di una connessione SSL per la singola sessione.

Se è abilitata l'autenticazione SSL, tutte le comunicazioni nell'ambito di un'istanza Essbase vengono cifrate per garantire la sicurezza dei dati.

Nelle distribuzioni predefinite dei componenti di Essbase in modalità sicura vengono utilizzati certificati con firma automatica per abilitare le comunicazioni SSL, principalmente a scopo di test. Oracle consiglia di utilizzare certificati di CA di terze parti note per abilitare per SSL Essbase in ambienti di produzione.



In genere, in un Oracle Wallet viene memorizzato il certificato che abilita le comunicazioni SSL con i client che utilizzano Essbase RTC, mentre in un keystore Java viene memorizzato il certificato che abilita le comunicazioni SSL con componenti che utilizzano JAPI per le comunicazioni. Per stabilire comunicazioni SSL, i client e gli strumenti Essbase memorizzano il certificato radice della CA che ha firmato i certificati del server e dell'agente Essbase.

Certificati richiesti e relativa posizione

Oracle consiglia di utilizzare certificati di CA di terze parti note per abilitare per SSL Essbase in un ambiente di produzione. È possibile utilizzare i certificati con firma automatica predefiniti a scopo di test.

> **Nota:**
>
> Essbase supporta l'utilizzo di certificati con caratteri jolly, che possono proteggere più sottodomini con un certificato SSL. Utilizzando un certificato con caratteri jolly è possibile ridurre i tempi e i costi di gestione.
>
> Non è possibile utilizzare i certificati con caratteri jolly se è abilitata la verifica del nome host.

Sono necessari i certificati elencati di seguito.

- Un certificato CA radice.
  Per i componenti che utilizzano Essbase RTC per stabilire una connessione a Essbase, il certificato CA radice deve essere memorizzato nell'Oracle Wallet. Per i componenti che utilizzano JAPI per stabilire una connessione, il certificato CA radice deve essere memorizzato in un keystore Java. I certificati richiesti e le relative posizioni sono indicati nella tabella riportata di seguito.

  > **Nota:**
  >
  > Potrebbe non essere necessario installare un certificato CA radice se si utilizzano certificati di una CA di terze parti nota il cui certificato radice è già installato nell'Oracle Wallet.

- Certificato firmato per il server Essbase e l'agente Essbase.

Tabella 2-4 Certificati richiesti e relative posizioni

Componente[1]	Keystore	Certificato [2]
MaxL	Oracle Wallet	Certificato CA radice
Server Administration Services	Oracle Wallet	Certificato CA radice
Provider Services	Oracle Wallet	Certificato CA radice
Database Oracle Enterprise Performance Management System	Oracle Wallet	Certificato CA radice
Planning	• Oracle Wallet • Keystore Java	Certificato CA radice
Financial Management	Keystore Java	Certificato CA radice
Essbase (server e agente) [3]	• Oracle Wallet • Keystore Java	• Certificato CA radice • Certificato firmato per server e agente Essbase
Repository Oracle Hyperion Shared Services		

[1] È sufficiente una sola istanza del keystore per supportare più componenti che utilizzano un keystore simile.

[2] Più componenti possono utilizzare un certificato radice installato in un keystore.

[3] I certificati devono essere installati nell'Oracle Wallet predefinito e nel keystore Java.

Installazione e distribuzione dei componenti Essbase

Il processo di configurazione consente di selezionare una porta sicura dell'agente (la porta predefinita è la 6423), che può essere modificata durante la configurazione di Oracle Essbase. Per impostazione predefinita, il processo di distribuzione installa i certificati autofirmati necessari per creare una distribuzione sicura funzionante a fini di test.

Il programma di installazione di EPM System installa un certificato Oracle Wallet autofirmato all'interno di *ARBOR_PATH* nel computer che ospita l'istanza di Essbase se è installato Oracle HTTP Server. Nelle distribuzioni con host singolo, tutti i componenti Essbase condividono tale certificato.

Utilizzo di certificati CA di terze parti sicuri per Essbase

Creazione di richieste di certificati e ottenimento di certificati

Generare una richiesta di certificato per ottenere un certificato per il server che ospita il server Oracle Essbase e l'agente Essbase. Una richiesta di certificato contiene informazioni cifrate specifiche del nome comune del server in uso (CN=). La richiesta di certificato viene sottomessa a un'autorità di certificazione per ottenere un certificato SSL.

Per creare una richiesta di certificato viene utilizzato un keytool oppure Oracle Wallet Manager. Per informazioni dettagliate sulla creazione di una richiesta di certificato, fare riferimento alla documentazione relativa allo strumento in uso.

Esempi di utilizzo di keytool

Creare un Java Keystore (JKS) e generare una chiave privata:

```
keytool.exe -genkey -dname "cn=myserver, ou=EPM, o=Oracle, c=US"
-alias essbase_ssl -keypass password -keystore
C:\oracle\Middleware\EPMSystem11R1\ssl\EPM.JKS -storepass password
-validity 365 -keyalg RSA -keysize 2048 -sigalg SHA256withRSA -noprompt
```

Generare la richiesta di un certificato:

```
keytool -certreq -alias essbase_ssl -file
C:\oracle\Middleware\EPMSystem11R1\ssl\essabse_server.csr -keypass
password
-keystore C:\oracle\Middleware\EPMSystem11R1\ssl\EPM.JKS -storepass
password
```

Esportare la chiave privata. Per eseguire questi passi, è richiesta la utility `openssl`:

1. `openssl.exe pkcs12 -in C:\oracle\Middleware\EPMSystem11R1\ssl\EPM.JKS -passin pass:password -legacy -nocerts -out c:\Apache24\ssl\Apache24.key -passout pass:password`
2. Firmare la richiesta di certificato appena generata utilizzando la propria CA (Certifying Authority) e incollandola nel file seguente: `C:\oracle\Middleware\EPMSystem11R1\ssl\essbase.cer`.

Ottenimento e installazione del certificato CA radice

Il certificato CA radice verifica la validità del certificato utilizzato per supportare SSL. Contiene la chiave pubblica a fronte della quale viene confrontata per una corrispondenza la chiave privata utilizzata per firmare il certificato in modo da verificarlo. È possibile ottenere il certificato CA radice dall'autorità di certificazione che ha firmato i certificati SSL.

Installare il certificato radice dell'autorità CA che ha firmato il certificato del server Essbase nei client che si connettono al server o all'agente Essbase. Assicurarsi che il certificato radice sia installato nel keystore appropriato per il client. Fare riferimento alla sezione Certificati richiesti e relativa posizione .

> **Nota:**
>
> Un certificato CA radice installato in un server può essere utilizzato da più componenti.

Installazione di certificati con firma CA

Per installare i certificati con firma CA, vedere i collegamenti seguenti:

- Impostazione della connessione Weblogic TLS per Essbase
- Aggiornamento dei certificati TLS

Aggiornare il file `tls.properties` in

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

Dove:

```
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.
```

Per aggiornare il server Essbase con i nuovi certificati, eseguire quanto segue:

```
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
```

Aggiornamento delle impostazioni SSL di Essbase

Customizzare le impostazioni SSL dei client e del server Essbase specificando i valori dei seguenti elementi in `essbase.cfg`.

- L'impostazione per abilitare la modalità sicura
- L'impostazione per abilitare la modalità non cifrata
- La modalità preferita per comunicare con i client (utilizzata solo dai client)
- La porta sicura
- Le suite di cifratura
- Il percorso dell'Oracle Wallet

> **Nota:**
>
> In `essbase.cfg`, aggiungere gli eventuali parametri obbligatori mancanti, in particolare `EnableSecureMode`, `AgentSecurePort` e impostare i relativi valori.

Per aggiornare `essbase.cfg` con il seguente percorso:

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

1. Specificare le impostazioni in base alle esigenze. È implicito l'utilizzo delle impostazioni di Essbase predefinite. Se si desidera modificare il comportamento predefinito, aggiungere le impostazioni per il comportamento customizzato in `essbase.cfg`. Ad esempio, l'impostazione `EnableClearMode` è applicata per impostazione predefinita e in base a essa il server Essbase è abilitato a comunicare su un canale non cifrato. Per disattivare la capacità del server Essbase di comunicare su un canale non cifrato, specificare `EnableClearMode FALSE` in `essbase.cfg`. Fare riferimento alla tabella riportata di seguito:

Tabella 2-5 Impostazioni SSL di Essbase

Impostazione	Descrizione[1]
`EnableClearMode`[2]	Abilita le comunicazioni non cifrate tra le applicazioni Essbase e l'agente Essbase. Se questa proprietà è impostata su `FALSE`, Essbase non gestisce le richieste non SSL. **Valore predefinito:** `EnableClearMode TRUE` **Esempio:** `EnableClearMode FALSE`
`EnableSecureMode`	Abilita le comunicazioni cifrate SSL tra i client Essbase e l'agente Essbase. Questa proprietà deve essere impostata su `TRUE` per supportare SSL. **Valore predefinito:** `FALSE` **Esempio:** `EnableSecureMode TRUE`

Tabella 2-5 (Cont.) Impostazioni SSL di Essbase

Impostazione	Descrizione[1]
`SSLCipherSuites`	Elenco di suite di cifratura, in ordine di preferenza, da utilizzare per le comunicazioni SSL. L'agente Essbase utilizza una di queste suite di cifratura per le comunicazioni SSL. Alla prima suite di cifratura nell'elenco è assegnata la priorità più alta quando l'agente sceglie una suite di cifratura. **Valore predefinito:** `SSL_RSA_WITH_RC4_128_MD5` **Esempio:** `SSLCipherSuites SSL_RSA_WITH_AES_256_CBC_SHA256,SSL_RSA_WITH_AES_256_GCM_SHA384`
`APSRESOLVER`	URL di Oracle Hyperion Provider Services. Se si utilizzano più server Provider Services, separare i singoli URL utilizzando il punto e virgola. **Esempio:** `https://exampleAPShost1:`*`PORT`*`/essbase;https://exampleAPShost2:`*`PORT`*`/essbase`
`AgentSecurePort`	Porta sicura su cui è in ascolto l'agente. **Valore predefinito:** `6423` **Esempio:** `AgentSecurePort 16001`
`WalletPath`	Posizione dell'Oracle Wallet (meno di 1024 caratteri) in cui sono memorizzati il certificato CA radice e il certificato firmato. **Valore predefinito:** *`ARBORPATH`*`/bin/wallet` **Esempio:** `WalletPath/usr/local/wallet`
`ClientPreferredMode` [3]	Modalità (Secure o Clear) per la sessione client. Se questa proprietà è impostata su Secure, viene utilizzata la modalità SSL per tutte le sessioni. Se questa proprietà è impostata su Clear, il trasporto viene scelto a seconda che nella richiesta di accesso client sia contenuta la parola chiave di trasporto sicuro. Fare riferimento alla sezione Attivazione di una connessione SSL per la singola sessione. **Valore predefinito:** `CLEAR` **Esempio:** `ClientPreferredMode SECURE`

- [1] Il valore predefinito viene applicato se le proprietà non sono disponibili in `essbase.cfg`.
- [2] Essbase diventa non operativo se `EnableClearMode` e `EnableSecureMode` sono entrambi impostati su `FALSE`.
- [3] I client utilizzano questa impostazione per determinare se devono stabilire una connessione sicura o non sicura con Essbase.

2. Salvare e chiudere `essbase.cfg`.

Aggiornamento dei nodi Essbase distribuiti per SSL

> **Nota:**
>
> Questa sezione è valida solo per la distribuzione distribuita di Essbase

Verificare che la cartella del wallet (ad esempio, `WalletPath/usr/local/wallet`) contenga il certificato CA radice e che il certificato firmato si trovi nella posizione richiesta in ogni nodo distribuito.

1. Importare tutti i nuovi certificati CA utilizzando strumenti TLS.

   Per ulteriori informazioni, vedere i collegamenti seguenti:

   - Impostazione della connessione Weblogic TLS per Essbase
   - Aggiornamento dei certificati TLS

2. Accedere alla posizione di origine `ESSBASE_DOMAIN_HOME\config\fmwconfig\essconfig\essbase` e modificare le proprietà seguenti nel file `essbase.properties`:

   - `essbase.ssleverywhere=true`
   - `olap.server.ssl.alwaysSecure=true`
   - `APSRESOLVER=`*`APS_URL`*
     Sostituire *`APS_URL`* con l'URL di Provider Services. Se si utilizzano più server Provider Services, separare i singoli URL utilizzando un punto e virgola.

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

3. Copiare le cartelle `Wallet` e `Walletssl` e i file `essbase.cfg` e `essbase.properties` nei percorsi di destinazione indicati di seguito.

Tabella 2-6 Percorsi di destinazione

Percorsi di destinazione	Wallet	Walletssl	essbase.cfg	essbase.properties
`EPM_ORACLE_HOME\common\EssbaseRTC-21C\11.1.2.0\bin`	Sì	Sì	Sì	Sì
`EPM_ORACLE_HOME\common\EssbaseJavaAPI-21C\11.1.2.0\bin`	Sì	Sì	Sì	Sì
`ESSBASE_DOMAIN_HOME\config\fmwconfig\essconfig\aps`	Sì	Sì	Sì	Sì
`ESSBASE_DOMAIN_HOME\config\fmwconfig\essconfig\essbase`	Sì	Sì	Sì	Sì
`MIDDLEWARE_HOME\essbase\products\Essbase\template_files\essbase`	Sì	Sì	Sì	Sì
`MIDDLEWARE_HOME\essbase\products\Essbase\EssbaseServer\bin`	Sì	Sì	Sì	Sì
`MIDDLEWARE_HOME\essbase\products\Essbase\aps\bin`	Sì	Sì	Sì	Sì
`MIDDLEWARE_HOME\essbase\products\Essbase\eas`	Sì	Sì	Sì	Sì

Tabella 2-6 (Cont.) Percorsi di destinazione

Percorsi di destinazione	Wallet	Wallet ssl	essbase.cfg	essbase.properties
`MIDDLEWARE_HOME\essbase\common\EssbaseJavaAPI\bin`	Sì	Sì	Sì	Sì
Solo per Oracle Hyperion Financial Reporting `EPM_ORACLE_HOME/products/financialreporting/bin/EssbaseJAPI/bin/` **Nota:** negli ambienti SSL completi, Financial Reporting necessita del nome del cluster Essbase per stabilire una connessione. Le connessioni hanno esito negativo se il nome host viene utilizzato per la connessione.	Sì	Sì	Sì	Sì
Solo per Oracle Hyperion Planning `EPM_ORACLE_HOME/products/Planning/config/` `EPM_ORACLE_HOME/products/Planning/lib/`	Sì	Sì	Sì	Sì

4. Impostare le variabili di ambiente.
   - **Windows:** creare una nuova variabile di ambiente con nome `API_DISABLE_PEER_VERIFICATION` e impostarla su `1`.
   - **Linux:** aggiungere la direttiva `API_DISABLE_PEER_VERIFICATION=1` in `setCustomParamsPlanning.sh`.

Customizzazione delle proprietà SSL dei client JAPI

Sono presenti diverse proprietà predefinite per i componenti Essbase che si basano su JAPI. Le proprietà predefinite possono essere sostituite includendo le proprietà in `essbase.properties`.

> **Nota:**
>
> Solo alcune delle proprietà SSL identificate nella tabella che segue sono esternalizzate in `essbase.properties`. Devono essere aggiunte le proprietà che non sono esternalizzate.

Per aggiornare le proprietà SSL dei client JAPI, procedere come segue.

1. Aprire `EPM_ORACLE_HOME/common/EssbaseJavaAPI-21C/11.2.0/bin/essbase.properties` con un editor di testo.
2. Aggiornare le proprietà in base alle esigenze. Fare riferimento alla tabella che segue per una descrizione delle proprietà client JAPI customizzabili.
   Se una proprietà desiderata non è inclusa in `essbase.properties`, aggiungerla.

Tabella 2-7 Proprietà SSL predefinite per i client JAPI

Proprietà	Descrizione
`olap.server.ssl.alwaysSecure`	Imposta la modalità che deve essere utilizzata dai client in tutte le istanze di Essbase. Modificare il valore di questa proprietà impostandolo su `true` per applicare la modalità SSL. **Valore predefinito:** `false`
`olap.server.ssl.securityHandler`	Nome del package per la gestione del protocollo. È possibile modificare questo valore per indicare un altro handler. **Valore predefinito:** `java.protocol.handler.pkgs`
`olap.server.ssl.securityProvider`	Oracle utilizza l'implementazione del protocollo Sun SSL. È possibile modificare questo valore per indicare un altro provider. **Valore predefinito:** `com.sun.net.ssl.internal.www.protocol`
`olap.server.ssl.supportedCiphers`	Elenco di voci separate da virgole contenente cifrature aggiuntive da abilitare per le comunicazioni sicure. È necessario specificare solo le cifrature supportate da Essbase. **Esempio**: `SSL_RSA_WITH_AES_256_CBC_SHA256,SSL_RSA_WITH_AES_256_GCM_SHA384`
`olap.server.ssl.trustManagerClass`	Classe TrustManager da utilizzare per convalidare il certificato SSL verificando la firma e controllando la data di scadenza del certificato. Per impostazione predefinita, questa proprietà non è impostata per applicare tutti i controlli di verifica. Per non applicare i controlli di verifica, impostare il valore di questo parametro su `com.essbase.services.olap.security.EssDefaultTrustManager`, ovvero la classe TrustManager predefinita che consente di superare tutti i controlli di verifica. Per implementare una classe TrustManager customizzata, specificare un nome di classe completo della classe TrustManager che implementi l'interfaccia `javax.net.ssl.X509TrustManager`. **Esempio**: `com.essbase.services.olap.security.EssDefaultTrustManager`

3. Salvare e chiudere `essbase.properties`.
4. Riavviare tutti i componenti di Essbase.

Attivazione di una connessione SSL per la singola sessione

I componenti Oracle Essbase, ad esempio MaxL, sono in grado di controllare SSL a livello di sessione mediante la connessione all'agente Essbase con `secure` come parola chiave per il trasporto. Ad esempio, è possibile stabilire una connessione sicura

tra MaxL e l'agente Essbase eseguendo da una console MaxL uno dei comandi riportati di seguito:

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

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

Il controllo a livello di singola sessione ha la priorità sulle impostazioni di configurazione specificate nel file `essbase.cfg`. Se non viene specificata alcuna parola chiave per il trasporto, i client Essbase utilizzano il valore impostato per `ClientPreferredMode` per stabilire se avviare una connessione sicura a Essbase. Se l'impostazione `ClientPreferredMode` non è configurata su secure, la comunicazione avviene su un canale non sicuro.

3

Abilitazione dell'SSO con gli agenti di protezione

Vedere anche:

- Metodi SSO supportati
- Single Sign-On da Oracle Access Manager
- OracleAS Single Sign-On
- Protezione dei prodotti di EPM System per l'SSO
- Accesso SSO basato su intestazione con prodotti di gestione delle identità
- Configurazione di EPM System per l'accesso SSO basato su intestazione con Oracle Identity Cloud Services
- SSO con SiteMinder
- Single Sign-On con Kerberos
- Configurazione di EPM System per l'SSO
- Opzioni Single Sign-On per Smart View

Metodi SSO supportati

Con SSO, la soluzione di gestione delle identità Web passa il nome di accesso degli utenti autenticati ai prodotti Oracle Enterprise Performance Management System. È possibile utilizzare i metodi EPM System standard descritti di seguito per integrare EPM System con soluzioni SSO commerciali e customizzate basate sul Web.

- Intestazione HTTP
- Classe di accesso customizzata
- Intestazione di autorizzazione HTTP
- Richiama utente remoto da richiesta HTTP
- Autenticazione basata su intestazione con prodotti di gestione delle identità

> **Attenzione:**
>
> Come misura di sicurezza, Oracle consiglia di implementare l'autenticazione con certificato client (autenticazione SSL bidirezionale) tra il server Web e il server applicazioni se nell'organizzazione vengono utilizzati metodi con l'identità dell'utente nell'intestazione per la propagazione dell'identità.

Intestazione HTTP

Se si utilizza Oracle Single Sign-On (OSSO), SiteMinder oppure Oracle Access Manager come soluzione di gestione delle identità Web, la funzionalità di sicurezza di EPM System seleziona automaticamente l'intestazione HTTP customizzata per passare il nome di accesso degli utenti autenticati ai componenti di EPM System.

Il nome di accesso dell'utente di un prodotto EPM System viene determinato dall'elemento `Login Attribute` specificato durante la configurazione delle directory utenti in Oracle Hyperion Shared Services. Fare riferimento alla sezione "Configurazione di OID, Active Directory e altre directory utenti basate su LDAP" nella *Oracle Enterprise Performance Management System User Security Administration Guide (in lingua inglese)* per una breve descrizione di `Login Attribute`.

L'intestazione HTTP deve contenere il valore dell'attributo impostato come `attributo di accesso`. Se ad esempio il valore di `Login Attribute` è `uid`, l'intestazione HTTP deve includere il valore dell'attributo `uid`.

Per informazioni dettagliate sulla definizione e la generazione di intestazioni HTTP customizzate, fare riferimento alla documentazione della propria soluzione di gestione delle identità Web.

La funzionalità di sicurezza di EPM System analizza l'intestazione HTTP e convalida il nome di accesso in essa contenuto a fronte delle directory utenti configurate in Shared Services.

Classe di accesso customizzata

Quando un utente esegue l'accesso, la soluzione di gestione delle identità Web lo autentica a fronte di un server directory e incapsula le credenziali dell'utente autenticato in un meccanismo SSO per consentire l'accesso SSO con sistemi a valle. Se la soluzione di gestione delle identità Web utilizza un meccanismo non supportato dai prodotti EPM System o se il valore di `Login Attribute` non è disponibile nel meccanismo SSO, è possibile utilizzare una classe di accesso customizzata per recuperare il valore di `Login Attribute` e passarlo ai prodotti EPM System.

L'utilizzo di una classe di accesso customizzata consente l'integrazione di EPM System con agenti di sicurezza che utilizzano l'autenticazione basata sul certificato X509. L'utilizzo di questo meccanismo di autenticazione richiede l'implementazione di API di Shared Services standard per definire l'interfaccia SSO tra i componenti di EPM System e la soluzione di gestione delle identità Web. La classe di accesso custom deve quindi passare il valore dell'`attributo di accesso` ai prodotti di EPM System. Fare riferimento alla sezione "Configurazione di OID, Active Directory e altre directory utenti basate su LDAP" nel manuale *Oracle Enterprise Performance Management System User Security Administration Guide (in lingua inglese)* per una breve descrizione di `Login Attribute`. Per il codice campione e i passi di implementazione, fare riferimento alla sezione Implementazione di una classe di accesso customizzata.

Per poter utilizzare una classe di accesso customizzata (il nome predefinito è `com.hyperion.css.sso.agent.X509CertificateSecurityAgentImpl`), deve essere disponibile un'implementazione dell'interfaccia `com.hyperion.css.CSSSecurityAgentIF` nel classpath. `CSSSecurityAgentIF` definisce il metodo getter per il recupero del nome utente e della password (facoltativo). Se l'interfaccia restituisce una password con valore null, l'autenticazione di protezione considera il provider attendibile e verifica l'esistenza dell'utente nei provider configurati. Se l'interfaccia restituisce un valore diverso da null per la password, EPM

System tenta di autenticare la richiesta utilizzando il nome utente e la password restituiti da questa implementazione.

`CSSSecurityAgentIF` include due metodi: `getUserName` e `getPassword`.

Metodo getUserName

Questo metodo restituisce il nome utente per l'autenticazione.

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

Il parametro `req` identifica la richiesta HTTP che trasporta le informazioni utilizzate per determinare il nome utente. Il parametro `res` non viene utilizzato (è preimpostato per la compatibilità con le versioni precedenti).

Metodo getPassword

Questo metodo restituisce la password con testo in chiaro per l'autenticazione. Il recupero della password è opzionale.

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

Il parametro `req` identifica la richiesta HTTP che trasporta le informazioni utilizzate per determinare il nome utente. Il parametro `res` non viene utilizzato (è preimpostato per la compatibilità con le versioni precedenti).

Intestazione di autorizzazione HTTP

La funzionalità di sicurezza di EPM System supporta l'utilizzo di un'intestazione di autorizzazione HTTP per passare il valore di `Login Attribute` ai prodotti EPM System da soluzioni di gestione delle identità Web. I prodotti EPM System analizzano l'intestazione dell'autorizzazione per recuperare il nome di accesso dell'utente.

Richiama utente remoto da richiesta HTTP

La funzionalità di sicurezza di EPM System supporta l'utilizzo di una richiesta HTTP per passare il valore di `Login Attribute` ai prodotti EPM System da soluzioni di gestione delle identità Web. Utilizzare questo metodo SSO se la soluzione di gestione delle identità Web passa una richiesta HTTP contenente il valore di `Login Attribute`, che viene ipostato utilizzando la funzione `setRemoteUser`.

Autenticazione basata su intestazione con prodotti di gestione delle identità

EPM System supporta qualsiasi prodotto di gestione delle identità, ad esempio Oracle Identity Cloud Services, Microsoft Azure AD e Okta, che supporti l'autenticazione basata su intestazione. Il flusso di lavoro concettuale è il seguente.

- Un'applicazione gateway che funge da proxy inverso protegge i componenti di EPM System limitando l'accesso alla rete non autenticato.

- L'applicazione gateway intercetta le richieste HTTP(S) dirette ai componenti di EPM System e garantisce che il prodotto di gestione delle identità autentichi gli utenti prima che le richieste vengano inoltrate ai componenti di EPM System.
- Durante l'inoltro delle richieste ai componenti di EPM System, l'applicazione gateway propaga l'identità dell'utente autenticato al componente di EPM System mediante richieste con intestazione HTTP.

Per supportare questo scenario di autenticazione, EPM System deve essere configurato per utilizzare l'identità dell'utente autenticato che viene propagata mediante richieste con intestazione HTTP(S).

Accesso Single Sign-On da Oracle Access Manager

Oracle Enterprise Performance Management System si integra con Oracle Access Manager accettando un'intestazione HTTP customizzata (nome predefinito `HYPLOGIN`) contenente il valore dell'attributo di accesso. L'attributo di accesso viene impostato quando si configura una directory utenti esterna in Oracle Hyperion Shared Services. Fare riferimento alla sezione "Configurazione di OID, Active Directory e altre directory utenti basate su LDAP" nella *Oracle Enterprise Performance Management System User Security Administration Guide (in lingua inglese)* per una breve descrizione di `Login Attribute`.

È possibile utilizzare qualsiasi nome di intestazione che fornisca il valore dell'attributo di accesso a EPM System. Il nome di intestazione viene utilizzato durante la configurazione di Shared Services per SSO da Oracle Access Manager.

In EPM System il valore dell'attributo di accesso viene utilizzato per autenticare l'utente a fronte di una directory utenti configurata (in questo caso, la directory utenti a fronte della quale Oracle Access Manager autentica gli utenti) e quindi viene generato un token SSO EPM che consente l'accesso SSO su EPM System. Le informazioni di assegnazione ruoli dell'utente vengono controllate nella directory nativa per autorizzare l'utente per le risorse EPM System.

> **Nota:**
>
> La console Oracle Essbase Administration Services, che è un thick client, non supporta l'accesso SSO da Oracle Access Manager.

Per informazioni sulla configurazione di Oracle Access Manager e sull'esecuzione di task quali la configurazione dell'intestazione HTTP e dei domini dei criteri, fare riferimento alla documentazione di Oracle Access Manager. In questa guida si presuppone che si disponga di una distribuzione di Oracle Access Manager funzionante in cui sono stati completati i task elencati di seguito.

- Impostazione dei domini di criteri necessari per i componenti di EPM System
- Configurazione di un'intestazione HTTP per passare il valore dell'attributo di accesso a EPM System
- Protezione delle risorse EPM System elencate nella sezione Risorse da proteggere; le richieste di accesso alle risorse protette vengono effettuate da Oracle Access Manager

- Rimozione della protezione dalle risorse EPM System elencate nella sezione Risorse da cui rimuovere la protezione; le richieste di accesso alle risorse da cui è stata rimossa la protezione vengono effettuate da Oracle Access Manager

Per configurare EPM System per SSO da Oracle Access Manager, procedere come segue.

1. Aggiungere la directory utenti utilizzata da Oracle Access Manager per autenticare gli utenti come directory utenti esterna in EPM System. Fare riferimento alla sezione "Configurazione di OID, Active Directory e altre directory utenti basate su LDAP" nella *Oracle Enterprise Performance Management System User Security Administration Guide (in lingua inglese)*.

   > **Nota:**
   >
   > Assicurarsi che sia selezionata la casella di controllo **Sicuro** nella schermata delle informazioni di connessione per indicare che la directory utenti è un'origine SSO sicura.

2. Configurare EPM System per SSO. Fare riferimento alla sezione Configurazione di EPM System per l'SSO.

   Selezionare Oracle Access Manager dall'elenco **Provider o agente SSO**. Se nell'intestazione HTTP di Oracle Access Manager viene utilizzato un nome diverso da `HYPLOGIN`, immettere il nome dell'intestazione customizzata nella casella di testo accanto all'elenco **Meccanismo SSO**.

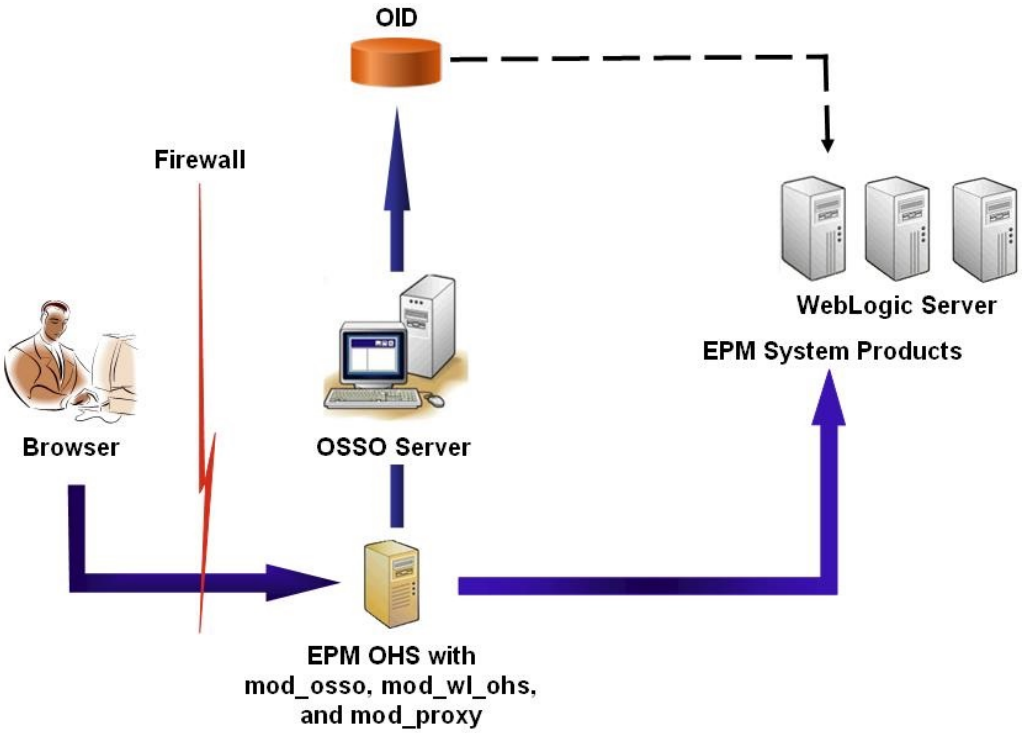
3. Solo in Oracle Data Relationship Management procedere come segue.
   a. Configurare Data Relationship Management per l'autenticazione Shared Services.
   b. Abilitare SSO in Data Relationship Management Console.

