LDAP を使用した Cisco VCS アカウントの認証

導入ガイド

VCS X7.2

D14526.05

2012 年 8 月

目次

はじめに

デバイスやシステムにログインするためにユーザが認証クレデンシャル（ユーザ名とパスワード）を入力しなければならない機会はますます増えています。各デバイスのユーザ名とパスワードを個別に覚えるよりも、単一のログイン クレデンシャル セットを LDAP でアクセス可能なサーバで中央管理する方が、ユーザにとって簡単で好ましい方法です。

デバイスにアクセスしようとすると、そのデバイスは、デバイス自身の内部データベースでユーザ名およびパスワードを検索するのではなく、LDAP アクセス可能なサーバに接続してユーザ認証を行い、さらに、要求された機能の実行をデバイスから許可されたグループに、その認証されたユーザが属しているかどうかを検査します。

また、中央のログイン 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。

このマニュアルでは、LDAP を使用してログイン アカウントの認証を行うように Cisco TelePresence Video Communication Server（Cisco VCS）を設定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、Cisco 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 ログインで使用されます。

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、Telnet、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、デバイスのプロビジョニングが TMS エージェント レガシー モードであるか、TMS なしで FindMe を使用している場合に限られます。

使用方法

オペレータ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

管理者アクセス権で VCS にログインするユーザ、あるいは FindMe を設定するためにログインするユーザ（VCS の設定によって異なります）は、LDAP サーバの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。

VCS の設定

VCS への LDAP サーバの詳細の設定

1. [ログイン アカウント LDAP 設定（Login account LDAP configuration）] ページ（[メンテナンス（Maintenance）] > [ログイン アカウント（Login accounts）] > [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（*付録 1：IT 依頼書（認証サーバのアクセス用）*の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）。

