

WebCenter Portal での SAML 2.0 フェデレーテッド SSO

Oracle ホワイト・ペーパー | 2016 年 4 月





免責事項

下記事項は、弊社の一般的な製品の方向性に関する概要を説明するものです。また、情報提供を唯一の目的とするものであり、いかなる契約にも組み込むことはできません。マテリアルやコード、機能の提供をコミットメント（確約）するものではなく、購買を決定する際の判断材料になさらないで下さい。オラクルの製品に関して記載されている機能の開発、リリース、および時期については、弊社の裁量により決定されます。

目次

| | |
|--|----|
| 免責事項 | 1 |
| はじめに | 3 |
| 前提条件 | 4 |
| ソフトウェアをインストールして構成する | 4 |
| WebCenter Portal ドメインに SSL を構成する | 4 |
| webCenter.ear を更新して再デプロイする | 4 |
| WebCenter Portal ドメインにアイデンティティ・ストアを構成する | 6 |
| アイデンティティ・プロバイダを構成する | 6 |
| IIS でサーバー認証証明書を構成する | 7 |
| ADFS をスタンドアロンのフェデレーション・サーバーとして構成する | 7 |
| ADFS の SAML 2.0 メタデータをダウンロードする | 8 |
| ADFS で WebCenter Portal をサービス・プロバイダとして構成する | 8 |
| WLS をサービス・プロバイダとして構成する | 10 |
| SAML 2.0 アイデンティティ・アサーション・プロバイダを構成する | 11 |
| SAML 2.0 サービス・プロバイダのサービスを構成する | 13 |
| SAML 2.0 全般サービスを構成する | 14 |
| アイデンティティ・プロバイダ・パートナーを作成および構成する | 16 |
| SAML 2.0 ベースのフェデレーテッド SSO をテストする | 19 |

はじめに

WebCenter Portal では、リリース 11.1.1.6.0 から SAML 1.1 ベースの SSO をサポートしています。このホワイト・ペーパーの目的は、WebCenter Portal 11.1.1.8.0 以降で SAML 2.0 を使用して SSO をサポートするための構成手順を説明することです。

SAML 認証には、次の 2 つのプロバイダが関係します。

- » **アイデンティティ・プロバイダ (IDP)**。認証および SAML アサーションの生成を行います。
- » **サービス・プロバイダ (SP)**。SAML アサーションをアサートします。

SAML 1.0 の WebCenter Portal では、WebLogic Server (WLS) を IDP と SP の両方として使用することがサポートされていました。SAML 1.0 のサポートについて、詳しくは「[SAML ベースのシングル・サインオンの構成](#)」を参照してください。現在、WebCenter Portal での SAML 2.0 のサポートでは、WLS の同じトポロジが IDP および SP としてサポートされているだけでなく、ADFS、Ping Federate、OAM などの他の標準準拠の SAML 2.0 IDP もサポートされています。このホワイト・ペーパーでは、ADFS を SAML 2.0 の IDP、WLS を SP として記述しています。ADFS の手順を OAM、WLS、Ping Federate などの SAML 2.0 準拠の他の IDP に置き換えても、同様の結果が得られます。このホワイト・ペーパーの SSO 検証では、WebCenter Portal をパートナー・アプリケーションとして使用しています。WebCenter Portal は例として使用しており、SSO を確立する必要がある他のパートナー・アプリケーションに置き換えることができます。図 1 は、SAML ベースの SSO のさまざまなロールを示しています。

