InterSystems SQL の基礎：LDAP との統合

Version 2023.1
2024-01-02

InterSystems Corporation　1 Memorial Drive　Cambridge MA 02142　www.intersystems.com

InterSystems SQL の基礎 : LDAP との統合
InterSystems IRIS Data Platform　Version 2023.1　2024-01-02

インターシステムズ社の製品に関するサポートやご質問は、以下にお問い合わせください：

InterSystems Worldwide Response Center (WRC)
Tel:　+1-617-621-0700
Tel:　+44 (0) 844 854 2917
Email:　support@InterSystems.com

目次

InterSystems SQL の基礎 : LDAP との統合

InterSystems IRIS® データ・プラットフォームでは、LDAP (Lightweight Directory Access Protocol) サーバと統合し、この広く使用されているテクノロジを使用してユーザをシームレスに認証できます。LDAP を介して承認を提供することも容易です。

ユーザが InterSystems IRIS にログインしようとすると、ユーザ名とパスワードが LDAP サーバに送信されて、そのユーザが存在することが確認されます。ユーザの識別情報が認証されたら、LDAP サーバは、ユーザが属するグループについての情報を InterSystems IRIS に送信します。これらのグループは、ユーザが実行を承認されているアクションと、ユーザがコンテンツを読み書きできるかどうかを制御する InterSystems IRIS のロールに対応しています。このように、InterSystems IRIS は、そのセキュリティ方策の認証と承認の両方の側面において LDAP テクノロジを使用します。

このドキュメントの手順に従うことにより、LDAP サーバに接続して、LDAP サーバが InterSystems IRIS のセキュリティにどのように影響するかを確認できます。これらの演習では、Windows Active Directory サーバと統合するように InterSystems IRIS を構成します。他の LDAP サーバもサポートされていますが、LDAP 認証および承認に関するこのツアーでは Active Directory の使用に的を絞っています。

1 LDAP 認証の設定

LDAP ユーザとしてログインして InterSystems IRIS の LDAP ベースのセキュリティを確認する前に、以下を行う必要があります。

- InterSystems IRIS インスタンスを選択する
- LDAP 構成を定義する
- LDAP ドメインを既定として選択する
- InterSystems IRIS で LDAP 認証を有効にする
- LDAP サーバのセキュリティ証明書をインストールする

1.1 InterSystems IRIS インスタンスの選択

この手順を使用するには、稼動中の InterSystems IRIS インスタンスが必要です。選択肢としては、いくつかのタイプのライセンス付与されたインスタンスおよび無料の評価版インスタンスがあります。操作しているシステムでインスタンスをホストする必要はありません (ただし、相互のネットワーク・アクセスが必要です)。操作を実行するインスタンスをまだ用意できていない場合にインスタンスのタイプ別の導入方法の詳細を確認するには、"InterSystems IRIS の基礎 : IDE の接続" の "InterSystems IRIS の導入" を参照してください。

1.2 LDAP 構成の定義

InterSystems IRIS は、LDAP 構成を使用して、LDAP サーバへの接続とユーザの検索に必要な情報を定義します。新しい LDAP 構成を作成して定義するには、以下の手順に従います。

1. ブラウザで、インスタンスの管理ポータルを開きます。使用する URL は、選択したインスタンスのタイプによって異なります。適切な URL の特定に関する詳細は、"InterSystems IRIS の基礎 : IDE の接続" の "InterSystems IRIS 接続情報" を参照してください。

2. [セキュリティ LDAP 構成] ページ ([システム管理]→[セキュリティ]→[システム・セキュリティ]→[LDAP 構成]) に移動します。
3. [新規 LDAP 構成の作成] をクリックします。
4. [名前] フィールドに、irisldap.com と入力します。
5. [有効] チェック・ボックスにチェックを付けます。
6. [LDAP サーバが Windows アクティブ・ディレクトリ・サーバ] チェック・ボックスにチェックを付けます。
7. 以下のフィールドを定義します。

