CUCMバージョン12.xでのOS AdminおよびDRSのSSOの設定

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[設定](#)
[既存のOS管理者ユーザを使用](#)
[新しいユーザーの使用](#)
[確認](#)
[トラブルシュート](#)

概要

このドキュメントでは、Cisco Unified Communications Manager(CUCM)バージョン12.0以降で導入された、オペレーティングシステム(OS)管理およびディザスタリカバリシステム(DRS)のシングルサインオン(SSO)機能について説明します。

12.0よりも前のバージョンのCUCMは、CM Administration、Serviceability、およびReportingページに対してのみSSOをサポートしています。この機能により、管理者は異なるコンポーネントを迅速に移動し、より優れたユーザエクスペリエンスを得ることができます。OS AdminとDRSのSSOが壊れた場合に備えて、リカバリURLを使用するオプションもあります。

前提条件

要件

CUCMバージョン12.0以降に関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、Cisco Call Manager(CCM)バージョン12.0.1.21900-7に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

OS AdminとDRSのSSOを有効にするには、CM Administration口グインに対してSSOがすでに有

効になっている必要があります。これに加えて、新しいユーザまたは既存のユーザのいずれかであるプラットフォームレベルのユーザも必要です。

既存のOS管理者ユーザを使用

インストール時に作成されたプラットフォームユーザは、OS AdminおよびDRSコンポーネントのSSOログイン用に設定できます。この場合の唯一の要件は、Identity Provider(IdP)が認証されるActive Directory(AD)にこのプラットフォームユーザを追加する必要があることです。

新しいユーザーの使用

SSO OS AdminおよびDRSログイン用に新しいユーザを有効にするには、次の手順を実行します。

ステップ 1：PublisherのCLIアクセスから、特権レベル1/0の新しいユーザを作成します。

新しいユーザを作成するには、インストール時に作成されたプラットフォームユーザが所有するプラットフォーム4レベルのアクセスが必要です。

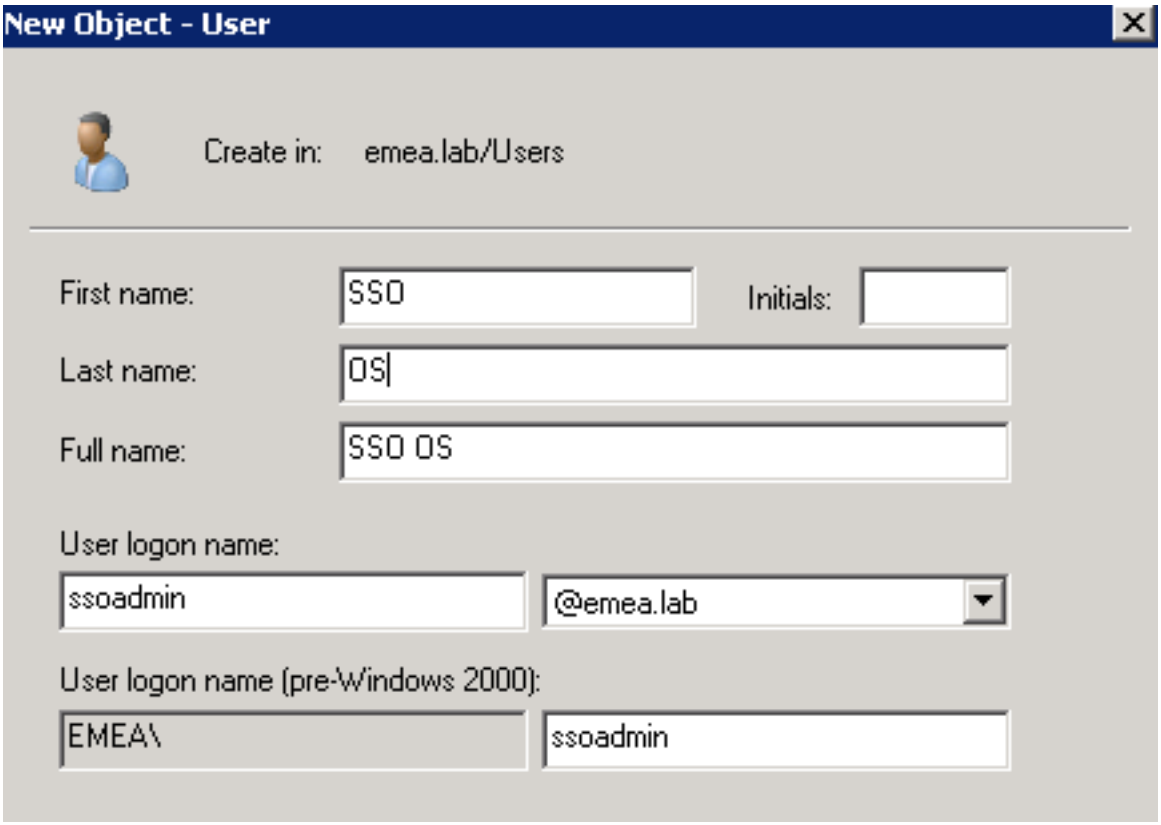
レベル0の権限はユーザに読み取りアクセス権のみを与え、レベル1の権限は読み取り権限と書き込み権限の両方を与えます。

```
admin:set account name ssoadmin



Privilege Levels are:

   Ordinary - Level 0

   Advanced - Level 1



Please enter the privilege level :1

Allow this User to login to SAML SSO-enabled system through Recovery URL ? (Yes / No) :yes

To authenticate a platform login for SSO, a Unique Identifier (UID) must be provided that
identifies this user to LDAP (such as sAMAccountName or UPN).

        Please enter the appropriate LDAP Unique Identifier (UID) for this user:[ssoadmin]

Storing the default SSO UID value as username

Please enter the password :********

            re-enter to confirm :********

Account successfully created
```

