Cisco Expressway による LDAP を使用したアカウントの認証

導入ガイド

Cisco Expressway X8.2

D15059.02
2014 年 8 月

目次

はじめに

本書では、一元管理された LDAP アクセス可能サーバ上で Cisco Expressway（Expressway）を設定して、ログイン アカウントを認証および許可する方法について説明します。

LDAP の認証および許可は、Expressway の管理者アカウントへの Web ログインに使用できます。独自の内部データベースのユーザ名とパスワードを検索する代わりに、Expressway は LDAP アクセス可能サーバに接続し、ユーザを認証するとともに、認証したユーザが Expressway へのアクセスを許可されたグループに所属しているかどうかを確認します。

統合ログイン クレデンシャル データベースを使用することで、企業はパスワードの再設定間隔や複雑さのレベルなどのパスワード ポリシーを定義し、全システムのパスワードに確実に適用できるようになります。

現時点で、Expressway がサポートする LDAP でアクセス可能なサーバは、Windows の Active Directory のみです。

シリアル および SSH などのその他のログインでは、引き続き Expressway に設定された管理者アカウントが使用されます。

プロセスのまとめ

管理者は次を行う必要があります。

- LDAP アクセス可能なサーバで、ユーザ（とパスワード）を設定します
- LDAP アクセス可能なサーバで、ユーザの権限を定義するグループを設定します
- LDAP アクセス可能なサーバで、ユーザにグループを関連付けます
- LDAP を使用できるように Expressway を設定します

Expressway にログインしたユーザは、LDAP サーバに保存されたクレデンシャルを使用して認証されます。

ユーザ名とパスワードは、どちらも大文字と小文字が区別されます。

LDAP アクセス可能な認証サーバの設定

認証サーバでのグループの定義

認証サーバ内のグループの定義は、通常、IT 部門が行います。要求フォームの例のコピー(「IT 要求(認証サーバへのアクセス用) [p.15]」を参照)を使用して、IT 部門に関連するグループを設定し、それらのグループにユーザを割り当てるよう要求します。

一般的に、次のグループの設定が必要です。

- 読み書きが可能な管理者(例:exp_admin_rw グループ)
- 読み取り専用の管理者(例:exp_admin_ro グループ)
- オーディタ管理者(例:exp_auditor グループ)

Expressway の設定

DNS サーバの設定

必ず 1 つ以上の DNS サーバ アドレスを Expressway に設定してください（[システム（System）] > [DNS]）。
DNS は次の用途に必要です。

- IP アドレスではなく名前を使用して LDAP サーバを定義した場合に、LDAP サーバの IP アドレスを検索します。
- SASL を有効にした場合にセキュリティ プロセスの一部として、IP アドレスから名前を解決する検査、つまり、LDAP サーバについてのリバース DNS 検索を実行します。SASL を有効にする場合は、DNS サーバがリバース DNS 検索をサポートしている必要があります。

Expressway への LDAP サーバの詳細の設定

1. [ユーザ（Users）] > [LDAP 設定（LDAP configuration）] に移動します。
2. Expressway が LDAP サーバに接続してログイン アカウントの認証およびグループ メンバーシップの検査を実行できるように、次のフィールドを設定します（質問表を使用すると IT 部門から適切な情報を入手できます）。