フィールド	内容
LDAPドメイン名 (Windows のみ)	irisldap.intersystems.com
LDAP ホスト名	irisldapdc1.irisldap.intersystems.com
検索に使用する LDAP ユーザ名	• (Windows) sidLDAPQuery • (UNIX®) CN=sidLDAPQuery,CN=Users,DC=irisldap,DC=intersystems,DC=com
LDAPユーザ名パスワード	[新規パスワード入力] を選択して、パスワード Cach3L3arning を入力します。
検索に使用するLDAPベースDN	DC=irisldap,DC=intersystems,DC=com
LDAPユニーク検索属性	sAMAccountName

8. [LDAPセッションに TLS/SSL 暗号化を使用する] チェック・ボックスにチェックを付けます。
9. [ロール/ルーチン/ネームスペースに LDAP グループを使用する] チェック・ボックスにチェックを付けます。
10. [ユニバーサル・グループ承認を許可] チェック・ボックスにチェックを付けます。
11. [保存] をクリックします。

1.3 新しい LDAP ドメインの既定としての選択

LDAP サーバの LDAP 構成を定義したら、新しい LDAP 構成を既定の LDAP ドメインとして設定する必要があります。LDAP サーバを既定として設定するには、以下の手順に従います。

1. 管理ポータルのホーム・ページから、[システムワイドセキュリティパラメータ] ページ ([システム管理]→[セキュリティ]→[システム・セキュリティ]→[システムワイドセキュリティパラメータ]) に移動します。
2. [デフォルトセキュリティドメイン] ドロップダウン・リストから [irisldap.com] を選択します。
3. [保存] をクリックします。

1.4 LDAP 認証の有効化

LDAP サーバの使用は、InterSystems IRIS で利用可能な認証方法の 1 つです。InterSystems IRIS のインスタンス全体で LDAP 認証を有効にする必要があるだけでなく、LDAP ユーザがアクセスする必要がある InterSystems IRIS の各コンポーネントでも LDAP 認証を有効にする必要があります。以下の手順では、インスタンス、およびこの InterSystems IRIS セキュリティ・ツアーに必要なコンポーネントに対して LDAP 認証を有効にします。

1. 管理ポータルのホーム・ページで、[**認証/ウェブセッションオプション**] ページ ([**システム管理**]→[**セキュリティ**]→[**システム・セキュリティ**]→[**認証/ウェブセッションオプション**]) に移動します。
2. [**LDAP認証を許可**] チェック・ボックスにチェックを付けます。
3. [**保存**] をクリックします。
4. 管理ポータルのホーム・ページで、[**ウェブ・アプリケーション**] ページ ([**システム管理**]→[**セキュリティ**]→[**アプリケーション**]→[**ウェブ・アプリケーション**]) に移動します。

   このページで、この InterSystems IRIS ツアーでアクセスする管理ポータルの各セクションに対して LDAP 承認を有効にします。管理ポータルの他のセクションでは LDAP 承認は有効にならないので、これらのセクションを操作しようとした場合、ログインするよう求められることがあります。
5. [/csp/sys] をクリックして、Web アプリケーションの構成に使用するページを表示します。
6. [**セキュリティの設定**] セクションで、[**許可された認証方法**] フィールドの [LDAP] チェック・ボックスにチェックを付けます。
7. [**保存**] をクリックします。
8. 設定が保存されたら、[**キャンセル**] をクリックして [**Web アプリケーション**] ページに戻ります。
9. [/csp/sys/sec] をクリックします。この Web アプリケーションには、管理ポータルのセキュリティに関するページが含まれます。
10. [**セキュリティの設定**] セクションで、[**許可された認証方法**] フィールドの [LDAP] チェック・ボックスにチェックを付けます。
11. [**保存**] をクリックします。
12. 設定が保存されたら、[**キャンセル**] をクリックして [**Web アプリケーション**] ページに戻ります。
13. [/csp/sys/op] をクリックします。この Web アプリケーションには、管理ポータルの操作に関するページが含まれます。
14. [**セキュリティの設定**] セクションで、[**許可された認証方法**] フィールドの [LDAP] チェック・ボックスにチェックを付けます。
15. [**保存**] をクリックします。