      Per informazioni dettagliate, fare riferimento alla documentazione di Data Relationship Management.

OracleAS Single Sign-On

La soluzione OracleAS Single Sign-On (OSSO) fornisce l'accesso SSO ad applicazioni Web con Oracle Internet Directory (OID) come directory utenti. Gli utenti utilizzano un nome utente e una password definiti in OID per accedere a prodotti Oracle Enterprise Performance Management System.

Flusso del processo



Viene descritto di seguito il processo OSSO.

1. Utilizzando un URL EPM System, ad esempio, `http://OSSO_OHS_Server_NAME:OSSO_OHS_Server_PORT/interop/index.jsp`, gli utenti accedono a un componente di EPM System definito come applicazione protetta da OSSO.
2. Poiché l'URL è protetto tramiteOSSO, il modulo `mod_osso`, distribuito in Oracle HTTP Server, intercetta la richiesta. Utilizzando `mod_osso`, Oracle HTTP Server cerca un cookie valido. Se non è disponibile un cookie valido nella richiesta, Oracle HTTP Server reindirizza gli utenti al server OSSO, che richiede loro le credenziali ed esegue l'autenticazione a fronte di OID.
3. Il server OSSO crea obSSOCookie e restituisce il controllo al modulo `mod_osso` in Oracle HTTP Server, che imposta obSSOCookie nel browser. Reindirizza inoltre la richiesta alla risorsa EPM System tramite `mod_wl_ohs` (Oracle WebLogic Server). Prima di inoltrare la richiesta a una risorsa EPM System, Oracle HTTP Server imposta l'intestazione `Proxy-Remote-User`, utilizzata dalla funzionalità di sicurezza di EPM System per abilitare SSO.
4. Il componente di EPM System verifica che l'utente di cui viene recuperata l'identità da `Proxy-Remote-User` sia presente in OID. Affinché questo processo funzioni correttamente, la directory OID nel server OSSO deve essere configurata come directory utenti esterna in Oracle Hyperion Shared Services.

Prerequisiti

1. Un'istanza di Oracle Application Server Infrastructure completamente funzionante.

   Per definire un'istanza di Oracle Application Server Infrastructure, installare e configurare Oracle Identity Management Infrastructure 10.1.4. Assicurarsi che sia abilitato OSSO. L'installazione di Oracle Identity Management Infrastructure 10.1.4 include i componenti elencati di seguito per supportare OSSO.

- Server OSSO Oracle 10*g*.
- Una directory OID, utilizzata dal server OSSO per convalidare le credenziali. Fare riferimento ai manuali elencati di seguito.
  - *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* (in lingua inglese)
  - *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* (in lingua inglese)
- Oracle HTTP Server come front end del server OSSO. Questa installazione include `mod_osso`, che consente di definire applicazioni partner per OSSO.

  > **Nota:**
  >
  > Questa istanza di Oracle HTTP Server fa parte dell'infrastruttura OSSO e non è utilizzata direttamente per configurare OSSO per i componenti di EPM System.

  Durante il processo di installazione, assicurarsi che il modulo `mod_osso` sia registrato nel server OSSO come applicazione partner.

2. Una distribuzione di EPM System completamente funzionante.
   Quando si configura il server Web per i componenti di EPM System, EPM System Configurator configura `mod_wl_ohs.conf` in Oracle HTTP Server per utilizzare un proxy per inviare le richieste a WebLogic Server.

Test della distribuzione

Al termine della distribuzione dell'autenticazione SSL, verificare che funzioni tutto.

Per testare la distribuzione, procedere come segue.

1. Accedere con un browser all'URL sicuro di Oracle Hyperion Enterprise Performance Management Workspace riportato di seguito.

   Se si è utilizzato `epm.myCompany.com` come alias del server per le comunicazioni esterne e `4443` come porta SSL, l'URL di EPM Workspace è

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

2. Immettere il nome utente e la password nella schermata di accesso.
3. Fare clic su **Accedi**.
4. Verificare di poter accedere in modo sicuro ai componenti di Oracle Enterprise Performance Management System distribuiti.

Abilitazione di OSSO per EPM System

In questa sezione si presuppone che si disponga di un'infrastruttura OSSO completamente configurata. Fare riferimento al manuale *Oracle Application Server Administrator's Guide* (in lingua inglese).

Registrazione del server Web EPM System come applicazione partner

Utilizzando lo strumento di registrazione SSO di Oracle Identity Manager (`ssoreg.sh` o `ssoreg.bat`), è possibile registrare il server Web Oracle Enterprise Performance Management System come applicazione partner nell'istanza di Oracle HTTP Server che funge da front-end per il server OSSO.

Eseguire questa procedura nel server che ospita l'istanza di Oracle HTTP Server che funge da front-end per il server OSSO. Tale processo genera e memorizza un file `osso.conf` cifrato nella posizione scelta dall'utente.

Per registrare il server Web EPM System come applicazione partner, procedere come segue.

1. Aprire una console nel server che ospita l'istanza di Oracle HTTP Server che funge da front-end per il server OSSO e passare alla directory *`ORACLE_HOME`*`/sso/bin` di Oracle HTTP Server, ad esempio a `C:/OraHome_1/sso/bin` (Windows).
2. Eseguire un comando simile al seguente con l'opzione `-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
   ```

   Di seguito vengono descritti i parametri utilizzati in questo comando. In tale descrizione, per applicazione partner si intende l'istanza di Oracle HTTP Server utilizzata come server Web EPM System.

   - `-site_name` identifica il sito Web dell'applicazione partner, ad esempio `epm.myCompany.com`.
   - `-mod_osso_url` indica l'URL dell'applicazione partner, in formato *`PROTOCOL://HOST_NAME:PORT`*. Si tratta dell'URL in cui il server Web EPM System accetta le richieste client in entrata, ad esempio `http://epm.myCompany.com:19000`.
   - `-config_mod_osso` indica che l'applicazione partner utilizza `mod_osso`. È necessario includere il parametro `config_mod_osso` per generare `osso.conf`.
   - `-update_mode` indica la modalità aggiornamento. Utilizzare `CREATE`, la modalità predefinita, per generare un nuovo record.
   - `-remote_midtier` indica che l'applicazione partner `mod_osso` si trova in un livello intermedio remoto. Utilizzare questa opzione quando l'applicazione partner si trova in una directory *`ORACLE_HOME`* diversa da quella del server OSSO.
   - `-virtualhost` indica che l'URL dell'applicazione partner corrisponde a un host virtuale. Non specificare questo parametro se non si utilizza un host virtuale. Se si sta registrando un URL di applicazione partner associato a un host virtuale, è necessario definire tale host in `httpd.conf`. Fare riferimento alla sezione Facoltativo: Definizione dell'host virtuale.
   - `-config_file` indica il percorso in cui deve essere generato il file `osso.conf`.

Facoltativo: Definizione dell'host virtuale

Se è stato utilizzato l'URL di un host virtuale durante la registrazione dell'applicazione partner, è necessario definire tale host aggiornando `httpd.conf` nell'istanza di Oracle HTTP Server utilizzata come server Web EPM System.

Per definire un host virtuale, procedere come segue.

1. Utilizzando un editor di testo, aprire *EPM_ORACLE_INSTANCE*`/httpConfig/ohs/config/OHS/ohs_component/httpd.conf`.
2. Aggiungere una definizione simile alla seguente. In tale definizione si presuppone che il server Web sia in esecuzione nel server virtuale `epm.myCompany.com` sulla porta `epm.myCompany.com:19400`. Modificare le impostazioni in base alle proprie esigenze.

```
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>
```

Creazione di `mod_osso.conf`

Creare `mod_osso.conf` nell'istanza di Oracle HTTP Server che funge da front-end per il server Web EPM System.

Per creare `mod_osso.conf`, procedere come segue.

1. Creare un file utilizzando un editor di testo.
2. Copiare nel file il contenuto seguente e modificarlo in base all'ambiente in uso.