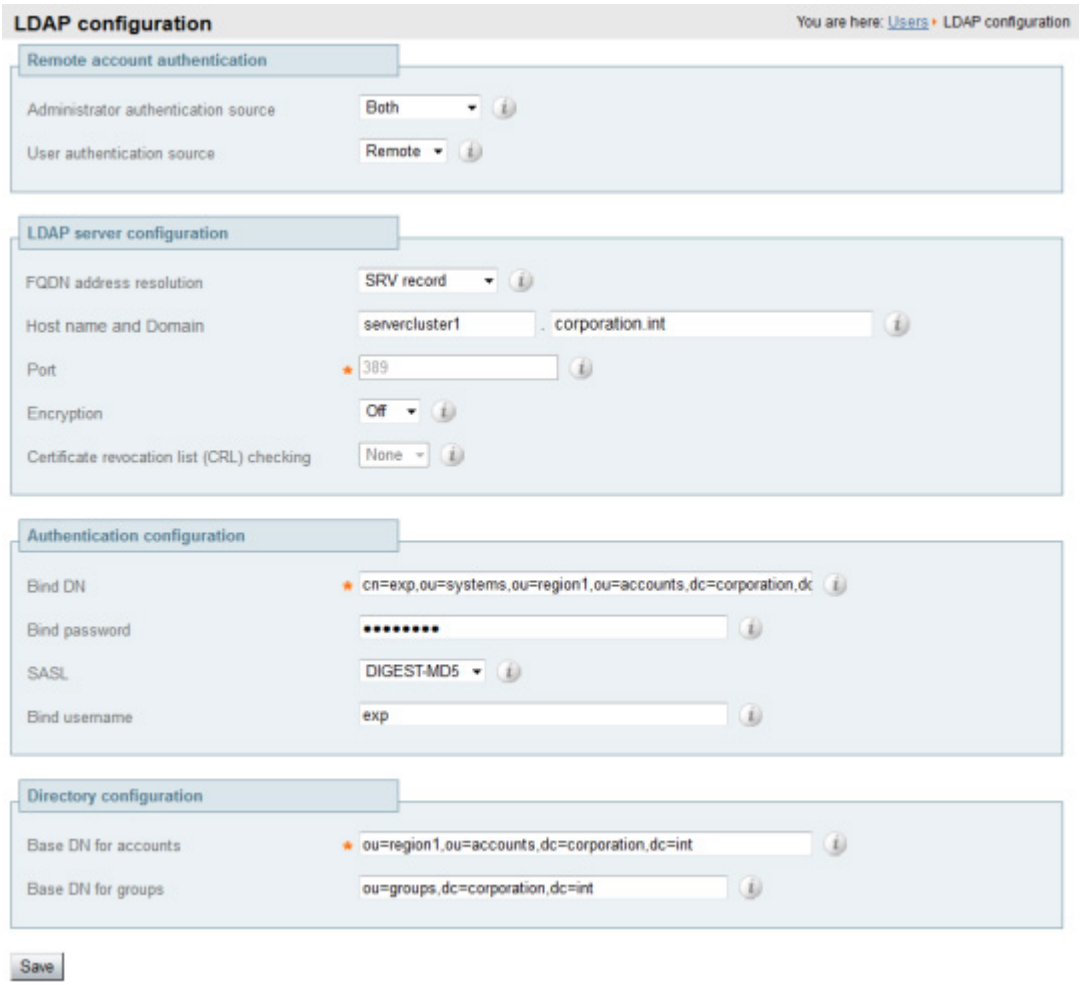
フィールド	説明	使用方法のヒント
管理者認証ソース（Administrator authentication source）	[両方（Both）] を選択します。	[両方（Both）] を選択すると、ローカルで定義したアカウントを引き続き使用できます。これは、LDAP サーバとの接続や認証の問題をトラブルシューティングするときに役立ちます。 [リモートのみ（Remote only）] の認証が使用されている場合は、デフォルトの **admin** アカウントを含め、ローカルで設定した管理者アカウントを使用してログインできません。注：Expressway が Cisco TMS によって管理されている場合に限り、[Remote only（リモートのみ）] は使用しないでください。
FQDN アドレス解決（FQDN address resolution）	LDAP サーバ アドレスを解決する方法を定義します。 [SRV レコード（SRV record）]：DNS SRV レコード検索。 [アドレス レコード（Address record）]：DNS A レコードまたは AAAA レコード検索。	