ここで使用されるUnique Identifier（UID；固有識別子）には、IdPがアサーション応答で提供する任意の値を指定するか、値を空白にしておくことができます。空白のままにすると、CUCMはUIDとして**userid**を使用します。

ステップ 2：次の図に示すように、IdPが認証されるADサーバで以前と同じユーザIDを持つユー

ザを追加します。



ステップ 3：図に示すように、新しく作成されたユーザがCUCMに入力されるように、Lightweight Directory Access Protocol(LDAP)サーバの同期も必要です。

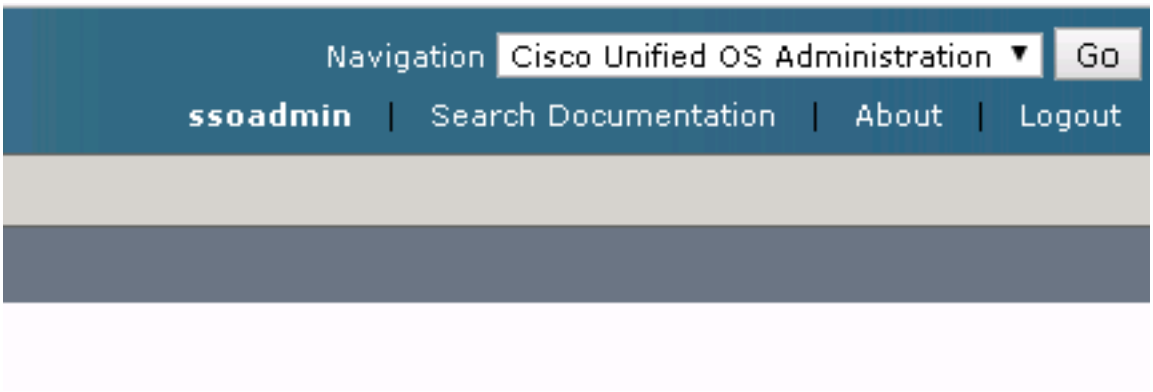
ステップ 4：ADへの追加後に作成されたユーザに対しては、パスワードのリセット（CLIを再び使用）が必要です。

```
login as: ssoadmin

ssoadmin@10.106.96.92's password:

WARNING: Your password has expired.

You must change your password now and login again!

Changing password for user ssoadmin.

Changing password for ssoadmin.

(current) UNIX password:

New password:

Re-enter password:
```

確認

ここでは、設定が正常に機能しているかどうかを確認します。

OS AdminとDRSに対してSSOが正常に有効になると、図に示すように、以前に作成したユーザのADのクレデンシャルを使用してログインが動作する必要があります。



トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。