1.5 LDAP サーバのセキュリティ証明書のインストール

LDAP サーバは TLS で保護されているため、サーバに正常にアクセスするには、セキュリティ証明書をインストールする必要があります。必要な証明書の内容が含まれる .cer ファイルを作成してから、そのファイルをセキュリティ証明書として指定します。

1.5.1 .cer ファイルの作成

セキュリティ証明書としてインストールされるファイルを作成するには、以下の手順に従います。

1. メモ帳などのテキスト・エディタを開いて新しいファイルを作成します。
2. 以下の内容をすべてコピーして、テキスト・エディタで新しいファイルに貼り付けます。新しいファイルは `-----BEGIN CERTIFICATE-----` で始まり、`-----END CERTIFICATE-----` で終わる必要があります。

```
-----BEGIN CERTIFICATE-----
MIIDuTCCAqGgAwIBAgIQO5hG2uC7G7ZBxcXt/J+z3TANBgkqhkiG9w0BAQsFADBv
MRMwEQYKCZImiZPyLGQBGRYDY29tMRwwGgYKCZImiZPyLGQBGRYMaW50ZXJzeXN0
ZW1zMRgwFgYKCZImiZPyLGQBGRYIaXJpc2xkYXAxIDAeBgNVBAMTF2lyaXNsZGFw
LUlSSVNMREFQREMxLUNBMB4XDTE4MDQwOTE0MDUzMloXDTIzMDQwOTE0MTUzMlow
bzETMBEGCgmSJomT8ixkARkWA2NvbTEcMBoGCgmSJomT8ixkARkWDGludGVyc3lz
dGVtczEYMBYGCgmSJomT8ixkARkWCGlyaXNsZGFwMSAwHgYDVQQDExdpcmlzbGRh
cC1JUklTTERBUERMS1DQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
```

```
AL/aNDJJNbzGh6tXG8+hmEEplb80UQMcIhLvoanz/RKKZXBBY68rO5pkYUwn/24g
pryGy0OUjA997KKol5rdbXWzK7vUMuVSp0atw1m4vF9hmp1bpKBC60OXmV39Fqar
ej1dkRl0ZXOmCexP8JqTyNwhpOLXvazzzvsNRr4ts9u1m6y9kFYecu4PRqtFCgoC
T6rbgqz1Ew3VrhQHi0HWvq1sR2CngxdyG8AnlSo6nz3X/IrTwrw5lauNLfpsRda5
D5YfUpxYeqpONSUB650u9bC0l5eRWe8kS33Xr+u5Odkhy087I/zN+GK7xMGzxYMR
OWNINIGRvlLuDRshKQl4gP0CAwEAAaNRME8wCwYDVR0PBAQDAgGGMA8GA1UdEwEB
/wQFMAMBAf8wHQYDVR0OBBYEFM3Ofv4R/zkEgHkp4ayvTkAvxJikMBAGCSsGAQQB
gjcVAQQDAgEAMA0GCSqGSIb3DQEBCwUAA4IBAQC8hhvc/+WsDeipNezBo+ovum2z
7q0fStr73Tj84cDGSyCmT2Q/h0qFvkfjtRd8AUBdG0qjhIB4VLVyWmrWDl1jAUcr
3AzygfO6UZjNRT+4c8r8R2xOhE3wJEJWibzXD9bPCtCkhYNJT6bi5PSRgUq+r9GU
IHnAUmaQa+K+kNEpAvBfIeQ2ox9NPbtUfj/fswKpubWzZZc2udeU8SQLacl6tZMA
tXgZPT6lQfoZU2WmDG1EnoC4Ji1++Sf6Ho2i6kxg1m6geyOPSsGPdsAVjYCqCjuZ
pxjAsfZXV2juLyTBM51rrmV/Rqfougnikh4zhFRBrOHtMP71ZxCptMVz3RHe
-----END CERTIFICATE-----
```