フィールド	説明	使用方法のヒント
	[IP アドレス(IP address)]: IP アドレスとして直接入力。	
[ホスト 名(Host Name)]と [ドメイン (Domain)] または **サーバ アドレス(Server address)**	サーバ アドレスの指定方法は、**FQDN アドレス解決**の設定によって異なります。 [SRV レコード(SRV record)]:サーバ アドレスの **ドメイン**部分だけが必要です。 [アドレス レコード(Address record)]:**ホスト名**と**ドメイン**を入力します。これらは組み合わされて、DNS アドレス レコードを検索するための完全なサーバ アドレスになります。 [IP アドレス(IP address)]:**サーバ アドレス**を IP アドレスとして直接入力します。	TLS を使用する場合、ここに入力するアドレスは、LDAP サーバから提示される証明書に含まれる CN(コモン ネーム)と一致している必要があります。
ポート(Port)	LDAP サーバで使用する IP ポート。	通常、非セキュア接続は *389*、セキュア接続は *636* を使用します。
暗号化(Encryption)	LDAP サーバへの接続がトランスポート層セキュリティ(TLS)を使用して暗号化するかどうかを決定します。 TLS:LDAP サーバへの接続に TLS 暗号化を使用します。 [オフ(Off)]:暗号化は使用されません。	TLS が有効になっている場合は、LDAP サーバ証明書に Expressway の信頼済み CA 証明書ファイル内の認証局が署名する必要があります。 [TLS 用の CA 証明書をアップロード(Upload a CA certificate file for TLS)([関連タスク(Related tasks)] セクション)をクリックし、[信頼できる CA 証明書(Trusted CA)] ページに移動します。
証明書失効リスト(CRL)の確認中(Certificate revocation list (CRL) checking)	LDAP サーバとの TLS 接続を確立するときに証明書失効リスト(CRL)を確認するかどうかを指定します。 [なし(None)]:CRL チェックは実行されません。 [ピア(Peer)]:LDAP サーバの証明書を発行した CA に関連付けられた CRL のみを確認します。 [すべて(All)]:LDAP サーバの証明書を発行した CA の信頼できる証明書チェーン内のすべての CRL を確認します。	失効リストを使用している場合は、必要な CRL データも CA 証明書ファイル内に含める必要があります。

フィールド	説明	使用方法のヒント
Bind DN	LDAP サーバにバインドするときに Expressway で使用される識別名（大文字と小文字の区別なし）。 cn=、ou=、dc= の順に DN を指定する必要があります。	名前の中に含まれる特殊文字は、LDAP 標準（*RFC 4514*）に従ってバックスラッシュでエスケープする必要があります。名前と名前の間の区切り文字はエスケープしないでください。 通常、バインド アカウントは特別な権限を持たない読み取り専用のアカウントです。
パスワードのバインド（Bind Password）	LDAP サーバにバインドするときに Expressway で使用される識別名（大文字と小文字の区別あり）。	プレーン テキストの最大長は 60 文字で、暗号化されます。
SASL	LDAP サーバにバインドするときに使用する SASL（Simple Authentication and Security Layer）のメカニズム。 [なし（None）]：メカニズムを使用しません。 [DIGEST-MD5]：DIGEST-MD5 メカニズムを使用します。	企業のポリシーに応じて、Simple Authentication and Security Layer を有効にします。
バインド ユーザ名（Bind Username）	Expressway が LDAP サーバにログインするときに使用するアカウントのユーザ名（大文字と小文字の区別あり）。 SASL が有効になっている場合にのみ必要です。	これは、sAMAccountName（セキュリティ アクセス マネージャ アカウント名）になるように設定します（AD では、これはアカウントのユーザ ログオン名です）。
アカウントのベース DN（Base DN for accounts）	データベース構造においてユーザ アカウント検索の開始点となる識別名の ou= および dc= 定義（大文字と小文字の区別なし）。 ou=、dc= の順に DN を指定する必要があります。	アカウントとグループのベース DN は、dc レベル以下にする必要があります（必要に応じてすべての dc= 値と ou= 値を含めてください）。LDAP 認証では、サブ dc アカウントを確認しません。下のレベルの ou= および cn= レベルのみを確認します。
グループのベース DN（Base DN for groups）	データベース構造においてグループ検索の開始点となる識別名の ou= および dc= 定義（大文字と小文字の区別なし）。 ou=、dc= の順に DN を指定する必要があります。	**グループのベース DN** を指定しない場合は、アカウントのベース DN がグループおよびアカウントの両方に使用されます。

3. [保存(Save)] をクリックします。

たとえば、「付録 3：Active Directory 構造の例の [p.17]」の値を使用します。



接続状況

LDAP サーバへの接続のステータスはページの下部に表示されます。

[状態（State）] = [アクティブ（Active）]

エラー メッセージは表示されません。

[状態（State）] = [失敗（Failed）]