- **アイデンティティ・プロバイダ (IdP) /アサート側**
- **サービス・プロバイダ (SP) /証明書利用者**
- **ユーザー**

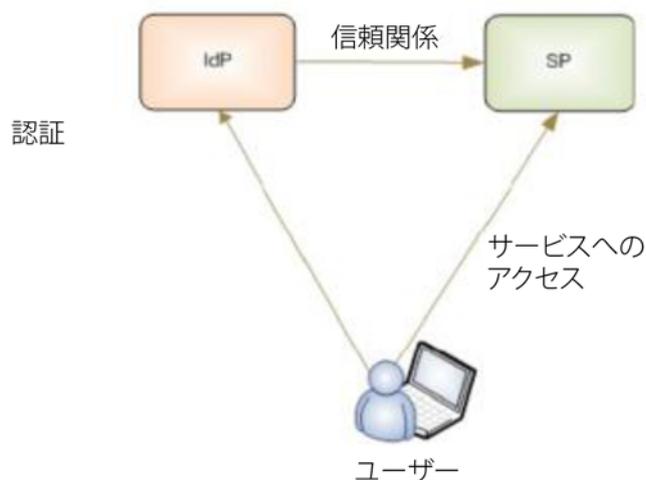


図 1 : SAML ベースの SSO のロール

SAML ベースの SSO の一般的なユースケースでは、ユーザーが SP にリソースをリクエストします。

このホワイト・ペーパーでは、SP は WebCenter Portal をホストする WLS サーバーです。IDP が最終的に認証を行うため、保護されているページをユーザーが WebCenter Portal にリクエストすると、WLS SP がユーザーを IDP にリダイレクトします。IDP は、ユーザーを認証すると、SAML 2.0 アサーションを生成してユーザーを SP にリダイレクトし直します。SP は、以前の証明書交換により、IDP との間で信頼関係があります。そのため、SP は IDP の SAML 2.0 アサーションをアサートし、リソースにユーザーがアクセスできるように、認証されたセッションを作成します。

以下に、SAML 2.0 ベースの SSO を構成するための手順概要を示します。

1. [前提条件](#)
2. [アイデンティティ・プロバイダを構成する](#)
3. [WLS をサービス・プロバイダとして構成する](#)

前提条件

ソフトウェアをインストールして構成する

以下のソフトウェアをインストールする必要があります。

- » Windows Server 2008 R2 上で実行される ADFS 2.0 IDP。
異なる IDP を使用する場合は、この手順を無視して構いません。詳しくは、「[Active Directory Federation Services \(ADFS\) 2.0 のインストールおよび構成](#)」を参照してください。
- » WebCenter Portal (WCP)。詳しくは、「[Oracle WebCenter Portal ソフトウェアのインストール](#)」を参照してください。

WebCenter Portal ドメインに SSL を構成する

SAML 2.0 プロトコルを使用して ADFS と統合するためには、HTTPS/SSL をエンドポイントとして使用するよう WebCenter Portal を構成する必要があります。このように構成しないと、フェデレーションの信頼を確立するときに、ADFS で WCP の SAML 2.0 メタデータが受け入れられません。WebCenter Portal での SSL の有効化について、詳しくは「[SSL の概要](#)」を参照してください。

webCenter.ear を更新して再デプロイする

インストールした webcenter.ear ファイルでは、Cookie パスが /webcenter で設定されています。「WebCenter Portal ドメインに SSL を構成する」で説明している WLS SAML 2.0 の制限のために、Cookie パスを "/" で設定する必要があります。この設定が必要になるのは、WLS SP では SAML 2.0 の Cookie パスとして "/" のみサポートされているためです。

これを行うには、次の手順を実行します。

1. WebCenter Oracle ホーム・ディレクトリにナビゲートします。
2. webcenter.ear ファイル
(`$WebCenter_Install_Dir/archives/applications`) を解凍します。
3. Spaces EAR ファイルを解凍します。
4. XML エディタで weblogic.xml (`/WEB_INF/weblogic.xml`) を開いて、session-

descriptor の下にある Cookie パス要素を次の値に変更します。

```
<cookie-path>/</cookie-path>
```

5. IDP によって提供されるアサーションを WebCenter Portal で使用するためには、WebCenter Portal の認証タイプを CLIENT-CERT に変更する必要があります。これを行うには、XML エディタで web.xml (/WEB_INF/web.xml) を開いて、login-config を次のように変更します。

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

6. weblogic.xml と web.xml を更新したら、jar コーティリティを使用して webcenter.ear を再度 zip 形式で圧縮し、Weblogic コンソールで再デプロイします。
7. Weblogic コンソールにログインしたら、デプロイメントにナビゲートし、[図 2](#) に示すように、WebCenter アプリケーション・デプロイメントを見つけます。