3. アクセスできるディレクトリに、このファイルを irisldap.cer という名前で保存します。

1.5.2 Windows でのセキュリティ証明書のインストール

InterSystems IRIS を Windows 上で実行している場合は、以下の手順を実行して、作成したセキュリティ証明書のインストール・プロセスを完了します。

1. Windows エクスプローラを使用して、セキュリティ・ファイル irisldap.cer を保存したディレクトリで、このファイルをダブルクリックします。
2. **[証明書のインストール]** をクリックします。
3. **[ローカル コンピューター]** を選択して **[次へ]** をクリックします。
4. **[はい]** をクリックして、デバイスへの変更を許可します。
5. **[証明書をすべて次のストアに配置する]** を選択して、**[参照]** をクリックします。
6. **[信頼されたルート証明機関]** を選択して、**[OK]** をクリックします。
7. **[次へ]** をクリックします。
8. **[完了]** をクリックします。

1.5.3 UNIX® でのセキュリティ証明書のインストール

InterSystems IRIS を UNIX® 上で実行している場合は、以下の手順を実行して、作成したセキュリティ証明書のインストール・プロセスを完了します。

1. 管理ポータルに `_system` ユーザとしてログインしている間に、**[セキュリティ LDAP 構成]** ページ (**[システム管理]→[セキュリティ]→[システム・セキュリティ]→[LDAP 構成]**) に移動します。
2. LDAP 構成のリストから [irisldap.com] をクリックします。
3. **[TLS/SSL証明書ファイル]** フィールドに、作成して保存したファイル irisldap.cer のパスとファイル名を入力します。

2 LDAP ユーザとグループの操作

LDAP 接続を構成して LDAP 認証を有効にしたので、LDAP サーバを使用して InterSystems IRIS にログインできます。この LDAP サーバには、user1、user2、および user3 の 3 人のユーザが含まれています。user1 は intersystems-Role-%Operator グループに属し、user2 は intersystems-Role-%Manager グループに属し、user3 は intersystems-Role-%Developer グループに属します。各グループは、InterSystems IRIS の対応するロールに属する特権を付与します。例えば、user1 が LDAP サーバによって正常に認証されると、**%Operator** ロールが割り当てられます。

このツアーでは、3 人のユーザすべてとして InterSystems IRIS にログインし、各ユーザに関連付けられているロールに基づいて利用可能なアクションを調べます。有効な LDAP ユーザとして InterSystems IRIS にログインすると、InterSystems IRIS によって自動的にそのユーザが作成されます。前もって手動でユーザを追加しておく必要はありません。

2.1 User1 : オペレータ

user1 としてログインして InterSystems IRIS を操作するには、以下の手順に従います。

1. 現在 InterSystems IRIS にログインしている場合は、管理ポータルの左上にある **[ログアウト]** リンクをクリックします。
2. 以下の認証情報を使用して InterSystems IRIS にログインします。

   ユーザ名 : `user1`

   パスワード : `Password1`

   User1 は intersystems-Role-%Operator グループのメンバです。このグループに基づいて、user1 が認証されると、InterSystems IRIS の **`%Operator`** ロールに関連付けられている特権が自動的に付与されます。
3. 管理ポータルのホーム・ページで、**[データベース]** ページ (**[システムオペレーション]→[データベース]**) に移動します。**`%Operator`** ロールに関連付けられているページの操作が LDAP サーバによって許可されているため、User1 はこのページにアクセスできます。
4. 管理ポータルのホーム・ページで、**[システム管理]** メニューが無効になっていることを確認します。**`%Operator`** ロールに適切な特権が含まれていないため、User1 はこのメニューにアクセスできません。

2.2 User2 : マネージャ

user2 としてログインして InterSystems IRIS を操作するには、以下の手順に従います。

1. 管理ポータルの上部にある **[ログアウト]** リンクをクリックします。
2. 以下の認証情報を使用して InterSystems IRIS にログインします。