次のエラー メッセージが表示されることがあります。

エラー メッセージ	理由/解決方法
DNS はリバース検索を実行できません（DNS unable to do reverse lookup）	SASL 認証にはリバース DNS 検索が必要です。
DNS で LDAP サーバ アドレスを解決できません（DNS unable to resolve LDAP server address）	有効な DNS サーバが設定されていることと、LDAP サーバのアドレスのスペルを確認します。
LDAP サーバへの接続に失敗しました。サーバのアドレスとポートを確認してください（Failed to connect to LDAP server. Check server address and port）	LDAP サーバの詳細が正しいことを確認します。
TLS 接続の設定に失敗しました。CA 証明書を確認してください（Failed to setup TLS connection. Check your CA certificate）	TLS には、CA 証明書、秘密キー、およびサーバ証明書が必要です。
サーバへの接続に失敗しました。コードが返されました <戻りコード>（Failure connecting to server. Returned code<return code>）	その他の一般的な問題。
無効なアカウントのベース DN です（Invalid Base DN for accounts）	**アカウントのベース DN** を確認してください。現在の値は、LDAP ディレクトリの有効な部分を記述したものではありません。
無効なサーバ名または DNS 障害（Invalid server name or DNS failure）	LDAP サーバ名の DNS 解決に失敗しました。
無効なバインド クレデンシャル（Invalid bind credentials）	[バインド DN（Bind DN）] および [バインド パスワード（Bind password）] を確認してください。このエラーは、SASL を [なし（None）] に設定すべき場合に [DIGEST-MD5] に設定した場合にも表示されることがあります。
無効なバインド DN（Invalid bind DN）	[バインド DN（Bind DN）] を確認してください。現在の値は LDAP ディレクトリ内の有効なアカウントを記述したものではありません。 **バインド DN** の長さが 74 文字以上ある場合に、この失敗した状態が誤って報告されることがあります。実際に失敗したかどうかを確認するには、有効なグループ名を使

エラー メッセージ	理由/解決方法
	用して Expressway 上で管理者グループを設定します。Expressway から「保存されました（saved）」と報告された場合は問題ありません（Expressway は指定されたグループが見つかるかどうかを確認します）。グループが見つからないと報告された場合は、**バインド DN** が誤っているか、グループが誤っているか、あるいはその他の設定項目が誤っている可能性があります。
インストールされた CA 証明書がありません（There is no CA certificate installed）	TLS には、CA 証明書、秘密キー、およびサーバ証明書が必要です。
設定を取得できません（Unable to get configuration）	LDAP サーバ情報がないか、誤っています。

Expressway でのグループの定義

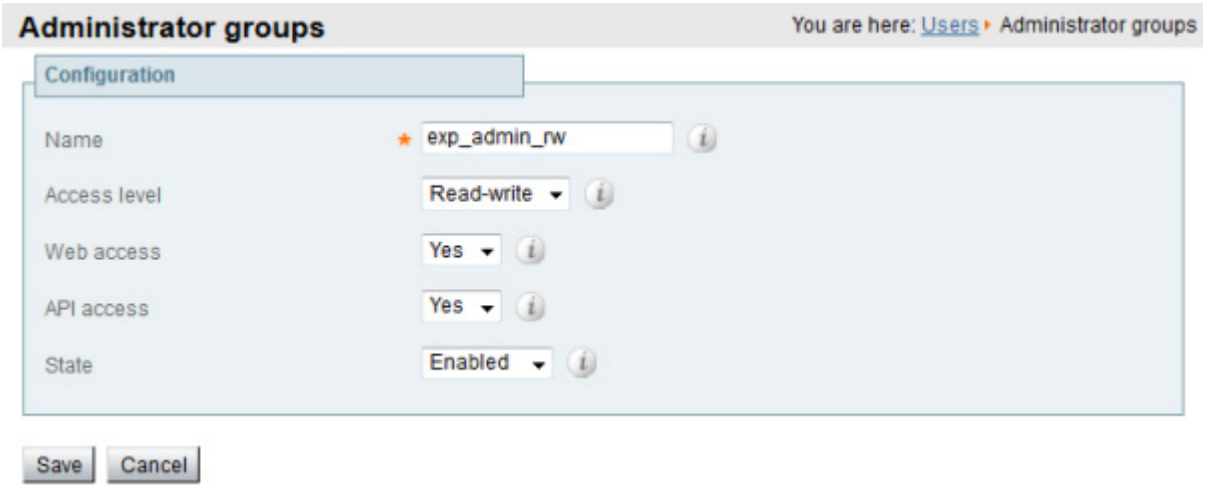
LDAP アクセス可能なデータベースでは、ユーザに特定の権限を付与するためにユーザにグループを割り当てます。Expressway でも同じグループを定義し、Expressway アクセスに必要な許可レベルを各グループに設定する必要があります。