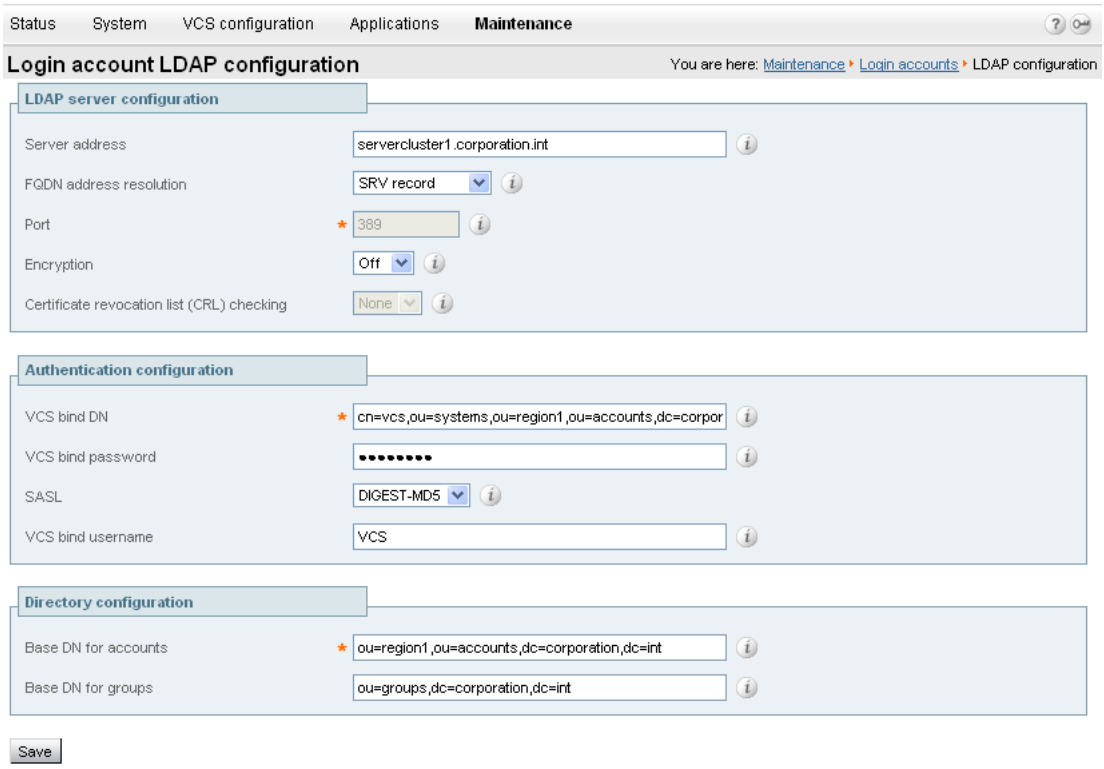
サーバ アドレス（Server address）	LDAP サーバの完全修飾ドメイン名（大文字と小文字の区別なし）または LDAP サーバの IP アドレス。 TLS を使用する場合、ここに入力するサーバ アドレスは、LDAP サーバから提示される証明書に含まれる CN（一般名）と一致している必要があります。
FQDN アドレス解決（FQDN address resolution）	[アドレス レコード（Address Record）]：上記の [サーバ アドレス（Server address）] が IP アドレスではない場合に、その値を IPv4 DNS A レコードまたは IPv6 DNS AAAA レコードとして検索します。 [SRV レコード（SRV Record）]：上記の [サーバ アドレス（Server address）] が IP アドレスではない場合に、その値を DNS SRV レコードとして検索します。
ポート（Port）	LDAP サーバで使用する IP ポート。一般的に、暗号化がオフの場合は 389、暗号化が TLS に設定されている場合は 636 です。
暗号化（Encryption）	LDAP サーバで TLS 暗号化がサポートされる場合は [TLS] に設定します。サポートされない場合は [オフ] に設定します。 注：暗号化を TLS に設定した場合は、[セキュリティ証明書（Security certificates）] ページ（[メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）]）で、有効な CA 証明書、秘密キー、およびサーバ証明書を VCS にアップロードする必要があります。
証明書失効リスト（CRL）の確認中（Certificate revocation list（CRL）checking）	暗号化が TLS の場合にのみ適用されます。 [なし（None）]：CRL を検査しません。 [ピア（Peer）]：LDAP サーバの証明書を発行した認証局に直接関連付けられている CRL のみ検査します。 [すべて（All）]：LDAP サーバの証明書の信頼チェーンに含まれている全認証局の CRL を検査します。
VCS バインド DN（VCS Bind DN）	VCS にデータベースのクエリーを許可するアカウント オブジェクトの cn=、ou=、および dc= 定義（大文字と小文字の区別なし）。*付録 3：Active Directory の構造*を参照してください。 この DN は、cn=、ou=、dc= という順序で指定することが重要です。
VCS バインド パスワード（VCS Bind password）	VCS がデータベースに照会するときに使用するアカウント オブジェクトのパスワード（大文字と小文字の区別あり）。
SASL	企業のポリシーに応じて、Simple Authentication and Security Layer を有効にします。
VCS バインド ユーザ名（VCS 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。 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）を設定します。

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）。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。 この DN は、ou= の次に dc= という順序で指定することが重要です。
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）。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。 この DN は、ou= の次に dc= という順序で指定することが重要です。

次の点に注意してください。

- 通常、VCS 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。
- 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 認証では下位の dc アカウントは検索されません。下位の ou= および cn= レベルのみが検索されます。

たとえば、付録 3：Active Directory の構造の値を使用すると次のようになります。



サーバ アドレス（Server address）	servercluster1.corporation.int
FQDN アドレス解決（FQDN address resolution）	*SRV レコード（SRV Record）*
ポート（Port）	389（これはデフォルト値であり、アドレス解決が [SRV レコード（SRV Record）] の場合は変更できません）。
暗号化（Encryption）	オフ（Off）（または [TLS]。[TLS] にする場合は、関連する証明書を必ずロードしてください）。

