LDAP を使用した Cisco VCS アカウントの認証

導入ガイド

初版：2009 年 12 月

最終更新：2015 年 11 月

Cisco VCS X8.7

はじめに

本書では、一元管理された LDAP アクセス可能なサーバ上で Cisco TelePresence Video Communication Server（VCS）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 による認証および許可は、VCS の管理者アカウントおよびユーザ（FindMe）アカウントへの Web ログインで使用できます。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、VCS は LDAP アクセス可能なサーバに接続し、ユーザを認証するとともに、認証したユーザが VCS 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。

現在のところ、VCS 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。

次の点に注意してください。

- シリアル、SSH などのその他のログインでは、引き続き VCS に設定された管理者アカウントが使用されます。
- ユーザ アカウントの Web ログインを使用できるのは、Cisco TMS なしで FindMe を使用している場合に限られます。

プロセスの概要

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 VCS を設定します

管理者アクセスまたは FindMe の設定のために VCS にログインするユーザは、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 への要求（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セットアップし、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）
- VCS ユーザ（例：exp_user グループ）

[%=call_control.VCSShort%] 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 VCS にセットアップしてください（[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。

VCS 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. VCS 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（質問表を使用して IT 部門から適切な情報を入手しておきます）。

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：VCS が Cisco TMS によって管理されている場合、[リモートのみ（Remote only）] は使用しないでください。

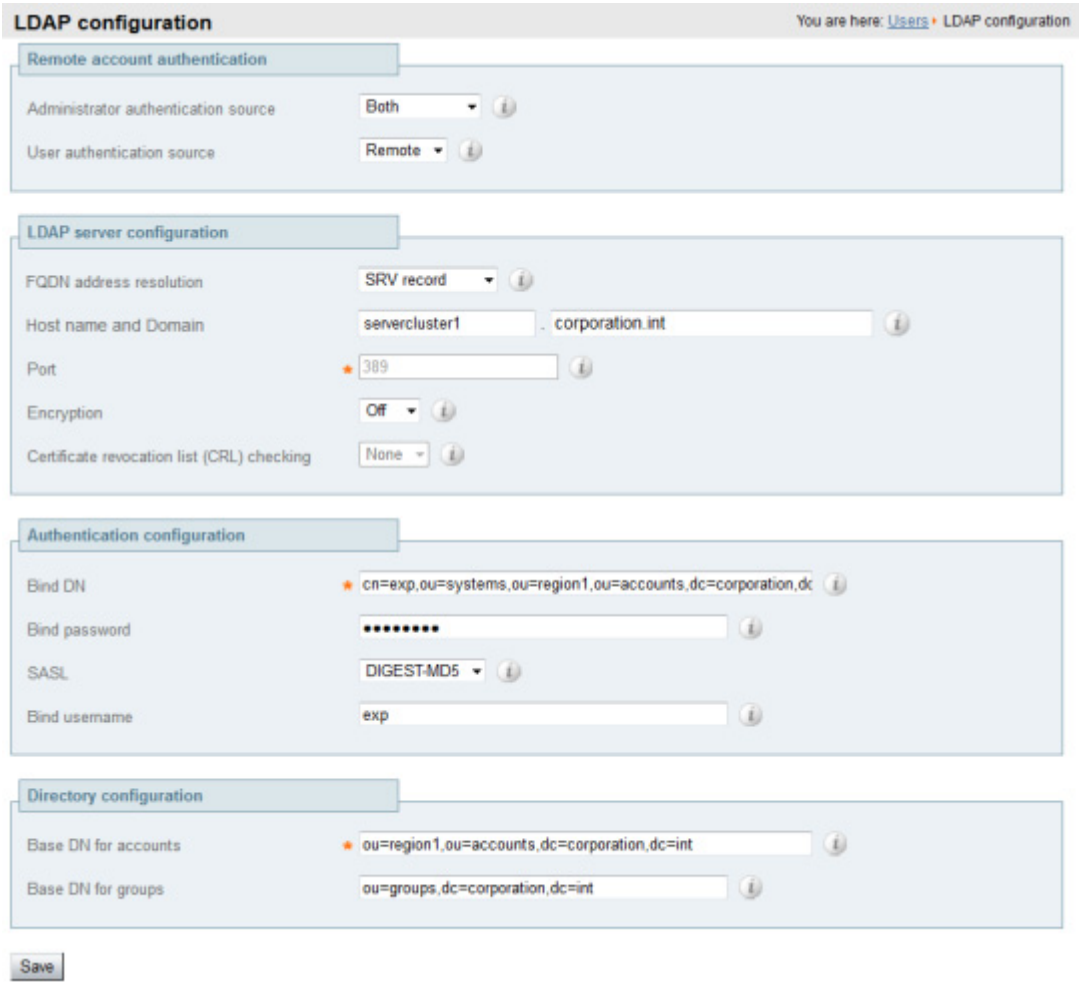
フィールド	説明	使用方法のヒント
FindMe 認証ソース（FindMe authentication source）	[リモート（Remote）] を選択します。	このオプションを使用できるのは、Cisco TMS なしで FindMe を使用している場合に限られます。
FQDN アドレス解決（FQDN address resolution）	LDAP サーバ アドレスを解決する方法を定義します。 [SRV レコード（SRV record）]：DNS SRV レコード検索。 [アドレス レコード（Address record）]：DNS A レコードまたは AAAA レコード検索。 [IP アドレス（IP address）]：IP アドレスとして直接入力。 **注：**SRV レコードを使用する場合は、レコードが LDAP 用の標準ポートを使用していることを確認してください。`_ldap._tcp.`*<domain>* は 389 を、`_ldaps._tcp.`*<domain>* は 636 を使用する必要があります。VCS は LDAP 用に他のポート番号をサポートしていません。	SRV ルックアップは、**暗号化**が有効かどうかによって、_ldap._tcp または _ldaps._tcp レコードのいずれかに対して実行されます。複数のサーバが返された場合、各 SRV レコードのプライオリティとウェイトによって、サーバが使用される順序が決まります。
ホスト名（Host name）およびドメイン（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。	非セキュア接続は *389*、セキュア接続は *636* を使用します。

フィールド	説明	使用方法のヒント
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、VCS の信頼済み CA 証明書ファイル内の認証局が LDAP サーバ証明書に署名する必要があります。 [TLS 用の CA 証明書ファイルをアップロード（Upload a CA certificate file for TLS）]（[関連タスク（Related tasks）] セクション内）をクリックし、[信頼できる CA 証明書（Trusted CA certificate）] 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。
バインド DN（Bind DN）	LDAP サーバにバインドするときに VCS 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。
バインド パスワード（Bind Password）	LDAP サーバにバインドするときに VCS で使用されるパスワード（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）	VCS 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）。

フィールド	説明	使用方法のヒント
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。	これが、管理者ログイン要求とユーザ ログイン要求の両方の認証で使用されます。 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。	認証済みのユーザに、管理者としてのログイン、またはユーザ アカウントへのログインを許可するために使用されます。 **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」（p.17）の値を使用すると以下のようになります。



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	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。

エラー メッセージ	理由/解決方法
address）	
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（Base DN for accounts）] 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（Bind 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用して VCS 上で管理者グループをセットアップします。VCS 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（VCS 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（Bind 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。

VCS へのグループの定義

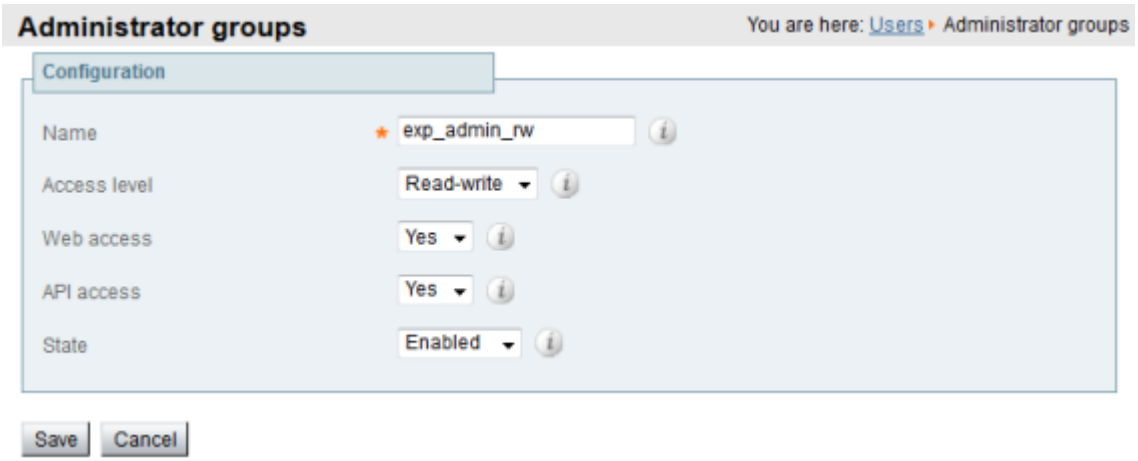
LDAP アクセス可能なデータベースでは、ユーザに特定の権限を付与するためにユーザにグループを割り当てます。VCS でも同じグループを定義し、VCS アクセスに必要な許可レベルを各グループに設定する必要があります。

管理者用のログイン用グループ

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：書き込みアクセス用 exp_admin_ro：読み取り専用アクセス用 exp_auditor：オーディタ アクセス用 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）] ページと [ログ（Log）] ページへのアクセス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 VCS 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。

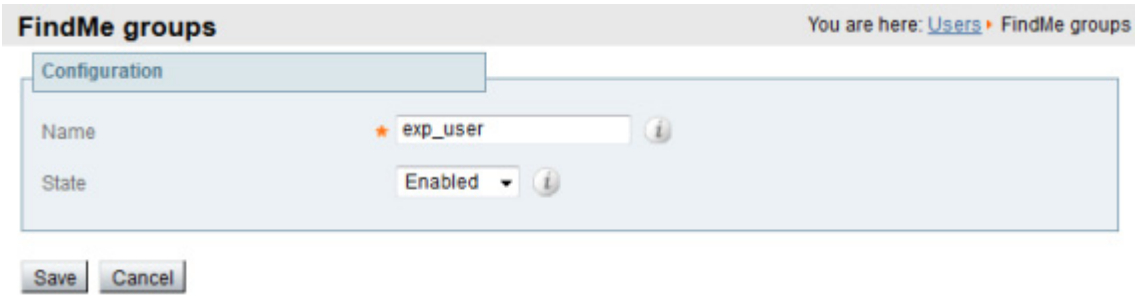
ユーザ ログイン用グループ

ユーザ アカウントの Web ログインを使用できるのは、Cisco TMS なしで FindMe を使用している場合に限られます。

1. [ユーザ（Users）] > [FindMe グループ（FindMe 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）	読み取り/書き込みアカウントに使用するグループ名を入力します（例：exp_user）。 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）。
状態（State）	[有効（Enabled）] を選択します。

4. [保存（Save）] をクリックします。



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

ユーザ アカウントへログインするときに使用する必要があるログイン 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。

VCS 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 VCS 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。

VCS 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、VCS はこれらを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。VCS 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、つまりは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 VCS 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 VCS Deployment Guide*』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 VCS 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。

VCS の [LDAP 設定（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る CN（コモン ネーム）と一致している必要があります。

VCS 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 VCS 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 への要求（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 サーバにアクセスできるように VCS を設定するので、次の詳細情報をお知らせください。

アクセス許可のため、VCS 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
- _____：ユーザ ログイン用の読み取り/書き込みアクセスを許可

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	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
VCS のバインド DN：VCS アカウント オブジェクト（cn=、ou=、dc= フィールドなどすべて）の場所	
VCS ログイン アカウント用の VCS バインド パスワード	
SASL：MD5 ダイジェスト認証で SASL を有効にするかどうか。	はい / いいえ
VCS バインド ユーザ名：VCS 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 への要求（グループ設定）

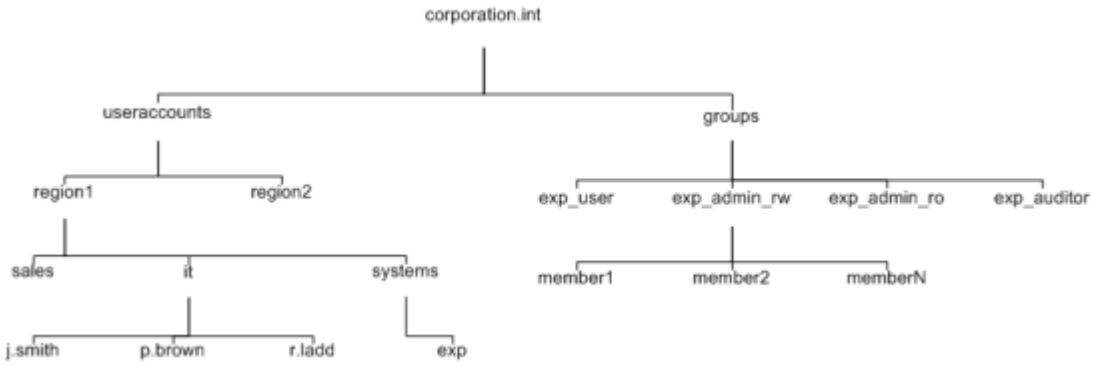
宛先：IT 部門

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 VCS 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 VCS **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。
  VCS で、VCS 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ことが重要です。

- VCS **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）。VCS 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 でのグループの設定

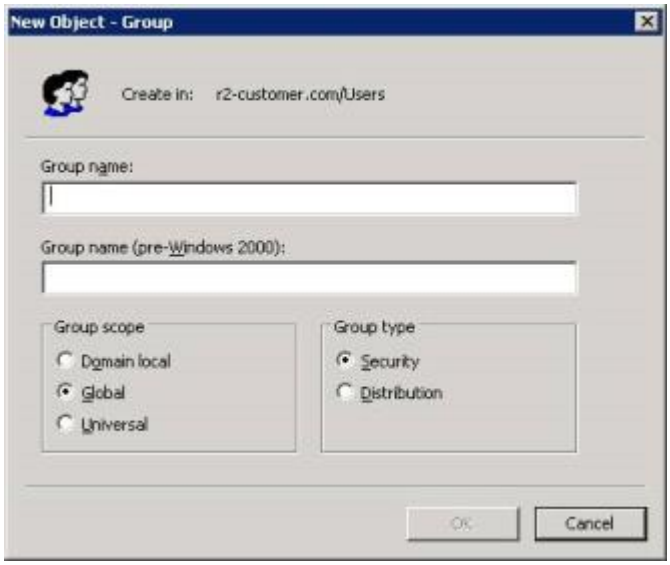
Active Directory でグループにユーザを割り当てるには、グループ オブジェクトを作成してから、ユーザをそのグループのメンバーにする必要があります。

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）	VCS 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。

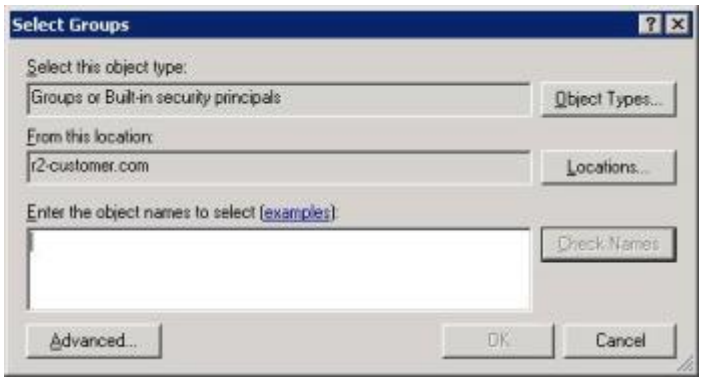
5. 読み取り専用アクセス用に第 2 のグループを作成します（例：**Group name** = exp_admin_ro）。
6. 監査アクセス用に第 3 のグループを作成します（例：**Group name** = exp_auditor）。
7. ユーザ アクセス用に第 4 のグループを作成します（例：**Group name** = exp_user）。



ユーザをグループのメンバーにする

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。

日付	説明
2015 年 11 月	新しいテンプレートを適用。X8.7 用に再発行。
2014 年 12 月	X8.5 用に再発行。
2014 年 6 月	X8.2 用に再発行。
2013 年 12 月	VCS X8.1 に関する内容を更新。
2012 年 8 月	Cisco VCS X7.2 での管理者グループおよびユーザ グループの設定方法の変更を反映。
2011 年 2 月	Cisco VCS X6 用の更新
2010 年 10 月	新しいドキュメント スタイルを適用。
2010 年 3 月	Cisco VCS X5.1 に関する内容を更新。
2009 年 12 月	初版。

シスコの法的情報

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

ハード コピーおよびソフト コピーの複製は公式版とみなされません。最新版はオンライン版を参照してください。

シスコは世界各国 200 箇所にオフィスを開設しています。各オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/go/offices [英語]）をご覧ください。

シスコの商標または登録商標

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. シスコの商標の一覧は www.cisco.com/web/JP/trademark_statement.html に掲載されています。Third-party trademarks mentioned are the property of their respective owners.The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1110R)