Cisco Unity Connection 10.x における SAML SSO アクセスのトラブルシューティング

次の項を参照してください。

IdP へのリダイレクションが失敗する

エンド ユーザが Unity Connection でサポートされている Web ブラウザを使用して SAML 対応 Web アプリケーションにログインしようとすると、認証の詳細を入力するために設定された Identity Provider（IdP）にリダイレクトされません。

ソリューション

次の条件が満たされていることを確認します。

- IdP がアップの状態で、稼働中である。
- 正しい IdP メタデータ ファイル（idp.xml）が Cisco Unity Connection にアップロードされている。
- サーバと IdP が信頼と同じ範囲にあるかどうかを確認する。

IdP 認証が失敗する

エンド ユーザが IdP によって認証されません。

ソリューション

次の条件が満たされていることを確認します。

- LDAP ディレクトリが IdP にマッピングされている。
- ユーザが LDAP ディレクトリに追加されている。問題が解消されない場合には、Unity Connection と IdP に関連付けられた NTP サーバを確認します。これらの両方のサーバに関連付けられた NTP サーバの時刻が同期化されていることを確認します。
- LDAP アカウントがアクティブである。
- ユーザ ID とパスワードが正しい。

Unity Connection へのリダイレクションが失敗する

IdP で認証された後でも、ユーザが SAML SSO 対応 Web アプリケーションにリダイレクトされません。

ソリューション

- Unity Connection および IdP のクロックが同期化されている。クロックの同期の詳細については、『*Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection*』の「NTP Settings」の項を参照してください。
- 必須属性の uid が IdP で設定されている。
- 正しい Unity Connection サーバのメタデータ ファイルが IdP にアップロードされている。
- ユーザに必要な権限がある。

[テストの実行（Run Test）] が失敗する

[テストの実行（Run Test）] が Unity Connection で失敗する場合

ソリューション

「IdP へのリダイレクションが失敗する」（P.28-1）、「IdP 認証が失敗する」（P.28-1）、および「Unity Connection へのリダイレクションが失敗する」（P.28-2）で説明されている修正処置を参照してください。

パブリッシャおよびサブスクライバ サーバの SAML ステータスの不一致

Unity Connection のパブリッシャ サーバとサブスクライバ サーバの SAML ステータスに不一致が発生した場合

ソリューション

- IdP メタデータがサブスクライバ サーバで正しいかどうかを確認します。正しくない場合、[SAML シングルサインオン（SAML Single Sign-On）] Web ページから [メタデータの再インポート（Re-import Meta Data）] オプションを選択します。
- 問題が解消されない場合には、[無効になっているすべてのサーバを修正（Fix All Disabled Servers）] オプションを選択します。

（注）　Unity Connection クラスタの場合は、パブリッシャ サーバのメタデータを再インポートするオプションはありません。

SAML SSO 機能のステータスが Unity Connection クラスタ内の 2 台のサーバで正しくない

SAML SSO 機能のステータスが Unity Connection クラスタ内の 2 台のサーバで異なる場合

ソリューション：

- SAML SSO のステータスがサブスクライバ サーバで無効で、パブリッシャ サーバで有効の場合、サブスクライバ サーバで Cisco Unity Connection の管理 にログインし、[無効になっているすべてのサーバを修正（Fix All Disabled Servers）] オプションを選択します。
- パブリッシャ サーバが到達不能な場合、サブスクライバ サーバの SAML SSO 機能を無効にする場合は、パブリッシャ サーバから SAML SSO 機能を明示的に無効にする必要があります。逆の場合も同様になります。問題が解消されない場合は、サーバをリブートする必要もあります。
- パブリッシャの再構築では、管理者が明示的にクラスタのパブリッシャ サーバの IdP メタデータ ファイルを更新する必要があります。

SAML SSO アクセスでの問題の診断トレース

Unity Connection トレース レベルを有効にして、SAML SSO 機能に関連した問題を検出し、調査することができます。トレースは、システム サーバへのコマンドライン アクセス（CLI）から始まります。

特定のコマンドによって、SAML SSO のトレースがオンになります。

admin: **set samltrace level <trace-level>**

定義されたトレースは、次のとおりです。

- デバッグ（Debug）
- 情報（Info）
- 警告（Warning）
- エラー（Error）
- 重大（Fatal）

トレースは、Unity Connection の次の場所で収集されます。

/var/log/active/tomcat/logs/ssosp