証明書失効リスト（CRL）の確認中（Certificate revocation list（CRL）checking）	*なし（None）*
VCS バインド DN（VCS Bind DN）	cn=vcs,ou=systems,ou=region1,ou=accounts,dc=corporation,dc=int
VCS バインド パスワード（VCS Bind password）	<password for VCS account>
SASL	[DIGEST-MD5]（または [なし（None）]）
VCS バインド ユーザ名（VCS Bind username）	VCS
アカウントのベース DN（Base DN for accounts）	ou=region1,ou=accounts,dc=corporation,dc=int
グループのベース DN（Base DN for groups）	ou=groups,dc=corporation,dc=int

[ログイン アカウント LDAP 設定（Login account LDAP configuration）] ページのステータス メッセージ

[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。
サーバに接続できませんでした。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。

エラー メッセージ	理由/解決方法
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。
サーバ名が無効か、DNS エラーです（Invalid server name or DNS failure）	LDAP サーバ名の DNS 解決に失敗しました。
VCS バインド クレデンシャルが無効です（Invalid VCS bind credentials）	[VCS バインド DN（VCS Bind DN）] および [VCS バインド パスワード（VCS 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。
VCS バインド DN が無効です（Invalid VCS bind DN）	[VCS バインド DN（VCS 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。 VCS バインド DN の長さが 74 文字以上ある場合に、この失敗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調べるには、有効なグループ名を使用して VCS 上で管理者グループまたはユーザ グループを設定してください。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、VCS 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 サーバ情報が欠落しているか誤っている可能性があります。

DNS サーバの設定

必ず 1 つ以上の DNS サーバアドレスを VCS に設定してください（[システム（System）] > [DNS]）。

注：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。

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。

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。

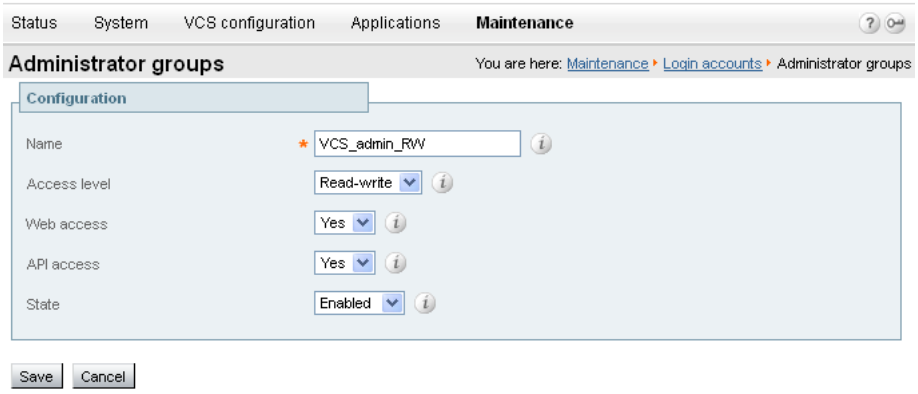
管理者ログオン用グループ

1. [管理者グループ（Administrator groups）] ページに移動します（[メンテナンス（Maintenance）] > [ログイン アカウント（Login accounts）] > [管理者グループ（Administrator groups）]）。

   この段階では、「警告：これらのグループはアクティブではありません。これらのグループを使用するには、[管理者認証ソース（Administrator authentication source）] を [リモート（Remote）] または [両方（Both）] に設定する必要があります。（Warning: These groups are not active. To use these groups you must set the Administrator authentication source to Remote or Both.）」という警告は無視してください。これは後で設定します。
2. [新規（New）] をクリックします。
3. 次のようにフィールドを設定します。

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。 VCS_admin_RW：書き込み可能アクセス用 VCS_admin_RO：読み取り専用アクセス用 VCS_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）	次の中から、適切な項目を選択します。 [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。 [監査（Auditor）]：イベント ログ、設定ログ、および概要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。



（注）

- 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 ログオン用グループ

ユーザ アカウントの Web ログインを使用できるのは、デバイスのプロビジョニングが TMS エージェント レガシー モードであるか、TMS なしで FindMe を使用している場合に限られることに注意してください。