   ユーザ名 : `user2`

   パスワード : `Password2`

   User2 は intersystems-Role-%Manager グループのメンバです。このグループに基づいて、user2 が認証されると、**`%Manager`** ロールに関連付けられている特権が自動的に付与されます。これらの特権には、user1 が表示できなかったページへのアクセスが含まれていることがわかります。
3. 管理ポータルのホーム・ページで、**[ユーザ]** ページ (**[システム管理]→[セキュリティ]→[ユーザ]**) に移動します。user1 は **[システム管理]** メニューにアクセスできなかったことを思い出してください。
4. ユーザのリストから user1 をクリックします。
5. **[ロール]** タブをクリックします。

   `%Operator` が user1 に割り当てられている唯一のロールであることを確認します。
6. **[キャンセル]** をクリックして **[ユーザ]** ページに戻ります。
7. ユーザのリストに user3 のエントリがないことを確認します。user3 がログインした際にこのユーザが自動的に作成され、その際に InterSystems IRIS は LDAP サーバを使用してこのユーザを認証します。

2.3 User3 : 開発者

user3 としてログインして InterSystems IRIS を操作するには、以下の手順に従います。

1. 管理ポータルの上部にある **[ログアウト]** リンクをクリックします。
2. 以下の認証情報を使用して InterSystems IRIS にログインします。

   ユーザ名 : `user3`

   パスワード : `Password3`

   User3 は intersystems-Role-%Developer グループのメンバです。このグループに基づいて、user3 が認証されると、**%Developer** ロールに関連付けられている特権が自動的に付与されます。
3. このユーザは **[システムエクスプローラ]** メニューにはアクセスできますが、**[システムオペレーション]** メニューおよび **[システム管理]** メニューにはアクセスできないことを確認します。user3 に割り当てられている **%Developer** ロールは、user1 と user2 に割り当てられているロールとは異なる特権を持っていることがわかります。このため、user3 は自身のユーザ・プロファイルを表示できません。**[ユーザ]** ページは **[システム管理]** メニューにあるためです。

2.4 ユーザの自動作成

最初に新しいユーザを作成することなく InterSystems IRIS にログインしました。ユーザが LDAP サーバで見つかった場合、これらのユーザは InterSystems IRIS によって自動的に作成されます。以下の図は、このプロセスを示しています。

1. 管理ポータルの上部にある **[ログアウト]** リンクをクリックします。
2. 以下の認証情報を使用して InterSystems IRIS にログインします。

   ユーザ名 : `user2`

   パスワード : `Password2`

   user2 は **%Manager** ロールを持っていることを思い出してください。
3. 管理ポータルのホーム・ページで、**[ユーザ]** ページ (**[システム管理]→[セキュリティ]→[ユーザ]**) に移動します。
4. リストで user3 を見つけ、その行にある **[削除]** をクリックします。

   この時点で、user3 (**%Developer** ロールを持つユーザ) は InterSystems IRIS 内に存在しなくなります。
5. 管理ポータルの上部にある **[ログアウト]** リンクをクリックします。
6. 以下の認証情報を使用して InterSystems IRIS にログインします。

   ユーザ名 : `user3`

   パスワード : `Password3`

   user3 は LDAP サーバ上には引き続き存在しているため、InterSystems IRIS でこのユーザ・アカウントを削除しても、再度 user3 として InterSystems IRIS にログインできます。
7. 必要であれば、InterSystems IRIS に再度ログインして、user3 がユーザになっていることを確認できます。
   a. 管理ポータルの上部にある **[ログアウト]** リンクをクリックします。
   b. 以下の認証情報を使用して InterSystems IRIS にログインします。

      ユーザ名 : `user2`

      パスワード : `Password2`
   c. 管理ポータルのホーム・ページで、**[システム管理]** > **[セキュリティ]** > **[ユーザ]** に移動します。先ほどユーザ・アカウントを削除したにもかかわらず、user3 がリストに存在しています。

3 LDAP とセキュリティの詳細

以下のリソースを使用して、LDAP および他のセキュリティの概念を詳細に学習できます。

- InterSystems IRIS での LDAP の使用についての詳細は、"LDAP ガイド" を参照してください。
- InterSystems IRIS のロールベースのセキュリティの概要は、"インターシステムズの承認について" を参照してください。