1. [ユーザ（Users）] > [管理者グループ（Administrator groups）] に移動します。
2. [新規（New）] をクリックします。
3. フィールドを次のように設定します。

名前（Name）	必要とするアカウントのタイプに対して使用するグループ名を入力します。次に例を示します。 exp_admin_rw – for writeable access exp_admin_ro – for read-only access exp_auditor – for auditor access 注：ここに入力するグループ名は、AD またはその他の認証サーバに入力されているグループ名と完全に一致している必要があります（大文字と小文字の区別があります）。
アクセス レベル（Access level）	次のように適切なエントリを選択します。 [読み取り - 書き込み（Read-write）]：書き込みアクセスが必要な場合。 [読み取り専用（Read-only）]：読み取り専用アクセスが必要な場合。 [オーディタ（Auditor）]：[概要（Overview）] ページにアクセスし、[ログ（Log）] ページのみを許可する場合。
Web アクセス（Web Access）	[はい（Yes）] を選択します。

API アクセス（API access）	Cisco TMS などのシステムによる XML および REST API へのアクセスを制御します。このグループのメンバーがシステムの API にアクセスする必要がある場合は、[はい（Yes）] を選択します。
状態（State）	[有効（Enabled）] を選択します。

4. [保存（Save）] をクリックします。



管理者ユーザが複数のグループで見つかった場合、それらの全グループの中で最も高いレベルの許可が各アクセス設定に割り当てられるように、アクセス レベルの優先順位付けが行われます。

グループ名が見つからない場合、[管理者グループ（Administrator groups）] ページの上部に警告が表示されます。

設定時および運用時に Expressway へのログインに使用する必要があるユーザ名は、sAMAccountName、つまり Security Access Manager のアカウント名（AD におけるアカウントのユーザ ログオン名）です。

付録 1: トラブルシューティング

LDAP データベースの表示と検索

Windows

グラフィカルな「Softerra LDAP Administrator」パッケージなどの LDAP データベース ビューアを使用すると、LDAP データベースの内容を確認できます。

Expressway 用に割り当てられたログイン クレデンシャルを使用して、LDAP ビューアでユーザおよびグループを検索できます。

ユーザまたはグループを選択し、その DN(識別名)を照会して、ユーザおよびグループのパスが正しいことを確認できます。ユーザの DN は、アカウントのベース DN のスーパーセットになっている必要があり、グループの DN は、グループのベース DN のスーパーセットになっている必要があります。

UNIX または Linux

ldapsearch(openldap スイートの一部のプログラム)を使用して ldap データベースを問い合わせることができます。次に例を示します。

```
ldapsearch -v -x -W -D
"cn=exp,ou=systems,ou=region1,ou=useraccounts,dc=corporation,dc=int" -b
cn=p.brown,ou=it,ou=region1,ou=useraccounts,dc=corporation,dc=int
-h server.corporation.int
```

これは、「exp」として LDAP サーバ「server.corporation.int」にバインドされ、「p.brown」アカウントに対して格納されているディレクトリ情報を返します(グループ メンバーシップなどの情報が表示されます)。

ldapsearch の詳細については、ldapsearch タイプをサポートするシステム上で次を実行してください。

```
man ldapsearch
```

リモート認証に切り替え後ログインできない

リモート認証を選択した場合でも、引き続き admin ログインには Expressway 上に設定されているパスワードを使用してアクセス可能です。

Expressway 上の LDAP およびグループの設定が正しいことを確認してください。特に、タイプミスやスペースの使用に注意してください。グループ名にはスペースを入れることができます。

AD の「Domain Users」グループにログインできない

「Domain Users」グループなどの Active Directory のデフォルト グループは、LDAP からは空のグループとして表示されるため、アクセス権限を定義するグループとして使用しないでください。これらを選択した場合、Expressway はユーザなしのグループとして扱います。