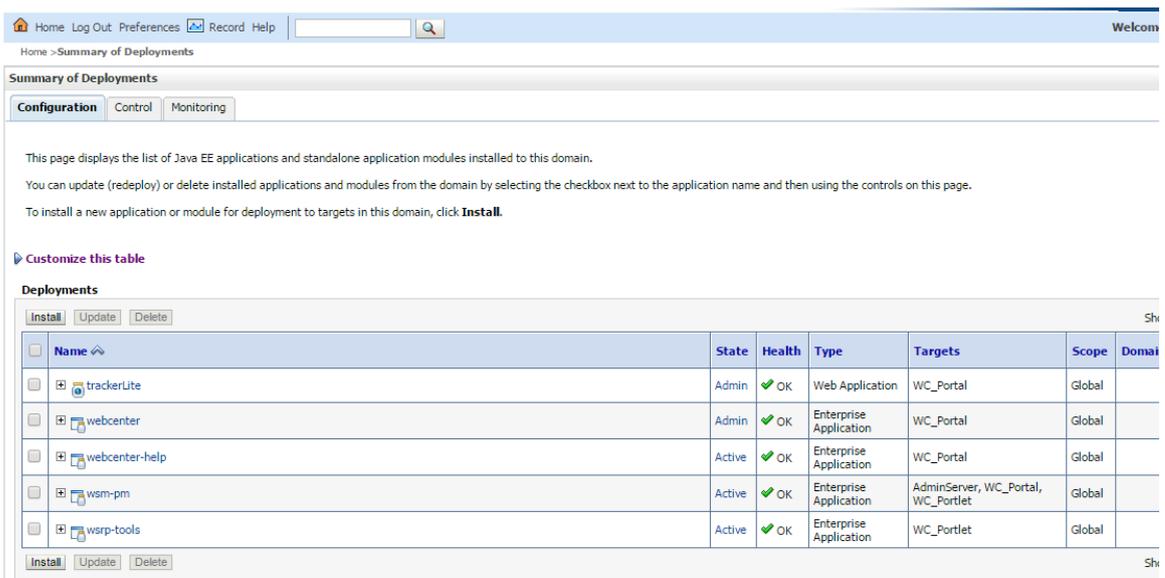


図 2 : WebCenter アプリケーション・デプロイメント

8. WebCenter を選択して「Update」をクリックします。[図 3](#) に示すようなページが表示されます。

図 3 : WebCenter アプリケーション・パスの選択

9. 「Source path」を選択して webcenter.ear を更新し、「Finish」をクリックして、webcenter.ear を再デプロイします

WebCenter Portal ドメインにアイデンティティ・ストアを構成する

WebCenter Portal での認証は、IDP と同じディレクトリ、つまり ADFS ユーザーを指すように構成する必要があります。IDP と SP の両方を、共通の LDAP を使用するように構成する必要があります。IDP と SP を別々の LDAP を使用するように構成する場合は、IDP の LDAP と SP の LDAP 間でユーザー属性を同期させる必要があります。また、別々の LDAP を使用する場合は、電子メール・アドレスを共通のユーザー属性として使用できるように、同じユーザー・セットが両方のシステムに存在し、各ユーザーが同じ電子メール・アドレスを使用する必要があります。詳しくは、「[アイデンティティ・ストアの構成](#)」を参照してください。

アイデンティティ・プロバイダを構成する

このホワイト・ペーパーでは、Active Directory Federation Service (ADFS) をアイデンティティ・プロバイダ (IP) として使用しています。ADFS は Microsoft が開発したソフトウェア・コンポーネントで、複数の組織境界にわたって配置されているシステムとアプリケーションにユーザーがシングル・サインオンでアクセスできるようにするものです。ADFS では、要求ベースのアクセス制御認可モデルを使用することにより、アプリケーションのセキュリティを維持してフェデレーテッド ID を実装します。

Ping Federate、OAM、Shibboleth、その他の IDP を使用する場合は、この項をスキップしてください。IDP の製品ドキュメントを使用してインストールと構成を行ったら、SP の構成の項に進んでください。IDP の各ドキュメントには SP の構成に関する項があり、この項で SP のメタデータ・ファイルを IDP にインポートします。

ADFS を構成するには、次の手順を実行します。

- » [IIS でサーバー認証証明書を構成する](#)
- » [ADFS をスタンドアロンのフェデレーション・サーバーとして構成する](#)
- » [ADFS の SAML 2.0 メタデータをダウンロードする](#)
- » [ADFS で WebCenter Portal をサービス・プロバイダとして構成する](#)

IISでサーバー認証証明書を構成する

自己署名の Secure Sockets Layer (SSL) 証明書を作成し、IIS マネージャ・コンソールを使用してデフォルトの Web サイトにバインドします。

1. インターネット・インフォメーション・サービス (IIS) マネージャ・コンソールを開きます。
2. 「スタート」メニューで「すべてのプログラム」を選択し、「管理ツール」、「インターネット インフォメーション サービス (IIS) マネージャー」の順に選択します。
3. コンソール・ツリーで、コンピュータの名前が含まれたルート・ツリーをクリックし、詳細ウィンドウで、IIS グループの「サーバー証明書」アイコンをダブルクリックします。
4. 操作ウィンドウで、「自己署名入り証明書の作成」をクリックします。
5. 「フレンドリ名を指定します」ページで、証明書のわかりやすい名前を入力し、「OK」をクリックします。
6. コンソール・ツリーで、「既定の Web サイト」をクリックします。
7. 操作ウィンドウで、「バインド」をクリックします。
8. サイト・バインド・ダイアログ・ボックスで、「追加」をクリックします。
9. サイト・バインドの追加ダイアログ・ボックスで、「種類」ドロップダウン・リストから http を選択し、「SSL 証明書」ドロップダウン・リストからマシンの証明書を選択します。「OK」をクリックして「閉じる」をクリックします。
10. インターネット・インフォメーション・サービス (IIS) マネージャ・コンソールを閉じます。