```
LoadModule osso_module C:/Oracle/Middleware/ohs/ohs/modules/mod_osso.so
<IfModule mod_osso.c>
   OssoIpCheck off
   OssoIdleTimeout off
   OssoSecureCookies off
   OssoConfigFile C:/Oracle/Middleware/user_projects/epmsystem1/
httpConfig/
      ohs/config/OHS/ohs_component/osso/osso.conf
```

3. All'interno della definizione `<IfModule mod_osso.c`, includere definizioni di posizione simili alla seguente per identificare ciascuna risorsa che si intende proteggere tramite OSSO.

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

4. Salvare il file denominandolo `mod_osso.conf`.

Riposizionamento di `osso.conf`

Il processo di registrazione del server Web EPM System come applicazione partner (fare riferimento alla sezione Registrazione del server Web EPM System come applicazione partner) crea un file `osso.conf` cifrato nella posizione identificata dalla direttiva `-config_file`.

Per riposizionare `osso.conf`, procedere come segue.

1. Individuare il file `osso.conf` creato quando il server Web EPM System è stato registrato come applicazione partner. Fare riferimento alla sezione Registrazione del server Web EPM System come applicazione partner.
2. Copiare `osso.conf` nella directory (nell'istanza di Oracle HTTP Server che funge da front-end per il server OSSO) identificata dalla proprietà `OssoConfigFile` definita in `mod_osso.conf`. Fare riferimento alla sezione Creazione di mod_osso.conf.

Configurazione di EPM System per OSSO

Configurare l'istanza di OID integrata nella soluzione OSSO come directory utenti esterna in EPM System, quindi abilitare SSO.

Per configurare EPM System per OSSO, procedere come segue.

1. Configurare l'istanza di OID utilizzata dalla soluzione OSSO come directory utenti esterna. Fare riferimento alla sezione "Configurazione di OID, Active Directory e altre directory utenti basate su LDAP" nella *Oracle Enterprise Performance Management System User Security Administration Guide (in lingua inglese)*.
2. Abilitare SSO in EPM System. Configurazione di EPM System per l'SSO

> **Nota:**
>
> Per configurare OSSO come soluzione di gestione identità, è necessario scegliere `Other` in **Provider o agente SSO**, `Custom HTTP Header` in **Meccanismo SSO** e immettere `Proxy-Remote-User` come nome dell'intestazione HTTP customizzata.

3. Assegnare ad almeno un utente OID il ruolo di amministratore di Oracle Hyperion Shared Services.
4. Riavviare i prodotti EPM System e le applicazioni custom che utilizzano le API di protezione di Shared Services.

> **Nota:**
>
> Assicurarsi che l'istanza di OID configurata con Shared Services sia in esecuzione prima di avviare i prodotti EPM System.

Facoltativo: Abilitazione dei messaggi di debug nel server OSSO

Per registrare i messaggi di debug nel server OSSO, modificare `policy.properties`. Tali messaggi vengono scritti in *`ORACLE_HOME/sso/log/ssoServer.log`*.

Per registrare i messaggi di debug, procedere come segue.

1. Utilizzando un editor di testo, aprire *ORACLE_HOME/sso/conf/policy.properties*, ad esempio `C:\OraHome_1\sso\conf\policy.properties`, nel server OSSO.
2. Impostare il valore della proprietà `debugLevel` su DEBUG.

   ```
   debugLevel = DEBUG
   ```

3. Salvare e chiudere `policy.properties`.

Facoltativo: Abilitazione dei messaggi di debug per le risorse protette

Per registrare i messaggi di debug OSSO per le risorse protette utilizzando `mod_osso.conf`, modificare `httpd.conf` nel server Web EPM System. I messaggi di debug vengono scritti in *EPM_ORACLE_INSTANCE*`/httpConfig/ohs/diagnostics/logs/OHS/ohs_component/ohs_component.log`.

Per registrare i messaggi di debug per le risorse protette, procedere come segue.

1. Utilizzando un editor di testo, aprire *EPM_ORACLE_INSTANCE*`/httpConfig/ohs/config/OHS/ohs_component/httpd.conf`.
2. Impostare il valore della proprietà `OraLogSeverity` su TRACE.

   ```
   OraLogSeverity TRACE:32
   ```

3. Salvare e chiudere `httpd.conf`.

Protezione dei prodotti di EPM System per l'SSO

È necessario proteggere le risorse Oracle Enterprise Performance Management System in modo che le richieste SSO degli utenti vengano reindirizzate all'agente di sicurezza (OAM, OSSO o SiteMinder).

Oracle HTTP Server utilizza `mod_osso` per il reindirizzamento degli utenti al server OSSO. Gli utenti vengono reindirizzati solo se gli URL che richiedono sono configurati in `mod_osso` per essere protetti. Fare riferimento alla sezione Gestione della sicurezza nel manuale *Oracle HTTP Server Administrator's Guide* (in lingua inglese).

Per informazioni sulla protezione delle risorse per l'SSO con SiteMinder, vedere la documentazione di SiteMinder.

Solo per OAM: come impedire l'aggiunta delle intestazioni predefinite alle risposte

Per impostazione predefinita, OAM aggiunge due intestazioni, Pragma: no-cache e Cache-Control: no-cache, agli URL protetti. Poiché queste intestazioni creano un conflitto con direttive di inserimento nella cache simili aggiunte dalle applicazioni EPM System e Web, i browser potrebbero non inserire il contenuto degli URL protetti nella cache, provocando un rallentamento delle prestazioni.

Per informazioni dettagliate su come impedire l'aggiunta di queste intestazioni OAM alle risposte, fare riferimento a "*Tuning degli agenti OAM*" nella sezione "Oracle Access Management Performance Tuning" della *Guida per gli amministratori di Fusion Middleware per Oracle Access Manager con Oracle Security Token Service*.

Risorse da proteggere

Nella tabella che segue sono riportati i contesti che è necessario proteggere. La sintassi per proteggere una risorsa (utilizzando `interop` come esempio) per OSSO, è la seguente:

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

Il parametro `allow from` consente di specificare i server da cui è possibile ignorare la protezione del contesto.

Per Oracle Hyperion Enterprise Performance Management Workspace e Oracle Hyperion Financial Reporting è necessario impostare solo i parametri indicati nell'esempio seguente:

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

Tabella 3-1 Risorse di EPM System da proteggere

Prodotto EPM System	Contesto da proteggere
Oracle Hyperion Shared Services	• /interop • /interop/.../*
EPM Workspace	• /workspace • /workspace/.../*
Financial Reporting	• /hr • /hr/.../*
Oracle Hyperion Planning	• /HyperionPlanning • /HyperionPlanning/.../*
Oracle Integrated Operational Planning	• /interlace • /interlace/.../*
Oracle Hyperion Financial Management	• /hfmadf • /hfmadfe/.../* • /hfmofficeprovider • /hfmofficeprovider/.../* • /hfmsmartviewprovider • /hfmsmartviewprovider/.../*
Oracle Hyperion Financial Reporting Web Studio	/frdesigner/**
Oracle Data Relationship Management	• /drm-web-client • /drm-web-client/.../*

Tabella 3-1 (Cont.) Risorse di EPM System da proteggere

Prodotto EPM System	Contesto da proteggere
Oracle Essbase Administration Services	• /hbrlauncher • /hbrlauncher/.../*
Oracle Hyperion Financial Data Quality Management	• /HyperionFDM • /HyperionFDM/.../*
Oracle Hyperion Calculation Manager	• /calcmgr • /calcmgr/.../*
Oracle Hyperion Provider Services	• /aps • /aps/.../*
Oracle Hyperion Profitability and Cost Management	• /profitability • /profitability/.../*
Gestione riconciliazione conti	• /arm • /arm/.../*
Oracle Hyperion Financial Close Management	• /fcc • /fcc/.../*
Oracle Hyperion Financial Data Quality Management Enterprise Edition	• /aif • /aif/.../*
Oracle Hyperion Tax Governance	/tss
Operazioni imposte	/taxop
Oracle Hyperion Tax Provision	/taxprov
Gestione dati supplementari	• /sdm* • /sdm/** • /sdm/../** • /SDM-Datamodel-context-root/**
Oracle Essbase	• /essbase/.../* • /essbase/** • /essbase*

Risorse da cui rimuovere la protezione

Nella tabella che segue sono riportati i contesti per i quali è necessario rimuovere la protezione. La sintassi per rimuovere la protezione di una risorsa (utilizzando `/interop/framework(.*)` come esempio) per OSSO, è la seguente:

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

Tabella 3-2 Risorse di EPM System da non proteggere

Prodotto EPM System	Contesti da cui rimuovere la protezione
Shared Services	• /interop/framework • /interop/framework* • /interop/framework.* • /interop/framework/.../* • /interop/Audit • /interop/Audit* • /interop/Audit.* • /interop/Audit/.../* • /interop/taskflow • /interop/taskflow* • /interop/taskflow/.../* • /interop/WorkflowEngine • /interop/WorkflowEngine/* • /interop/WorkflowEngine/.../* • /interop/TaskReceiver • /framework/lcm/HSSMigration
EPM Workspace	• /epmstatic/.../* • /workspace/bpmstatic/.../* • /workspace/static/.../* • /workspace/cache/.../*
Planning	• /HyperionPlanning/Smartview • /HyperionPlanning/faces/PlanningCentral • /HyperionPlanning/servlet/HspDataTransfer • /HyperionPlanning/servlet/HspLCMServlet • /HyperionPlanning/servlet/HspADMServlet/.../* • /HyperionPlanning/servlet/HspADMServlet/** • /HyperionPlanning/servlet/HspADMServlet* • /HyperionPlanning/servlet/HspAppManagerServlet/.../* • /HyperionPlanning/servlet/HspAppManagerServlet/** • /HyperionPlanning/servlet/HspAppManagerServlet*

Tabella 3-2 (Cont.) Risorse di EPM System da non proteggere

Prodotto EPM System	Contesti da cui rimuovere la protezione
Financial Reporting	• /hr/common/HRLogon.jsp • /hr/services • /hr/services/* • /hr/services/.../* • /hr/modules/com/hyperion/reporting/web/reportViewer/HRStaticReport.jsp • /hr/modules/com/hyperion/reporting/web/repository/HRObjectListXML.jsp • /hr/modules/com/hyperion/reporting/web/reportViewer/HRHtmlReport.jsp • /hr/modules/com/hyperion/reporting/web/bookViewer/HRBookTOCFns.jsp • /hr/modules/com/hyperion/reporting/web/bookViewer/HRBookPdf.jsp
Data Relationship Management	/drm-migration-client
Calculation Manager	• /calcmgr/importexport.postExport.do • /calcmgr/common.performAction.do • /calcmgr/lcm.performAction.do* • /calcmgr/lcm.performAction.do/*
Administration Services	• /eas • /easconsole • /easdocs
Financial Management	• /hfm/EIE/EIEListener.asp • /hfmapplicationservice • /oracle-epm-fm-webservices • /hfmlcmservice
Financial Close Management	• /FCC-DataModel-context-root • /oracle-epm-erpi-webservices/* • /ARM-DataModel-context-root • /oracle-epm-erpi-webservices/** • /arm/batch/armbatchexecutionservlet • /ARM-DataModel-context-root

Tabella 3-2 (Cont.) Risorse di EPM System da non proteggere

Prodotto EPM System	Contesti da cui rimuovere la protezione
Integrated Operational Planning	• /interlace/services/ • /interlace/services/* • /interlace/services/.* • /interlace/services/.../* • /interlace/anteros • /interlace/anteros/* • /interlace/anteros/.* • /interlace/anteros/.../* • /interlace/interlace • /interlace/interlace/* • /interlace/interlace/.* • /interlace/interlace/.../* • /interlace/WebHelp • /interlace/WebHelp/* • /interlace/WebHelp/.* • /interlace/WebHelp/.../* • /interlace/html • /interlace/html/* • /interlace/html/.* • /interlace/html/.../* • /interlace/email-book • /interlace/email-book/* • /interlace/email-book/.* • /interlace/email-book/.../*
Profitability and Cost Management	• /profitability/cesagent • /profitability/lcm • /profitability/control • /profitability/ApplicationListener • /profitability/HPMApplicationListener
Oracle Essbase	• /essbase/agent/.../* • /essbase/jet/logout.html • /essbase/jet/.+\.(js|css|gif|jpe?g|png)$
FDMEE	• /aif/services/FDMRuleService • /aif/services/RuleService • /aif/LCMServlet

Accesso SSO basato su intestazione con prodotti di gestione delle identità

Prerequisiti

- Deve essere presente un'istanza di Oracle Enterprise Performance Management System completamente configurata. Il server directory del prodotto di gestione delle identità deve essere configurato in EPM System come directory utenti per autorizzare gli utenti.

- Deve essere presente un prodotto di gestione delle identità (Microsoft Azure AD, Okta e così via) completamente configurato che supporti l'autenticazione basata su intestazione.

La configurazione di EPM System per l'accesso SSO basato su intestazione con un prodotto di gestione delle identità compatibile comporta l'esecuzione dei processi generici descritti di seguito. Poiché i passi specifici da eseguire dipendono dal prodotto in uso, per la procedura dettagliata fare riferimento ai manuali del prodotto di gestione delle identità di cui si dispone.

Per i passi dettagliati di configurazione dell'autenticazione basata su intestazione con Oracle Identity Cloud Services, fare riferimento alla sezione Configurazione di EPM System per l'accesso SSO basato su intestazione con Oracle Identity Cloud Services.

1. Registrare EPM System come applicazione aziendale nel prodotto di gestione delle identità. Questo passo consente all'amministratore della gestione delle identità di configurare l'autenticazione nell'applicazione aziendale con le funzioni supportate, ad esempio l'autenticazione con più fattori.
   Utilizzare il nome di dominio completamente qualificato (FQDN) del gateway seguito da `workspace/index.jsp` (ad esempio, `https://gateway.server.example.com:443/workspace/index.jsp`) come URL dell'applicazione aziendale per EPM System.

   Configurare l'applicazione aziendale EPM System per propagare un'intestazione HTTP. È possibile scegliere qualsiasi nome di intestazione non riservato come nome dell'intestazione HTTP. Il valore dell'intestazione deve essere la proprietà che identifica in modo univoco gli utenti di EPM System.
2. Installare, configurare e registrare un gateway applicazione per essere certi che l'applicazione aziendale inoltri solo le richieste autenticate a EPM System.
   Utilizzare le impostazioni di configurazione riportate di seguito.
   - FQDN del server gateway (ad esempio, `gateway.server.example.com:443`) come punto di accesso
   - FQDN di EPM System (ad esempio, `epm.server.example.com:443`) come risorsa alla quale devono essere inoltrate le richieste HTTP(S) autenticate
3. Abilitare l'accesso SSO in EPM System per rispettare le intestazioni HTTP(S) propagate dal gateway applicazione. Per informazioni dettagliate, vedere Impostazione delle opzioni di sicurezza.
   Per abilitare l'accesso SSO, procedere come segue.
   a. Accedere a Oracle Hyperion Shared Services Console come amministratore di sistema. Fare riferimento alla sezione Avvio di Shared Services Console.
   b. Selezionare **Amministrazione**, quindi **Configura directory utenti**.
   c. Fare clic su **Opzioni sicurezza**.
   d. Nella sezione **Configurazione Single Sign-On** eseguire i passi sotto riportati.
      i. Selezionare la casella di controllo **Abilita SSO**.
      ii. Dall'elenco a discesa **Provider o agente di sicurezza SSO** selezionare **Altro**.
      iii. Dall'elenco a discesa **Meccanismo SSO** selezionare **Intestazione HTTP customizzata** e quindi specificare il nome dell'intestazione che l'agente di sicurezza passa a EPM System.
   e. Fare clic su **OK**.
4. Aggiornare l'impostazione Invia URL disconnessione di Oracle Hyperion Enterprise Performance Management Workspace specificando l'URL della pagina Web che si desidera venga visualizzata agli utenti quando eseguono la disconnessione da EPM System.

Per aggiornare l'impostazione Invia URL disconnessione in EPM Workspace, procedere come segue.

a. Accedere a EPM Workspace come amministratore di sistema. Fare riferimento alla sezione Accesso a EPM Workspace.

b. Selezionare **Naviga**, quindi **Impostazioni area di lavoro** e infine **Impostazioni server**.

c. In **Impostazioni server Workspace** impostare **Invia URL disconnessione** sull'URL della pagina Web che si desidera venga visualizzata agli utenti quando eseguono la disconnessione da EPM System.

d. Fare clic su **OK**.

5. Riavviare Oracle Hyperion Foundation Services e tutti i server gestiti di EPM System.

Configurazione di EPM System per l'accesso SSO basato su intestazione con Oracle Identity Cloud Services

In questo scenario Oracle Identity Cloud Services autentica gli utenti di Oracle Enterprise Performance Management System e propaga le intestazioni HTTP necessarie per abilitare SSO.

In questa sezione vengono illustrati i passi da eseguire per impostare e configurare EPM System per supportare SSO con Oracle Identity Cloud Services. È possibile estrapolare questi passi per supportare l'autenticazione basata su intestazione di EPM System con qualsiasi sistema di gestione delle identità (ad esempio, Azure AD) o provider IaaS (Infrastructure as a Service) che supporti questo tipo di autenticazione.

Il flusso di lavoro concettuale è il seguente.

- Un'applicazione gateway che funge da proxy inverso protegge i componenti di EPM System limitando l'accesso alla rete non autenticato.
- L'applicazione gateway intercetta le richieste HTTP(S) dirette ai componenti di EPM System e garantisce che il prodotto di gestione delle identità autentichi gli utenti prima che le richieste vengano inoltrate ai componenti di EPM System.
- Durante l'inoltro delle richieste ai componenti di EPM System, l'applicazione gateway propaga l'identità dell'utente autenticato al componente di EPM System mediante richieste con intestazione HTTP.

Prerequisiti e URL di esempio

Per stabilire l'accesso SSO basato su intestazione con Oracle Identity Cloud Services, procedere come segue.

- Deve essere presente un'istanza di Oracle Enterprise Performance Management System completamente configurata.
- Un host o un contenitore con un'istanza di Oracle App Gateway completamente configurata, che funga da proxy inverso per proteggere EPM System limitando l'accesso non autorizzato.
  Oracle App Gateway deve essere configurato in modo da intercettare le richieste HTTP dirette ai componenti di EPM System e garantire che gli utenti vengano autenticati da Oracle Identity Cloud Services prima che le richieste vengano

inoltrate a EPM System. Durante l'inoltro delle richieste ai componenti di EPM System, Oracle App Gateway deve propagare l'identità dell'utente autenticato mediante richieste con intestazione HTTP.

- Accesso da amministratore di dominio a Oracle Identity Cloud Services.

In questa discussione vengono utilizzati gli URL di esempio riportati di seguito.

- URL di base del nome di dominio completamente qualificato (FQDN) del server Oracle Identity Cloud Services (provider di identità): `https://identity.server.example.com:443/`
- FQDN del server Oracle App Gateway (che ospita l'applicazione gateway): `https://gateway.server.example.com:443/`
- URL dell'applicazione aziendale per EPM System. Si tratta dell'FQDN del server Oracle App Gateway seguito da `workspace/index.jsp`: `https://gateway.server.example.com:443/workspace/index.jsp`

> **Note:**
>
> Oracle Identity Cloud Services e Oracle App Gateway sono configurati con il supporto HTTPS. Il supporto HTTPS per EPM System è facoltativo.
> In questa discussione si presuppone che EPM System sia stato configurato con il supporto HTTPS.

Abilitazione dell'autenticazione basata su intestazione per EPM System

L'abilitazione dell'autenticazione basata su intestazione per Oracle Enterprise Performance Management System comporta l'esecuzione dei passi sotto riportati.

- Aggiunta dell'applicazione EPM System e del gateway a Oracle Identity Cloud Services
- Configurazione del gateway applicazione
- Configurazione della directory utenti per l'autorizzazione
- Abilitazione dell'SSO in EPM System
- Aggiornamento delle impostazioni di EPM Workspace

Aggiunta dell'applicazione EPM System e del gateway a Oracle Identity Cloud Services

Per impostare l'autenticazione basata su intestazione, è necessario creare Oracle Enterprise Performance Management System come applicazione aziendale.

Aggiungere EPM System come applicazione aziendale in Oracle Cloud Identity Console

Per aggiungere EPM System come applicazione aziendale, procedere come segue.

1. Accedere a Oracle Cloud Identity Console come amministratore di dominio.
   a. Utilizzando un browser, passare alla pagina Web all'indirizzo `https://www.oracle.com/cloud/sign-in.html`.

b. Immettere il nome del proprio account Oracle Fusion Cloud EPM.

c. Nella pagina Accesso all'account Oracle Fusion Cloud EPM immettere il proprio nome utente e la propria password, quindi fare clic su **Accedi**.

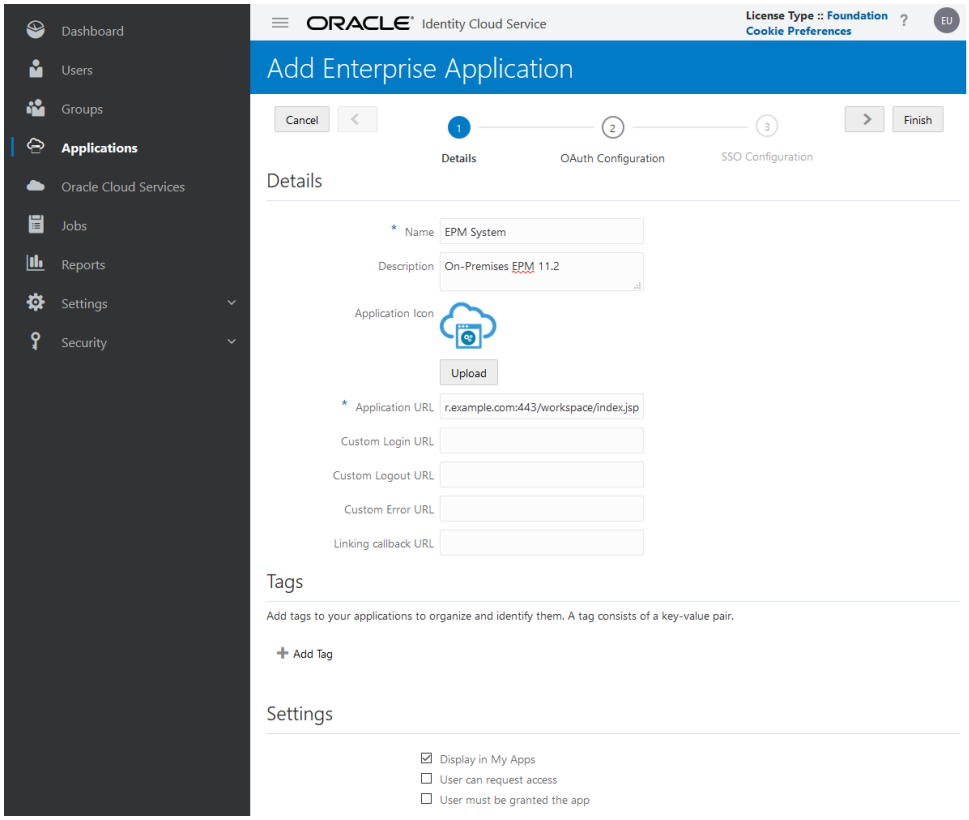
d. Nel **cassetto di navigazione** fare clic su **Utenti** e quindi su **Identità (principale)**.

e. Fare clic su **Identity Console**.

2. Aggiungere EPM System come applicazione aziendale.

a. Nel cassetto di navigazione fare clic su **Applicazioni**.

b. Fare clic su **Aggiungi** e quindi su **Applicazione aziendale**.



3. Aggiungere i dettagli dell'applicazione procedendo come segue.

a. In **Nome** immettere un nome univoco per identificare l'applicazione aziendale EPM System.

b. Immettere una descrizione facoltativa.

c. Facoltativamente, caricare un'icona dell'applicazione per EPM System. Fare clic su **Carica** per selezionare e caricare l'icona.

d. In **URL applicazione** immettere l'URL di avvio al quale il gateway deve reindirizzare gli utenti. Si tratta dell'FQDN di Oracle App Gateway seguito da `workspace/index.jsp`, che è il contesto dell'applicazione EPM System.

e. In **Impostazioni** selezionare **Visualizza nelle applicazioni personali** per visualizzare l'applicazione aziendale EPM System nella scheda

Configurazione SSO della pagina **Applicazioni personali** in Oracle Cloud Identity Console.

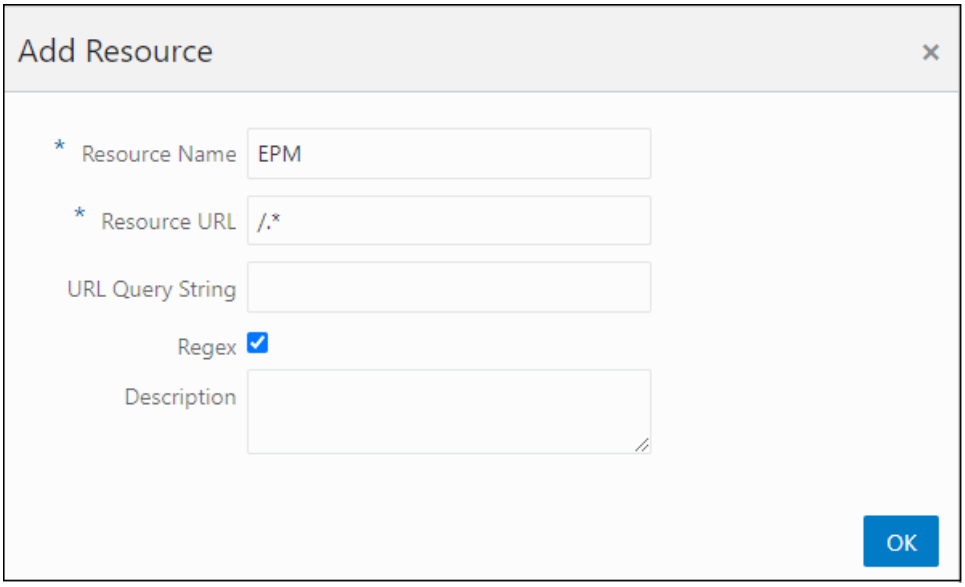
f. Fare clic su **Avanti**.

4. Specificare i dettagli della configurazione SSO.

   a. Fare clic su **Configurazione SSO**.

   b. Aggiungere una risorsa per l'applicazione aziendale.
   In **Configurazione SSO** espandere **Risorse**.

      i. Fare clic su **Aggiungi**.



      ii. Specificare un nome univoco per la risorsa.

      iii. In **URL risorsa** immettere `/.*`.

      iv. Selezionare la casella di controllo **Regex**.

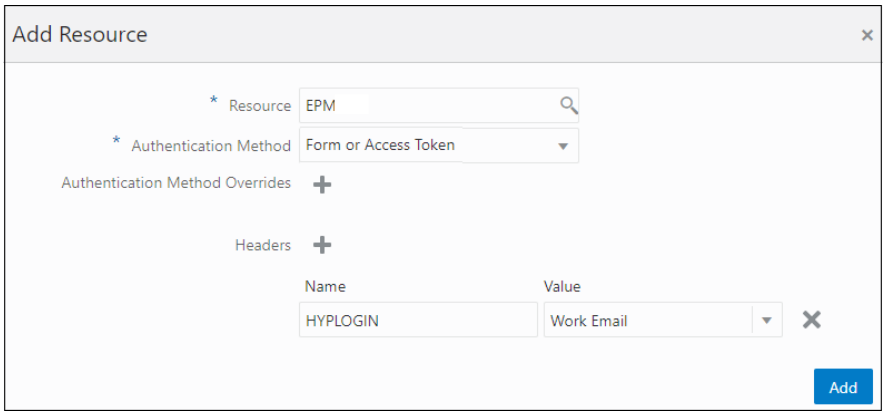
      v. Fare clic su **OK**.

      vi. In **Configurazione SSO** espandere **Risorse**.

   c. Aggiungere un criterio di autenticazione.
   In **Configurazione SSO** espandere **Criterio di autenticazione**.

      i. Selezionare le caselle di controllo **Consenti CORS** e **Richiedi cookie sicuri**.

      ii. In **Risorse gestite** fare clic su **Aggiungi** e definire **Form o token di accesso** come metodo di autenticazione per la risorsa SSO.



iii. In **Risorsa** selezionare la risorsa SSO aggiunta nel passo precedente.

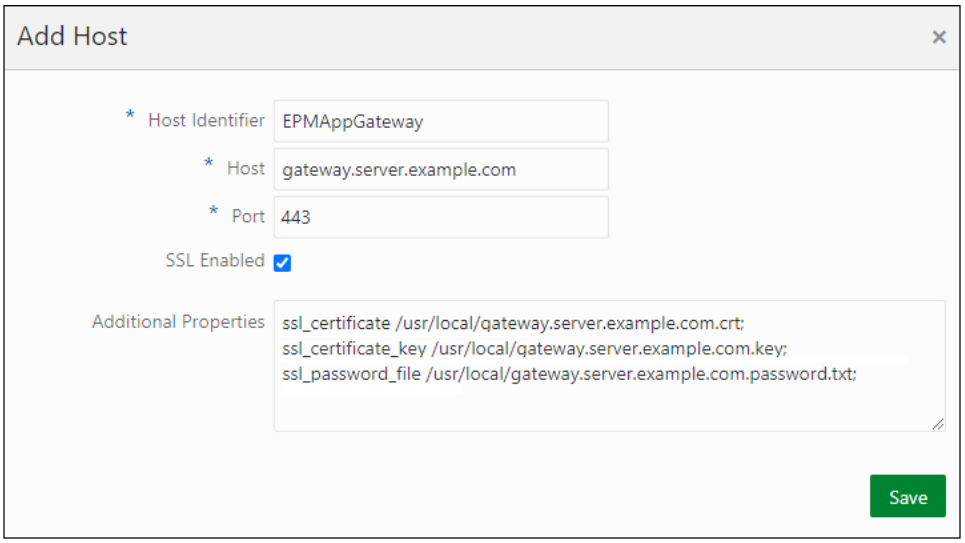
iv. Espandere **Intestazioni**.

v. Immettere il nome dell'intestazione HTTP che verrà propagata a EPM System.
Il nome predefinito per l'intestazione di autenticazione è `HYPLOGIN`. È tuttavia possibile utilizzare qualsiasi nome si desideri.

vi. In **Valore** selezionare la proprietà che identifica in modo univoco gli utenti di EPM System.
Il valore di questo campo deve corrispondere all'identità dell'utente in EPM System. Ad esempio, se l'identità dell'utente in EPM System è l'ID e-mail, selezionare Email ufficio come valore.

vii. Fare clic su **Salva**.

5. Fare clic su **Fine** per creare l'applicazione aziendale.
6. Fare clic su **Attiva** per abilitare l'applicazione.
7. Registrare un gateway applicazione, quindi impostare l'host e l'applicazione per EPM System.
   a. Nel **cassetto di navigazione** fare clic su **Sicurezza** e quindi su **Gateway applicazioni**.
   b. Fare clic su **Aggiungi**.
   c. In **Dettagli** immettere un nome univoco per il gateway e una descrizione facoltativa.
   d. Fare clic su **Avanti** per visualizzare la schermata Host.
   e. Aggiungere un host del gateway applicazione per EPM System.
      i. Nella schermata Host fare clic su **Aggiungi**.



ii. In **Identificativo host** immettere `EPMAppGateway`.

iii. In **Host** immettere il nome di dominio completamente qualificato del computer che ospita il server del gateway applicazione, ad esempio `gateway.server.example.com`.

iv. In **Porta** immettere la porta sulla quale il server del gateway applicazione risponde alle richieste HTTPS.

v. Selezionare la casella di controllo **SSL abilitato**.

vi. In **Proprietà aggiuntive** immettere quanto segue.

- Posizione del certificato SSL
- Chiave del certificato SSL
- File della password SSL (se necessario)

Per informazioni dettagliate, fare riferimento alla sezione "Registrare un gateway applicazione" in "Impostazione di un gateway applicazione" in *Amministrazione di Oracle Identity Cloud Service*.

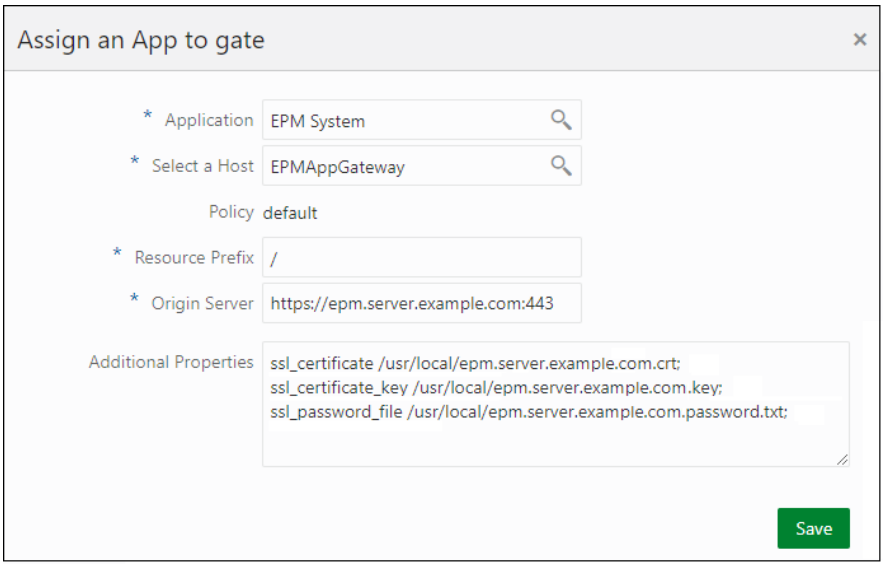
vii. Fare clic su **Salva**.

viii. Fare clic su **Avanti** per visualizzare la schermata Applicazioni.

f. Aggiungere l'applicazione aziendale EPM System al gateway applicazione.

i. In **Applicazioni** fare clic su **Aggiungi**.

ii. In **Applicazione** selezionare l'applicazione aziendale EPM System aggiunta in precedenza a Oracle Cloud Identity Console.



iii. In **Seleziona un host** selezionare `EPMAppGateway` (l'host EPM System aggiunto al gateway applicazione).

iv. In **Prefisso risorsa** immettere `/` per inoltrare tutte le richieste all'host EPM System.

v. In **Server di origine** immettere il nome di dominio completamente qualificato del computer che ospita Oracle Hyperion Enterprise Performance Management Workspace e il numero di porta utilizzato da EPM Workspace.

vi. Fare clic su **Salva**.

8. Registrare l'ID client e il segreto client del gateway applicazione. Questi valori sono necessari per impostare il gateway applicazione.

   a. Nel **cassetto di navigazione** fare clic su **Sicurezza** e quindi su **Gateway applicazioni**.

   b. Fare clic sul nome del gateway aggiunto per l'applicazione aziendale EPM System.

   c. Copiare l'ID client (una stringa alfanumerica) in un editor di testo.

   d. Fare clic su **Mostra segreto** per visualizzare il codice segreto client.

   e. Copiare il segreto client (una stringa alfanumerica) nell'editor di testo.

   f. Salvare il file di testo.

> **Note:**
>
> È necessario riavviare il server del gateway applicazione ogni volta che si aggiorna la configurazione di Oracle Identity Cloud Services. Per avviare e arrestare il server del gateway applicazione, fare riferimento alla sezione Avvio e arresto del gateway applicazione.

Configurazione del gateway applicazione

Per informazioni dettagliate, fare riferimento alla sezione "Impostazione di un gateway applicazione" in *Amministrazione di Oracle Identity Cloud Service*.

Per configurare il server del gateway applicazione sono necessari l'ID client e il segreto client registrati nella sezione precedente.

Configurazione della directory utenti per l'autorizzazione

Alcuni prodotti di gestione delle identità, ad esempio Oracle Identity Cloud Services e Microsoft Azure, non possono essere configurati direttamente come directory utenti in Oracle Enterprise Performance Management System. È possibile configurare tali prodotti con Oracle Unified Directory o Oracle Virtual Directory e quindi configurare quest'ultimo come directory utenti in EPM System. Per i passi dettagliati di configurazione delle directory utenti, fare riferimento alla sezione Configurazione delle directory utenti.

Abilitazione dell'SSO in EPM System

È necessario configurare le opzioni di sicurezza in Oracle Enterprise Performance Management System per abilitare SSO. Per istruzioni dettagliate, vedere Impostazione delle opzioni di sicurezza.

Per abilitare l'accesso SSO, procedere come segue.

1. Accedere a Oracle Hyperion Shared Services Console come amministratore di sistema. Fare riferimento alla sezione Avvio di Shared Services Console.
2. Selezionare **Amministrazione**, quindi **Configura directory utenti**.
3. Fare clic su **Opzioni sicurezza**.
4. Nella sezione **Configurazione Single Sign-On** eseguire i passi sotto riportati.
    a. Selezionare la casella di controllo **Abilita SSO**.
    b. Dall'elenco a discesa **Provider o agente di sicurezza SSO** selezionare **Altro**.
    c. Dall'elenco a discesa **Meccanismo SSO** selezionare **Intestazione HTTP customizzata** e quindi specificare il nome dell'intestazione che l'agente di sicurezza passa a EPM System (`HYPLOGIN` o il nome customizzato specificato durante l'aggiunta della risorsa per l'applicazione aziendale in Oracle Cloud Identity Console).
5. Fare clic su **OK**.

> **Note:**
>
> Verificare il riavvio di tutti i servizi EPM System Services dopo qualsiasi modifica della configurazione SSO.

Aggiornamento delle impostazioni di EPM Workspace

1. Accedere a Oracle Hyperion Enterprise Performance Management Workspace come amministratore di sistema. Fare riferimento alla sezione Accesso a EPM Workspace.
2. Selezionare **Naviga**, quindi **Impostazioni area di lavoro** e infine **Impostazioni server**.

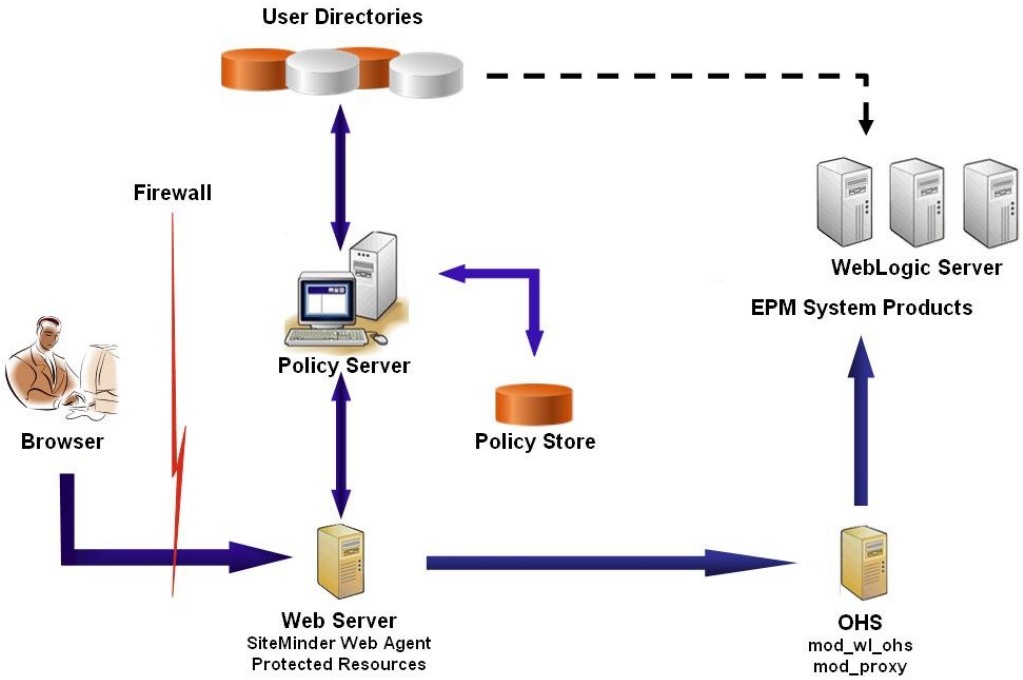
3. In **Impostazioni server Workspace** impostare **Invia URL disconnessione** sull'URL della pagina Web che si desidera venga visualizzata agli utenti quando eseguono la disconnessione da Oracle Enterprise Performance Management System.
4. Fare clic su **OK**.
5. Riavviare Oracle Hyperion Foundation Services e tutti i componenti di EPM System.

SSO con SiteMinder

SiteMinder è una soluzione esclusivamente per il Web. Le applicazioni desktop e i relativi add-in, ad esempio, Microsoft Excel e Report Designer, non possono utilizzare l'autenticazione mediante SiteMinder Tuttavia, Oracle Smart View for Office può utilizzare l'autenticazione SiteMinder.

Flusso del processo

La figura che segue è una panoramica dell'accesso SSO abilitato per SiteMinder:



Viene descritto di seguito il processo Single Sign-On con SiteMinder.

1. Gli utenti tentano di accedere a una risorsa Oracle Enterprise Performance Management System protetta da SiteMinder. Utilizzano un URL che li connette al server Web che funge da front end per il server dei criteri SiteMinder, ad esempio `http://WebAgent_Web_Server_Name:WebAgent_Web_ServerPort/interop/index.jsp`.
2. Il server Web reindirizza gli utenti al server dei criteri, che richiede loro le credenziali. Dopo aver verificato le credenziali a fronte delle directory utenti configurate, il server dei criteri passa le credenziali al server Web che ospita l'agente Web di SiteMinder.

3. Il server Web che ospita l'agente Web di SiteMinder reindirizza la richiesta al computer Oracle HTTP Server che funge da front end per EPM System. Oracle HTTP Server reindirizza gli utenti all'applicazione richiesta distribuita in Oracle WebLogic Server.
4. Il componente di EPM System controlla le informazioni di assegnazione ruoli e fornisce il contenuto. Per il corretto funzionamento di questo processo, le directory utenti utilizzate da SiteMinder per l'autenticazione degli utenti devono essere configurate come directory utenti esterne in EPM System. Queste directory devono essere configurate come sicure.

Considerazioni speciali

SiteMinder è una soluzione esclusivamente per il Web. Le applicazioni desktop e i relativi add-in, ad esempio, Microsoft Excel e Report Designer, non possono utilizzare l'autenticazione mediante SiteMinder Tuttavia, Smart View può utilizzare l'autenticazione SiteMinder.

Prerequisiti

1. Un'installazione di SiteMinder completamente funzionante contenente i componenti elencati di seguito.
   - Server dei criteri SiteMinder in cui sono definiti i criteri e gli oggetti dell'agente
   - Agente Web di SiteMinder installato nel server Web che funge da front end per il server dei criteri SiteMinder
2. Una distribuzione di EPM System completamente funzionante.
   Quando si configura il server Web per i componenti di EPM System, EPM System Configurator configura `mod_wl_ohs.conf` per inviare tramite proxy le richieste al server WebLogic.

Abilitazione dell'agente Web di SiteMinder

L'agente Web è installato in un server Web che intercetta le richieste per le risorse EPM System. Se utenti non autenticati tentano di accedere a risorse EPM System protette, l'agente Web chiederà loro di specificare le credenziali SSO. Quando un utente viene autenticato, il server dei criteri ne aggiunge il nome di accesso che viene trasportato dall'intestazione. La richiesta HTTP viene quindi passata al server Web EPM System, che reindirizza le richieste. I componenti di EPM System estraggono dalle intestazioni le credenziali degli utenti autenticati.

SiteMinder supporta l'accesso SSO nei prodotti EPM System in esecuzione su piattaforme di server Web eterogenee. Se i prodotti EPM System utilizzano server Web diversi, è necessario garantire il passaggio del cookie di SiteMinder tra i server Web presenti nello stesso dominio. A tale scopo, specificare il dominio delle applicazioni EPM System appropriato come valore della proprietà `Cookiedomain` nel file `WebAgent.conf` di ciascun server Web.

Fare riferimento alla sezione "Configurazione degli agenti Web" nel *guida degli agenti di Netegrity SiteMinder*.

> **Nota:**
>
> Poiché per proteggere il proprio contenuto Oracle Hyperion Shared Services utilizza l'autenticazione di base, questa deve essere configurata nel server Web che intercetta le richieste per Shared Services affinché l'accesso SSO con SiteMinder possa essere supportato.

Per configurare l'agente Web, eseguire la configurazione guidata dell'agente Web di SiteMinder (eseguendo *WEBAGENT_HOME*/install_config_info/nete-wa-config, ad esempio C:\netegrity\webagent\install_config_info\nete-wa-config.exe in Windows). Il processo di configurazione crea un file WebAgent.conf per il server Web SiteMinder.

Per abilitare l'agente Web di SiteMinder, procedere come segue.

1. Aprire WebAgent.conf con un editor di testo. La posizione di questo file dipende dal server Web in uso.
2. Impostare il valore della proprietà enableWebAgent su Yes.

   ```
   enableWebAgent="YES"
   ```

3. Salvare e chiudere il file di configurazione dell'agente Web.

Esempio 3-1 Configurazione del server dei criteri di SiteMinder

Un amministratore di SiteMinder può configurare il server dei criteri per abilitare il Single Sign-On per i prodotti EPM System.

Il processo di configurazione prevede le operazioni descritte di seguito.

- Creazione di un agente Web di SiteMinder e aggiunta di oggetti di configurazione appropriati per il server Web SiteMinder.
- Creazione di un realm per ogni risorsa EPM System da proteggere e aggiunta dell'agente Web al realm. Fare riferimento alla sezione Risorse da proteggere.
- Nel realm creato per le risorse EPM System protette, creare realm per le risorse da cui è stata rimossa la protezione. Fare riferimento alla sezione Risorse da cui rimuovere la protezione.
- Creazione di un riferimento a un'intestazione HTTP. L'intestazione deve fornire il valore di Login Attribute alle applicazioni EPM System. Fare riferimento alla sezione "Configurazione di OID, Active Directory e altre directory utenti basate su LDAP" nel manuale *Oracle Enterprise Performance Management System User Security Administration Guide (in lingua inglese)* per una breve descrizione di Login Attribute.
- Creazione di regole nei realm con Get, Post e Put come azioni dell'agente Web.
- Creazione di un attributo di risposta con hyplogin=<%userattr="SM_USERLOGINNAME"%> come valore.
- Creazione di un criterio, assegnazione dell'accesso alle directory utenti e aggiunta delle regole create per EPM System all'elenco dei membri correnti.
- Impostazione delle risposte per le regole create per i componenti di EPM System.

Esempio 3-2 Configurazione del server Web SiteMinder per l'inoltro delle richieste al server Web EPM System

Configurare il server Web che ospita l'agente Web di SiteMinder in modo da inoltrare le richieste di utenti autenticati (contenenti l'intestazione che identifica l'utente) al server Web EPM System.

Per i server Web basati su Apache, utilizzare direttive simili alla seguente per inoltrare le richieste autenticate:

```
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
```

In questa direttiva, sostituire *EPM_WEB_SERVER* ed *EPM_WEB_SERVER_PORT* con i valori effettivi per il proprio ambiente.

Esempio 3-3 Abilitazione di SiteMinder in EPM System

L'integrazione con SiteMinder richiede l'abilitazione dell'autenticazione di SiteMinder per i prodotti di EPM System. Fare riferimento alla sezione Configurazione di EPM System per l'SSO.

Single Sign-On con Kerberos

Panoramica

I prodotti Oracle Enterprise Performance Management System supportano SSO con Kerberos se il server applicazioni in cui sono ospitati i prodotti EPM System è impostato per l'autenticazione Kerberos.

Kerberos è un servizio di autenticazione sicuro in cui ciascun client Kerberos considera attendibili e quindi valide le identità degli altri client Kerberos, ovvero utenti, servizi di rete e così via.

Di seguito viene illustrato cosa si verifica quando un utente accede a un prodotto EPM System.

1. Da un computer Windows l'utente esegue l'accesso a un dominio Windows, che è anche un realm Kerberos.
2. Utilizzando un browser configurato per l'utilizzo dell'Autenticazione integrata di Windows, l'utente tenta di accedere ai prodotti di EPM System in esecuzione sul server applicazioni.
3. Il server applicazioni (Negotiate Identity Asserter) intercetta la richiesta e ottiene il token SPNEGO, ovvero Simple and Protected GSSAPI (Generic Security Services API) Negotiation Mechanism, con il ticket Kerberos dall'intestazione di autorizzazione del browser.
4. Asserter convalida l'identità dell'utente inclusa nel token a fronte della relativa area memorizzazione identità per passare le informazioni sull'utente al prodotto EPM System. Il prodotto EPM System convalida il nome utente a fronte di un'istanza di Active Directory. Il prodotto EPM System emette un token SSO che supporta SSO in tutti i prodotti EPM System.

Limitazioni relative al supporto

L'SSO con Kerberos è supportato per tutti i prodotti di EPM System con le seguenti eccezioni:

- SSO con Kerberos non è supportato per i client thick diversi da Oracle Smart View for Office.
- Smart View supporta l'integrazione con Kerberos solo per i provider di Oracle Essbase, Oracle Hyperion Planning e Oracle Hyperion Financial Management.

Presupposti

In questo documento, contenente le procedure di configurazione di Kerberos a livello di applicazione, si presuppone che si conosca la configurazione di Kerberos a livello di sistema. Prima di iniziare tali procedure, verificare che siano soddisfatti i prerequisiti per questi task.

All'interno del documento si presuppone che si stia operando in un ambiente di rete abilitato per Kerberos e completamente funzionante in cui i computer client Windows sono configurati per l'autenticazione Kerberos.

- L'istanza aziendale di Active Directory è configurata per l'autenticazione Kerberos. Fare riferimento alla sezione documentazione di Microsoft Windows Server.
- I browser utilizzati per accedere ai prodotti EPM System sono configurati per eseguire la negoziazione con ticket Kerberos.
- Nella sincronizzazione dell'ora vi è un disallineamento di cinque minuti al massimo tra il computer KDC e il computer client. Fare riferimento alla pagina Web relativa agli errori di autenticazione causati da clock non sincronizzati all'indirizzo http://technet.microsoft.com/en-us/library/cc780011(WS.10).aspx.

SSO con Kerberos mediante WebLogic Server

SSO (Single Sign-On) con Kerberos mediante Oracle WebLogic Server utilizza Negotiate Identity Asserter per negoziare e decodificare i token SPNEGO allo scopo di abilitare l'accesso SSO con i client Microsoft. WebLogic Server decodifica i token SPNEGO per ottenere il ticket Kerberos, quindi convalida e mappa il ticket su un utente di WebLogic Server. È possibile utilizzare l'autenticatore di Active Directory di WebLogic Server con Negotiate Identity Asserter per configurare Active Directory come directory utenti per gli utenti di WebLogic Server.

Quando il browser richiede l'accesso a un prodotto EPM System, KDC emette un ticket Kerberos per il browser, il quale crea un token SPNEGO contenente i tipo di token GSS supportati. Negotiate Identity Asserter decodifica il token SPNEGO e utilizza le API GSS (GSSAPI) per accettare il contesto di sicurezza. L'identità dell'utente che ha iniziato la richiesta viene mappata su un nome utente e passata nuovamente a WebLogic Server. WebLogic Server inoltre determina i gruppi a cui appartiene l'utente. A questo punto, il prodotto EPM System richiesto viene reso disponibile per l'utente.

> **Nota:**
>
> Per accedere ai prodotti EPM System in esecuzione in WebLogic Server, gli utenti devono utilizzare un browser che supporti SPNEGO, ad esempio Internet Explorer o Firefox.

Utilizzando l'ID utente ottenuto dal processo di autenticazione, il processo di autorizzazione del prodotto di EPM System verifica la presenza dei dati dell'assegnazione ruoli. L'accesso al prodotto EPM System è limitato in base ai dati dell'assegnazione ruoli.

Procedure di WebLogic Server per supportare l'autenticazione Kerberos

Per supportare l'autenticazione Kerberos, un amministratore deve completare i task seguenti.

- Creare il dominio WebLogic per EPM System. Fare riferimento alla sezione Creazione del dominio WebLogic per EPM System.
- Creare un provider di autenticazione. Fare riferimento alla sezione Creazione di un provider di autenticazione LDAP in WebLogic Server.
- Creare un Negotiate Identity Asserter. Fare riferimento alla sezione Creazione di un Negotiate Identity Asserter.
- Creare un'identificazione Kerberos. Fare riferimento alla sezione Creazione di un'identificazione Kerberos per WebLogic Server.
- Aggiornare le opzioni JVM per Kerberos. Fare riferimento alla sezione Aggiornamento delle opzioni JVM per Kerberos.
- Configurare i criteri di autorizzazione. Fare riferimento alla sezione Configurazione dei criteri di autorizzazione.
- Distribuire e utilizzare SSODiag per verificare che WebLogic Server sia pronto a supportare SSO con Kerberos per EPM System. Fare riferimento alla sezione Utilizzo di SSODiag per testare l'ambiente Kerberos.

Creazione del dominio WebLogic per EPM System

In genere, i componenti di EPM System vengono distribuiti nel dominio WebLogic `EPMSystem` (la posizione predefinita è *`MIDDLEWARE_HOME`*`/user_projects/domains/EPMSystem`).

Per configurare il dominio WebLogic EPM System per l'autenticazione Kerberos, procedere come segue.

1. Installare i componenti di EPM System.
2. Distribuire solo Oracle Hyperion Foundation Services.
   La distribuzione di Foundation Services crea il dominio WebLogic EPM System predefinito.
3. Eseguire l'accesso a Oracle Hyperion Shared Services Console per verificare che la distribuzione di Foundation Services abbia avuto esito positivo. Fare riferimento alla sezione Avvio di Shared Services Console.

Creazione di un provider di autenticazione LDAP in WebLogic Server

Un amministratore di WebLogic Server crea il provider di autenticazione LDAP, che memorizza le informazioni su utenti e gruppi in un server LDAP esterno. Con WebLogic Server interagiscono i server LDAP conformi a LDAP v2 o v3. Consultare i documenti di riferimento riportati di seguito.

- Configurazione dei provider di autenticazione LDAP nella guida *Oracle Fusion Middleware Securing Oracle WebLogic Server* (in lingua inglese)
- Configurare i provider di autenticazione e di Identity Assertion nella *Guida in linea di Oracle Fusion Middleware Oracle WebLogic Server Administration Console*

Creazione di un Negotiate Identity Asserter

Il provider di Negotiate Identity Assertion abilita SSO con i client Microsoft. Esso decodifica i token SPNEGO per ottenere i token Kerberos, convalida i token Kerberos e mappa i token

sugli utenti di WebLogic. Il provider di Negotiate Identity Assertion, un'implementazione dell'interfaccia SSPI (Security Service Provider Interface) definita da WebLogic Security Framework, offre la logica necessaria per autenticare un client in base al token SPNEGO del client stesso.

- Configurazione di un provider di Negotiate Identity Assertion nella guida di *Oracle Fusion Middleware Securing Oracle WebLogic Server* (in lingua inglese)
- Configurare i provider di autenticazione e di Identity Assertion nella *Guida in linea di Oracle Fusion Middleware Oracle WebLogic Server Administration Console*

Durante la creazione del provider di Negotiate Identity Assertion, impostare l'opzione relativa al flag di controllo JAAS su `SUFFICIENT` per tutti gli autenticatori. Fare riferimento alla sezione "Impostazione del flag di controllo JAAS" nella Guida in linea di Oracle Fusion Middleware Oracle WebLogic Server Administration Console.

Creazione di un'identificazione Kerberos per WebLogic Server

Nel computer controller di dominio Active Directory, creare gli oggetti utente che rappresentano WebLogic Server e il server Web di EPM System, quindi mapparli sui nomi dell'entità servizio (SPN) che rappresentano l'istanza di WebLogic Server e il server Web in uso nel realm Kerberos. I client non sono in grado di individuare un servizio che non dispone di un SPN. È possibile memorizzare gli SPN in file keytab che vengono copiati nel dominio di WebLogic Server per essere utilizzati nel processo di accesso.

Per le procedure dettagliate, fare riferimento alla sezione Creazione di un'identificazione per WebLogic Server nella guida *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

Per creare un'identificazione Kerberos per WebLogic Server, procedere come segue.

1. Nel computer controller di dominio Active Directory, creare un account utente, ad esempio `epmHost`, per il computer che ospita il dominio di WebLogic Server.

   > **Nota:**
   >
   > Creare l'identificazione come un oggetto utente, non come un computer. Utilizzare il nome semplice del computer. Ad esempio, utilizzare `epmHost` se l'host è denominato `epmHost.example.com`.
   >
   > Prendere nota della password utilizzata durante la creazione dell'oggetto utente. Sarà necessaria per creare gli SPN.
   >
   > Non selezionare opzioni relative alla password, soprattutto l'opzione `User must change password at next logon`.

2. Modificare l'oggetto utente in modo che sia conforme al protocollo Kerberos. L'account deve richiedere la preautenticazione Kerberos.
   - Nella scheda **Account**, selezionare una cifratura da utilizzare.
   - Assicurarsi che non siano selezionate altre opzioni relative all'account, soprattutto `Do not require Kerberos pre-authentication`.
   - Poiché l'impostazione del tipo di cifratura potrebbe avere danneggiato la password dell'oggetto, reimpostare la password in modo che corrisponda a quella impostata durante la creazione dell'oggetto.

3. Nel computer che ospita il controller di dominio Active Directory, aprire una finestra del prompt dei comandi e passare alla directory in cui sono installati gli strumenti di supporto di Active Directory.
4. Creare e configurare gli SPN necessari.
   a. Utilizzando un comando simile al seguente, verificare che gli SPN siano associati all'oggetto utente (`epmHost`) creato nel passo 1 di questa procedura.

      ```
      setspn -L epmHost
      ```

   b. Utilizzando un comando simile al seguente, configurare l'SPN per WebLogic Server in Active Directory Domain Services e generare un file keytab contenente la chiave segreto condiviso.

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

5. Creare un file keytab nel computer che ospita WebLogic Server.
   a. Aprire un prompt dei comandi.
   b. Passare a *MIDDLEWARE_HOME*`/jdk/bin`.
   c. Eseguire un comando come il seguente:

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

   d. Quando viene richiesto di specificare una password, immettere quella impostata durante la creazione dell'utente nel passo 1 di questa procedura.
6. Copiare il file keytab nella directory di avvio all'interno del dominio WebLogic, ad esempio in `C:\Oracle\Middleware\user_projects\domains\EPMSystem`.
7. Verificare che l'autenticazione Kerberos funzioni correttamente.

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

   In questo comando, `account-name` indica l'entità Kerberos, ad esempio `HTTP/`*`epmHost.example.com@EXAMPLE.COM`*. L'output di questo comando deve essere simile a quello riportato di seguito:

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

Aggiornamento delle opzioni JVM per Kerberos

Fare riferimento alle sezioni Utilizzo degli argomenti di avvio per l'autenticazione Kerberos con WebLogic Server e Creazione di un file di accesso JAAS nel manuale *Oracle Fusion Middleware Securing Oracle WebLogic Server 11g Release 1 (10.3.1)* (in lingua inglese).

Se i server gestiti EPM System vengono eseguiti come servizi Windows, aggiornare il Registro di sistema di Windows per impostare le opzioni di avvio JVM.

Per aggiornare le opzioni di avvio JVM nel Registro di sistema di Windows, procedere come segue.

1. Aprire l'editor del Registro di sistema di Windows.

2. Selezionare **Computer**, **HKEY_LOCAL_MACHINE**, **Software**, **Soluzioni Hyperion**, **Foundationservices0** e infine **HyS9EPMServer_epmsystem1**.
3. Creare i valori stringa riportati di seguito.

> **Nota:**
>
> I nomi riportati nella tabella che segue sono forniti come esempio.

Tabella 3-3 Opzioni di avvio JVM per l'autenticazione Kerberos

Nome	Tipo	Dati
JVMOption44	REG_SZ	`-Djava.security.krb5.realm=`*`Active Directory Realm Name`*
JVMOption45	REG_SZ	`-Djava.security.krb5.kdc=`*`Active Directory host name or IP address`*
JVMOption46	REG_SZ	`-Djava.security.auth.login.config=`*`location of Kerberos login configuration file`*
JVMOption47	REG_SZ	`-Djavax.security.auth.useSubjectCredsOnly=false`

4. Aggiornare il valore DWORD JVMOptionCount in modo che rifletta le opzioni JVM (JVMOption) aggiunte (aggiungere 4 al valore decimale corrente).

Configurazione dei criteri di autorizzazione

Per informazioni sulla configurazione dei criteri di autorizzazione per gli utenti di Active Directory che accedono a EPM System, fare riferimento alla sezione Opzioni per proteggere le risorse di tipo applicazione Web ed EJB nella guida *Oracle Fusion Middleware Securing Resources Using Roles and Policies for Oracle WebLogic Server* (in lingua inglese).

Per la procedura di configurazione dei criteri campione, fare riferimento alla sezione Creazione dei criteri per SSODiag.

Utilizzo di SSODiag per testare l'ambiente Kerberos

SSODiag è un'applicazione Web di diagnostica che verifica se WebLogic Server nell'ambiente Kerberos in uso è pronto per supportare EPM System.

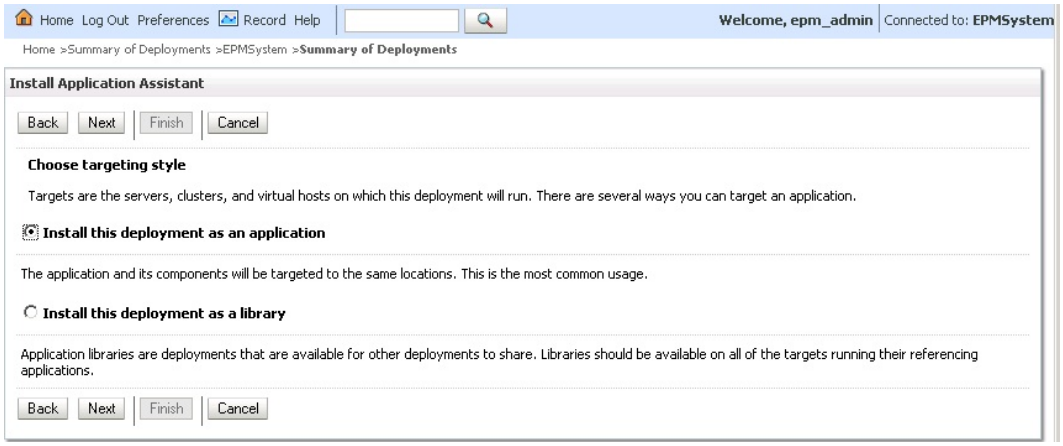
Distribuzione di SSODiag

Distribuire SSODiag utilizzando le credenziali di amministratore di WebLogic Server (il nome utente predefinito è `epm_admin`) specificate durante la distribuzione di Foundation Services.

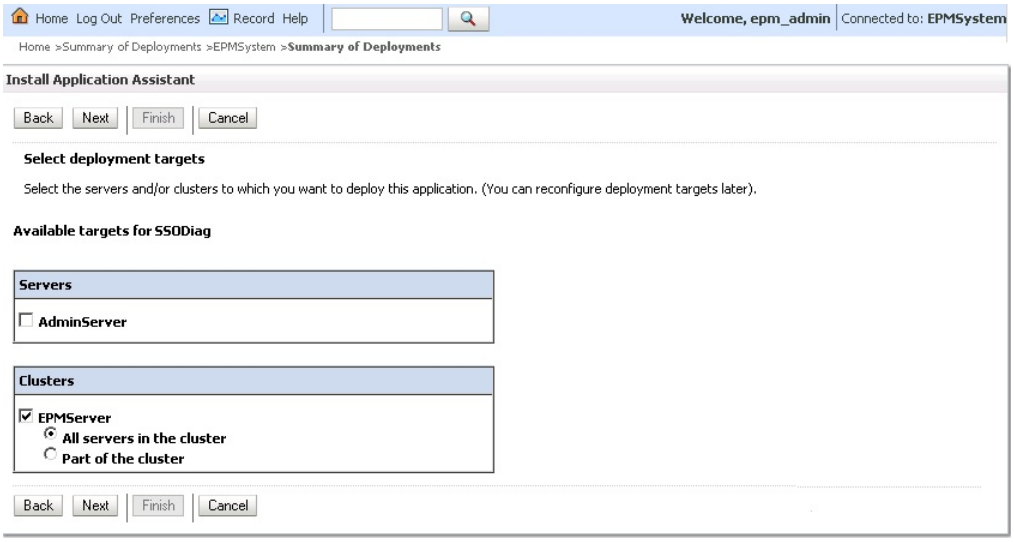
Per distribuire e configurare SSOdiag, procedere come segue.

1. Eseguire l'accesso alla console di amministrazione di WebLogic Server per il dominio di EPM System.
2. Nel Centro modifiche, selezionare **Blocca e modifica**.

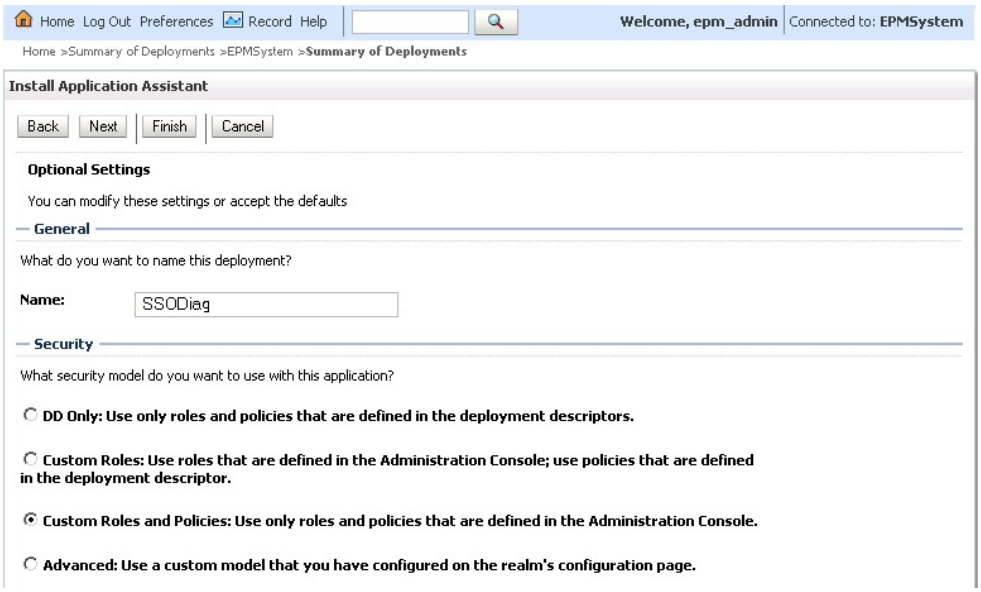
3. Da **EPMSystem** in **Struttura dominio**, fare clic su **Distribuzioni**.
4. In **Riepilogo delle distribuzioni**, fare clic su **Installa**.
5. In **Percorso**, selezionare *EPM_ORACLE_HOME*`/products/Foundation/AppServer/InstallableApps/common/SSODiag.war`.
6. Fare clic su **Avanti**.
7. In **Scegli stile di determinazione destinazioni**, assicurarsi che sia selezionata l'opzione **Installa questa distribuzione come applicazione**, quindi fare clic su **Avanti**.



8. In **Seleziona destinazioni distribuzione**, selezionare quanto segue, quindi fare clic su **Avanti**.
   - **EPMServer**
   - **Tutti i server nel cluster**



9. In **Impostazioni facoltative**, come modello di sicurezza selezionare **Ruoli e criteri personalizzati: vengono utilizzati solo i ruoli e i criteri definiti nella console di amministrazione**.



10. Fare clic su **Avanti**.
11. Nella schermata di revisione, selezionare l'opzione per rivedere la configurazione in un secondo momento.
12. Fare clic su **Fine**.
13. Nel Centro modifiche, selezionare **Attiva modifiche**.

Configurazione di Oracle HTTP Server per SSODiag

Aggiornare il file `mod_wl_ohs.conf` per configurare Oracle HTTP Server in modo che le richieste di URL di SSODiag vengano inoltrate a WebLogic Server.

Per configurare l'inoltro degli URL in Oracle HTTP Server, procedere come segue.

1. Aprire *EPM_ORACLE_INSTANCE*`/httpConfig/ohs/config/fmwconfig/components/OHS/ohs_component/mod_wl_ohs.conf` con un editor di testo.
2. Aggiungere una definizione `LocationMatch` per SSODiag:

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

   Nel campione precedente, `myServer` indica il computer host di Foundation Services e `28080` rappresenta la porta su cui Oracle Hyperion Shared Services resta in ascolto delle richieste.
3. Salvare e chiudere `mod_wl_ohs.conf`.
4. Riavviare Oracle HTTP Server.

Creazione dei criteri per SSODiag

Nella console di amministrazione di WebLogic Server creare un criterio per proteggere l'URL seguente di SSODiag:

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

In questo campione, *OHS_HOST_NAME* indica il nome del server che ospita Oracle HTTP Server e *PORT* indica la porta su cui Oracle HTTP Server resta in ascolto delle richieste.

Per creare i criteri per proteggere SSODiag, procedere come segue.

1. Nel Centro modifiche nella console di amministrazione di WebLogic Server per il dominio di EPM System, selezionare **Blocca e modifica**.
2. Selezionare **Distribuzioni**, **SSODiag**, quindi **Sicurezza**, **URLPatterns** e infine **Criteri**.
3. Creare i pattern di URL riportati di seguito.
   - `/`
   - `/index.jsp`
4. Modificare ogni pattern di URL creato procedendo come segue.
   a. Nell'elenco di pattern di URL in **Pattern di URL per applicazione Web standalone**, aprire il pattern (/) creato facendo clic su di esso.
   b. Selezionare **Aggiungi condizioni**.
   c. In **Lista di predicati**, selezionare **Utente**.
   d. Selezionare **Avanti**.
   e. In **Nome argomento utente**, immettere l'utente di Active Directory il cui account viene utilizzato per accedere a un desktop client configurato per l'autenticazione Kerberos (ad esempio, `krbuser1`), quindi selezionare **Aggiungi**. `krbuser1` è un utente desktop di Active Directory o Windows.
   f. Selezionare **Fine**.
5. Selezionare **Salva**.

Utilizzo di SSODiag per testare la configurazione di WebLogic Server per l'autenticazione Kerberos

Se la configurazione di WebLogic Server per l'autenticazione Kerberos funziona correttamente, nella pagina di *Oracle Hyperion Kerberos SSO diagnostic Utility V 1.0* viene visualizzato il messaggio seguente:

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

> **Attenzione:**
>
> Non configurare i componenti di EPM System per l'autenticazione Kerberos se SSODiag non riesce a recuperare il nome dell'entità Kerberos.

Per testare la configurazione di WebLogic Server per l'autenticazione Kerberos, procedere come segue.

1. Avviare Foundation Services e Oracle HTTP Server.
2. Tramite la console di amministrazione di WebLogic Server, avviare l'applicazione Web SSODiag per gestire tutte le richieste.
3. Eseguire l'accesso a un computer client configurato per l'autenticazione Kerberos utilizzando credenziali di Active Directory valide.
4. Utilizzando un browser, connettersi all'URL seguente di SSODiag:

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

   In questo campione, *OHS_HOST_NAME* indica il nome del server che ospita Oracle HTTP Server e *PORT* indica la porta su cui Oracle HTTP Server resta in ascolto delle richieste.

   Se l'autenticazione Kerberos funziona correttamente, SSODiag visualizza le informazioni seguenti:

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

   Se invece l'autenticazione Kerberos non funziona correttamente, SSODiag visualizza le informazioni seguenti:

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

Modifica del modello di sicurezza

Il modello di sicurezza predefinito per le applicazioni Web protette tramite il realm di sicurezza è `DDonly`. È necessario cambiare modello di sicurezza impostando `CustomRolesAndPolicies`.

Per cambiare modello di sicurezza, procedere come segue.

1. Utilizzando un editor di testo, aprire *MIDDLEWARE_HOME*`/user_projects/domains/EPMSystem/config/config.xml`.
2. Individuare l'elemento seguente nel descrittore della distribuzione dell'applicazione per ogni componente Foundation Services:

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

3. Cambiare modello di sicurezza come segue per ogni componente:

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

4. Salvare e chiudere `config.xml`.

Aggiornamento della configurazione di sicurezza di EPM System

Modificare la configurazione di sicurezza di EPM System in modo da abilitare SSO con Kerberos.

Per configurare EPM System per l'autenticazione Kerberos, procedere come segue.

1. Eseguire l'accesso a Shared Services Console come amministratore.
2. Aggiungere il dominio di Active Directory configurato per l'autenticazione Kerberos come directory utenti esterna in Shared Services. Fare riferimento alla sezione "Configurazione di OID, Active Directory e altre directory utenti basate su LDAP" nel manuale *Oracle Enterprise Performance Management System User Security Administration Guide (in lingua inglese)*.
3. Abilitare SSO. Fare riferimento alla sezione Configurazione di OID, Active Directory e altre directory utenti basate su LDAP.
   In **Opzioni di sicurezza**, selezionare le impostazioni nella tabella che segue per abilitare SSO con Kerberos.

Tabella 3-4 Impostazioni per abilitare SSO con Kerberos

Campo	Impostazione richiesta
Abilita SSO	Selezionato
Provider o agente SSO	Altro
Meccanismo SSO	Richiama utente remoto da richiesta HTTP

4. Riavviare Foundation Services.

Test di SSO con Kerberos

Eseguire l'accesso a Foundation Services per verificare che SSO con Kerberos funzioni correttamente.

Per testare SSO con Kerberos, procedere come segue.

1. Verificare che Foundation Services e Oracle HTTP Server siano in esecuzione.
2. Eseguire l'accesso a un computer client configurato per l'autenticazione Kerberos utilizzando credenziali di Active Directory valide.
3. Utilizzando un browser, connettersi all'URL di Foundation Services.

Configurazione dei componenti di EPM System

Utilizzando EPM System Configurator, configurare e distribuire gli altri componenti di EPM System nel dominio WebLogic in cui è stato distribuito Foundation Services.

Configurazione dei server gestiti di EPM System per l'autenticazione Kerberos

Negli ambienti Microsoft Windows, i server gestiti EPM System vengono eseguiti come servizi Windows. È necessario modificare le opzioni JVM di avvio per ogni server gestito WebLogic. Di seguito è riportato un elenco completo di server gestiti in modalità distribuzione non compatta.

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

- FoundationServices0
- HpsAlerter0
- HpsWebReports0
- Planning0
- Profitability0

Se le applicazioni Web EPM System vengono distribuite in modalità distribuzione compatta, è necessario aggiornare le opzioni JVM di avvio solo del server gestito `EPMSystem0`. Se si dispone di più server gestiti compatti, è necessario aggiornare le opzioni JVM di avvio per tutti i server gestiti.

Fare riferimento alla sezione Utilizzo degli argomenti di avvio per l'autenticazione Kerberos con WebLogic Server nella guida *Oracle Fusion Middleware Securing Oracle WebLogic Server* (in lingua inglese).

> **Nota:**
>
> Nella procedura seguente viene descritto come impostare le opzioni JVM di avvio per il server gestito FoundationServices. È necessario eseguire questo task per ogni server gestito WebLogic presente nella distribuzione.

Per le procedure dettagliate per la configurazione delle opzioni JVM negli script di avvio di WebLogic Server, fare riferimento alla sezione Aggiornamento delle opzioni JVM per Kerberos.

Per configurare le opzioni JVM negli script di avvio di WebLogic Server

Configurazione dei criteri di autorizzazione

Configurare i criteri di autorizzazione per gli utenti di Active Directory che accederanno a componenti di EPM System diversi da Foundation Services. Per informazioni sulla configurazione dei criteri di sicurezza dalla console di amministrazione WebLogic, fare riferimento alla sezione Configurazione dei criteri di autorizzazione.

Modifica del modello di sicurezza predefinito dei componenti di EPM System

Per utilizzare un modello di sicurezza diverso da quello predefinito, è necessario modificare il file di configurazione di EPM System. Per le distribuzioni non compatte di EPM System, è necessario specificare un modello di sicurezza diverso da quello predefinito per ogni applicazione Web EPM System registrata in `config.xml`. Di seguito è riportato un elenco di applicazioni Web EPM System.

- AIF
- APS
- CALC
- EAS
- FINANCIALREPORTING
- PLANNING
- PROFITABILITY
- SHAREDSERVICES

- WORKSPACE

Per cambiare modello di sicurezza, procedere come segue.

1. Utilizzando un editor di testo, aprire *MIDDLEWARE_HOME*/user_projects/domains/EPMSystem/config/config.xml
2. Nella definizione app-deployment di ogni componente di EPM System, impostare il valore di <security-dd-model> su CustomRolesAndPolicies come illustrato nell'esempio seguente:

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

3. Salvare e chiudere config.xml.
4. Riavviare WebLogic Server.

Creazione dei criteri di protezione URL per i componenti di EPM System

Nella console di amministrazione di WebLogic Server, creare un criterio di protezione URL per proteggere l'URL di ogni componente di EPM System. Per informazioni dettagliate, fare riferimento alla sezione Opzioni per proteggere le risorse di tipo applicazione Web ed EJB nella guida *Oracle Fusion Middleware Securing Resources Using Roles and Policies for Oracle WebLogic Server* (in lingua inglese).

Per creare i criteri di protezione URL, procedere come segue.

1. Nel Centro modifiche nella console di amministrazione di WebLogic Server per il dominio di EPM System, fare clic su **Blocca e modifica**.
2. Fare clic su **Distribuzioni**.
3. Espandere un'applicazione aziendale EPM System (ad esempio, PLANNING) nella distribuzione, quindi fare clic sulla relativa applicazione Web (ad esempio, HyperionPlanning). Per un elenco dei componenti di EPM System, fare riferimento alla sezione Modifica del modello di sicurezza predefinito dei componenti di EPM System.

> **Nota:**
>
> Alcune applicazioni aziendali, ad esempio Oracle Essbase Administration Services, includono diverse applicazioni Web per le quali devono essere definiti pattern di URL.

4. Creare un criterio che abbia come ambito un pattern di URL per l'applicazione Web.
   - AIF
   - APS
   - CALC

- EAS
- FINANCIALREPORTING
- PLANNING
- PROFITABILITY
- SHAREDSERVICES
- WORKSPACE

a. Fare clic su **Sicurezza**, quindi su **Criteri** e infine su **Nuovo**.

b. In **Pattern URL** , immettere gli URL protetti e non protetti dei prodotti EPM System. Per ulteriori dettagli, fare riferimento alla sezione Protezione e rimozione della protezione per le risorse di EPM System.

c. Fare clic su **OK**.

d. Fare clic sul pattern di URL creato.

e. Fare clic su **Aggiungi condizioni**.

f. In **Lista di predicati**, selezionare una condizione per il criterio, quindi fare clic su **Avanti**.
Oracle consiglia di utilizzare la condizione `Group`, che concede questo criterio di sicurezza a tutti i membri di un determinato gruppo.

g. Specificare gli argomenti rilevanti per il predicato scelto. Ad esempio, se è stato scelto `Group` nel passo precedente, è necessario completare le operazioni riportate di seguito.

h. In **Nome argomento gruppo**, immettere il nome del gruppo contenente gli utenti a cui deve essere consentito l'accesso all'applicazione Web. Il nome immesso deve corrispondere esattamente al nome di un gruppo di Active Directory.

   - Fare clic su **Aggiungi**.
   - Ripetere i passi precedenti per aggiungere ulteriori gruppi.

i. Fare clic su **Fine**.
WebLogic Server visualizza un messaggio di errore se non riesce a individuare il gruppo in Active Directory. È necessario correggere tale errore prima di continuare.

j. Selezionare **Salva**.

5. Ripetere i passi 3 e 4 di questa procedura per gli altri componenti di EPM System nella distribuzione.
6. Nel Centro modifiche, fare clic su **Rilascia configurazione**.
7. Riavviare WebLogic Server.

Abilitazione dell'autenticazione basata su certificati client nelle applicazioni Web

Inserire la definizione `login-config` nel file di configurazione degli archivi di applicazioni seguenti contenuti in *`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`

Per abilitare l'autenticazione basata su certificati client, procedere come segue.

1. Arrestare i componenti e i processi di EPM System.
2. Utilizzando 7 Zip, espandere un archivio Web contenuto all'interno dell'archivio aziendale, ad esempio,*EPM_ORACLE_HOME*`/products/Essbase/eas/server/AppServer/InstallableApps/Common/eas.ear/eas.war`.
3. Passare a `WEB-INF`.
4. Modificare `web.xml` aggiungendo la definizione `login_config` seguente subito prima dell'elemento `</webapp>`:

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

5. Salvare `web.xml`.
6. Quando 7-Zip richiede se si desidera aggiornare l'archivio, fare clic su **Yes**.

Aggiornamento della configurazione di sicurezza di EPM System

Configurare la sicurezza di EPM System in modo che sia conforme a SSO. Fare riferimento alla sezione Configurazione di EPM System per l'SSO.

Configurazione di EPM System per l'SSO

È necessario che i prodotti Oracle Enterprise Performance Management System siano configurati per supportare l'agente di sicurezza per SSO. La configurazione specificata in Oracle Hyperion Shared Services determina, per tutti i prodotti EPM System, quanto indicato di seguito.

- Se accettare o meno l'SSO da un agente di protezione
- Il meccanismo di autenticazione da accettare per l'SSO

In un ambiente abilitato per l'SSO, il prodotto di EPM System a cui l'utente accede per primo analizza il meccanismo SSO per recuperare l'ID dell'utente autenticato che esso contiene. Il prodotto EPM System verifica l'ID utente a fronte delle directory utenti configurate in Shared Services per stabilire se l'utente è un utente valido di EPM System. Emette inoltre un token che consente l'SSO tra i prodotti di EPM System.

La configurazione specificata in Shared Services consente di abilitare l'SSO determinando il meccanismo di autenticazione per l'accettazione dell'SSO da parte di tutti i prodotti di EPM System.

Per abilitare SSO da una soluzione di gestione identità Web, procedere come segue.

1. Avviare Oracle Hyperion Shared Services Console come amministratore di Shared Services. Fare riferimento alla sezione Avvio di Shared Services Console.
2. Selezionare **Amministrazione**, quindi **Configura directory utenti**.
3. Verificare che le directory utenti utilizzate dalla soluzione di gestione identità Web siano configurate come directory utenti esterne in Shared Services.

   Ad esempio, per abilitare SSO con Kerberos, è necessario configurare l'istanza di Active Directory configurata per l'autenticazione Kerberos come una directory utenti esterna.

Per istruzioni, fare riferimento alla sezione Configurazione delle directory utenti.

4. Selezionare **Opzioni sicurezza**.
5. Selezionare **Mostra opzioni avanzate**.
6. Nella sezione **Configurazione Single Sign-On** della schermata Directory definite dall'utente, procedere come segue::
   a. Selezionare **Abilita SSO**.
   b. In **Provider o agente SSO**, selezionare una soluzione di gestione identità Web. Scegliere **Altro** se si sta configurando SSO con Kerberos.

      Il meccanismo SSO supportato viene selezionato automaticamente. Fare riferimento alla tabella riportata di seguito. Inoltre, fare riferimento alla sezione Metodi SSO supportati.

> **Nota:**
>
> Se non si sta utilizzando il meccanismo SSO supportato, è necessario scegliere `Altro` in **Provider o agente SSO**. Ad esempio, per utilizzare un meccanismo diverso dall'intestazione HTTP per SiteMinder, scegliere `Other` in **Provider o agente SSO**, quindi in **Meccanismo SSO** selezionare il meccanismo SSO desiderato.

Tabella 3-5 Meccanismi SSO preferiti per le soluzioni di gestione delle identità sul Web

Soluzione di gestione delle identità sul Web	Meccanismo SSO consigliato
Oracle Access Manager	`Custom HTTP Header` [1]
OSSO	`Custom HTTP Header`
SiteMinder	`Custom HTTP Header`
Kerberos	`Richiama utente remoto da richiesta HTTP`

[1] Il nome predefinito dell'intestazione HTTP è `HYPLOGIN`. Se si sta utilizzando un'intestazione HTTP custom, sostituire il nome.

7. Fare clic su **OK**.

Opzioni Single Sign-On per Smart View

Anche se Oracle Smart View for Office è un thick client e non un browser, si connette ai componenti server utilizzando HTTP e si comporta in modo simile a un browser dal punto di vista del sistema. Smart View supporta tutti i metodi di integrazione standard basati sul Web supportasti dalle interfacce dei browser. Esistono tuttavia alcune limitazioni, elencate di seguito.

- Se si avvia Smart View da una sessione di browser esistente connessa a un componente di Oracle Enterprise Performance Management System, gli utenti

devono eseguire di nuovo l'accesso a Smart View perché non condivide il cookie dalla sessione esistente.

- Se si utilizza un form di accesso HTML customizzato anziché il form di accesso predefinito di Oracle Access Manager, assicurarsi che il codice sorgente del form customizzato includa la stringa `loginform`, necessaria per consentire il funzionamento dell'integrazione di Smart View con Oracle Access Manager.

4

Configurazione delle directory utenti

Vedere anche:

- Directory utenti e sicurezza di EPM System
- Operazioni correlate alla configurazione della directory utente
- Oracle Identity Manager ed EPM System
- Informazioni su Active Directory
- Configurazione di OID, Active Directory e altre directory utenti basate su LDAP
- Configurazione dei database relazionali come directory utente
- Test delle connessioni delle directory utente
- Modifica delle impostazioni delle directory utente
- Eliminazione delle configurazioni delle directory utente
- Gestione dell'ordine di ricerca delle directory utente
- Impostazione delle opzioni di sicurezza
- Rigenerazione delle chiavi di cifratura
- Utilizzo di caratteri speciali

Directory utenti e sicurezza di EPM System

I prodotti Oracle Enterprise Performance Management System sono supportati in un ampio numero di sistemi per la gestione degli utenti e delle identità, denominati collettivamente directory utenti. Queste directory includono directory utenti abilitate per Lightweight Directory Access Protocol (LDAP), ad esempio Sun Java System Directory Server (in precedenza denominato SunONE Directory Server) e Active Directory. EPM System supporta inoltre database relazionali come directory utente esterne.

In genere, i prodotti EPM System utilizzano la directory nativa e directory utenti esterne per il processo di assegnazione ruoli. Per un elenco delle directory utenti supportate, fare riferimento alla sezione Matrice per la certificazione di Oracle Enterprise Performance Management System.

I prodotti EPM System richiedono un account di directory utente per ogni utente che vi accede. Tali utenti possono essere assegnati a gruppi per facilitare l'assegnazione ruoli. Agli utenti e ai gruppi è possibile assegnare ruoli di EPM System e ACL di oggetti. Per evitare un sovraccarico delle attività amministrative, Oracle sconsiglia di assegnare ruoli ai singoli utenti. Gli utenti e i gruppi di tutte le directory utenti configurate sono visibili da Oracle Hyperion Shared Services Console.

Per impostazione predefinita, EPM System Configurator configura il repository di Shared Services come directory nativa per il supporto dei prodotti EPM System. Gli utenti con ruolo Gestione directory eseguono le operazioni di accesso e gestione della directory nativa tramite Shared Services Console.

Operazioni correlate alla configurazione della directory utente

Per supportare SSO e l'autorizzazione, gli amministratori di sistema devono configurare directory utenti esterne. In Oracle Hyperion Shared Services Console, gli amministratori di sistema possono eseguire diversi task correlati alla configurazione e alla gestione delle directory utenti. Le istruzioni vengono fornite negli argomenti riportati di seguito.

- Configurazione delle directory utenti:
  - Configurazione di OID, Active Directory e altre directory utenti basate su LDAP
  - Configurazione dei database relazionali come directory utente
- Test delle connessioni delle directory utente
- Modifica delle impostazioni delle directory utente
- Eliminazione delle configurazioni delle directory utente
- Gestione dell'ordine di ricerca delle directory utente
- Impostazione delle opzioni di sicurezza

Oracle Identity Manager ed EPM System

Oracle Identity Manager è una soluzione per la gestione di utenti e ruoli che consente di automatizzare il processo di aggiunta, aggiornamento ed eliminazione di account utente e diritti a livello di attributi delle risorse enterprise. Oracle Identity Manager è disponibile come prodotto stand-alone oppure come parte di Oracle Identity and Access Management Suite Plus.

Oracle Enterprise Performance Management System si integra con Oracle Identity Manager mediante ruoli enterprise che rappresentano gruppi LDAP. I ruoli dei componenti di EPM System possono essere assegnati ai ruoli enterprise. Gli utenti o i gruppi aggiunti ai ruoli enterprise di Oracle Identity Manager ereditano automaticamente i ruoli di EPM System assegnati.

Si supponga ad esempio di utilizzare un'applicazione di Oracle Hyperion Planning denominata *Budget Planning*. Per supportare tale applicazione, è possibile creare in Oracle Identity Manager tre ruoli enterprise, ovvero Utente interattivo Budget Planning, Utente finale Budget Planning e Amministratore Budget Planning. Durante l'assegnazione dei ruoli per EPM System, assicurarsi che i responsabili della gestione assegnazione ruoli assegnino ai ruoli enterprise di Oracle Identity Manager i ruoli necessari di *Budget Planning* e degli altri componenti di EPM System, incluso Shared Services. Tutti gli utenti e i gruppi assegnati ai ruoli enterprise in Oracle Identity Manager ereditano i ruoli di EPM System. Per informazioni sulla distribuzione e la gestione di Oracle Identity Manager, fare riferimento alla documentazione di Oracle Identity Manager.

Per integrare Oracle Identity Manager con EPM System, gli amministratori devono eseguire i passi seguenti.

- Assicurarsi che i membri (utenti e gruppi) dei ruoli enterprise di Oracle Identity Manager che devono essere utilizzati per l'assegnazione dei ruoli di EPM System

siano definiti in una directory utenti abilitata per LDAP, ad esempio OID o Active Directory.

- Configurare la directory utenti abilitata per LDAP in cui sono definiti i membri dei ruoli enterprise come directory utenti esterna in EPM System. Fare riferimento alla sezione Configurazione di OID, Active Directory e altre directory utenti basate su LDAP.

Informazioni su Active Directory

In questa sezione vengono illustrati alcuni concetti correlati a Microsoft Active Directory utilizzati nel presente documento.

Ricerca del DNS e del nome host

Gli amministratori di sistema possono configurare Active Directory in modo che Oracle Hyperion Shared Services sia in grado di identificarla mediante una ricerca basata su nome host statico o su DNS. La ricerca del nome host statico non supporta il failover di Active Directory.

L'utilizzo della ricerca DNS garantisce un'elevata disponibilità di Active Directory in scenari in cui quest'ultimo è configurato in più controller di dominio per garantire un'alta disponibilità. Quando è configurato in modo da eseguire una ricerca DNS, Shared Services esegue una query nel server DNS per identificare i controller di dominio registrati e si connette al controller di dominio con il maggior peso. Se nel controller di dominio a cui è connesso Shared Services si verifica un errore, Shared Services passa in modo dinamico al successivo controller di dominio disponibile con il maggior peso.

> **Nota:**
>
> La ricerca DNS può essere impostata solo se è disponibile una configurazione di Active Directory ridondante che supporta il failover. Per informazioni, vedere la documentazione Microsoft.

Catalogo globale

Un catalogo globale è un controller di dominio in cui è memorizzata una copia di tutti gli oggetti di Active Directory in una foresta. Questo catalogo include una copia completa di tutti gli oggetti della directory per il relativo dominio host e una copia parziale di tutti gli oggetti per tutti gli altri domini della foresta, che vengono utilizzati nelle operazioni di ricerca degli utenti standard. Per informazioni sull'impostazione di un catalogo globale, vedere la documentazione Microsoft.

Se nell'organizzazione viene utilizzato un catalogo globale, per configurare Active Directory utilizzare uno dei metodi descritti di seguito.

- Configurare il server del catalogo globale come directory utente esterna (consigliato).
- Configurare ciascun dominio di Active Directory come directory utenti esterna separata.

La configurazione del catalogo globale, anziché dei singoli domini di Active Directory, consente ai prodotti Oracle Enterprise Performance Management System di accedere ai gruppi locali e universali all'interno della foresta.

Configurazione di OID, Active Directory e altre directory utenti basate su LDAP

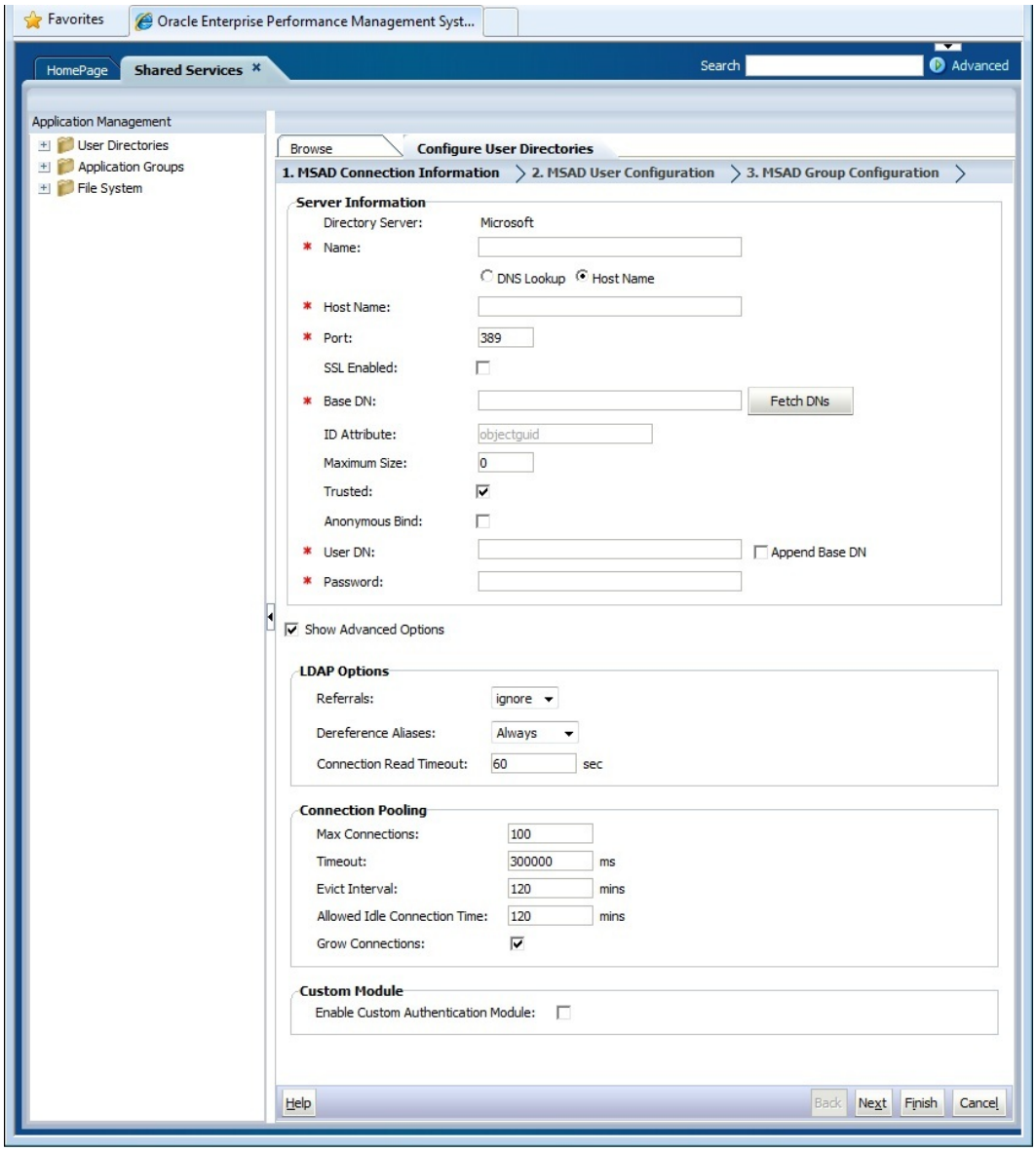
Gli amministratori di sistema utilizzano le procedure descritte in questa sezione per configurare directory utenti aziendali basate su LDAP, come OID, Sun Java System Directory Server, Oracle Virtual Directory, Active Directory, IBM Tivoli Directory Server o una directory utenti basata su LDAP non elencata nella schermata di configurazione.

Per configurare OID, Active Directory e altre directory utenti basate su LDAP, procedere come segue.

1. Accedere a Oracle Hyperion Shared Services Console come amministratore di sistema. Fare riferimento alla sezione Avvio di Shared Services Console.
2. Selezionare **Amministrazione**, quindi **Configura directory utenti**.

   Viene visualizzata la scheda Configurazione provider. In questa schermata sono elencate tutte le directory utenti configurate, compresa la directory nativa.
3. Fare clic su **Nuovo**.
4. In **Tipo directory** selezionare un'opzione:
   - **Lightweight Directory Access Protocol (LDAP)** per configurare una directory utenti basata su LDAP diversa da Active Directory. Selezionare questa opzione per configurare Oracle Virtual Directory.
   - **Microsoft Active Directory (MSAD)** per configurare Active Directory.

     Solo Active Directory e Active Directory Application Mode (ADAM): se si desidera utilizzare un attributo ID custom (un attributo diverso da `ObjectGUID`, ad esempio `sAMAccountName` con Active Directory o ADAM, selezionare **Lightweight Directory Access Protocol (LDAP)**, e in Tipo directory specificare `Other`.
5. Fare clic su **Avanti**.



6. Immettere i parametri richiesti.

Tabella 4-1 Schermata Informazioni connessione

Etichetta	Descrizione
Server delle directory	Selezionare una directory utenti. Il valore **Attributo ID** viene impostato sull'attributo di identità costante univoco consigliato per il prodotto selezionato. Questa proprietà viene selezionata automaticamente se nel passo 4 è stato scelto Active Directory. Selezionare `Other` nei seguenti casi: • Si desidera configurare un tipo di directory utenti non incluso nell'elenco, ad esempio Oracle Virtual Directory • Si desidera configurare una directory utenti abilitata per LDAP inclusa nell'elenco (ad esempio, OID), ma si intende utilizzare un attributo ID customizzato. • Si desidera configurare Active Directory o ADAM per l'utilizzo di un attributo ID customizzato. **Nota:** Poiché Oracle Virtual Directory fornisce un'astrazione virtualizzata delle directory LDAP e dei repository dati RDMBS in un'unica vista di directory, Oracle Enterprise Performance Management System la considera una singola directory utenti esterna indipendentemente dal numero e dal tipo di directory utenti supportate da Oracle Virtual Directory. **Esempio:** `Oracle Internet Directory`
Nome	Nome descrittivo per la directory utente. Utilizzato per identificare una directory utente specifica in presenza di più directory utente configurate. Il nome non deve contenere caratteri speciali oltre allo spazio e al trattino di sottolineatura. **Esempio:** `Corporate_OID`

Tabella 4-1 (Cont.) Schermata Informazioni connessione

Etichetta	Descrizione