AD で参照すると「Domain Users」グループにメンバー（自動的に追加されたメンバー）がいるように表示されますが、そのグループに対して LDAP 検索を実行しても、メンバー リストが得られません。Expressway は、LDAP のメンバー リストを使用して、ユーザがグループのメンバーかどうか、つまりそのグループのアクセス権限がユーザにあるかどうかを判別します。

予期されるグループのユーザに対してグループからアクセス権限が与えられない場合は、LDAP ブラウザを使用して、メンバー リストが存在し、そのメンバー リストに、予期されるユーザが含まれていることを確認してください。

付録 2：追加情報

TLS の証明書

TLS を使用して Expressway を LDAP サーバに接続する場合は、LDAP サーバのサーバ証明書の正当性を証明するルート CA 証明書をロードする必要があります。

大規模な組織では、IT 部門が、関連する証明書情報を提供することができます。提供された証明書の処理方法、および OCS サーバを使用してルート CA 証明書を作成する方法の詳細については『*Certificate Creation and Use with Expressway Deployment Guide*（Expressway を使用した証明書の作成と使用展開ガイド）』を参照してください。

他の目的に必要なルート CA 証明書がすでにロードされている場合は、この新しいルート CA 証明書を、他のルート CA 証明書（信頼できる CA 証明書）、および Expressway にアップロードされた 2 つの証明書を含んだ 1 つのファイルと連結する必要があります。

Expressway の [ログイン アカウント LDAP 設定（Login account LDAP configuration）] ページで入力したサーバ アドレスは、LDAP サーバから提示される証明書に含まれた CN（コモン ネーム）と一致している必要があります。

Expressway クラスタでの使用

すべての LDAP 設定はクラスタ ピア間で複製されますが、DNS サーバは各 Expressway ピア上で独立して設定可能です。各ピアが参照する DNS サーバが、LDAP サーバの検索と、（SASL が有効な場合は）LDAP サーバの IP アドレスのリバース検索を実行できることを確認してください。

IT 要求（認証サーバへのアクセス用）

宛先：IT 部門

ログイン ユーザの認証および許可のため LDAP サーバにアクセスする Expressway を設定できるよう、次の詳細情報をお知らせください。

アクセス許可のため、Expressway は次のグループのユーザを検索します。

- _____：管理者ログイン用の読み取り/書き込みアクセスを許可
- _____：管理者ログイン用の読み取り専用アクセスを許可

LDAP サーバの完全修飾ドメインまたは IP アドレス	
FQDN の場合、A / AAAA レコードと SRV レコードのどちらですか。	A または AAAA/SRV
ポート： LDAP サーバの IP ポート（通常は 389 または 636）	
暗号化：LDAP サーバへのアクセスに TLS 暗号化を使用しますか。 証明書の場所はどこか	YES/NO（はい/いいえ） 証明書ファイルへのパス：
証明書失効リスト	確認なし/ 単一 CA の確認/ 信頼チェーン内のすべての CA の確認
Expressway のバインド DN： Expressway アカウント オブジェクト（cn=、ou=、dc= フィールドなど）の場所	
Expressway ログイン アカウントの Expressway バインド パスワード	
SASL： MD5 ダイジェスト認証で SASL が有効か。	YES/NO（はい/いいえ）
Expressway バインド ユーザ名： Expressway ログイン アカウントのユーザ名、sAMAccountName（Security Access Manager のアカウント名）（AD におけるアカウントのユーザ ログオン名）	
アカウントのベース DN： ユーザ アカウントの開始検索場所（すべての ou=、dc= フィールドなどを含む）	
グループのベース DN： グループの開始検索場所（すべての ou=、dc= フィールドなどを含む）	

IT 要求（グループ設定の場合）

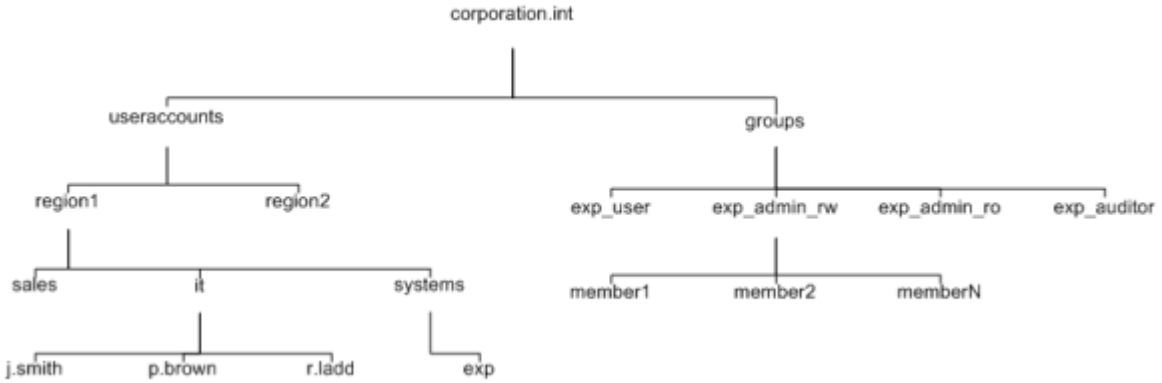
宛先：IT 部門

ユーザ認証サーバに_____というグループを作成し、そのグループに次のユーザを割り当ててください。

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.
14.
15.
16.
17.
18.
19.
20.
21.
22.
23.
24.
25.

付録 3：Active Directory 構造の例

下の図は、corporation.int の Active Directory ツリー構造の例を示しています。



LDAP サーバへの接続に必要な Expressway 設定の一部に、識別名（DN）のセットの指定があります。DN は、次の要素で構成されます。

- **cn** コモン ネーム（通常はツリーの葉。下記の注を参照）
- **ou** 組織単位（枝）
- **dc** ドメイン コンテンツ（ツリーの最上位）

これらの要素は、カンマ区切り値として 1 行にリストします。カンマの直前および直後にスペースを入れてはいけませんが、共通名、組織単位名、およびドメイン コンテンツ名の中にスペースを使用することはできます。

この Active Directory 構造の例を使用した場合は、次のような Expressway **バインド DN** を定義できます。

```
cn=vcs,ou=systems,ou=region1,ou=useraccounts,dc=corporation,dc=int
```

region 1 のスタッフをサポートするには、次のような**アカウントのベース DN** を定義します。

```
ou=region1,ou=useraccounts,dc=corporation,dc=int
```

世界中のスタッフをサポートするには、次のような**アカウントのベース DN** を定義します。

```
ou=useraccounts,dc=corporation,dc=int
```

グループのベース DN は次のようになります。

```
ou=groups,dc=corporation,dc=int
```

（注）

- 最初にデータベースをどのように設定したかによって、cn= を単に「葉」として予約できない場合があります。たとえば、デフォルトでは、Microsoft AD データベースには「コンテナ」（cn=）内にユーザが存在し、組織ユニット（ou=）には存在しません。
  Expressway で、Expressway の [バインド DN（Bind DN）] フィールドと [ベース DN（Base DN）] フィールドを設定するときは、同じ dc タグ、ou タグ、cn タグを使用し、それらをデータベースと同じ順序で使用する必要があります。

- Expressway **バインド DN** は、アカウントを指定するオブジェクトまでの（そのオブジェクトも含む）ディレクトリ構造です（AD 用語では Active Directory の「ユーザ」オブジェクト）。Expressway へのログインに使用するアカウント名および SASL に使用するアカウント名は、sAMAccountName、つまり Security Access Manager のアカウント名（AD におけるアカウントのユーザ ログオン名）です。

- **アカウントのベース DN** と**グループのベース DN** は、dc レベル以下にする必要があります（すべての dc= 値と、場合によっては ou= 値も含めてください）。ベース DN を dc=int にすることはサポートされません。