ADFSをスタンドアロンのフェデレーション・サーバーとして構成する

1. ADFS 2.0 管理コンソールを開いて、「ADFS 2.0」を選択します。
2. 詳細ウィンドウで、「ADFS 2.0 フェデレーション サーバーの構成ウィザード」リンクをクリックしてウィザードを開始します。
3. ようこそページで、「新しいフェデレーション サービスを作成する」をクリックし、「次へ」をクリックします。
4. スタンドアロン展開またはファーム展開の選択ページで、「スタンドアロン フェデレーション サーバー」をクリックし、「次へ」をクリックします。
5. フェデレーション・サービス名の指定ページで、「IIS でサーバー認証証明書を構成する」で作成した証明書名が選択されていることを確認し、「次へ」をクリックします。
6. Ready to Apply Settings ページで、設定を確認して「次へ」をクリックします。
7. 構成の結果ページで、「閉じる」をクリックします。

図 4 に示すように、ページの左ウィンドウに ADFS ノードが表示されます。

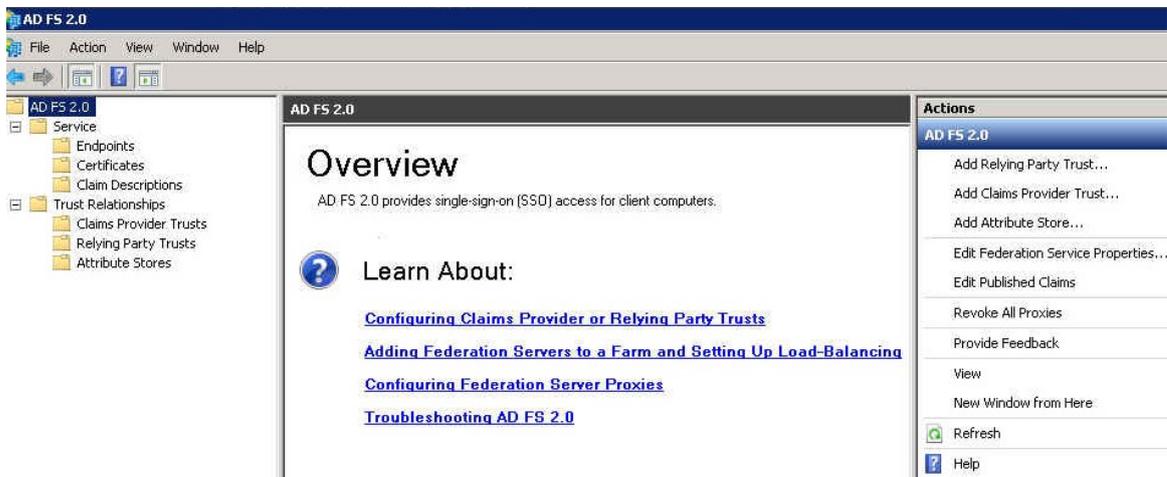


図 4 : ADFS の概要ページ

ADFSのSAML 2.0メタデータをダウンロードする

ADFS の SAML 2.0 メタデータをダウンロードするには、次の手順を実行します。

1. 次の URL で、xml ファイルを見つけます。
<https://adfsHost:adfsPort/FederationMetadata/2007-06/FederationMetadata.xml> (例 :
<https://localhost/FederationMetadata/2007-06/FederationMetadata.xml>)
2. 「WebCenter Portal をサービス・プロバイダとして構成する」の手順で ADFS を WLS で構成するために、このファイルを `idp_metadata.xml` としてローカルに保存します。

他の製品を IDP として使用する場合は、その製品のドキュメントを確認して、その IDP の SAML 2.0 メタデータ・ファイルをダウンロードします。このメタデータ・ファイルを WebCenter Portal の WLS にインポートする必要があるため、この手順は必須です。

ADFSでWebCenter Portalをサービス・プロバイダとして構成する

この時点では、この項をスキップして、「WLS をサービス・プロバイダとして構成する」を完了します。「SAML 2.0 全般サービスを構成する」の項で SP のメタデータ・ファイルを作成したら、ここに戻ってこの項を完了します。