Ricerca DNS	**Solo per Active Directory:** selezionare questa opzione per abilitare la ricerca DNS. Fare riferimento alla sezione Ricerca del DNS e del nome host. Oracle consiglia di configurare la ricerca DNS come metodo per la connessione ad Active Directory in ambienti di produzione per evitare problemi di connessione. **Nota:** Non selezionare questa opzione se è in corso la configurazione di un catalogo globale. Se si seleziona questa opzione, vengono visualizzati i campi visualizzati di seguito. • **Dominio**: nome di dominio di una foresta di Active Directory. **Esempi:** `example.com` oppure `us.example.com` • **Sito di AD**: nome del sito di Active Directory, di solito il nome distinto relativo dell'oggetto sito memorizzato nel contenitore della configurazione di Active Directory. Il sito di AD identifica di solito un'ubicazione geografica, come una città, uno stato, un'area o un paese. **Esempi:** `Santa Clara` oppure `US_West_region` • **Server DNS**: nome DNS del server che supporta la ricerca dei controller di dominio da parte del server DNS.
Nome host	**Solo per Active Directory:** selezionare questa opzione per abilitare la ricerca del nome host statico. Fare riferimento alla sezione Ricerca del DNS e del nome host. **Nota:** Selezionare questa opzione se si sta configurando un catalogo globale di Active Directory.

Tabella 4-1 (Cont.) Schermata Informazioni connessione

Etichetta	Descrizione
Nome host	Nome DNS del server della directory utenti. Utilizzare il nome di dominio completamente qualificato se la directory utenti deve essere utilizzata per il supporto di SSO da SiteMinder. Oracle consiglia di utilizzare il nome host per stabilire una connessione ad Active Directory solo per l'esecuzione di test. **Nota:** Se si sta configurando un catalogo globale di Active Directory, specificare il nome host del server del catalogo globale. Fare riferimento alla sezione Catalogo globale. **Esempio:** `MyServer`
Porta	Il numero di porta su cui è in esecuzione la directory utente. **Nota:** Se si sta configurando un catalogo globale di Active Directory, specificare la porta utilizzata dal server del catalogo globale (l'impostazione predefinita è 3268). Fare riferimento alla sezione Catalogo globale. **Esempio:** `389`
SSL abilitato	La casella di spunta che abilita la comunicazione protetta con questa directory utente. La directory utente deve essere configurata per la comunicazione protetta.
DN di base	Nome distinto (DN) del nodo in cui iniziare la ricerca di gruppi e utenti. È anche possibile utilizzare il pulsante **Recupera DN** per elencare i DN di base disponibili e selezionare poi il DN di base adeguato dall'elenco. **Nota:** Se è in corso la configurazione di un catalogo globale, specificare il DN di base della foresta. Per le limitazioni relative all'utilizzo dei caratteri speciali, fare riferimento alla sezione Utilizzo di caratteri speciali. Oracle raccomanda di selezionare il DN di livello più basso contenente tutti gli utenti e i gruppi dei prodotti EPM System. **Esempio:** `dc=example,dc=com`

Tabella 4-1 (Cont.) Schermata Informazioni connessione

Etichetta	Descrizione
Attributo ID	Il valore di questo attributo può essere modificato solo se in **Tipo directory** è selezionato `Altro`. Questo attributo deve essere un attributo comune presente negli oggetti utente e gruppo sul server delle directory. Il valore consigliato di questo attributo viene impostato automaticamente per OID (`orclguid`), SunONE (`nsuniqueid`), IBM Directory Server (`Ibm-entryUuid`), Novell eDirectory (`GUID`) e Active Directory (`ObjectGUID`). **Esempio:** `orclguid` Valore dell'attributo ID se lo si imposta manualmente dopo aver selezionato il valore `Altro` in **Server delle directory**. Ad esempio, per configurare un'istanza di Oracle Virtual Directory, deve avere le caratteristiche seguenti. • Deve puntare a un attributo univoco. • Non deve essere specifico della posizione. • Non deve cambiare nel tempo.
Dimensioni massime	Numero massimo di risultati che possono essere restituiti da una ricerca. Se questo valore supera quello supportato dalle impostazioni della directory utente, viene utilizzato il valore di quest'ultima. Per le directory utenti diverse da Active Directory, lasciare vuoto questo campo per recuperare tutti gli utenti e i gruppi che soddisfano i criteri di ricerca. Per Active Directory, impostare questo valore su `0` per recuperare tutti gli utenti e i gruppi che soddisfano i criteri di ricerca. Se si sta configurando Oracle Hyperion Shared Services in modalità Amministrazione delegata, impostare questo valore su 0.
Sicuro	Casella di controllo per indicare che questo provider è un'origine SSO attendibile. I token SSO provenienti dalle origini attendibili non contengono la password dell'utente.
Autenticazione anonima	Casella di controllo per consentire a Shared Services l'autenticazione anonima alla directory utente per la ricerca di utenti e gruppi. Utilizzabile solo se la directory utente consente autenticazioni anonime. Se questa opzione non è selezionata, è necessario specificare, in DN utente, un account con autorizzazioni di accesso sufficienti all'esecuzione di ricerche nella directory contenente le informazioni sugli utenti. Oracle raccomanda di non utilizzare l'autenticazione anonima. **Nota:** L'autenticazione anonima non è supportata per OID.

Tabella 4-1 (Cont.) Schermata Informazioni connessione

Etichetta	Descrizione
DN utente	Questa opzione è disabilitata se è stato selezionato **Autenticazione anonima**. Nome distinto dell'utente che deve essere utilizzato da Shared Services per l'autenticazione con la directory utente. L'utente deve disporre del privilegio di ricerca per l'attributo RDN nel DN. Ad esempio, nel DN `cn=John Doe, ou=people, dc=myCompany, dc=com`, l'utente dell'autenticazione deve disporre dell'accesso per la ricerca dell'attributo `cn` . In DN utente è necessario specificare i caratteri speciali utilizzando i caratteri di escape. Per le limitazioni, fare riferimento alla sezione Utilizzo di caratteri speciali. **Esempio:** `cn=admin,dc=myCompany,dc=com`
Aggiungi DN di base	Casella di controllo per l'aggiunta del DN di base al DN utente. Se viene utilizzato l'account Directory Manager come DN utente, non aggiungere il DN di base. Questa casella di controllo è disabilitata se è stata selezionata l'opzione Autenticazione anonima.
Password	Password del DN utente. Questa casella è disabilitata se è stata selezionata l'opzione Autenticazione anonima. **Esempio:** `UserDNpassword`
Mostra opzioni avanzate	Casella di controllo per la visualizzazione delle opzioni avanzate.
Riferimenti	**Solo per Active Directory:** se il servizio Active Directory è configurato per seguire i riferimenti, selezionare `follow` per seguire automaticamente i riferimenti LDAP. Selezionare `ignora` per non utilizzare i riferimenti.
Elimina riferimenti alias	Selezionare il metodo da utilizzare nelle ricerche di Shared Services per l'eliminazione dei riferimenti alias nella directory utente in modo che le ricerche recuperino l'oggetto a cui punta il DN dell'alias. Selezionare quanto segue. • **Sempre**: per eliminare sempre i riferimenti alias. • **Mai**: per non eliminare mai i riferimenti alias. • **Trova**: per eliminare i riferimenti alias solo durante la risoluzione dei nomi. • **Ricerca**: per eliminare i riferimenti alias solo dopo la risoluzione dei nomi.
Timeout lettura connessione	Intervallo (in secondi) dopo il quale il provider LDAP interrompe il tentativo di lettura LDAP se non ottiene una risposta. **Valore predefinito:** 60 secondi
N. massimo connessioni	Numero massimo di connessioni nel connection pool. L'impostazione predefinita è 100 per le directory basate su LDAP, inclusa Active Directory. **Valore predefinito:** 100
Timeout	Timeout per ottenere una connessione dal pool. Trascorso questo periodo, viene generata un'eccezione. **Valore predefinito:** 300000 millisecondi (5 minuti)

Tabella 4-1 (Cont.) Schermata Informazioni connessione

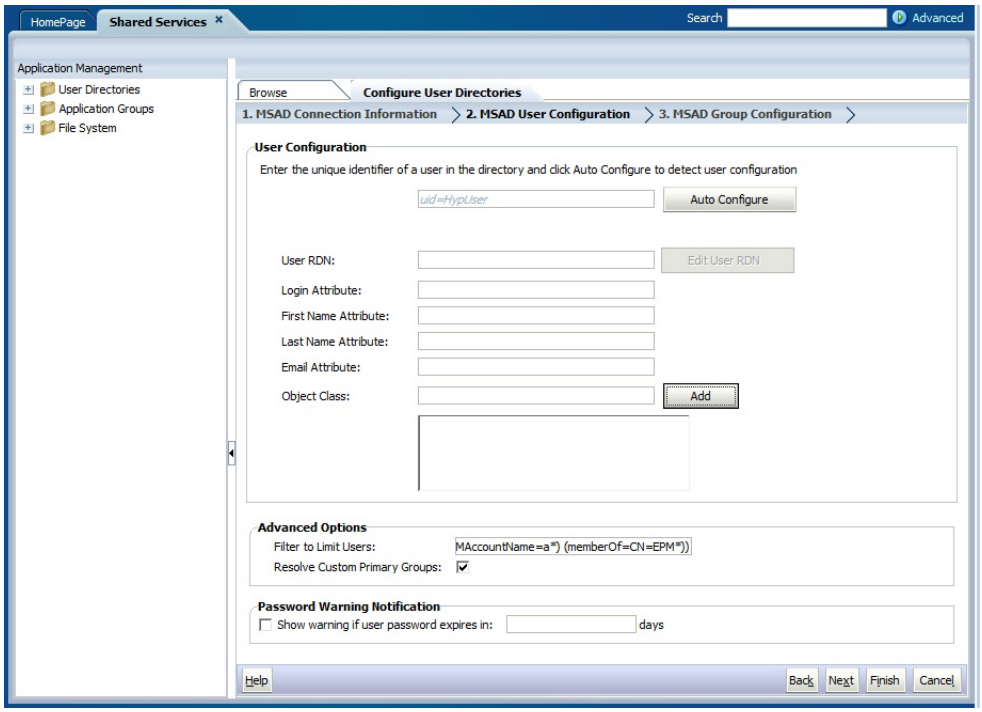
Etichetta	Descrizione
Intervallo di eliminazione	**Facoltativo:** intervallo per l'esecuzione del processo di rimozione per ripulire il pool. Il processo comporta la rimozione delle connessioni inattive che hanno superato il valore del `Tempo di inattività consentito per la connessione`. **Valore predefinito:** 120 minuti
Tempo di inattività consentito per la connessione	**Facoltativo:** tempo trascorso il quale le connessioni inattive vengono rimosse dal pool con il processo di rimozione. **Valore predefinito:** 120 minuti
Aumenta connessioni	Questa opzione indica se il connection pool può superare il valore di `N. massimo connessioni` È selezionata per impostazione predefinita. Se non si consente l'espansione del pool, il sistema restituirà un errore se la connessione non è disponibile entro l'intervallo di tempo impostato per `Timeout`.
Abilita modulo di autenticazione custom	Casella di controllo per abilitare l'utilizzo di un modulo di autenticazione custom per l'autenticazione degli utenti definiti nella directory utente. È necessario immettere inoltre il nome completo della classe Java del modulo di autenticazione nella schermata Opzioni protezione. Fare riferimento alla sezione Impostazione delle opzioni di sicurezza. Per i client thin e thick l'autenticazione di un modulo di autenticazione custom è trasparente e non richiede modifiche di distribuzione del client. Fare riferimento alla sezione "Modulo autenticazione custom" nella *Guida alla configurazione della sicurezza di Oracle Enterprise Performance Management System*.

7. Fare clic su **Avanti**.

In Shared Services le proprietà impostate nella schermata Configurazione utente vengono utilizzate per creare un URL utente, a sua volta utilizzato per determinare il nodo in cui avviare la ricerca degli utenti. L'utilizzo di questo URL rende più rapida la ricerca.

> **Attenzione:**
>
> L'URL utente non deve puntare a un alias. Per la protezione di EPM System, è necessario che l'URL utente punti a un utente effettivo.

Oracle consiglia di recuperare le informazioni necessarie dall'area Configurazione automatica della schermata.



> **Nota:**
>
> Per un elenco dei caratteri speciali che è possibile utilizzare nella configurazione utente, fare riferimento alla sezione Utilizzo di caratteri speciali.

8. Nella casella **Configurazione automatica**, immettere un identificativo utente univoco in formato `attribute=identifier`, ad esempio `uid=jdoe`.

   Gli attributi dell'utente vengono visualizzati nell'area Configurazione utente.

   Se si sta configurando OID, non è possibile configurare automaticamente il filtro utenti perché il DSE radice di OID non contiene voci nell'attributo Contesti di denominazione. Fare riferimento alla sezione Gestione dei contesti di denominazione nel manuale *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* (in lingua inglese).

> **Nota:**
>
> È possibile immettere manualmente gli attributi richiesti nelle caselle di testo dell'area Configurazione utente.

Tabella 4-2 Schermata Configurazione utente

Etichetta	Descrizione[1]
RDN utente	DN relativo dell'utente. Ogni componente di un DN viene detto RDN e rappresenta una diramazione nell'albero della directory. L'RDN di un utente generalmente equivale all'`uid` o al `cn`. Per le limitazioni, fare riferimento alla sezione Utilizzo di caratteri speciali. **Esempio:** `ou=People`
Attributo di accesso	Attributo univoco (può essere un attributo customizzato) in cui viene memorizzato il nome di accesso dell'utente. Gli utenti usano il valore di questo attributo come nome utente durante l'accesso ai prodotti EPM System. Gli ID utente (valore dell'attributo di accesso) devono essere univoci in tutte le directory utente. Ad esempio, è possibile utilizzare `uid` e `sAMAccountName` come attributo di accesso rispettivamente per le configurazioni SunONE e Active Directory. I valori di questi attributi devono essere univoci in tutte le directory utenti, compresa la directory nativa. **Nota:** Gli ID utente non fanno distinzione tra maiuscole e minuscole. **Nota:** Se si sta configurando OID come directory utenti esterna per prodotti EPM System distribuiti in Oracle Application Server in un ambiente Kerberos, è necessario impostare questa proprietà su `userPrincipalName`. **Valore predefinito** • **Active Directory:** `cn` • **Directory LDAP diverse da Active Directory:** `uid`
Attributo nome	Attributo in cui viene memorizzato il nome dell'utente. **Valore predefinito:** `givenName`
Attributo cognome	Attributo in cui viene memorizzato il cognome dell'utente. **Valore predefinito:** `sn`
Attributo e-mail	**Facoltativo**: attributo in cui viene memorizzato l'indirizzo e-mail dell'utente. **Valore predefinito:** `mail`

Tabella 4-2 (Cont.) Schermata Configurazione utente

Etichetta	Descrizione[1]
Classe oggetto	Classi oggetto dell'utente (attributi obbligatori e facoltativi associabili con l'utente). In Shared Services le classi oggetto elencate in questa schermata vengono utilizzate nel filtro di ricerca. Grazie a queste classi oggetto, in Shared Services è possibile individuare tutti gli utenti che richiedono l'assegnazione di ruoli. **Nota:** Se per Active Directory o ADAM si configura il tipo di directory utenti `Other` per utilizzare un attributo ID customizzato, è necessario impostare questo valore su `user`. Se necessario, è possibile aggiungere classi oggetto manualmente. Per aggiungere una classe oggetto, immetterne il nome nella casella **Classe oggetto**, quindi fare clic su **Aggiungi**. Per eliminare classi oggetto, selezionarle e fare clic su **Rimuovi**. **Valore predefinito** • **Active Directory:** `user` • **Directory LDAP diverse da Active Directory:** `person, organizationalPerson, inetorgperson`
Filtro per limitare gli utenti	Query LDAP che recupera solo gli utenti a cui sono stati assegnati ruoli dei prodotti di EPM System. Ad esempio, la query LDAP `(uid=Hyp*)` recupera solo gli utenti il cui nome inizia con il prefisso `Hyp`. Nella schermata Configurazione utente viene eseguita la convalida dell'RDN utente e, se necessario, viene consigliato l'utilizzo di un filtro utenti. Il filtro utenti consente di limitare il numero di utenti restituiti durante una query e risulta particolarmente importante se il nodo identificato dall'RDN utente contiene molti utenti a cui non è necessario assegnare ruoli. È possibile progettare filtri utenti per escludere gli utenti a cui non assegnare ruoli e ottenere quindi prestazioni migliori.

Tabella 4-2 (Cont.) Schermata Configurazione utente

Etichetta	Descrizione[1]
Attributo ricerca utenti per RDN con attributi multipli	**Solo per directory utente abilitate per LDAP diverse da Active Directory:** impostare questo valore solo se il server della directory è configurato per l'utilizzo di un RDN con attributi multipli. Il valore impostato deve essere uno dei gli attributi RDN. Il valore dell'attributo deve essere univoco e per l'attributo deve essere consentita la ricerca. Ad esempio, si supponga che un server della directory SunONE sia configurato in modo da combinare gli attributi cn (`cn=John Doe`) e uid (`uid=jDoe12345`) per creare un RDN con attributi multipli simile a quello riportato di seguito: `cn=John Doe+uid=jDoe12345, ou=people, dc=myCompany, dc=com` In questo caso è possibile utilizzare `cn` o `uid`, a condizione che questi attributi soddisfino le condizioni riportate di seguito. • L'utente identificato nel DN utente registrato nella scheda delle informazioni di connessione deve poter eseguire la ricerca dell'attributo. • L'attributo richiede l'impostazione di un valore univoco nella directory utente
Risoluzione gruppi primari personalizzati	**Solo per Active Directory:** casella di controllo che indica se identificare i gruppi primari di utenti per determinare i ruoli effettivi. Per impostazione predefinita la casella di controllo è selezionata. Si consiglia di non modificare questa impostazione.
Mostra avviso in caso di scadenza password utente tra:	**solo per Active Directory:** casella di controllo che indica se visualizzare un messaggio di avviso qualora la password utente di Active Directory scada entro il numero specificato di giorni.

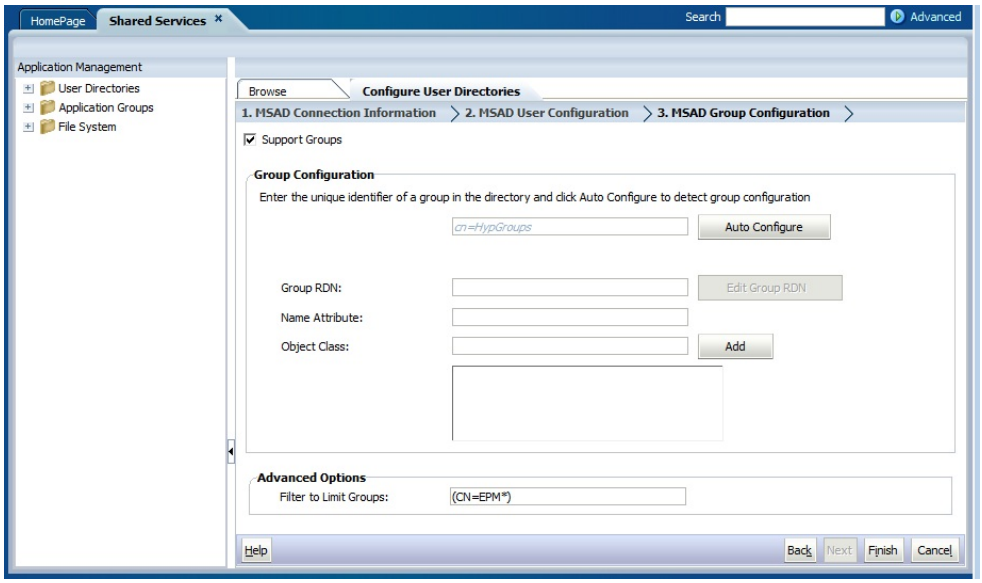
[1] Nella protezione di EPM System è possibile utilizzare valori predefiniti per alcuni campi per i quali il valore di configurazione è facoltativo. Se non si inserisce un valore in tali campi, in fase di esecuzione verranno utilizzati i valori predefiniti.

9. Fare clic su **Avanti**.

Viene visualizzata la schermata Configurazione gruppo. In Shared Services le proprietà impostate in questa schermata vengono utilizzate per creare l'URL del gruppo che determina il nodo in cui avviare la ricerca di gruppi. L'utilizzo di questo URL rende più rapida la ricerca.

> **Attenzione:**
>
> L'URL del gruppo non deve puntare a un alias. Per la protezione di EPM System, è necessario che l'URL del gruppo punti a un gruppo effettivo. Se si sta configurando Novell eDirectory che utilizza gli alias dei gruppi, gli alias e gli account dei gruppi devono essere disponibili nell'URL del gruppo.

> **Nota:**
>
> L'immissione di dati nella schermata Configurazione gruppo è facoltativa. Se non vengono specificate le impostazioni dell'URL del gruppo, in Shared Services la ricerca per individuare i gruppi viene eseguita nel DN di base, con un impatto negativo sulle performance, specie se la directory utente contiene molti gruppi.



10. Deselezionare **Supporta gruppi** se l'organizzazione non prevede di assegnare ruoli ai gruppi o se gli utenti non sono organizzati in gruppi nella directory utenti. Deselezionando questa opzione vengono disabilitati i campi in questa schermata.

    Se i gruppi sono supportati, Oracle consiglia di utilizzare la funzione di configurazione automatica per recuperare le informazioni richieste.

    Se si sta configurando OID come directory utenti, non è possibile utilizzare la funzionalità di configurazione automatica perché il DSE radice di OID non contiene voci nell'attributo Contesti di denominazione. Fare riferimento alla sezione Gestione dei contesti di denominazione nel manuale *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* (in lingua inglese).

11. Nella casella di testo **Configurazione automatica**, immettere un identificativo di gruppo univoco, quindi fare clic su **Vai**.

    È necessario specificare l'identificativo del gruppo in formato `attribute=identifier`, ad esempio `cn=western_region`.

    Gli attributi del gruppo vengono visualizzati nell'area Configurazione gruppo.

> **Nota:**
>
> È possibile immettere gli attributi del gruppo richiesti nelle caselle di testo Configurazione gruppo.

> **Attenzione:**
>
> Se l'URL gruppo non è impostato per directory utente contenenti i caratteri / (barra) o \ (barra rovesciata) nei nomi di nodo, la ricerca di utenti e gruppi non riesce. Ad esempio, qualsiasi operazione volta a elencare l'utente o il gruppo ha esito negativo se non viene specificato l'URL gruppo per una directory utenti in cui utenti e gruppi sono inseriti in un nodo del tipo `OU=child\ou,OU=parent/ou` o `OU=child/ou,OU=parent \ ou`.

Tabella 4-3 Schermata Configurazione gruppo

Etichetta	Descrizione[1]
RDN gruppo	DN relativo del gruppo. Questo valore, che è il percorso relativo al DN di base, viene utilizzato come URL del gruppo. Specificare un RDN gruppo che identifica il nodo di livello più basso nella directory utente in cui sono disponibili tutti i gruppi a cui si prevede di assegnare ruoli. Se si utilizza un gruppo primario di Active Directory per l'assegnazione ruoli, assicurarsi che tale gruppo rientri nell'RDN gruppo. Shared Services non recupera il gruppo primario se non è nell'ambito dell'URL del gruppo. L'RDN gruppo influisce significativamente sulle performance in accesso e ricerca. Poiché rappresenta il punto di partenza per tutte le ricerche di gruppi, è necessario identificare il nodo di livello più basso in cui siano disponibili tutti i gruppi per i prodotti EPM System. Per garantire performance ottimali, il numero di gruppi presenti nell'RDN gruppo non deve superare i 10.000. In presenza di più gruppi, utilizzare un filtro di gruppo per recuperare solo quelli a cui si desidera assegnare ruoli. **Nota:** In Shared Services viene visualizzato un avviso se il numero di gruppi disponibili nell'URL gruppo supera i 10.000. Per le limitazioni, fare riferimento alla sezione Utilizzo di caratteri speciali. **Esempio:** `ou=Groups`
Attributo nome	Attributo in cui viene memorizzato il nome del gruppo. **Valore predefinito** • **Directory LDAP che includono Active Directory:** `cn` • **Directory nativa:** `cssDisplayNameDefault`

Tabella 4-3 (Cont.) Schermata Configurazione gruppo

Etichetta	Descrizione[1]
Classe oggetto	Classi oggetto del gruppo. In Shared Services le classi oggetto elencate in questa schermata vengono utilizzate nel filtro di ricerca. Grazie a queste classi oggetto, in Shared Services è possibile trovare tutti i gruppi associati all'utente. **Nota:** Se per Active Directory o ADAM si configura il tipo di directory utenti `Other` per utilizzare un attributo ID customizzato, è necessario impostare questo valore su `group?member`. Se necessario, è possibile aggiungere classi oggetto manualmente. Per aggiungere una classe oggetto, immettere il nome nella casella di testo Classe oggetto e fare clic su **Aggiungi**. Per eliminare classi oggetto, selezionarle e fare clic su **Rimuovi**. **Valore predefinito** • **Active Directory:** `group?member` • **Directory LDAP diverse da Active Directory:** `groupofuniquenames?uniquemember, groupOfNames?member` • **Directory nativa:** `groupofuniquenames?uniquemember, cssGroupExtend?cssIsActive`
Filtro per limitare i gruppi	Query LDAP che recupera solo i gruppi a cui sono stati assegnati ruoli dei prodotti di EPM System. Ad esempio, la query LDAP `(|(cn=Hyp*)(cn=Admin*))` recupera solo i gruppi il cui nome inizia con `Hyp` o `Admin`. Il filtro gruppi, che consente di limitare il numero di gruppi restituiti durante una query, risulta particolarmente importante se il nodo identificato dall'RDN gruppo contiene molti gruppi a cui non è necessario assegnare ruoli. È possibile progettare filtri per escludere i gruppi a cui non assegnare ruoli e ottenere quindi performance migliori. Se si utilizza il gruppo primario di Active Directory per l'assegnazione ruoli, assicurarsi che gli eventuali filtri gruppi impostati consentano il recupero del gruppo primario contenuto nell'ambito dell'URL gruppo. Ad esempio, il filtro `(|(cn=Hyp*)(cn=Domain Users))` consente di recuperare i gruppi il cui nome inizia con `Hyp` e il gruppo primario denominato `Domain Users`.

[1] Nella protezione di EPM System è possibile utilizzare valori predefiniti per alcuni campi per i quali il valore di configurazione è facoltativo. Se non si inserisce un valore in tali campi, in fase di esecuzione verranno utilizzati i valori predefiniti.

12. Fare clic su **Fine**.

In Shared Services viene salvata la configurazione e viene nuovamente visualizzata la schermata Directory definite dall'utente, in cui è ora elencata la directory utente configurata.

13. Eseguire il test della configurazione. Fare riferimento alla sezione Test delle connessioni delle directory utente.
14. Se necessario, modificare l'assegnazione dell'ordine di ricerca. Per informazioni dettagliate, fare riferimento alla sezione Gestione dell'ordine di ricerca delle directory utente.
15. Se necessario, specificare le impostazioni di protezione. Per informazioni dettagliate, fare riferimento alla sezione Impostazione delle opzioni di sicurezza.
16. Riavviare Oracle Hyperion Foundation Services e gli altri componenti di EPM System.

Configurazione dei database relazionali come directory utente

È possibile utilizzare le informazioni sugli utenti e i gruppi delle tabelle di sistema dei database relazionali Oracle, SQL Server e IBM DB2 per supportare l'assegnazione ruoli. Se non è possibile ottenere le informazioni sui gruppi dallo schema di sistema del database, significa che Oracle Hyperion Shared Services non supporta l'assegnazione di ruoli a gruppi dal provider del database. Ad esempio, Shared Services non è in grado di estrarre le informazioni sui gruppi da versioni precedenti di IBM DB2, in quanto il database utilizza gruppi definiti nel sistema operativo. I responsabili della gestione assegnazione ruoli possono tuttavia aggiungere tali utenti ai gruppi presenti nella directory nativa e assegnare ruoli a tali gruppi. Per informazioni sulle piattaforme supportate, fare riferimento alla sezione *Matrice per la certificazione di Oracle Enterprise Performance Management System* pubblicata nella pagina Configurazioni di sistema supportate da Oracle Fusion Middleware su Oracle Technology Network (OTN).

> **Nota:**
>
> Se si utilizza un database DB2 il nome utente deve contenere almeno otto caratteri. Il valore del nome utente non deve superare 256 caratteri nei database Oracle e SQL Server e 1000 nei database DB2.

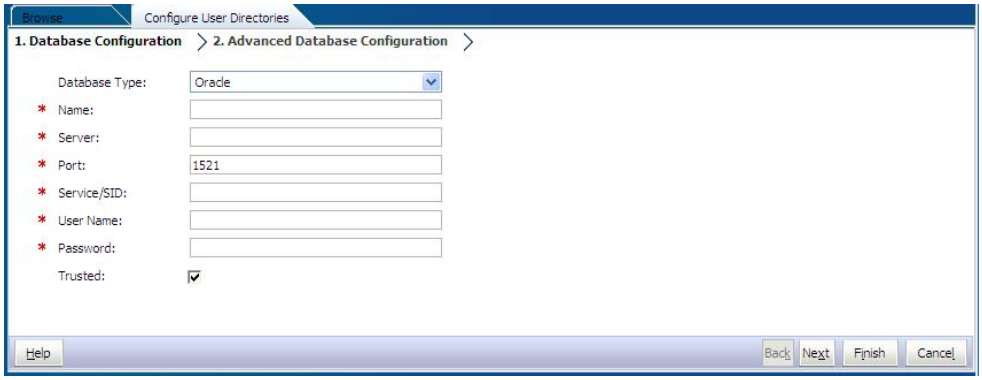
Per poter recuperare l'elenco di utenti e gruppi, configurare in Shared Services la connessione al database come amministratore del database, ad esempio come utente Oracle `SYSTEM`.

> **Nota:**
>
> Shared Services è in grado di recuperare solo gli utenti dei database attivi per l'assegnazione ruoli. Gli account utente di database non attivi o bloccati vengono ignorati.

Per configurare i provider di database, procedere come segue:

1. Accedere a Oracle Hyperion Shared Services Console come amministratore di sistema. Fare riferimento alla sezione Avvio di Shared Services Console.

2. Selezionare **Amministrazione**, quindi **Configura directory utenti**.
3. Fare clic su **Nuovo**.
4. Nella schermata **Tipo directory**, selezionare **Database relazionale (Oracle, DB2, SQL Server)**.
5. Fare clic su **Avanti**.



6. Nella scheda Configurazione database, immettere i parametri di configurazione.

Tabella 4-4 Scheda Configurazione database

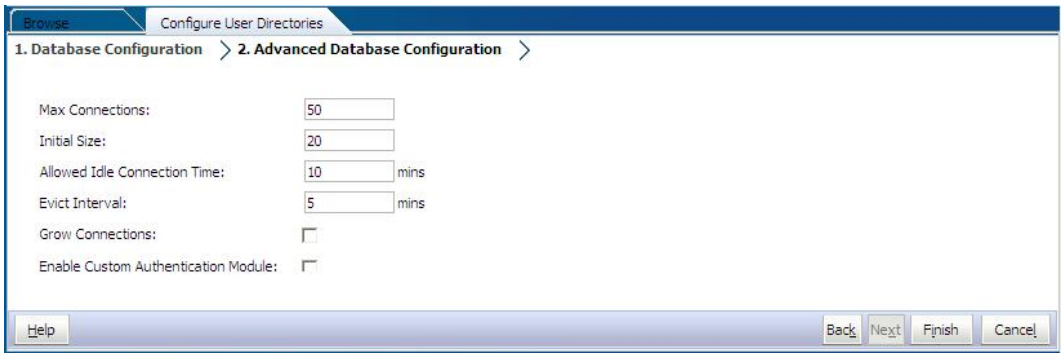
Etichetta	Descrizione
Tipo di database	Il provider del database relazionale. Shared Services supporta solo i database Oracle e SQL Server come provider di database. **Esempio:** `Oracle`
Nome	Nome di configurazione univoco per il provider del database. **Esempio:** `Oracle_DB_FINANCE`
Server	Nome DNS del computer in cui il server database è in esecuzione. **Esempio:** `myserver`
Porta	Numero di porta del server database. **Esempio:** `1521`
Servizio/SID (solo Oracle)	L'identificativo del sistema. Il valore predefinito è `orcl`. **Esempio:** `orcl`
Database (solo SQL Server e DB2)	Il database a cui Shared Services deve connettersi. **Esempio:** `master`
Nome utente	Il nome utente che Shared Services deve utilizzare per accedere al database. Questo utente del database deve disporre dei privilegi di accesso alle tabelle di sistema del database. Oracle consiglia di utilizzare l'account `system` per i database Oracle e il nome utente dell'amministratore del database per i database SQL Server. **Esempio:** `SYSTEM`
Password	La password dell'utente identificato in **Nome utente**. **Esempio:** `system_password`

Tabella 4-4 (Cont.) Scheda Configurazione database

Etichetta	Descrizione
Sicuro	La casella di controllo che consente di specificare che il provider è un'origine SSO attendibile. I token SSO provenienti dalle origini attendibili non contengono la password dell'utente.

7. **Opzionale:** fare clic su **Avanti** per configurare il connection pool.

   Viene visualizzata la scheda Configurazione database avanzata.



8. In Configurazione database avanzata, immettere i parametri del connection pool.

Tabella 4-5 Scheda Configurazione database avanzata

Etichetta	Descrizione
N. massimo connessioni	Il numero massimo di connessioni che è possibile includere nel pool. L'impostazione predefinita è 50.
Dimensione iniziale	Le connessioni disponibili quando il pool viene inizializzato. L'impostazione predefinita è 20.
Tempo di inattività consentito per la connessione	**Facoltativo:** tempo trascorso il quale le connessioni inattive vengono rimosse dal pool con il processo di rimozione. L'impostazione predefinita è 10 minuti.
Intervallo di eliminazione	**Facoltativo:** intervallo per l'esecuzione del processo di rimozione per il cleanup del pool. Il processo di rimozione consente di eliminare le connessioni inattive che hanno superato il valore specificato in `Tempo di inattività consentito per la connessione`. Il valore predefinito è cinque minuti.
Aumenta connessioni	Indica se il connection pool può essere espanso oltre il valore di `N. massimo connessioni`. Per impostazione predefinita, questa opzione è deselezionata a indicare che il pool non può essere espanso. Se non si consente l'espansione del pool, il sistema restituirà un errore se la connessione non è disponibile entro l'intervallo di tempo impostato per `Timeout`.

Tabella 4-5 (Cont.) Scheda Configurazione database avanzata

Etichetta	Descrizione
Abilita modulo di autenticazione custom	Casella di controllo per abilitare l'utilizzo di un modulo di autenticazione custom per l'autenticazione degli utenti definiti nella directory utente. È necessario immettere inoltre il nome completo della classe Java del modulo di autenticazione nella schermata Opzioni protezione. Fare riferimento alla sezione Impostazione delle opzioni di sicurezza. Il modulo di autenticazione custom è trasparente per i client thin e thick. Fare riferimento alla sezione "Modulo autenticazione custom" nella *Oracle Enterprise Performance Management System Security Configuration Guide (in lingua inglese)*.

9. Fare clic su **Fine**.
10. Fare clic su **OK** per tornare alla schermata Directory definite dall'utente.
11. Verificare la configurazione del provider del database. Fare riferimento alla sezione Test delle connessioni delle directory utente.
12. Modificare l'assegnazione dell'ordine di ricerca, se necessario. Per informazioni dettagliate, fare riferimento alla sezione Gestione dell'ordine di ricerca delle directory utente.
13. Specificare le impostazioni di protezione, se necessario. Fare riferimento alla sezione Impostazione delle opzioni di sicurezza.
14. Riavviare Oracle Hyperion Foundation Services e gli altri componenti di Oracle Enterprise Performance Management System.

Test delle connessioni delle directory utente

Dopo aver configurato una directory utenti, verificare la connessione per assicurarsi che Oracle Hyperion Shared Services sia in grado di connettersi alla directory utenti utilizzando le impostazioni correnti.

Per verificare la connessione della directory utente, procedere come segue:

1. Accedere a Oracle Hyperion Shared Services Console come amministratore di sistema. Fare riferimento alla sezione Avvio di Shared Services Console.
2. Selezionare **Amministrazione**, quindi **Configura directory utenti**.
3. Dall'elenco di directory utente selezionare una configurazione di directory utente esterna da verificare.
4. Fare clic su **Test**, quindi su **OK**.

Modifica delle impostazioni delle directory utente

Gli amministratori possono modificare qualsiasi parametro della configurazione di una directory utenti, ad eccezione del nome. Oracle consiglia di non modificare i dati di configurazione delle directory utente che sono state utilizzate per l'assegnazione ruoli.

> **Attenzione:**
>
> La modifica di alcune impostazioni, ad esempio l'`attributo ID`, nella configurazione della directory utente invalida i dati dell'assegnazione ruoli. È quindi necessario prestare la massima attenzione quando si modificano le impostazioni di una directory utente a cui sono stati assegnati i ruoli.

Per modificare la configurazione di una directory utente, procedere come segue:

1. Accedere a Oracle Hyperion Shared Services Console come amministratore di sistema. Fare riferimento alla sezione Avvio di Shared Services Console.
2. Selezionare **Amministrazione**, quindi **Configura directory utenti**.
3. Selezionare un directory utente da modificare.
4. Fare clic su **Modifica**.
5. Modificare le impostazioni di configurazione.

   > **Nota:**
   >
   > Non è possibile modificare il nome della configurazione. Se si sta modificando la configurazione di una directory utente LDAP, è possibile scegliere un server delle directory diverso o la voce `Altro` per le directory utente LDAP custom dall'elenco Server delle directory. I parametri della directory nativa non possono essere modificati.

   Per una descrizione dei parametri che è possibile modificare, vedere le seguenti tabelle:

   - Active Directory e altre directory utenti basate su LDAP, fare riferimento alle tabelle in Configurazione di OID, Active Directory e altre directory utenti basate su LDAP.
   - Database: fare riferimento alla tabella in Configurazione dei database relazionali come directory utente
6. Fare clic su **OK** per salvare le modifiche.

Eliminazione delle configurazioni delle directory utente

Gli amministratori di sistema possono eliminare la configurazione di una directory utenti esterna in qualsiasi momento. L'eliminazione della configurazione di una directory utente invalida tutte le informazioni sull'assegnazione ruoli relative agli utenti e ai gruppi in essa contenuti, determinando inoltre la rimozione della directory dall'ordine di ricerca.

> **Suggerimento:**
>
> Se non si desidera utilizzare una directory utente configurata che è stata utilizzata per l'assegnazione ruoli, rimuoverla dall'ordine di ricerca affinché non sia possibile eseguirvi ricerche di utenti e gruppi. Questo consente di mantenere l'integrità delle informazioni sull'assegnazione ruoli e di utilizzare la directory in un secondo momento.

Per eliminare la configurazione di una directory utente, procedere come segue:

1. Accedere a Oracle Hyperion Shared Services Console come amministratore di sistema. Fare riferimento alla sezione Avvio di Shared Services Console.
2. Selezionare **Amministrazione**, quindi **Configura directory utenti**.
3. Selezionare una directory.
4. Fare clic su **Elimina**.
5. Fare clic su **OK**.
6. Fare di nuovo clic su **OK**.
7. Riavviare Oracle Hyperion Foundation Services e gli altri componenti di Oracle Enterprise Performance Management System.

Gestione dell'ordine di ricerca delle directory utente

Quando un amministratore di sistema configura una directory utenti esterna, Oracle Hyperion Shared Services la aggiunge automaticamente all'ordine di ricerca e la assegna alla successiva sequenza di ricerca disponibile precedente a quella della directory nativa. L'ordine di ricerca viene utilizzato per scorrere in sequenza le directory utenti configurate quando in Oracle Enterprise Performance Management System viene eseguita la ricerca di utenti e gruppi.

Gli amministratori di sistema possono rimuovere una directory utenti dall'ordine di ricerca. In tal caso, Shared Services riassegna automaticamente l'ordine di ricerca alle directory rimanenti. Le directory utente non incluse nell'ordine di ricerca non vengono utilizzate per supportare i processi di autenticazione e assegnazione ruoli.

> **Nota:**
>
> Una volta rilevato l'account specificato, Shared Services interrompe la ricerca dell'utente o del gruppo. Oracle consiglia di posizionare la directory aziendale che contiene la maggior parte degli utenti di EPM System all'inizio dell'ordine di ricerca.

Per impostazione predefinita, la directory nativa è impostata come ultima directory nell'ordine di ricerca. Per gestire l'ordine di ricerca, gli amministratori possono eseguire i task riportati di seguito.

- Aggiunta di una directory utente all'ordine di ricerca
- Modifica dell'ordine di ricerca

- Rimozione di un'assegnazione dell'ordine di ricerca

Aggiunta di una directory utente all'ordine di ricerca

Una directory utente appena configurata viene automaticamente aggiunta all'ordine di ricerca. Se si è rimossa una directory dall'ordine di ricerca, è possibile aggiungerla alla fine dell'ordine di ricerca.

Per aggiungere una directory utente all'ordine di ricerca, procedere come segue:

1. Accedere a Oracle Hyperion Shared Services Console come amministratore di sistema. Fare riferimento alla sezione Avvio di Shared Services Console.
2. Selezionare **Amministrazione**, quindi **Configura directory utenti**.
3. Selezionare una directory utente disattivata da aggiungere all'ordine di ricerca.
4. Fare clic su **Includi**.

   Questo pulsante è disponibile solo se è stata selezionata una directory utente non inclusa nell'ordine di ricerca.
5. Fare clic su **OK** per tornare alla schermata Directory definite dall'utente.
6. Riavviare Oracle Hyperion Foundation Services e gli altri componenti di EPM System.

Rimozione di un'assegnazione dell'ordine di ricerca

La rimozione di una directory utente dall'ordine di ricerca non comporta l'invalidazione della configurazione, ma si limita alla rimozione della directory stessa dall'elenco di directory in cui vengono eseguite ricerche per l'autenticazione degli utenti. Lo stato di una directory non inclusa nell'ordine di ricerca viene impostato su `Disattivato`. Quando un amministratore rimuove una directory utenti dall'ordine di ricerca, la sequenza di ricerca assegnata alle altre directory utenti viene aggiornata automaticamente.

> **Nota:**
>
> La directory nativa non può essere rimossa dall'ordine di ricerca.

Per rimuovere una directory utente dall'ordine di ricerca, procedere come segue:

1. Accedere a Shared Services Console come amministratore di sistema. Fare riferimento alla sezione Avvio di Shared Services Console.
2. Selezionare **Amministrazione**, quindi **Configura directory utenti**.
3. Selezionare una directory da rimuovere dall'ordine di ricerca.
4. Fare clic su **Escludi**.
5. Fare clic su **OK**.
6. Fare clic su **OK** nella schermata Risultato configurazione directory.
7. Riavviare Foundation Services e gli altri componenti di EPM System.

Modifica dell'ordine di ricerca

L'ordine di ricerca predefinito assegnato a ciascuna directory utente si basa sulla sequenza in cui la directory è stata configurata. Per impostazione predefinita, la directory nativa è impostata come ultima directory nell'ordine di ricerca.

Per modificare l'ordine di ricerca, procedere come segue:

1. Accedere a Shared Services Console come amministratore di sistema. Fare riferimento alla sezione Avvio di Shared Services Console.
2. Selezionare **Amministrazione**, quindi **Configura directory utenti**.
3. Selezionare una directory per la quale si desidera modificare l'ordine di ricerca.
4. Fare clic su **Sposta su** o **Sposta giù**.
5. Fare clic su **OK**.
6. Riavviare Foundation Services, altri componenti di EPM System e le applicazioni custom che utilizzano le API di sicurezza di Shared Services.

Impostazione delle opzioni di sicurezza

Le opzioni di protezione comprendono parametri globali che è possibile applicare a tutte le directory utente incluse nell'ordine di ricerca.

Per impostare le opzioni di protezione, procedere come segue:

1. Accedere a Oracle Hyperion Shared Services Console come amministratore di sistema. Fare riferimento alla sezione Avvio di Shared Services Console.
2. Selezionare **Amministrazione**, quindi **Configura directory utenti**.
3. Selezionare **Opzioni sicurezza**.
4. In **Opzioni di protezione**, impostare i parametri globali.

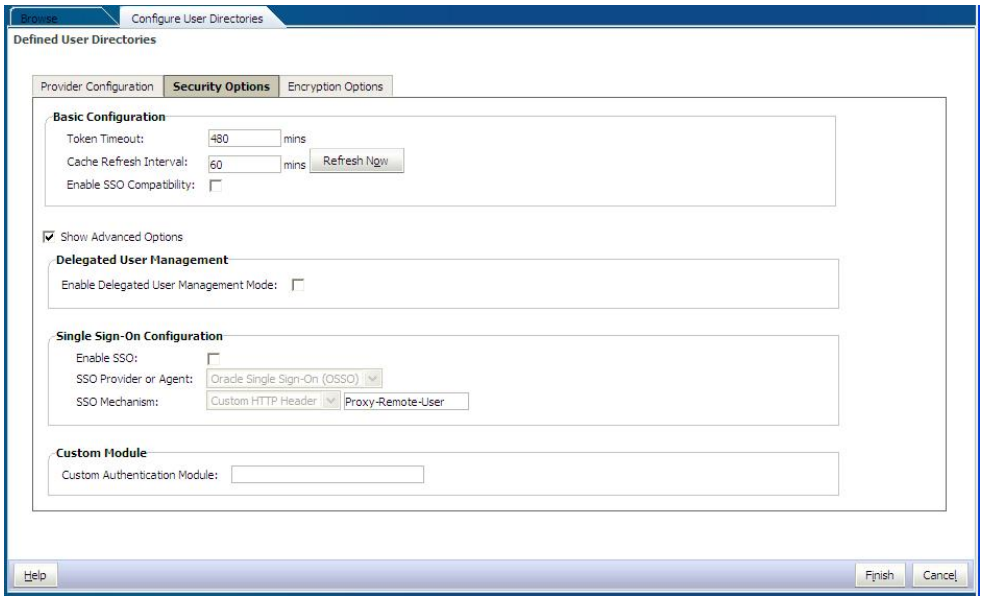


Tabella 4-6 Opzioni di protezione per le directory utente

Parametro	Descrizione
Timeout token	Intervallo di tempo, in minuti, trascorso il quale scade il token SSO emesso dai prodotti Oracle Enterprise Performance Management System oppure la soluzione di gestione identità Web. Una volta trascorso questo periodo, è necessario eseguire nuovamente l'accesso. Il timeout del token viene impostato in base al clock di sistema del server. L'intervallo predefinito è di 480 minuti. **Nota:** il timeout del token non corrisponde al timeout della sessione.
Intervallo aggiornamento cache	Intervallo, in minuti, per l'aggiornamento della cache di Oracle Hyperion Shared Services con i dati delle relazioni tra gruppi e utenti. L'intervallo predefinito è di `60` minuti. Shared Services inserisce nella cache le informazioni dei nuovi gruppi di directory utente esterne e dei nuovi utenti aggiunti a gruppi esistenti solo dopo l'aggiornamento successivo della cache. Agli utenti a cui è stato assegnato un ruolo tramite un nuovo gruppo di directory utente non ottengono il ruolo assegnato fino a quando non viene aggiornata la cache
Aggiorna ora	Fare clic su questo pulsante per inizializzare manualmente l'aggiornamento della cache di Shared Services contenente i gruppi in base ai dati di relazione degli utenti. È possibile che si desideri inizializzare un aggiornamento della cache dopo aver creato nuovi gruppi nelle directory utente esterne e assegnargli un ruolo oppure dopo aver aggiunto nuovi utenti a gruppi esistenti. La cache viene aggiornata solo dopo che Shared Services invia una chiamata che utilizza i dati nella cache.
Abilita compatibilità SSO	Selezionare questa opzione se la distribuzione è integrata con Oracle Business Intelligence Enterprise Edition release 11.1.1.5 o precedente.
Abilita modalità di gestione utente delegato	Consente di abilitare la gestione degli utenti delegati dei prodotti di EPM System per il supporto della gestione distribuita delle attività di assegnazione ruoli. Fare riferimento alla sezione "Gestione di utenti delegati" nel manuale *Oracle Enterprise Performance Management System User Security Administration Guide (in lingua inglese)*.
Abilita SSO	Consente di abilitare il supporto per SSO dagli agenti di protezione, ad esempio Oracle Access Manager.

Tabella 4-6 (Cont.) Opzioni di protezione per le directory utente

Parametro	Descrizione
Provider o agente SSO	Consente di selezionare la soluzione di gestione delle identità sul Web dalla quale i prodotti di EPM System devono accettare l'SSO. Selezionare **Altro** se la soluzione di gestione identità Web in uso, ad esempio Kerberos, non è elencata. Il nome e il meccanismo SSO preferito vengono selezionati automaticamente nel momento in cui si seleziona il provider SSO. Se necessario, è possibile modificare il nome del meccanismo SSO (intestazione HTTP o classe di accesso custom). Se si seleziona `Other` come agente o provider SSO, è necessario verificare che sia possibile utilizzare un meccanismo SSO supportato da EPM System. Fare riferimento alla sezione "Metodi SSO supportati" nel manuale *Oracle Enterprise Performance Management System Security Configuration Guide (in lingua inglese)*.
Meccanismo SSO	È il metodo che la soluzione selezionata per la gestione delle identità Web utilizza per fornire il nome di accesso dell'utente ai prodotti EPM System. Per una descrizione dei metodi SSO che è possibile utilizzare, fare riferimento alla sezione "Metodi SSO supportati" nel manuale *Oracle Enterprise Performance Management System Security Configuration Guide (in lingua inglese)*. • `Intestazione HTTP customizzata`: consente di impostare il nome dell'intestazione che l'agente di protezione passa a EPM System. • `Classe di accesso customizzata`: consente di specificare la classe Java customizzata che gestisce le richieste HTTP per l'autenticazione. Fare riferimento alla sezione "Classe di accesso customizzata" nel manuale *Oracle Enterprise Performance Management System Security Configuration Guide (in lingua inglese)*. **Nota:** La classe di accesso custom non è come l'autenticazione custom. • `Intestazione autorizzazione HTTP`: meccanismo HTTP standard. • `Richiama utente remoto da richiesta HTTP`: selezionare questa opzione per inserire l'utente remoto nella richiesta HTTP mediante l'agente di protezione.

Tabella 4-6 (Cont.) Opzioni di protezione per le directory utente

Parametro	Descrizione
Modulo autenticazione custom	Il nome completo della classe Java del modulo di autenticazione custom, ad esempio `com.mycompany.epm.CustomAuthenticationImpl`, da utilizzare per l'autenticazione degli utenti di tutte le directory utente per le quali è selezionato il modulo di autenticazione custom. Il modulo di autenticazione viene utilizzato per una directory utente solo se la configurazione della directory ne consente l'utilizzo (impostazione predefinita). Per Oracle Hyperion Foundation Services è necessario che il file JAR di autenticazione customizzata sia denominato `CustomAuth.jar`. `CustomAuth.jar` deve essere disponibile in *`MIDDLEWARE_HOME`*`\user_projects\domains\`*`WEBLOGIC_DOMAIN`*`\lib`, in genere `C:\Oracle/Middleware/user_projects/domains/EPMSystem/lib`. In tutte le installazioni client, `CustomAuth.jar` deve essere presente in *`EPM_ORACLE_HOME`*`/common/jlib/11.1.2.0`, in genere `C:\Oracle\Middleware\EPMSystem11R1\common\jlib\11.1.2.0`. È possibile utilizzare qualsiasi struttura del package e nome di classe all'interno del file JAR. Per ulteriori informazioni, fare riferimento alla sezione "Utilizzo di un modulo di autenticazione custom" nella *Oracle Enterprise Performance Management System Security Configuration Guide (in lingua inglese)*.

5. Fare clic su **OK**.
6. Riavviare Foundation Services e gli altri componenti di EPM System.

Rigenerazione delle chiavi di cifratura

Oracle Enterprise Performance Management System utilizza le chiavi riportate di seguito per garantire la sicurezza.