付録 4：Active Directory の設定グループ

Active Directory でグループにユーザを割り当てるには、グループ オブジェクトを作成してから、ユーザをそのグループのメンバーにする必要があります。

グループ オブジェクトの作成

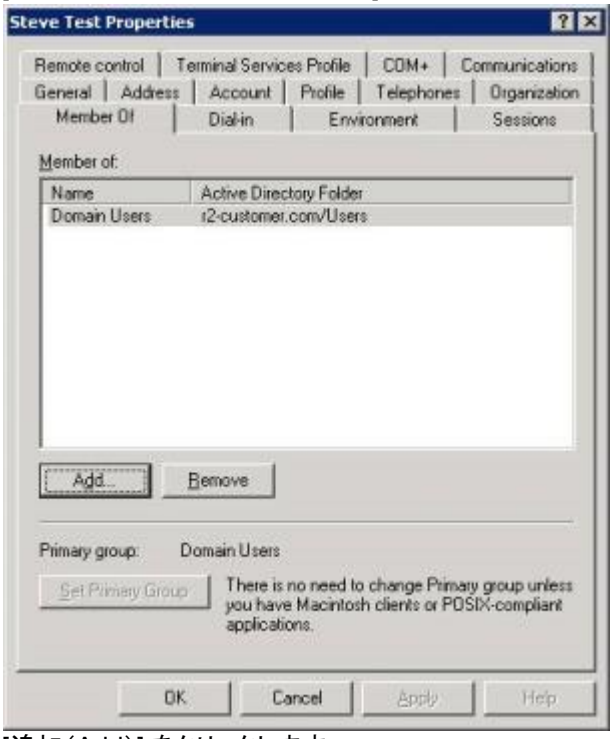
1. [スタート（Start）] メニューから、[Active Directory ユーザとコンピュータ（Active Directory Users and Computers）] を選択します。
2. 左側のフォルダの表示では、新しいグループを作成する関連フォルダを選択します。
3. 右側のパネルでエントリが選択されていないことを確認し、[操作（Action）] > [新規作成（New）] > [グループ（Group）] に移動します。
4. フィールドを次のように設定します。

グループ名（Group name）	Expressway への読み書きアカウント アクセス用の名前を入力します（例：exp_admin_rw）
グループのスコープ（Group scope）	必要に応じて [グローバル（Global）] などとします。
グループの種類（Group Type）	必要に応じて [配布（Distribution）] などとします。

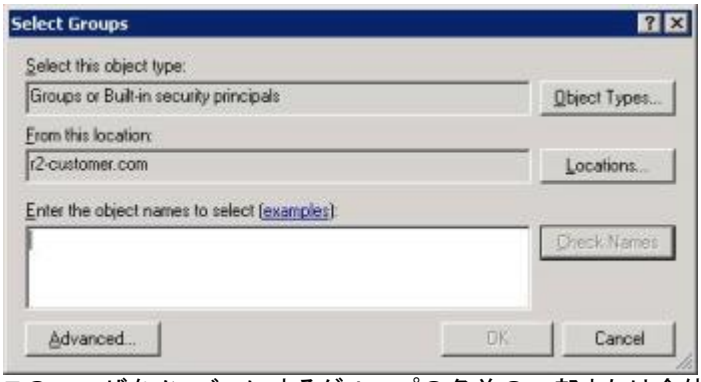
5. 読み取り専用アクセス用に第 2 のグループを作成します（例：**Group name** = exp_admin_ro）
6. 監査アクセス用に第 3 のグループを作成します（例：**Group name** = exp_auditor）

ユーザをグループのメンバーにします

1. [スタート(Start)] メニューから、[Active Directory ユーザとコンピュータ(Active Directory Users and Computers)] を選択します。
2. 左側のフォルダ表示で、ユーザが格納されたフォルダを選択します。
3. 必要なユーザをダブルクリックします。
4. [所属するグループ(Member Of)] タブを選択します。



5. [追加(Add)] をクリックします。



6. このユーザをメンバーにするグループの名前の一部または全体を入力します。
7. [名前の確認（Check Names）] をクリックします。
8. 表示された 1 つ以上のグループ名から、目的のエントリを選択します。
9. [OK] をクリックしてグループを確定します。
10. [OK] をクリックしてユーザのプロパティ ダイアログを閉じます。

一度に複数のユーザを 1 つのグループに割り当てるには、各ユーザを選択（Ctrl を押したまま各ユーザをクリック）して右クリックし、[グループに追加（Add to a group…）] を選択してから上記のステップ 6 以降を実行します。

マニュアルの変更履歴

次の表に、このマニュアルの変更履歴の要約を示します。

リビジョン	日付	説明
2	2014 年 6 月	X8.2 用に再発行。
1	2013 年 12 月	初版。