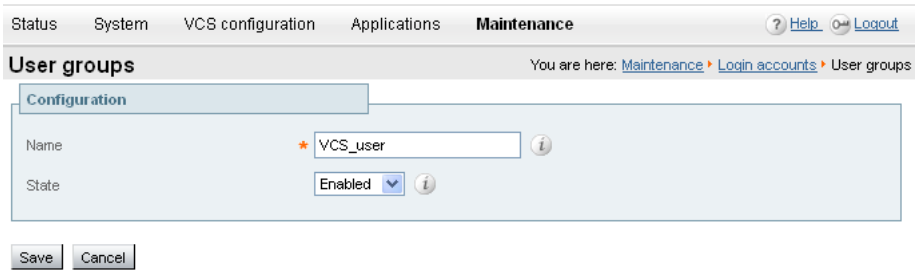
1. [ユーザ グループ（User groups）] ページに移動します（[メンテナンス（Maintenance）] > [ログイン アカウント（Login accounts）] > [ユーザ グループ（User groups）]）。

注：この段階では、「**警告**：これらのグループはアクティブではありません。これらのグループを使用するには、[ユーザ認証ソース（User authentication source）] を [リモート（Remote）] に設定する必要があります。（**Warning**: These groups are not active.To use these groups you must set the user authentication source to Remote.）」という警告は無視してください。これは後で設定します。

2. [新規（New）] をクリックします。
3. 次のようにフィールドを設定します。

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：VCS_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、[ユーザ グループ（User 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。

認証サーバでのグループの定義

通常、認証サーバにグループを定義する作業は IT 部門が実施します。*付録 2：IT 依頼書（グループ設定用*のコピーを使用して IT 部門に対して、関連するグループの設定およびそれらのグループへのユーザの割り当てを依頼してください。

一般的に、次のグループの設定が必要です。

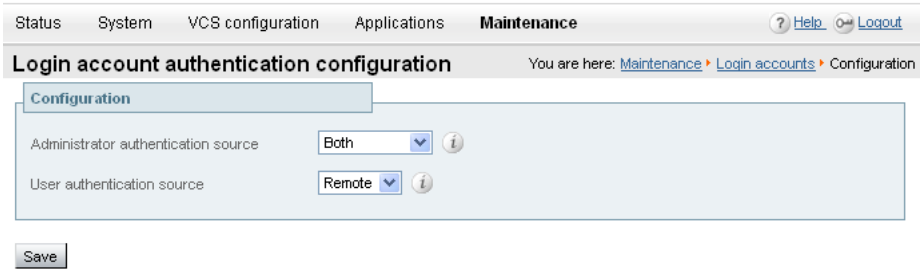
- 読み書きが可能な管理者（例：VCS_admin_RW グループ）
- 読み取り専用の管理者（例：VCS_admin_RO グループ）
- オーディタ管理者（例：VCS_auditor グループ）
- VCS ユーザ（例：VCS_User グループ）

リモート データベース使用のためのログイン認証の設定

1. [ログインアカウント認証設定（Login account authentication configuration）] ページに移動します（[メンテナンス（Maintenance）] > [ログイン アカウント（Login accounts）] > [設定（Configuration）]）。
2. 次のようにフィールドを設定します。

管理者認証ソース（Administrator authentication source）	[両方（Both）] を選択
ユーザ認証ソース（User authentication source）	[リモート（Remote）] を選択

3. [保存（Save）] をクリックします。



付録 1：IT 依頼書（認証サーバのアクセス用）

依頼先：　　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 Cisco VCS 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、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 ：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（Encryption） LDAP サーバへのアクセスに TLS 暗号化を使用しますか。 証明書の場所を教えてください。	はい　/　いいえ 証明書ファイルのパス：
証明書失効リスト	検査しない / CA を 1 つ検査 / 信頼チェーン内の全 CA を検査
VCS バインド DN - VCS アカウント オブジェクトの場所（すべての cn=、ou=、dc= フィールドを含めてください）	
VCS バインド パスワード - VCS ログイン アカウントのパスワード	
SASL - SASL で MD5 ダイジェスト認証が有効になっていますか。	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（Base DN for accounts） - ユーザ アカウントの検索開始点（すべての ou=、dc= フィールドを含めてください）	
グループのベース DN（Base DN for groups） - グループの検索開始点（すべての ou=、dc= フィールドを含めてください）	