- Chiave di cifratura Token Single Sign-On, utilizzata per cifrare e decifrare i token SSO di EPM System. Questa chiave è memorizzata nel registro di Oracle Hyperion Shared Services
- Chiave dei trusted service, utilizzata dai componenti di EPM System per verificare l'autenticità del servizio che fa richiesta di un token SSO
- Chiave di cifratura Configurazione provider, utilizzata per cifrare la password (password DN dell'utente per le directory utente abilitate per LDAP) utilizzata dalla protezione di EPM System per eseguire l'associazione con una directory utente esterna configurata. Questa password viene impostata durante la configurazione di una directory utente esterna.

Modificare periodicamente queste chiavi per rafforzare la sicurezza di EPM System. Oracle Hyperion Shared Services e il sottosistema di sicurezza di EPM System utilizzano la cifratura AES con chiavi a 128 bit.

> **Attenzione:**
>
> I flussi di task utilizzati da Oracle Hyperion Financial Management e Oracle Hyperion Profitability and Cost Management vengono invalidati quando si genera di nuovo la chiave di cifratura Single Sign-On. Dopo aver rigenerato la chiave, aprire e salvare i flussi di task per riconvalidarli.

Per rigenerare la chiave di cifratura Single Sign-On, il tasto Configurazione provider o la chiave dei trusted service:

1. Accedere a Oracle Hyperion Shared Services Console come amministratore di sistema. Fare riferimento alla sezione Avvio di Shared Services Console.
2. Selezionare **Amministrazione**, quindi **Configura directory utenti**.
3. Selezionare **Opzioni cifratura**.
4. In **Opzioni cifratura** selezionare la chiave che si desidera rigenerare.

Tabella 4-7 Opzioni cifratura di EPM System

Opzione	Descrizione
Token Single Sign-On	Selezionare per rigenerare la chiave di cifratura utilizzata per cifrare e decifrare i token SSO di EPM System. Selezionare uno dei pulsanti seguenti se l'opzione **Abilita compatibilità SSO** è selezionata in **Opzioni sicurezza**. • **Genera nuova chiave** per creare una nuova chiave di cifratura per i token SSO • **Ripristina valore predefinito** per ripristinare la chiave di cifratura predefinita per i token SSO **Nota:** Se si ripristina la chiave di cifratura predefinita, è necessario eliminare il file keystore esistente (*EPM_ORACLE_HOME*/`common/CSS/ssHandlerTK`) da tutti i computer host di EPM System.
Chiave dei trusted service	Selezionare questa opzione per rigenerare la chiave per l'autenticazione di accesso sicuro, utilizzata dai componenti di EPM System per verificare l'autenticità del servizio che fa richiesta di un token SSO.
Chiave configurazione provider	Selezionare questa opzione per rigenerare la chiave utilizzata per cifrare la password (password DN dell'utente per le directory utente abilitate per LDAP) utilizzata dalla protezione di EPM System per eseguire l'associazione con una directory utenti esterna configurata. Questa password viene impostata durante la configurazione di una directory utente esterna.

5. Fare clic su **OK**.

6. Se si sceglie di generare una nuova chiave di cifratura SSO, eseguire il passaggio riportato di seguito.
   a. Fare clic su **Scarica**.
   b. Fare clic su **OK** per salvare `ssHandlerTK`, il file del keystore che supporta la nuova chiave di cifratura SSO, in una cartella sul server che ospita Oracle Hyperion Foundation Services.
   c. Copiare `ssHandlerTK` in *EPM_ORACLE_HOME*`/common/CSS` su tutti i computer host di EPM System.
7. Riavviare Foundation Services e gli altri componenti di EPM System.

Utilizzo di caratteri speciali

Active Directory e altre directory utenti basate su LDAP consentono l'utilizzo di caratteri speciali all'interno di entità quali DN, nomi utente, ruoli e nomi di gruppi. Per consentire a Oracle Hyperion Shared Services di interpretare i caratteri speciali potrebbero essere necessari interventi specifici.

In genere, è necessario utilizzare caratteri di escape quando si specificano caratteri speciali nelle impostazioni delle directory utente, ad esempio per il DN di base e gli URL di utenti e di gruppi. Nella tabella che segue sono riportati i caratteri speciali che è possibile utilizzare in nomi utente, nomi di gruppi, URL di utenti e di gruppi e nel valore di OU nel DN utente.

Tabella 4-8 Caratteri speciali supportati

Carattere	Nome o significato	Carattere	Nome o significato
(	parentesi aperta	$	dollaro
)	parentesi chiusa	+	segno più
"	virgolette	&	e commerciale
'	virgolette singole	\	barra rovesciata
,	virgola	^	accento circonflesso
=	uguale a	;	punto e virgola
<	minore di	#	cancelletto
>	maggiore di	@	chiocciola

> **Nota:**
>
> Non utilizzare la barra (/) nei nomi di unità organizzativa inclusi nel DN di base

- I caratteri speciali non sono consentiti nel valore dell'attributo utente di accesso
- L'asterisco (*) non è supportato all'interno di nomi utente, nomi di gruppi, URL di utenti e URL di gruppi né nel nome di OU nel DN utente.
- I valori degli attributi contenenti una combinazione di caratteri speciali non sono supportati.

- La E commerciale (&) può essere utilizzata senza un carattere di escape. Per le impostazioni di Active Directory, il carattere & deve essere specificato con il formato seguente: `&`.
- I nomi di utenti e gruppi non possono contenere contemporaneamente la barra rovesciata (\) e la barra (/). Ad esempio, nomi come `test/\user` e `new\test/user` non sono supportati.

Tabella 4-9 Caratteri per cui non è necessario specificare un carattere di escape

Carattere	Nome o significato	Carattere	Nome o significato
(	parentesi aperta	'	virgolette singole
)	parentesi chiusa	^	accento circonflesso
$	dollaro	@	chiocciola
&	e commerciale		

> **Nota:**
>
> & deve essere specificata con il formato `&`.

È necessario utilizzare un carattere di escape per questi caratteri quando utilizzati nelle impostazioni delle directory utente, ad esempio nomi utente, nomi di gruppi, URL di utenti, URL di gruppi e DN utente.

Tabella 4-10 Carattere di escape per i caratteri speciali nelle impostazioni di configurazione delle directory utente

Carattere speciale	Carattere di escape	Impostazione di esempio	Esempio con carattere di escape
virgola (,)	barra rovesciata (\)	`ou=test,ou`	`ou=test\,ou`
segno più (+)	barra rovesciata (\)	`ou=test+ou`	`ou=test\+ou`
uguale a (=)	barra rovesciata (\)	`ou=test=ou`	`ou=test\=ou`
cancelletto (#)	barra rovesciata (\)	`ou=test#ou`	`ou=test\#ou`
punto e virgola (;)	barra rovesciata (\)	`ou=test;ou`	`ou=test\;ou`
minore di (<)	barra rovesciata (\)	`ou=test<ou`	`ou=test\<ou`
maggiore di (>)	barra rovesciata (\)	`ou=test>ou`	`ou=test\>ou`
virgolette doppie (")	due barre rovesciate (\\)	`ou=test"ou`	`ou=test\\"ou`
barra rovesciata (\)	tre barre rovesciate (\\\)	`ou=test\ou`	`ou=test\\\\ou`

Nota:

- Nei DN utente, per le virgolette (") è necessario utilizzare un carattere di escape, ovvero la barra rovesciata. Ad esempio, `ou=test"ou` deve essere specificato con il formato `ou=test\"ou`.
- Nei DN utente, per la barra rovesciata (\) è necessario utilizzare una barra rovesciata che funge da carattere di escape. Ad esempio, `ou=test\ou` deve essere specificato con il formato `ou=test\\ou`.

Attenzione:

Se l'URL dell'utente non è specificato, gli utenti creati nella radice RDN non devono contenere il carattere / (barra) o \ (barra rovesciata). In modo analogo, questi caratteri non devono essere utilizzati nei nomi dei gruppi creati nella radice RDN se non è stato specificato un URL per tali gruppi. Ad esempio, i nomi dei gruppi, come `OU=child\ou,OU=parent/ou` o `OU=child/ou,OU=parent\ou`, non sono supportati. Questo problema non si verifica se si utilizza un attributo univoco come `Attributo ID` nella configurazione delle directory utente.

Caratteri speciali nella directory nativa

I caratteri speciali sono supportati nei nomi di utenti e gruppi nella directory nativa.

Tabella 4-11 Caratteri speciali supportati: directory nativa

Carattere	Nome o significato	Carattere	Nome o significato
@	chiocciola	,	virgola
#	cancelletto	=	uguale a
$	dollaro	+	segno più
^	accento circonflesso	;	punto e virgola
(	parentesi aperta	!	punto esclamativo
)	parentesi chiusa	%	percentuale
'	virgolette singole		

5

Utilizzo di un modulo di autenticazione custom

Vedere anche:

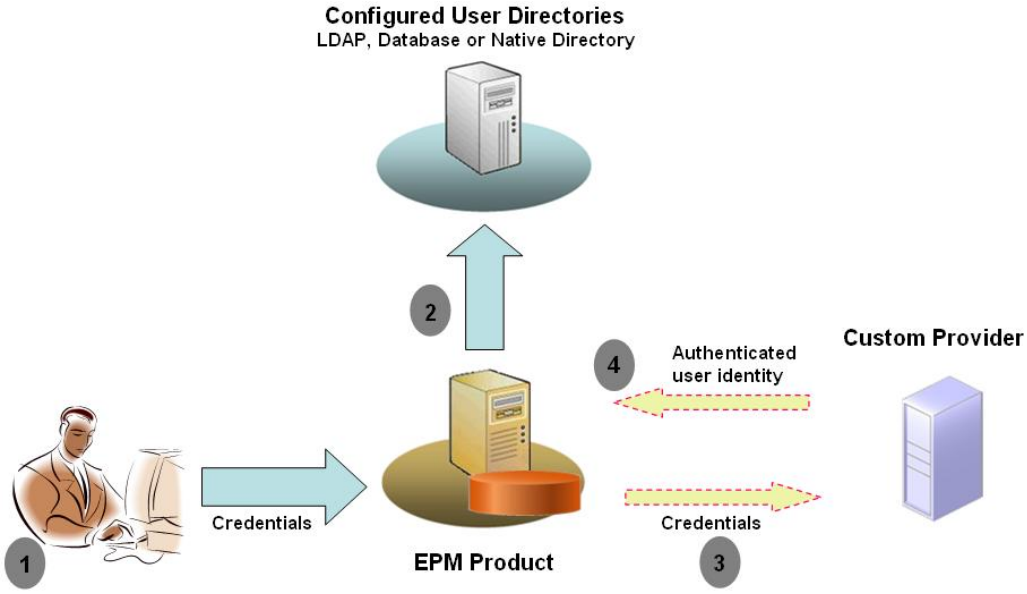
Panoramica

Un modulo di autenticazione customizzato è un modulo Java sviluppato e implementato dai clienti per l'autenticazione degli utenti Oracle Enterprise Performance Management System. I prodotti EPM System in genere utilizzano una schermata di accesso per acquisire il nome utente e la password, che vengono utilizzati per autenticare gli utenti. Anziché utilizzare l'autenticazione di EPM System, è possibile creare un modulo di autenticazione customizzato per autenticare gli utenti e passare le credenziali degli utenti autenticati a EPM System per un'ulteriore elaborazione. L'implementazione di un modulo di autenticazione customizzato non comporta la modifica dei prodotti EPM System.

È possibile utilizzare un modulo di autenticazione customizzato sia con thick client (ad esempio Oracle Smart View for Office e Oracle Essbase Studio) che con thin client (ad esempio Oracle Hyperion Enterprise Performance Management Workspace).

Il modulo di autenticazione customizzato utilizza le informazioni immesse da un utente durante l'accesso a un prodotto EPM System. Se abilitato per una directory utenti, autentica gli utenti tramite il modulo di autenticazione customizzato. Dopo aver eseguito correttamente l'autenticazione dell'utente, il modulo di autenticazione customizzato restituisce il nome utente a EPM System.

La figura riportata di seguito presenta uno scenario di autenticazione customizzata campione:



È ad esempio possibile utilizzare l'infrastruttura RSA SecurID come provider customizzato per garantire un'autenticazione avanzata trasparente in EPM System. Viene riportata di seguito una panoramica.

1. L'utente immette le credenziali (in genere nome utente e password) per accedere a un prodotto EPM System. Queste credenziali devono identificare in modo univoco l'utente per il provider utilizzato dal modulo di autenticazione customizzato. Se ad esempio si utilizza un'infrastruttura RSA SecurID per autenticare gli utenti, l'utente immette un ID utente e un PIN RSA (non un ID utente e una password EPM System).
2. Utilizzando l'ordine di ricerca (fare riferimento alla sezione Ordine di ricerca), EPM System attraversa ciclicamente le directory utenti configurate per individuare l'utente.
   - Se la directory utenti corrente non è configurata per l'autenticazione customizzata, EPM System tenta di individuare e autenticare l'utente tramite l'autenticazione di EPM System.
   - Se la directory utenti è configurata per l'autenticazione customizzata, EPM System delega il processo di autenticazione al modulo customizzato.
3. Se EPM System delega l'autenticazione al modulo customizzato, il modulo di autenticazione customizzato accetta le credenziali e utilizza la propria logica per indirizzare l'autenticazione utente a fronte di un provider customizzato, ad esempio l'infrastruttura RSA SecurID.
4. Se autentica l'utente a fronte del proprio provider, il modulo di autenticazione customizzato restituisce il nome utente a EPM System oppure restituisce un'eccezione Java.

   Il nome utente restituito dal modulo di autenticazione customizzato deve essere identico a un nome utente in una directory utenti abilitata per l'autenticazione customizzata.
   - Se il modulo di autenticazione customizzato restituisce un nome utente, EPM System individua l'utente in una directory utenti abilitata per l'autenticazione customizzata. A questo stadio, EPM System non esegue la ricerca nelle directory utenti non configurate per l'autenticazione customizzata.

- Se il modulo di autenticazione customizzato genera un'eccezione o restituisce un utente null, EPM System continua a cercare l'utente secondo l'ordine di ricerca nelle directory utenti rimanenti non abilitate per l'autenticazione customizzata. Se non viene trovato un utente corrispondente alle credenziali, EPM System visualizza un errore.

Esempi e limitazioni dei casi d'uso

Tra gli scenari di implementazione dell'autenticazione customizzata sono inclusi quelli elencati di seguito.

- Aggiunta del supporto di password monouso
- Esecuzione dell'autenticazione a fronte di un sistema Resource Access Control Facility (RACF)
- Aggiunta di un'autenticazione Simple Authentication and Security Layer (SASL) a directory utenti abilitate per LDAP anziché semplici autenticazioni LDAP

È possibile che l'autenticazione con un meccanismo di richieste di verifica/risposte non funzioni correttamente se si implementa un modulo di autorizzazione customizzato. I messaggi customizzati generati dal modulo non vengono propagati ai client. Poiché i client, ad esempio Oracle Hyperion Enterprise Performance Management Workspace, sostituiscono il messaggio di errore e visualizzano un messaggio generico, gli scenari descritti di seguito non sono validi.

- Due PIN RSA SecurID consecutivi
- Variante della password con richieste di verifica, ad esempio l'immissione del primo, dell'ultimo e del terzo carattere di una password

Prerequisiti

- Un archivio Java completamente testato denominato `CustomAuth.jar` contenente le librerie del modulo di autenticazione customizzato. `CustomAuth.jar` deve implementare l'interfaccia pubblica `CSSCustomAuthenticationIF`, definita nel package `com.hyperion.css` come parte delle API di Oracle Hyperion Shared Services standard. Fare riferimento alla sezione http://download.oracle.com/docs/cd/E12825_01/epm.111/epm_security_api_11111/client/com/hyperion/css/CSSCustomAuthenticationIF.html.
- Accesso a Shared Services come amministratore di Shared Services.

Considerazioni sulla progettazione e sulla scrittura di codice

Ordine di ricerca

Oltre alla directory nativa, è possibile configurare diverse directory utenti in Oracle Hyperion Shared Services. A tutte le directory utenti configurate viene assegnata una posizione di ordine di ricerca predefinita, il quale può essere modificato tramite Oracle Hyperion Shared Services Console. Ad eccezione della directory nativa, è possibile rimuovere dall'ordine di ricerca le directory utenti configurate. Oracle Enterprise Performance Management System non utilizza le directory utenti non incluse nell'ordine di ricerca. Fare riferimento al manuale *Oracle Enterprise Performance Management System User Security Administration Guide (in lingua inglese)*.

L'ordine di ricerca determina l'ordine in cui EPM System scorre in sequenza le diverse directory utenti per autenticare gli utenti. Se l'utente viene autenticato in una directory utenti, EPM System interrompe la ricerca e lo restituisce. EPM System rifiuta l'autenticazione e restituisce un errore se non è possibile autenticare l'utente a fronte delle directory utenti incluse nell'ordine di ricerca.

Impatto dell'autenticazione customizzata sull'ordine di ricerca

L'autenticazione customizzata influisce sul modo in cui la funzionalità di sicurezza di EPM System interpreta l'ordine di ricerca.

Se il modulo di autenticazione customizzato restituisce un nome utente, EPM System individua l'utente solo in una directory utenti abilitata per l'autenticazione customizzata. In questo stadio, EPM System ignora le directory utenti non configurate per questo tipo di autenticazione.

Descrizione del flusso di autenticazione customizzata

Per illustrare il flusso di autenticazione customizzata vengono utilizzati gli scenari dei casi d'uso riportati di seguito.

- Scenario del caso d'uso 1
- Scenario del caso d'uso 2
- Scenario del caso d'uso 3

Scenario del caso d'uso 1

Nella seguente tabella sono riportati la configurazione delle directory utenti di EPM System e l'ordine di ricerca utilizzati in questo scenario. In tale scenario si presuppone che il modulo di autenticazione customizzato utilizzi un'infrastruttura RSA per autenticare gli utenti.

Tabella 5-1 Impostazione per lo scenario 1

Tipo e nome della directory utenti	Ordine di ricerca	Autenticazione customizzata	Nomi di utenti campione	Password[1]

Directory nativa	1	Disabilitata	`test_user_1`
			`test_user_2`
			`test_user_3`
				`password`

Abilitata per LDAP SunONE_West	2	Disabilitata	`test_ldap1`
			`test_ldap_2`
			`test_user_3`
			`test_ldap_4`
				`ldappassword`

Abilitata per LDAP SunONE_East	3	Abilitata	`test_ldap1`
			`test_ldap_2`
			`test_user_3`
				`ldappassword` in SunONE e `RSA PIN` (PIN RSA) nel modulo customizzato

1 Per maggiore semplicità, si presuppone che la password della directory utenti sia la stessa per tutti gli utenti.

Per avviare il processo di autenticazione, un utente immette un nome utente e una password nella schermata di accesso di un prodotto EPM System. In questo scenario, il modulo di autenticazione customizzato esegue le operazioni riportate di seguito.

- Accetta un nome utente e un PIN RSA come credenziali utente
- Restituisce un nome utente in formato *username@providername*, ad esempio `test_ldap_2@SunONE_East`, alla funzionalità di sicurezza di EPM System

Tabella 5-2 Interazione dell'utente e risultati

Nome utente e password	Risultato dell'autenticazione	Directory utenti di accesso
`test_user_1/password`	Operazione riuscita	Directory nativa
`test_user_3/password`	Operazione riuscita	Directory nativa
`test_user_3/ldappassword`	Operazione riuscita	SunONE_West (ordine di ricerca 2)[1]
`test_user_3/RSA PIN`	Operazione riuscita	SunONE_East (ordine di ricerca 3)[2]
`test_ldap_2/ldappassword`	Operazione riuscita	SunONE_West (ordine di ricerca 2)
`test_ldap_4/RSA PIN`	Operazione non riuscita EPM System visualizza un errore di autenticazione.[3]	

1 L'autenticazione customizzata non può autenticare l'utente perché quest'ultimo ha immesso le credenziali di EPM System. EPM System può identificare tale utente solo in una directory utenti non abilitata per l'autenticazione customizzata. L'utente non è presente nella directory nativa (ordine di ricerca 1), ma viene identificato in SunONE_West (ordine di ricerca 2).

2 EPM System non trova l'utente nella directory nativa (ordine di ricerca 1) o in SunONE_West (ordine di ricerca 2). Il modulo di autenticazione customizzato convalida l'utente a fronte del server RSA e restituisce `test_user_3@SunONE_EAST` a EPM System. EPM System individua l'utente in SunONE_East (ordine di ricerca 3), che è una directory utenti abilitata per l'autenticazione customizzata.

3 Oracle consiglia che tutti gli utenti autenticati tramite il modulo customizzato siano presenti in una directory utenti abilitata per l'autenticazione customizzata e inclusa nell'ordine di ricerca. L'accesso ha esito negativo se il nome utente restituito dal modulo di autenticazione customizzato non è presente in una directory utenti abilitata per l'autenticazione customizzata e inclusa nell'ordine di ricerca.

Scenario del caso d'uso 2

Nella seguente tabella sono riportati la configurazione delle directory utenti di EPM System e l'ordine di ricerca utilizzati in questo scenario. In tale scenario si presuppone che il modulo di autenticazione customizzato utilizzi un'infrastruttura RSA per autenticare gli utenti.

In questo scenario, il modulo di autenticazione customizzato esegue le operazioni riportate di seguito.

- Accetta un nome utente e un PIN RSA come credenziali utente
- Restituisce un nome utente, ad esempio `test_ldap_2`, alla funzionalità di sicurezza di EPM System

Tabella 5-3 Ordine di ricerca campione

Directory utenti	Ordine di ricerca	Autenticazione customizzata	Nomi di utenti campione	Password[1]

Directory nativa	1	Disabilitata	`test_user_1`
			`test_user_2`
			`test_user_3`
				`password`

Abilitata per LDAP, ad esempio SunONE	2	Abilitata	`test_ldap1`
			`test_ldap2`
			`test_user_3`
				`ldappassword` in SunONE e `RSA PIN` (PIN RSA) nel modulo customizzato

1 Per maggiore semplicità, si presuppone che la password della directory utenti sia la stessa per tutti gli utenti.

Per avviare il processo di autenticazione, un utente immette un nome utente e una password nella schermata di accesso di un prodotto EPM System.

Tabella 5-4 Interazione dell'utente e risultati

Nome utente e password	Risultato dell'accesso	Directory utenti di accesso
`test_user_1/password`	Operazione riuscita	Directory nativa
`test_user_3/password`	Operazione riuscita	Directory nativa
`test_user_3/ldappassword`	Operazione non riuscita	SunONE[1]
`test_user_3/RSA PIN`	Operazione riuscita	SunONE[2]

1 L'autenticazione dell'utente a fronte della directory nativa ha esito negativo perché la password non corrisponde. L'autenticazione dell'utente con il modulo di autenticazione customizzato ha esito negativo perché la password utilizzata non è un PIN RSA valido. EPM System non tenta di autenticare l'utente in SunONE (ordine di ricerca 2) perché le impostazioni di autenticazione customizzata sostituiscono l'autenticazione di EPM System in questa directory.

2 L'autenticazione dell'utente a fronte della directory nativa ha esito negativo perché la password non corrisponde. Il modulo di autenticazione customizzato autentica l'utente e restituisce il nome utente `test_user_3` a EPM System.

Scenario del caso d'uso 3

Nella seguente tabella sono riportati la configurazione delle directory utenti di EPM System e l'ordine di ricerca utilizzati in questo scenario. In tale scenario si presuppone che il modulo di autenticazione customizzato utilizzi un'infrastruttura RSA per autenticare gli utenti.

Per maggiore chiarezza in tali scenari, Oracle consiglia che il modulo di autenticazione customizzato restituisca il nome utente in formato `username@providername`, ad esempio `test_ldap_4@SunONE`.

Tabella 5-5 Ordine di ricerca campione

Directory utenti	Ordine di ricerca	Autenticazione customizzata	Nomi di utenti campione	Password[1]

Directory nativa	1	Abilitata	`test_user_1`
			`test_user_2`
			`test_user_3`
				`RSA_PIN`

Abilitata per LDAP, ad esempio MSAD	2	Disabilitata	`test_ldap1`
			`test_ldap4`
			`test_user_3`
				`ldappassword`

Abilitata per LDAP, ad esempio SunONE	3	Abilitata	`test_ldap1`
			`test_ldap4`
			`test_user_3`
				`ldappassword` in SunONE e `RSA PIN` (PIN RSA) nel modulo customizzato

1 Per maggiore semplicità, si presuppone che la password della directory utenti sia la stessa per tutti gli utenti.

Per avviare il processo di autenticazione, un utente immette un nome utente e una password nella schermata di accesso di un prodotto EPM System.

Tabella 5-6 Interazione dell'utente e risultati

Nome utente e password	Risultato dell'autenticazione	Directory utenti di accesso
`test_user_1/password`	Operazione riuscita	Directory nativa
`test_user_3/RSA_PIN`	Operazione riuscita	Directory nativa
`test_user_3/ldappassword`	Operazione riuscita	MSAD (ordine di ricerca 2)
`test_ldap_4/ldappassword`	Operazione riuscita	MSAD (ordine di ricerca 2)
`test_ldap_4/RSA PIN`	Operazione riuscita	SunONE (ordine di ricerca 3)

Directory utenti e modulo di autenticazione customizzato

Per utilizzare il modulo di autenticazione customizzato, le directory utenti che contengono le informazioni su utenti e gruppi di EPM System possono essere configurate singolarmente per delegare l'autenticazione al modulo customizzato.

Gli utenti di EPM System autenticati tramite un modulo customizzato devono essere presenti in una delle directory utenti incluse nell'ordine di ricerca (fare riferimento alla sezione Ordine di ricerca). La directory utenti inoltre deve essere configurata per delegare l'autenticazione al modulo customizzato.

L'identità dell'utente nel provider customizzato (ad esempio, `1357642` nell'infrastruttura SecurID RSA) potrebbe essere diversa dal nome utente nella directory utenti (ad esempio, `jDoe` in Oracle Internet Directory) configurata in Shared Services. Dopo aver autenticato l'utente, il modulo di autenticazione customizzato deve restituire il nome utente `jDoe` a EPM System.

> **Nota:**
>
> Come miglior prassi, Oracle consiglia che il nome utente nelle directory utenti configurate in EPM System sia uguale a quelli disponibili nella directory utenti utilizzata dal modulo di autenticazione customizzato.

Interfaccia Java `CSSCustomAuthenticationIF`

Il modulo di autenticazione customizzato deve utilizzare l'interfaccia Java `CSSCustomAuthenticationIF` per l'integrazione con il framework di sicurezza di EPM System. Deve restituire la stringa del nome utente se l'autenticazione customizzata ha esito positivo oppure un messaggio di errore in caso contrario. Per il completamento del processo di autenticazione, è necessario che il nome utente restituito dal modulo di autenticazione customizzato sia presente in una delle directory utenti incluse nell'ordine di ricerca di Shared Services. Il framework di sicurezza di EPM System supporta il formato *`username@providerName`*.

> **Nota:**
>
> Assicurarsi che il nome utente restituito dal modulo di autenticazione customizzato non contenga un carattere * (asterisco), in quanto il framework di sicurezza di EPM System lo interpreta come un carattere jolly durante la ricerca degli utenti.

Per la firma dell'interfaccia `CSSCustomAuthenticationIF`, fare riferimento alla sezione Codice campione 1.

Il modulo di autenticazione customizzato (può trattarsi di un file classe) deve essere incluso in `CustomAuth.jar`. La struttura del package non è importante.

Per informazioni dettagliate sull'interfaccia `CSSCustomAuthenticationIF`, fare riferimento alla documentazione relativa all'API di sicurezza.

Il metodo `authenticate` di `CSSCustomAuthenticationIF` supporta l'autenticazione customizzata. Il metodo `authenticate` inoltre accetta le credenziali (nome utente e password) immesse dall'utente durante il tentativo di accedere a EPM System come parametri di input. Tale metodo restituisce una stringa (nome utente) se l'autenticazione customizzata ha esito positivo. Genera invece un'eccezione `java.lang.Exception` se l'autenticazione ha esito negativo. Il nome utente restituito dal metodo deve identificare in modo univoco un utente in una delle directory utenti incluse nell'ordine di ricerca di Shared Services. Il framework di sicurezza di EPM System supporta il formato *`username@providerName`*.

> **Nota:**
>
> Per inizializzare le risorse, ad esempio un pool di connessioni JDBC, utilizzare il costruttore di classi. In questo modo non si sovraccaricano le risorse per ogni autenticazione, con un conseguente miglioramento delle performance.

Distribuzione del modulo di autenticazione customizzato

Per una distribuzione di Oracle Enterprise Performance Management System è supportato un solo modulo customizzato. È possibile abilitare l'autenticazione customizzata per una o più directory utenti nell'ordine di ricerca.

Il modulo di autenticazione customizzato deve implementare l'interfaccia pubblica `CSSCustomAuthenticationIF`, definita nel package `com.hyperion.css`. In questo documento si presuppone che si disponga di un modulo customizzato completamente funzionante che definisce la logica per l'autenticazione degli utenti a fronte del provider utenti desiderato. Dopo aver sviluppato e testato un modulo di autenticazione customizzato, è necessario implementarlo nell'ambiente EPM System.

Panoramica dei passi

Il codice di autenticazione customizzato non deve utilizzare log4j per il logging degli errori. Se il codice utilizzato in una release precedente include log4j, è necessario rimuoverlo dal codice prima di utilizzarlo con questa release.

Per implementare il modulo di autenticazione customizzato, completare i passi riportati di seguito.

- Arrestare i prodotti EPM System, inclusi Oracle Hyperion Shared Services e gli eventuali sistemi che utilizzano API Shared Services.
- Copiare nella distribuzione l'archivio Java `CustomAuth.jar` del modulo di autenticazione customizzato procedendo come segue.
  - **WebLogic:** copiare `CustomAuth.jar` in *`MIDDLEWARE_HOME`*`/user_projects/domains/`*`WEBLOGIC_DOMAIN`*`/lib`, in genere `C:/Oracle/Middleware/user_projects/domains/EPMSystem/lib`.

    Se si sta eseguendo l'aggiornamento dalla Release 11.1.2.0 o 11.1.2.1 che aveva un'implementazione del modulo di autenticazione customizzato, spostare `CustomAuth.jar` da *EPM_ORACLE_HOME*`/common/jlib/11.1.2.0` a *`MIDDLEWARE_HOME`*`/user_projects/domains/`*`WEBLOGIC_DOMAIN`*`/lib`.
  - **Tutte le distribuzioni client**: copiare `CustomAuth.jar` in tutte le distribuzioni client di EPM System, nella posizione seguente:

    EPM_ORACLE_HOME`/common/jlib/11.1.2.0`, in genere `Oracle/Middleware/common/jlib/11.1.2.0`. Verificare che il file `CustomAuth.jar` sia sempre inserito nella directory *EPM_ORACLE_HOME*`/common/jlib/11.1.2.0`.

    Perché tutti i server e i client lavorino con autenticazione custom, è necessario che il file `CustomAuth.jar` sia presente nelle due posizioni seguenti:

    * *MIDDLEWARE_HOME*`/user_projects/domains/WEBLOGIC_DOMAIN/lib`
    * *EPM_ORACLE_HOME*`/common/jlib/11.1.2.0`

- Aggiornare le impostazioni della directory utenti in Shared Services. Fare riferimento alla sezione Aggiornamento delle impostazioni in Shared Services.
- Avviare Shared Services, e quindi altri prodotti EPM System.
- Testare l'implementazione. Fare riferimento alla sezione Test della distribuzione.

Aggiornamento delle impostazioni in Shared Services

Per impostazione predefinita, l'autenticazione customizzata è disabilitata per tutte le directory utenti. È possibile sostituire il funzionamento predefinito per abilitare l'autenticazione customizzata per directory utenti esterne specifiche o per la directory nativa.

Aggiornamento delle configurazioni delle directory utenti

È necessario aggiornare la configurazione della directory utenti per la quale deve essere abilitata l'autenticazione customizzata.

Per aggiornare la configurazione della directory utente, procedere come segue:

1. Avviare Oracle Hyperion Foundation Services.
2. Accedere a Oracle Hyperion Shared Services Console come amministratore di sistema.
3. Selezionare **Amministrazione**, quindi **Configura directory utenti**.
4. Nella schermata Directory definite dall'utente, selezionare la directory utenti per cui si desidera modificare l'impostazione di autenticazione customizzata.

> **Nota:**
>
> EPM System utilizza solo le directory utente incluse nell'ordine di ricerca.

5. Fare clic su **Modifica**.
6. Selezionare **Mostra opzioni avanzate**.
7. In **Modulo custom**, selezionare **Modulo di autenticazione** per abilitare il modulo customizzato per la directory utenti corrente.
8. Fare clic su **Fine**.
9. Ripetere la procedura per aggiornare la configurazione di altre directory utente nell'ordine di ricerca.

Aggiornamento delle opzioni di sicurezza

Assicurarsi che `CustomAuth.jar` sia disponibile in *EPM_ORACLE_HOME*`/user_projects/domains/`*`WEBLOGIC_DOMAIN`*`/lib` prima di iniziare la procedura descritta di seguito.

Per aggiornare le opzioni di protezione, procedere come segue:

1. Accedere a Shared Services Console come amministratore di sistema.
2. Selezionare **Amministrazione**, quindi **Configura directory utenti**.
3. Selezionare **Opzioni sicurezza**.

4. Selezionare **Mostra opzioni avanzate**.
5. In **Modulo di autenticazione**, immettere il nome di classe completamente qualificato del modulo di autenticazione customizzato che deve essere utilizzato per autenticare gli utenti in tutte le directory utenti per le quali è selezionato tale modulo. Ad esempio, `com.mycompany.epm.CustomAuthenticationImpl`.
6. Fare clic su **OK**.

Test della distribuzione

Se la directory nativa non è configurata per l'autenticazione customizzata, non utilizzare utenti della directory nativa per testare l'autenticazione customizzata.

> **Nota:**
>
> Si ha la responsabilità di identificare e risolvere gli eventuali problemi relativi al modulo di autenticazione customizzato. Oracle presuppone che il modulo customizzato funzioni senza problemi per mappare un utente della directory utenti utilizzata dal modulo customizzato su un utente di una directory utenti abilitata per l'autenticazione customizzata disponibile nell'ordine di ricerca di EPM System.

Per testare la distribuzione, eseguire l'accesso a EPM System utilizzando le credenziali utente della directory utenti; ad esempio, un'infrastruttura SecurID RSA, utilizzata dal modulo customizzato. Queste credenziali possono essere diverse da quelle di EPM System.

Si considera che l'implementazione abbia avuto esito positivo se i prodotti EPM System consentono di accedere alle relative risorse. Un errore che specifica l'impossibilità di trovare l'utente non sempre indica un'implementazione non riuscita. In tali casi, verificare che le credenziali immesse siano presenti nell'area di memorizzazione utenti customizzata e che un utente corrispondente sia incluso in una delle directory utenti abilitate per l'autenticazione customizzata nell'ordine di ricerca di EPM System.

Per testare l'autenticazione customizzata, procedere come segue.

1. Assicurarsi che i prodotti EPM System siano in esecuzione.
2. Accedere a un componente di EPM System, ad esempio Oracle Hyperion Enterprise Performance Management Workspace.
3. Eseguire l'accesso come utente definito in una directory utenti per la quale è abilitata l'autenticazione customizzata.
    a. In **Nome utente**, immettere il proprio identificativo utente, ad esempio un ID utente RSA.
    b. In **Password**, immettere una password, ad esempio un PIN RSA.
    c. Fare clic su **Accesso**.
4. Verificare di poter accedere alle risorse dei prodotti EPM System.

6

Linee guida per la sicurezza di EPM System

Vedere anche:

- Implementazione di SSL
- Modifica della password amministratore
- Rigenerazione delle chiavi di cifratura
- Modifica delle password per i database
- Protezione dei cookie
- Riduzione del timeout token SSO
- Esame dei report sicurezza
- Customizzazione del sistema di autenticazione per l'autenticazione avanzata
- Disabilitazione delle utility di debug di EPM Workspace
- Modifica delle pagine di errore predefinite del server Web
- Supporto per software di terze parti

Implementazione di SSL

SSL (Secure Sockets Layer) utilizza un sistema di cifratura che consente di cifrare i dati. Questo protocollo permette di creare una connessione sicura tra un client e un server grazie alla quale è possibile inviare i dati con un livello di sicurezza elevato.

Per proteggere l'ambiente Oracle Enterprise Performance Management System, proteggere tutti i canali di comunicazione utilizzati dalle applicazioni Web e dalle connessioni di directory utenti con SSL. Fare riferimento alla sezione Abilitazione per SSL dei componenti di EPM System.

Proteggere inoltre tutte le porte dell'agente, ad esempio la porta 6861, che è la porta dell'agente di Oracle Hyperion Reporting and Analysis, tramite un firewall. Gli utenti finali non hanno necessità di accedere alle porte dell'agente EPM System.

Modifica della password amministratore

L'account utente amministratore predefinito della directory nativa consente di accedere a tutte le funzioni di Oracle Hyperion Shared Services. Questa password viene impostata durante la distribuzione di Oracle Hyperion Foundation Services. È necessario modificare periodicamente la password di tale account.

Modificare l'account utente dell'*amministratore* per modificare la password. Fare riferimento alla sezione "Modifica degli account utente" nel manuale *Oracle Enterprise Performance Management System User Security Administration Guide (in lingua inglese)*.

Rigenerazione delle chiavi di cifratura

Utilizzare Oracle Hyperion Shared Services Console per rigenerare periodicamente gli elementi elencati di seguito.

- Token Single Sign-On

> **Attenzione:**
>
> I flussi di task utilizzati da Oracle Hyperion Financial Management e Oracle Hyperion Profitability and Cost Management vengono invalidati quando si genera un nuovo keystore. Dopo aver rigenerato il keystore, aprire e salvare i flussi di task per riconvalidarli.

- Chiave dei trusted service
- Chiave configurazione provider

Fare riferimento alla sezione Rigenerazione delle chiavi di cifratura.

> **Nota:**
>
> Oracle Hyperion Shared Services e il sottosistema di sicurezza di Oracle Enterprise Performance Management System utilizzano la cifratura AES con efficacia di chiave a 128 bit.

Modifica delle password per i database

Modificare periodicamente la password di tutti i database dei prodotti Oracle Enterprise Performance Management System. In questa sezione viene descritta in dettaglio la procedura di modifica della password per i database in Registro di Oracle Hyperion Shared Services.

Per le procedure dettagliate per la modifica della password di un database dei prodotti EPM System, fare riferimento alla *Guida di installazione e configurazione di Oracle Enterprise Performance Management System*.

Per cambiare le password per i database dei prodotti EPM System nel Registro di Shared Services procedere come segue:

1. Utilizzando la console di amministrazione dei database, modificare la password dell'account utente utilizzato per configurare il database dei prodotti EPM System.
2. Arrestare i prodotti EPM System (applicazioni Web, servizi e processi).
3. Utilizzando EPM System Configurator, configurare di nuovo il database attenendosi a una delle seguenti procedure.

   Solo Oracle Hyperion Shared Services:

> **Nota:**
>
> Negli ambienti distribuiti in cui i prodotti EPM System si trovano in computer diversi da Shared Services, è necessario eseguire la procedura su tutti i server.

a. A partire dai task di Foundation in EPM System Configurator, selezionare **Configura database**.
b. Nella pagina Configurazione di Shared Services e del database di registro, selezionare **Esegui connessione a un database Shared Services configurato precedentemente**.
c. Specificare la nuova password dell'utente il cui account è stato utilizzato per configurare il database di Shared Services. Non modificare altre impostazioni.
d. Proseguire con la configurazione e al termine fare clic su **Fine**.

Prodotti EPM System diversi da Shared Services:

> **Nota:**
>
> Eseguire la procedura per i prodotti EPM System distribuiti solo nel server corrente.

Per istruzioni dettagliate, fare riferimento al manuale *Guida di installazione e configurazione di Oracle Enterprise Performance Management System*.

4. Avviare i prodotti e i servizi EPM System.

Protezione dei cookie

L'applicazione Web Oracle Enterprise Performance Management System imposta un cookie per tenere traccia della sessione. Durante l'impostazione di un cookie, specie un cookie sessione, il server può impostare il flag di protezione, che forza il browser a inviare il cookie su un canale sicuro. Questo comportamento riduce il rischio di intercettazione della sessione.

> **Nota:**
>
> Proteggere i cookie solo se i prodotti EPM System vengono distribuiti in un ambiente abilitato per SSL.

Modificare il descrittore sessione di Oracle WebLogic Server per proteggere i cookie di WebLogic Server. Impostare il valore dell'attributo `cookieSecure` nell'elemento `session-param` su `true`. Fare riferimento alla sezione Protezione delle applicazioni Web nel manuale Oracle Fusion Middleware Programming Security for Oracle WebLogic Server 11g (in lingua inglese).

Riduzione del timeout token SSO

Il timeout del token SSO predefinito è 480 minuti. Ridurre il timeout del token SSO, ad esempio a 60 minuti, per ridurre al minimo il riutilizzo del token qualora risulti esposto. Fare riferimento alla sezione "Impostazione delle opzioni di sicurezza" nel manuale *Oracle Enterprise Performance Management System User Security Administration Guide (in lingua inglese)*.

Esame dei report sicurezza

Nel Report protezione sono contenute le informazioni di auditing relative ai task di protezione per i quali è configurato l'auditing. Generare e rivedere questo report da Oracle Hyperion Shared Services Console a intervalli regolari, soprattutto per identificare tentativi di accesso non riusciti nei prodotti Oracle Enterprise Performance Management System e modifiche dell'assegnazione ruoli. Come opzione di generazione del report, selezionare **Vista dettagliata** per raggruppare i dati del report in base agli attributi modificati e ai nuovi valori degli attributi. Fare riferimento alla sezione "Generazione dei report" nella *Oracle Enterprise Performance Management System User Security Administration Guide (in lingua inglese)*.

Customizzazione del sistema di autenticazione per l'autenticazione avanzata

È possibile utilizzare un modulo di autenticazione custom per aggiungere autenticazione restrittiva a EPM System. Ad esempio, è possibile utilizzare l'autenticazione a due fattori SecurID RSA in modalità diversa da challenge/response. Il modulo di autenticazione customizzato è trasparente per i client thin e thick e non richiede modifiche alla distribuzione lato client. Fare riferimento alla sezione Utilizzo di un modulo di autenticazione custom.

Disabilitazione delle utility di debug di EPM Workspace

- Ai fini della risoluzione dei problemi, Oracle Hyperion Enterprise Performance Management Workspace viene fornito con file JavaScript non compressi. Per motivi di sicurezza, è consigliabile rimuovere dall'ambiente di produzione tali file JavaScript non compressi procedendo come segue.
  - Creare una copia di backup della directory *EPM_ORACLE_HOME*`/common/epmstatic/wspace/js/`.
  - Ad eccezione del file *`DIRECTORY_NAME`*`.js`, eliminare i file `.js` da ogni sottodirectory di *EPM_ORACLE_HOME*`/common/epmstatic/wspace/js`.

    In ciascuna sottodirectory è contenuto un file `.js` avente lo stesso nome della directory. Ad esempio, *EPM_ORACLE_HOME*`/common/epmstatic/wspace/js/com/hyperion/bpm/web/common` contiene `Common.js`. Rimuovere tutti i file `.js` tranne il file con lo stesso nome della directory, in questo caso `Common.js`.
- EPM Workspace offre alcune utility di debug e applicazioni di test a cui è possibile accedere se EPM Workspace viene distribuito in modalità debug. Per motivi di

sicurezza, gli amministratori devono disattivare il debug lato client in EPM Workspace.

Per disattivare la modalità debug, procedere come segue.

1. Accedere a EPM Workspace come amministratore.
2. Selezionare **Naviga**, quindi **Amministra** e infine **Impostazioni server Workspace**.
3. In **ClientDebugEnabled** in Impostazioni server Workspace, selezionare **No**.
4. Fare clic su **OK**.

Modifica delle pagine di errore predefinite del server Web

Quando i server applicazioni non sono disponibili per accettare le richieste, il plugin del server Web per il server applicazioni back-end (ad esempio, il plugin Oracle HTTP Server per Oracle WebLogic Server) restituisce una pagina di errore predefinita in cui sono visualizzate le informazioni sulla build del plugin. Anche in altre situazioni, i server Web visualizzano delle pagine di errore predefinite. Gli hacker possono utilizzare queste informazioni per individuare le nuove vulnerabilità dei siti Web pubblici.

Customizzare le pagine di errore (del plugin del server applicazioni Web e del server Web) in modo che non contengano informazioni sui componenti del sistema di produzione, ad esempio la versione del server, il tipo di server, la data della build del plugin e il tipo di plugin. Per ulteriori informazioni, consultare la documentazione del fornitore del server applicazioni e del server Web.

Supporto per software di terze parti

Oracle riconosce e sostiene l'impegno alla compatibilità con le versioni precedenti da parte di fornitori di terze parti. Di conseguenza, per i fornitori che dichiarano la compatibilità con le versioni precedenti, è possibile utilizzare le successive release di manutenzione e i service pack. Se viene identificata un'incompatibilità, Oracle specificherà la release di una patch su cui distribuire il prodotto (e rimuovere la versione incompatibile dalla matrice supportata) o fornirà una release di manutenzione o una correzione per il prodotto Oracle.

Aggiornamenti lato server: il supporto degli aggiornamenti per componenti server di terzi è regolato dalla politica relativa alle release di manutenzione. In generale, Oracle supporta l'aggiornamento dei componenti server di terze parti alle successive release di manutenzione dei service pack della release correntemente supportata. Gli aggiornamenti alla release principale successiva non sono supportati.

Aggiornamenti lato client: Oracle supporta gli aggiornamenti automatici dei componenti client, inclusi gli aggiornamenti alle release principali successive di componenti client di terze parti. È ad esempio possibile aggiornare la versione JRE del browser alla versione JRE attualmente supportata.

A

Codice campione di autenticazione customizzata

Codice campione 1

> **Nota:**
>
> Il codice di autenticazione customizzato non deve utilizzare log4j per il logging degli errori. Se il codice di autenticazione customizzata utilizzato in una release precedente utilizzava log4j, è necessario rimuoverlo dal codice prima di utilizzarlo con questa release.

Lo snippet di codice seguente è un'implementazione vuota del modulo customizzato:

```
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;
      }
}
```

Di seguito sono elencati i parametri di input.

- Contesto: mappa contenente la coppia chiave-valore delle informazioni sulle impostazioni nazionali.
- Nome utente: identificativo che identifica in modo univoco l'utente nella directory utenti in cui il modulo customizzato autentica l'utente. L'utente immette il valore del parametro al momento dell'accesso a un componente di Oracle Enterprise Performance Management System.
- Password: password impostata per l'utente nella directory utenti in cui il modulo customizzato autentica l'utente. L'utente immette il valore del parametro al momento dell'accesso a un componente di EPM System.

Codice campione 2

Il codice campione riportato di seguito illustra l'autenticazione customizzata di utenti che utilizzano il nome utente e la password contenuti in un file flat. Per il corretto funzionamento dell'autenticazione customizzata, è necessario inizializzare gli elenchi di utenti e password nel costruttore di classe.

```
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(authenticatedUserK
ey))
                          .append("@").append(PROVIDER_NAME).toString(
);
                            return userNameStr;
  else throw new Exception("Invalid User Credentials");
          }
}
```

File di dati per il codice campione 2

Assicurarsi che il file di dati sia denominato `datafile.txt` (nome utilizzato nel codice campione) e che sia incluso nell'archivio Java creato.

Specificare quanto segue come contenuto del file flat utilizzato come directory utenti customizzata per supportare il modulo di autenticazione customizzato implementato tramite il codice campione 2. Fare riferimento alla sezione Codice campione 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
```