次の手順を実行して、ADFS IDP で WebCenter Portal をサービス・プロバイダとして追加します。

1. ADFS 2.0 管理コンソールを開きます。
2. 「**証明書利用者信頼**」を右クリックして「**証明書利用者信頼の追加**」を選択します。
3. 証明書利用者信頼の追加ウィザードで、「**開始**」をクリックします。

4. 「**証明書利用者についてのデータをファイルからインポートする**」を選択して、WLS SAML 2.0 メタデータ・ファイル (sp_metadata.xml) をポイントします。

このファイルを生成する手順は、「[SAML 2.0 全般サービスを構成する](#)」で説明しています。

5. 「**次へ**」をクリックし、「**表示名**」に、新しい WCP SAML 2.0 サービス・プロバイダの表示名を WCP SP と入力します。
6. 「**次へ**」をクリックし、「**すべてのユーザーに対してこの証明書利用者へのアクセスを許可する**」を選択します。
7. 「**次へ**」をクリックし、もう一度「**次へ**」をクリックし、「**閉じる**」をクリックします。「**Open the Edit claims**」ボックスはオンのままにします。
8. 規則の編集ウィンドウが開いたら、「**規則の追加**」をクリックします。
ユーザーのログイン名と指定名を LDAP から取得して名前 ID および指定名 SAML 属性として含めるように、ADFS を構成します。
9. 変換要求規則の追加ウィザードで、「**LDAP 属性を要求として送信**」を選択します。
10. 「**次へ**」をクリックし、要求規則名に名前を入力し、属性ストアドロップダウン・リストで「Active Directory」を選択し、「LDAP 属性」に「SAM アカウント名」を、「出力方向の要求の種類」に「名前 ID」を選択します ([図 5](#) を参照)。

| Claim rule name: | |
|---|---------------------|
| Name | |
| Rule template: Send LDAP Attributes as Claims | |
| Attribute store: | |
| Active Directory | |
| Mapping of LDAP attributes to outgoing claim types: | |
| LDAP Attribute | Outgoing Claim Type |
| SAML-Account-Name | Name ID |

図 5：変換要求規則の追加ウィザード - LDAP 規則の構成

11. 「**完了**」をクリックします。
12. 「**規則の追加**」をクリックし、「**LDAP 属性を要求として送信**」を選択します。
13. 「**次へ**」をクリックし、要求規則名に Given Name と入力します。
14. 「入力方向の要求の種類」で「Given Name」を選択し、「出力方向の要求の種類」で「Given Name」を選択します ([図 6](#) を参照)。

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

| | LDAP Attribute | Outgoing Claim Type |
|---|---|---|
| ▶ | <input type="text" value="Given Name"/> | <input type="text" value="Given Name"/> |

図 6: 「入力方向の要求を変換」オプションの規則ページの構成

15. 「完了」をクリックします。
16. 新しく作成した証明書利用者である WCP SP を右クリックし、「プロパティ」を選択します。
17. SHA-256 を使用して動作するように WLS を構成しない場合は、「詳細設定」タブをクリックして「SHA-1」を選択し、「OK」をクリックします。

WLSをサービス・プロバイダとして構成する

この項では、SSO に参加する各パートナー・アプリケーションを SP として構成する必要があります。このホワイト・ペーパーでは、WebCenter Portal を SP として構成する手順について説明してきました。同様の手順を Discussion、WebCenter Content Server、その他のパートナー・アプリケーションに対して実行する必要があります。

開始する前に、SAML フェデレーション IDP の SAML 2.0 アイデンティティ・プロバイダ・メタデータ・ファイルが必要です。メタデータ・ファイルは、SAML 2.0 仕様に準拠した標準形式になっている必要があります。アイデンティティ・プロバイダから SAML 2.0 IDP メタデータを取得する方法については、ベンダーのドキュメントを参照してください。ADFS の場合は、「ADFS の SAML 2.0 メタデータをダウンロードする」を参照してください。

この項で示している手順は、WebCenter Portal ドメインに対して実行する手順です。

サービス・プロバイダ (SP) を構成するには、次の手順を実行します。

- » [SAML 2.0 アイデンティティ・アサーション・プロバイダを構成する](#)
- » [SAML 2.0 サービス・プロバイダのサービスを構成する](#)
- » [SAML 2.0 全般サービスを構成する](#)
- » [アイデンティティ・プロバイダ・パートナーを作成および構成する](#)