付録 2：IT 依頼書（グループ設定用）

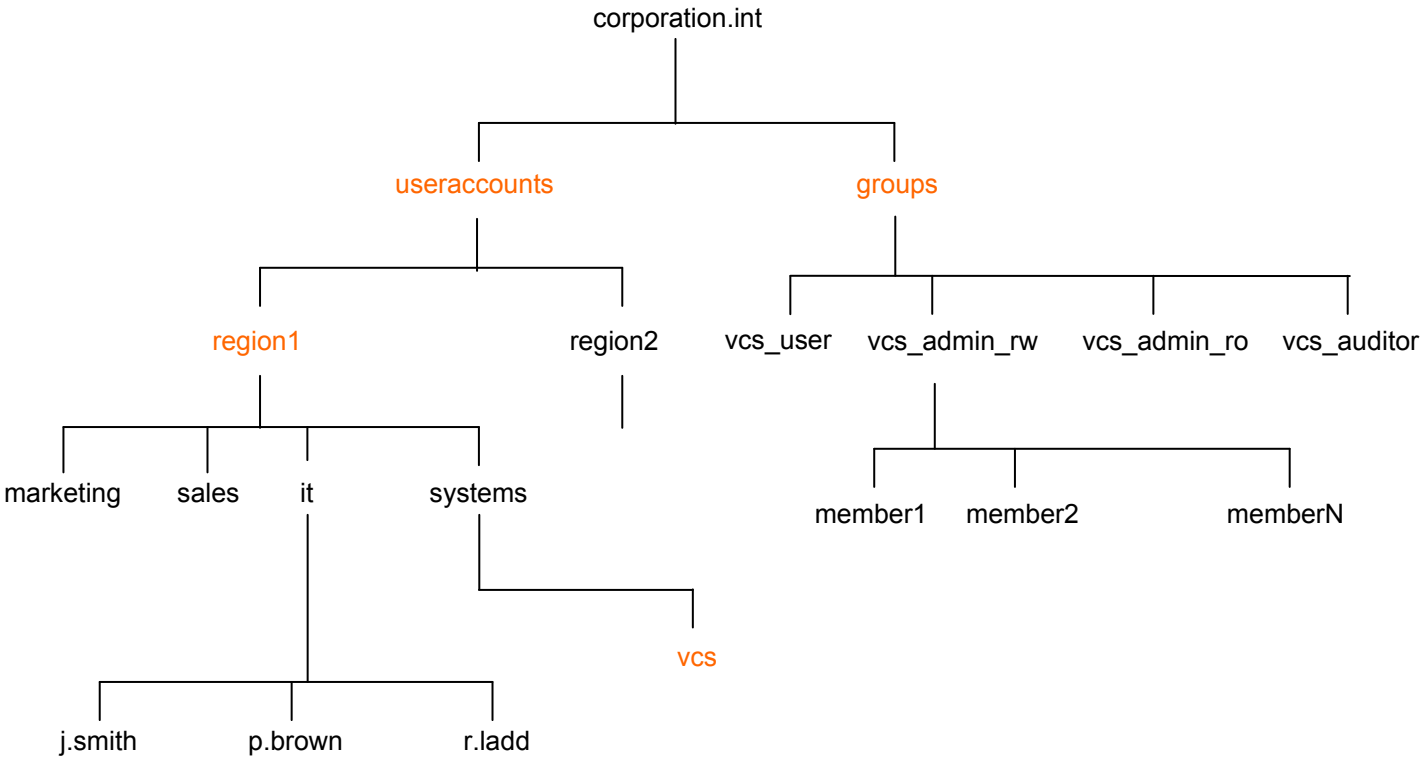
依頼先：　　IT 部門

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 の構造

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　　共通名（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、デフォルトの Microsoft AD データベースでは「Users」が組織単位（ou=）ではなく（cn=）の「コンテナ」に入っています。
  VCS で [VCS バインド DN（VCS Bind DN）] フィールドおよびベース DN の各フィールドを設定するときには、データベース内での指定と同じ順序で同じ **dc**、**ou**、**cn** タグを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. 左側のフォルダ表示で、新規グループを作成する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。