Specificare quanto segue come contenuto del file flat utilizzato come directory utenti customizzata se si intende restituire il nome utente in formato *username@providername*:

```
xyz:password:admin
test1:password:test1
test1@1:password:test1
user1_1:Password2:user1
user3:Password3:user3
DS1_1G100U_User61_1:Password123:DS1_1G100U_User61
DS1_1G100U_User61_1@1:Password123:DS1_1G100U_User61
TUser:password:TUser
```

B

Implementazione di una classe di accesso customizzata

Oracle Enterprise Performance Management System offre `com.hyperion.css.sso.agent.X509CertificateSecurityAgentImpl` per l'estrazione dell'identità utente (`DN`) dai certificati x509.

Se si ha l'esigenza di ottenere l'identità utente da un attributo del certificato diverso da DN, è necessario sviluppare e implementare una classe di accesso customizzata simile a `com.hyperion.css.sso.agent.X509CertificateSecurityAgentImpl`, come illustrato in questa appendice.

Codice campione della classe di accesso customizzata

Questo codice campione illustra l'implementazione della classe predefinita `com.hyperion.css.sso.agent.X509CertificateSecurityAgentImpl`. In genere, è necessario customizzare il metodo `parseCertificate(String sCertificate)` di questa implementazione per ottenere il nome utente da un attributo certificato diverso da 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 hostAdrress= 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
    {
        hostAdrress = 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 nane 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
```

Distribuzione di una classe di accesso customizzata

Per implementare la classe di accesso customizzata, completare i passi riportati di seguito.

1. Creare e testare la classe di accesso customizzata. Assicurarsi di non avere riferimenti a `log4j` nel codice. Fare riferimento alla sezione Codice campione della classe di accesso customizzata.

   È possibile utilizzare qualsiasi nome per la classe customizzata.

2. Includere la classe di accesso customizzata in `CustomAuth.jar`
3. Copiare `CustomAuth.jar` nella distribuzione procedendo come segue.

   - **WebLogic:** copiare `CustomAuth.jar` in *`MIDDLEWARE_HOME`*`/user_projects/domains/`*`WEBLOGIC_DOMAIN`*`/lib`, in genere `Oracle/Middleware/user_projects/domains/EPMSystem/lib`.

     > **Nota:**
     >
     > Se si sta eseguendo l'aggiornamento dalla Release 11.1.2.0 or 11.1.2.1 che aveva un'implementazione della classe di accesso customizzata, spostare `CustomAuth.jar` da *`EPM_ORACLE_HOME`*`/common/jlib/11.1.2.0` a *`MIDDLEWARE_HOME`*`/user_projects/domains/`*`WEBLOGIC_DOMAIN`*`/lib`.

   - **Distribuzioni client**: copiare `CustomAuth.jar` in tutte le distribuzioni client di Oracle Enterprise Performance Management System, nella posizione seguente:

     `EPM_ORACLE_HOME``/common/jlib/11.1.2.0`, in genere `Oracle/Middleware/common/jlib/11.1.2.0`

Oracle consiglia di abilitare l'autenticazione del certificato client se si utilizza una classe di accesso customizzata.

C

Migrazione di utenti e gruppi tra le directory utenti

Panoramica

Molti scenari possono determinare la perdita di validità delle identità utente e gruppo di utenti Oracle Enterprise Performance Management System con assegnazione ruoli. I componenti di EPM System diventano inaccessibili se le informazioni di assegnazione ruoli disponibili sono obsolete. Tra gli scenari che possono dare luogo a dati di assegnazione ruoli obsoleti sono inclusi quelli descritti di seguito.

- Disattivazione di una directory utenti: le organizzazioni possono disattivare una directory utenti dopo lo spostamento degli utenti in un'altra directory.
- Aggiornamento della versione: l'aggiornamento della versione di una directory utenti può comportare modifiche del nome del computer host o degli ambienti del sistema operativo.
- Cambiamento di fornitore: le organizzazioni possono cessare l'utilizzo di una directory utenti optando per una directory utenti di un altro fornitore e sostituendo ad esempio Oracle Internet Directory con SunONE Directory Server.

> **Nota:**
>
> - In questa appendice, la directory utenti che viene rimossa è indicata come directory utenti di *origine* e quella in cui vengono spostati gli account utente è indicata come directory utenti *target*.
> - La procedura di migrazione non supporta la migrazione degli account utente da una directory utente di origine in una directory utenti target, ma solo la loro associazione in applicazioni EPM. Gli utenti devono essere creati manualmente nella directory utenti target. Questo processo è applicabile agli utenti di qualsiasi directory utenti di origine, inclusa la directory nativa.
>
>   Se una directory utenti di origine configurata con Hyperion Shared Services conteneva gruppi diversi dai gruppi della directory nativa, nella directory utenti target dovranno essere creati anche questi gruppi.

Prerequisiti

- Gli utenti e i gruppi di Oracle Enterprise Performance Management System i cui dati di assegnazione ruoli vengono sottoposti a migrazione tra directory utenti devono essere disponibili nella directory utenti target.

  Le relazioni tra gruppi esistenti nella directory utenti di origine devono essere mantenute anche nella directory utenti target.

- I nomi degli utenti di EPM System devono essere identici nelle directory utenti di origine e target.

Procedura di migrazione

Esportazione dei dati della directory nativa

Eseguire la procedura seguente nell'ambiente di origine.

Utilizzare Oracle Hyperion Enterprise Performance Management System Lifecycle Management per esportare dalla directory nativa solo gli artifact di Shared Services elencati di seguito.

- Gruppi della directory nativa
- Ruoli assegnati
- Elenchi delegati

Lifecycle Management crea più file di esportazione, generalmente in *EPM_ORACLE_INSTANCE*`/import_export/`*`USER_NAME`*`/`*`EXPORT_DIR`*`/resource/Native Directory`, dove *`USER_NAME`* è l'identità dell'utente che ha eseguito l'operazione di esportazione, ad esempio `admin`, ed *`EXPORT_DIR`* è il nome della directory di esportazione. Vengono creati in genere i file elencati di seguito.

- `Groups.csv`
- `Assigned Roles.csv`
- `Delegated Lists.csv`
- `Assigned Roles/`*`PROD_NAME`*`.csv` per ogni applicazione distribuita, dove *`PROD_NAME`* è il nome di un componente di Oracle Enterprise Performance Management System, ad esempio `Shared Services`

> **Nota:**
>
> - Fare riferimento alla *Guida per Lifecycle Management di Oracle Enterprise Performance Management System* per istruzioni dettagliate sull'esportazione dei dati tramite Lifecycle Management.
> - Assicurarsi che il file `Users.csv` non venga esportato.

Dopo l'esportazione degli artifact, verificare che nel report sullo stato della migrazione lo stato dell'ultima operazione di esportazione sia visualizzato come `Completed`.

Per esportare i dati della directory nativa procedere come indicato di seguito.

1. Nel riquadro di visualizzazione di Oracle Hyperion Shared Services Console, nel gruppo applicazioni **Foundation**, selezionare l'applicazione **Shared Services**.
2. Per eseguire la migrazione, selezionare solo gli artifact necessari dall'elenco sottostante:
   - Gruppi della directory nativa
   - Ruoli assegnati

- Elenchi delegati

3. Fare clic su **Esporta**.
4. Immettere un nome per l'archivio di esportazione. Il valore predefinito è `admin` *DATE*, ad esempio `admin 13-03-18`.
5. Fare clic su **Esporta**.

Importazione dei dati della directory nativa

Eseguire i passi riportati di seguito nell'ambiente target.

1. Eseguire la creazione manuale degli elementi indicati di seguito.
   a. Utenti nella directory utenti target esterna simili a quelli della directory utenti di origine.
   b. Gruppi nella directory utenti target esterna simili a quelli della directory utenti di origine, ad eccezione dei gruppi della directory nativa.
2. Configurare la directory utenti target.
   Aggiungere la directory utenti target come directory utenti esterna in EPM System se gli account utente sono stati spostati dalla directory utenti di origine a un'altra directory utenti. Se ad esempio gli account utente sono stati spostati da Oracle Internet Directory a SunONE Directory Server, aggiungere SunONE Directory Server come directory utenti esterna. Fare riferimento al "Capitolo 3, Configurazione delle directory utenti" nel manuale *Oracle Enterprise Performance Management System User Security Administration Guide (in lingua inglese)*.

   > **Nota:**
   >
   > Assicurarsi che la directory utenti target contenga account utente e gruppi per tutti gli utenti di EPM System i cui dati vengono sottoposti a migrazione dalla directory utenti di origine.

   Se gli utenti sono stati spostati in una directory utenti già definita come directory utenti esterna, verificare che gli account utente siano visibili per Oracle Hyperion Shared Services. A tale scopo, cercare gli utenti da Shared Services Console. Fare riferimento alla sezione "Ricerca di utenti, gruppi, ruoli ed elenchi delegati" nel manuale *Oracle Enterprise Performance Management System User Security Administration Guide (in lingua inglese)*.

   Durante la configurazione della directory utenti target come directory utenti esterna, verificare che la proprietà Attributo di accesso punti all'attributo il cui valore era utilizzato in origine come nome utente nella directory utenti di origine. Fare riferimento alla sezione Prerequisiti.
3. Spostare la directory utenti target all'inizio dell'ordine di ricerca.

   > **Nota:**
   >
   > Se il nome della directory utenti target è identico a quello della directory di origine, è necessario eliminare la directory utenti di origine dalla configurazione di EPM System.

Shared Services assegna a una directory utenti appena aggiunta una priorità di ordine di ricerca più bassa rispetto all'ordine di ricerca assegnato alle directory esistenti. Modificare l'ordine di ricerca in modo che la directory utenti target abbia una priorità di ordine di ricerca più alta rispetto alla directory utenti di origine. Quest'ordine consente a Shared Services di individuare gli utenti nella directory utenti target prima di eseguire la ricerca nell'origine. Fare riferimento alla sezione "Gestione dell'ordine di ricerca delle directory utenti" nel manuale *Oracle Enterprise Performance Management System User Security Administration Guide (in lingua inglese)*.

4. Riavviare Oracle Hyperion Foundation Services e altri componenti di EPM System per applicare le modifiche apportate.
5. Importare i dati della directory nativa (esportati dall'ambiente di origine): Eseguire Lifecycle Management con l'opzione `create/update` per importare i dati esportati precedentemente (elencati di seguito) dalla directory nativa.
   - `Groups.csv`
   - `Assigned Roles.csv`
   - `Delegated Lists.csv`

   > **Nota:**
   >
   > - Fare riferimento alla *Guida per Lifecycle Management di Oracle Enterprise Performance Management System* per istruzioni dettagliate sull'importazione dei dati tramite Lifecycle Management.
   > - Assicurarsi che il file `Users.csv` non venga importato.

   Dopo l'importazione dei dati, verificare che nel report sullo stato della migrazione lo stato dell'ultima operazione di importazione venga visualizzato come `Completed`.

   Per importare i dati della directory nativa procedere come indicato di seguito.

   a. Nel riquadro di visualizzazione di Shared Services Console, espandere **File system**.
   b. Selezionare la posizione dei file di importazione nel file system.
   c. Selezionare il tipo di artifact per i quali si desidera importare le informazioni di assegnazione ruoli.
   d. Fare clic su **Importa**.
   e. Fare clic su **OK**.

Aggiornamenti specifici del prodotto

> **Attenzione:**
>
> Oracle consiglia di eseguire il backup dei dati degli utenti e dei gruppi presenti nel repository utilizzato dal componente di Oracle Enterprise Performance Management System prima di avviare aggiornamenti specifici del prodotto. Dopo aver aggiornato le informazioni nel repository del prodotto locale, è possibile ripristinare i dati precedenti relativi a utenti e gruppi del repository del prodotto locale solo dai backup.

Planning

In Oracle Hyperion Planning, le informazioni sugli utenti e i gruppi con assegnazione ruoli vengono memorizzate nel repository Planning. Se un'identità utente è stata modificata nella directory nativa come risultato della migrazione di utenti e gruppi tra directory utenti, è necessario sincronizzare le informazioni contenute nel repository Planning con quelle della directory nativa selezionando il pulsante di migrazione di utenti e gruppi disponibile in Planning quando si assegna l'accesso a form dati, membri ed elenchi di task.

Financial Management

In Oracle Hyperion Financial Management, le informazioni sugli utenti e i gruppi con ruoli di accesso agli oggetti vengono registrate in un repository Financial Management locale. Se le informazioni relative a utenti e gruppi nella directory nativa sono state modificate in seguito alla migrazione di utenti e gruppi tra directory utenti, è necessario sincronizzare le informazioni contenute nel repository Financial Management con quelle della directory nativa.