SAML 2.0アイデンティティ・アサーション・プロバイダを構成する

1. WebCenter Portal ドメイン用の Weblogic 管理コンソールにログインします。
2. 「**Security Realms**」、「**myrealm**」、「**Providers**」、「**Authentication**」の順に選択します。
3. 認証プロバイダのページ（図 7）で、「**New**」をクリックして「**SAML2IdentityAsserter**」を選択します。
4. 名前に SAML2IAsserter（または同様な名前）と入力して「**OK**」をクリックします。

注：このアサータには、プロバイダ固有の構成は必要ありません。

Home > Summary of Security Realms > myrealm > Providers

Create a New Authentication Provider

OK Cancel

Create a new Authentication Provider

The following properties will be used to identify your new Authentication Provider.
* Indicates required fields

The name of the authentication provider.

Name: SAM2IAsserter

This is the type of authentication provider you wish to create.

Type: SAML2IdentityAsserter

OK Cancel

図 7 : Create a New Authentication Provider

5. 「Activate Changes」をクリックします。

Home > Summary of Security Realms > myrealm > Providers

Messages

✔ All changes have been activated. However 2 items must be restarted for the changes to take effect.

Settings for myrealm

Configuration Users and Groups Roles and Policies Credential Mappings **Providers** Migration

Authentication Password Validation Authorization Adjudication Role Mapping Auditing Credential Mapping Certification Path Keystores

An Authentication provider allows WebLogic Server to establish trust by validating a user. You must have one Authentication provider in a security realm, and you providers are designed to access different data stores, such as LDAP servers or DBMS. You can also configure a Realm Adapter Authentication provider that allows

▶ **Customize this table**

Authentication Providers

New Delete Reorder

| <input type="checkbox"/> | Name | Description |
|--------------------------|-------------------------|---|
| <input type="checkbox"/> | OID Authenticator | Provider that performs LDAP authentication |
| <input type="checkbox"/> | DefaultAuthenticator | WebLogic Authentication Provider |
| <input type="checkbox"/> | DefaultIdentityAsserter | WebLogic Identity Assertion provider |
| <input type="checkbox"/> | IAMSuiteAgent | Oracle Access Manager Servlet Authentication Filter and Identity Asserter Provider |
| <input type="checkbox"/> | SAML2Asserter | SAML 2.0 Identity Assertion Provider. Supports Security Assertion Markup Language v2.0. |

New Delete Reorder

図 8 : 認証プロバイダのリスト

6. サーバーを再起動します。

アイデンティティ・アサーション・プロバイダの構成について、詳しくは「[ID アサーション・プロバイダの構成](#)」を参照してください。

クラスタ内で実行する場合は、[図 9](#)に示すように、SAML2IAsserter の「Replicated Cache Enabled」プロパティをオンにします。

Configuration Management Migration

Common **Provider Specific**

Save

Use this page to configure provider-specific information for this SAML 2.0 Identity Assertion provider.

Replicated Cache Enabled Specifies whether the replicated cache is used. [More Info...](#)

Identity Domain:

Login Token Association Enabled

Name Mapper Class Name: The custom Java class that overrides the default SAML 2.0 assertion name mapper class, which maps identity information contained in assertions to local Subjects. [More Info...](#)

Save

図 9 : クラスタでの SAML 2.0 アイデンティティ・アサーション・プロバイダの構成

SAML 2.0サービス・プロバイダのサービスを構成する

「Servers」、「WC_Portal」、「Federation Services」、「SAML 2.0 Service Provider」の順に選択し、次の変更を行います（[図 10](#)を参照）。

- » 「Enabled」チェック・ボックスをオンにします。
- » 「Always Sign Authentication Requests」チェック・ボックスをオンにします。
- » ドロップダウン・メニューから「Preferred Binding as POST」を選択します。
- » Default URL に `https://WCP_HOST:WCP_SSL_PORT/webcenter` と入力します。

Home > Summary of Servers > WC_Portal

Settings for WC_Portal

Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes

General Cluster Services Keystores SSL Federation Services Deployment Migration Tuning Overload Con

SAML 1.1 Source Site SAML 1.1 Destination Site SAML 2.0 General SAML 2.0 Identity Provider **SAML 2.0 Service Provider**

Save

This page configures the SAML 2.0 per server service provider properties

Enabled

Always Sign Authentication Requests

Force Authentication

Passive

Only Accept Signed Assertions

Authentication Request Cache Size:

Authentication Request Cache Timeout:

POST One Use Check Enabled

POST Binding Enabled

Artifact Binding Enabled

Preferred Binding:

Default URL:

Save

図 10 : SAML 2.0 サービス・プロバイダのサービスの構成

SAML 2.0全般サービスを構成する

SAML 2.0 全般サービスで次のことを構成します。

「**Servers**」、「**WC_Portal**」、「**Federation Services**」、「**SAML 2.0 General**」の順に選択し、次のプロパティ値を指定します（[図 11](#)）。

- » Replicated Cache Enabled：オンまたはオフ
注：レプリケーション・キャッシュの有効化は、クラスタなど、ドメイン内の複数の WebLogic Server インスタンスに SAML 2.0 サービスを構成する場合に必要です。
- » Contact Person Given Name
- » Contact Person Surname
- » Contact Person Type
- » Contact Person Company
- » Contact Person Telephone Number
- » Contact Person Email Address
- » Organization Name
- » Organization URL
- » Published Site URL：https://<DestinationSiteDNSName>:<SSL_PORT>/saml2
- » Entity ID：（宛先ドメイン名）
- » Single Sign-on Signing Key Alias
- » Single Sign-on Signing Key Pass Phrase
- » Confirm Single Sign-on Signing Key Pass Phrase

| | | | | | | | | | | |
|----------------------|---------------------------|-------------------------|----------------------------|---------------------------|----------------------------|-------------|-----------|----------|----------|---|
| Configuration | Protocols | Logging | Debug | Monitoring | Control | Deployments | Services | Security | Notes | |
| General | Cluster | Services | Keystores | SSL | Federation Services | Deployment | Migration | Tuning | Overload | C |
| SAML 1.1 Source Site | SAML 1.1 Destination Site | SAML 2.0 General | SAML 2.0 Identity Provider | SAML 2.0 Service Provider | | | | | | |

Save Publish Meta Data

This page configures the general SAML 2.0 per server properties

General

Replicated Cache Enabled

Site Info

Contact Person Given Name: john

Contact Person Surname: joe

Contact Person Type: support

Contact Person Company: AviPartner

Contact Person Telephone Number: 999-999-999

Contact Person Email Address: abc@example.com

Organization Name: Marketing

Organization URL: www.avipartner.com

Published Site URL: https://WCP_HOST:WCP_SSL_PORT/saml2

Entity ID: AviPartner_WebCenter

Bindings

Recipient Check Enabled

図 11：全体的な SAML 2.0 全般サービスの構成

このホワイト・ペーパーでは、WLS のデモ証明書で **demoidentity** キーストアを使用して検証しています。顧客のセットアップには、カスタムのキーストアおよび適切な署名証明書が含まれます。この項の署名キー情報を指定します（[図 12](#) を参照）。

注：demoidentity を例に使用しており、パスワードは DemoidentityPassPhrase です。

Create a SAML 2.0 Web Single Sign-on Identity Provider Partner

OK Cancel

Partner Properties

Use this page to:

- Enter the name of your new Single Sign-on Identity Provider partner
- Specify the name and location of the SAML 2.0 metadata file that you received from this

* Indicates required fields

Please specify the name of the partner.

* **Name:**

Please specify the name of the file containing the partner metadata document.

Path:

Recently Used Paths: (none)

Current Location:

- 📁 aime
- 📁 aime1
- 📁 aime10
- 📁 aime2
- 📁 aime3
- 📁 aime4
- 📁 aime5
- 📁 aime6
- 📁 aime7
- 📁 aime8
- 📁 aime9
- 📁 demo
- 📁 jsk_project
- 📁 mds
- 📁 nbshah
- 📁 optena
- 📁 oraInventory
- 📁 ses
- 📄 connections.xml
- 📄 idp_metadata.xml
- 📄 input.xml
- 📄 input_auth.xml
- 📄 input_f_doc.xml

図 13 : Create SAML 2.0 Web Single Sign-on Identity Provider Partner

ADFS メタデータのインポートが失敗する場合、WS-Trust メタデータ・コンテンツとメタデータ署名を削除すると、ほとんどのインポート・プロセスは成功します。WS-Trust メタデータ・コンテンツおよびメタデータ署名を削除するには、次の手順を実行します。

5. XML エディタで idp_metadata.xml を開きます。

6. 次の表に示されているファイルのセクションを削除します。

| 説明 | セクションの先頭 | セクションの末尾 |
|--|---|--------------------------------------|
| メタデータ・ドキュメント署名 | <code><ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"></code> | <code></ds:Signature></code> |
| WS-TrustおよびWS-Federation アプリケーション・サービス・メタデータ | <code><RoleDescriptor xsi:type="fed:ApplicationServiceType"</code> | <code></RoleDescriptor></code> |
| WS-TrustおよびWS-Federation セキュリティ・トークン・サービス・メタデータ | <code><RoleDescriptor xsi:type="fed:SecurityTokenServiceType"</code> | <code></RoleDescriptor></code> |

7. 自動生成の ADFS 2.0 メタデータ・ファイルには、IDP ロールと SP ロール両方の実行に関する情報が格納されます。これを前提に IDP を追加しようとした場合、WLS では、メタデータ・ファイルへの SAML 2.0 IDP 記述子と SP 記述子の両方の格納はサポートされていません。ファイルの次のセクションを削除します。

| 説明 | セクションの先頭 | セクションの末尾 |
|------------------|--|---------------------------------------|
| SAML 2.0 SPメタデータ | <code><SPSSODescriptor WantAssertionsSigned="true"</code> | <code></SPSSODescriptor></code> |

削除後のファイルの最初の2つの要素は、次のようになります。

```
<EntityDescriptor ID=...>  
  <IDPSSODescriptor WantAssertionsSigned="true" ...
```

8. 編集したファイルを保存して、インポート手順を再度実行します。

インポートが完了したら、「SAML_SSO_IDP01」をクリックして次のように入力します。

- » Name : SAML_SSO_IDP01
- » Enabled : チェック・ボックスをオン
- » Description : SAML_SSO_IDP01
- » Redirect URIs : /webcenter/*

これで、WCP SP の構成が完了しました。SSO に参加する各パートナー・アプリケーションに対して、同様な構成を行う必要があります。

ここで、「[ADFS で WebCenter Portal をサービス・プロバイダとして構成する](#)」に戻って手順を完了します。

SAML 2.0ベースのフェデレーテッドSSOをテストする

この時点で、WebCenter ドメインは SAML 2.0 のサービス・プロバイダで構成されており、ADFS は IDP として構成されています。フェデレーテッド SSO を検証するには、次の手順を実行します。

- » WebCenter Portal インスタンスを ADFS と同じ Oracle Internet Directory に接続するか、WebCenter Portal サーバーに接続されている Oracle Internet Directory に ADFS ユーザーが存在することを確認します。詳しくは、「[WebCenter Portal ドメインにアイデンティティ・ストアを構成する](#)」を参照してください。
- » WebCenter Portal SSL の URL (たとえば、`https://WCP_HOST:WCP_PORT/webcenter`) にアクセスします。ADFS にリダイレクトされて、基本認証チャレンジが動作します。Windows 資格情報 (ADFS 資格情報ストアの資格情報) を指定します。ログインが成功すると、WebCenter Portal ホームページが表示されます。

他のパートナー・アプリケーションが構成されている場合は、保護されているパートナー・アプリケーション・ページにアクセスします。ログインは求められずに、保護されているページに直接移動します。



Oracle Corporation, World Headquarters

500 Oracle Parkway
Redwood Shores, CA 94065, USA

海外からのお問い合わせ窓口

電話：+1.650.506.7000
ファクシミリ：+1.650.506.7200

CONNECT WITH US

-  blogs.oracle.com/oracle
-  facebook.com/oracle
-  twitter.com/oracle
-  oracle.com

Hardware and Software, Engineered to Work Together

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. 本文書は情報提供のみを目的として提供されており、ここに記載されている内容は予告なく変更されることがあります。本文書は一切間違いがないことを保証するものではなく、さらに、口述による明示または法律による黙示を問わず、特定の目的に対する商品性もしくは適合性についての黙示的な保証を含み、いかなる他の保証や条件も提供するものではありません。オラクルは本文書に関するいかなる法的責任も明確に否認し、本文書によって直接的または間接的に確立される契約義務はないものとします。本文書はオラクルの書面による許可を前もって得ることなく、いかなる目的のためにも、電子または印刷を含むいかなる形式や手段によっても再作成または送信することはできません。

Oracle および Java は Oracle およびその子会社、関連会社の登録商標です。その他の名称はそれぞれの会社の商標です。

Intel および Intel Xeon は Intel Corporation の商標または登録商標です。すべての SPARC 商標はライセンスに基づいて使用される SPARC International, Inc. の商標または登録商標です。AMD、Opteron、AMD ロゴおよび AMD Opteron ロゴは、Advanced Micro Devices の商標または登録商標です。UNIX は、The Open Group の登録商標です。0416

WebCenter Portal での SAML 2.0 フェデレーテッド SSO 2016 年 4 月

著者：Nitin Shah

共著者：Suresh Alagarswamy



Oracle is committed to developing practices and products that help protect the environment