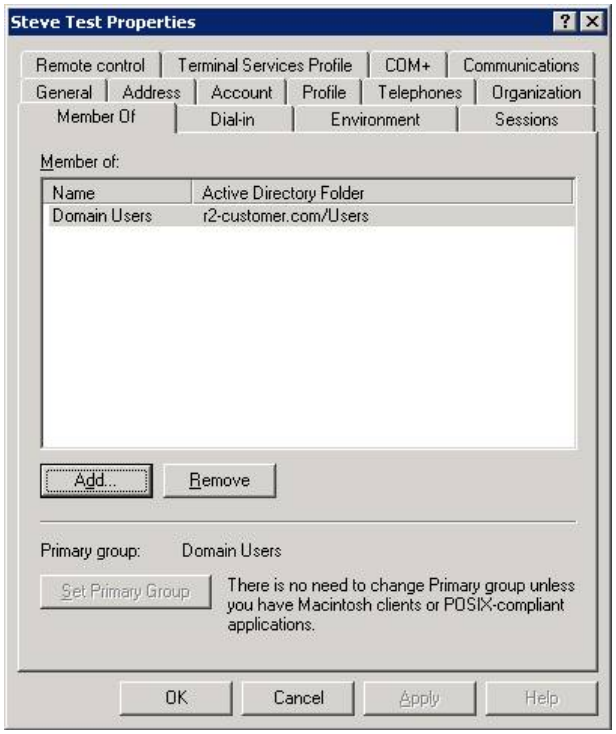
4. 次のようにフィールドを設定します。

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：VCS_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。

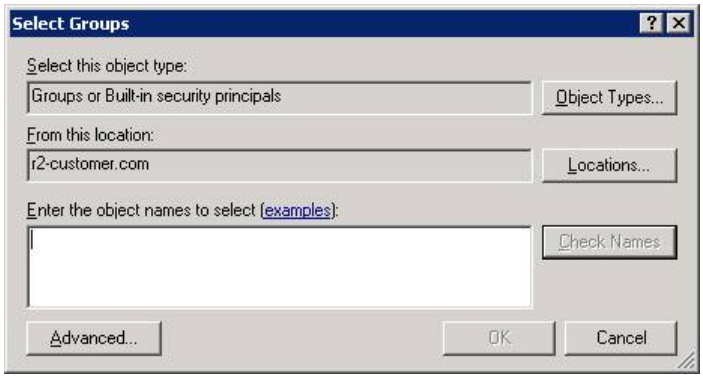
5. 読み取り専用アクセス用に第 2 のグループを作成します（例：[グループ名（Group name）] = VCS_admin_RO）
6. 監査アクセス用に第 3 のグループを作成します（例：[グループ名（Group name）] = VCS_auditor）
7. ユーザ アクセス用に第 4 のグループを作成します（例：[グループ名（Group name）] = VCS_User）

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。

付録 5：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 スイートの一部であるプログラム）を使用すると、LDAP データベースのクエリーを実行できます。次に例を示します。

```
ldapsearch -v -x -W -D
"cn=vcs,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、「vcs」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。それらを選択した場合、VCS はそれらのグループをユーザを持たない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 6：TLS 用の証明書

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 部門が該当する証明書情報を提供できます。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*』開発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 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 [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（一般名）と一致している必要があります。

付録 7：VCS クラスタの使用

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。

マニュアルの変更履歴

次の表に、これまでにこのマニュアルに対して行われた変更の概要を示します。

リビジョン	日付	説明
1	2009 年 12 月	初版。
2	2010 年 3 月	VCS X5.1 用に更新。
3	2010 年 10 月	新しい文書スタイルを適用。
4	2011 年 2 月	VCS X6 用に更新。
5	2012 年 8 月	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。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間 : 平日 10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter/