



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

【注意】 シスコ製品をご使用になる前に、安全上の注意
(www.cisco.com/jp/go/safety_warning/) をご確認ください。

本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。

あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目次

はじめに.....	3
使用方法.....	3
VCS の設定.....	4
VCS への LDAP サーバの詳細の設定.....	4
[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.....	6
DNS サーバの設定.....	7
VCS へのグループの定義.....	8
管理者ログオン用グループ.....	8
ユーザ ログオン用グループ.....	9
認証サーバでのグループの定義.....	10
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.....	10
付録 1 : IT 依頼書 (認証サーバのアクセス用)	11
付録 2 : IT 依頼書 (グループ設定用)	12
付録 3 : Active Directory の構造.....	13
付録 4 : Active Directory でのグループの設定.....	15
グループ オブジェクトの作成.....	15
ユーザをグループのメンバーにします。.....	16
付録 5 : トラブルシューティング.....	18
LDAP データベースの表示と検索.....	18
リモート認証に切り替え後ログインできない.....	18
AD の「Domain Users」グループにログインできない.....	18
付録 6 : TLS 用の証明書.....	20
付録 7 : VCS クラスタの使用.....	21
マニュアルの変更履歴.....	22

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時、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で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します。

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りです。

使用方法

オペレータは次を行う必要があります。

- LDAPで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で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で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せん。

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 (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。

The screenshot shows the 'Login account LDAP configuration' page in the VCS configuration tool. It is divided into three sections: LDAP server configuration, Authentication configuration, and Directory configuration. A 'Save' button is visible at the bottom left.

Section	Field	Value
LDAP server configuration	Server address	servercluster1.corporation.int
	FQDN address resolution	SRV record
	Port	389
	Encryption	Off
	Certificate revocation list (CRL) checking	None
Authentication configuration	VCS bind DN	cn=vcs,ou=systems,ou=region1,ou=accounts,dc=corpor
	VCS bind password	*****
	SASL	DIGEST-MD5
	VCS bind username	VCS
Directory configuration	Base DN for accounts	ou=region1,ou=accounts,dc=corporation,dc=int
	Base DN for groups	ou=groups,dc=corporation,dc=int

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

- [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。
- [新規 (New)] をクリックします。
- 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。

- [保存 (Save)] をクリックします。

The screenshot shows the 'Administrator groups' configuration page in the VCS interface. The breadcrumb trail is 'Maintenance > Login accounts > Administrator groups'. The configuration form is titled 'Configuration' and contains the following fields:

- Name: * VCS_admin_RW
- Access level: Read-write
- Web access: Yes
- API access: Yes
- State: Enabled

At the bottom of the form, there are 'Save' and 'Cancel' buttons.

(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。

The screenshot shows the 'User groups' configuration page in the VCS interface. The breadcrumb trail is 'Maintenance > Login accounts > User groups'. The 'Configuration' section has a 'Name' field with the value 'VCS_user' and a 'State' dropdown menu set to 'Enabled'. Information icons are present next to both fields. At the bottom, there are 'Save' and 'Cancel' buttons.

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。

The screenshot shows the 'Login account authentication configuration' page. The breadcrumb trail is 'Maintenance > Login accounts > Configuration'. The 'Configuration' section has two dropdown menus: 'Administrator authentication source' set to 'Both' and 'User authentication source' set to 'Remote'. Information icons are present next to both dropdowns. At the bottom, there is a 'Save' button.

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 を設定できるように、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)

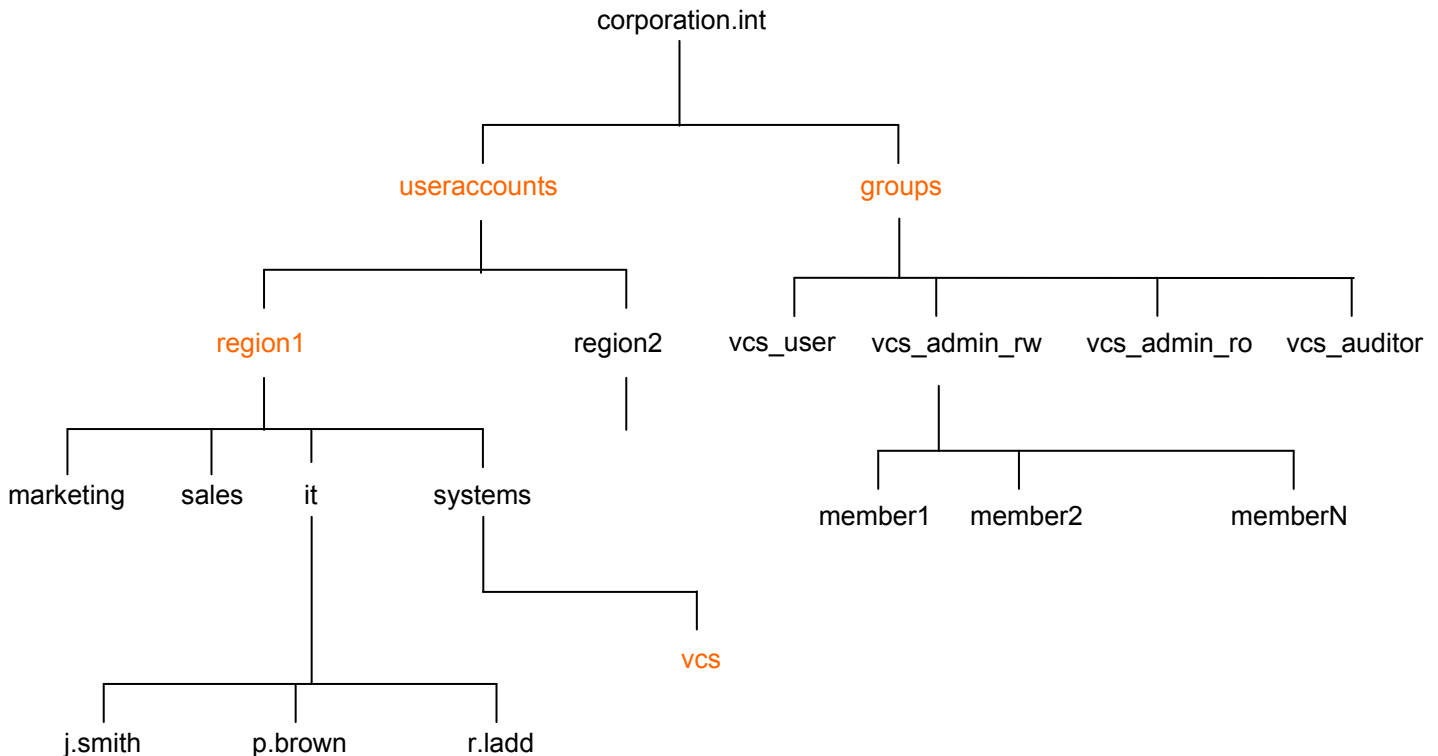
依頼先 : IT 部門

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。



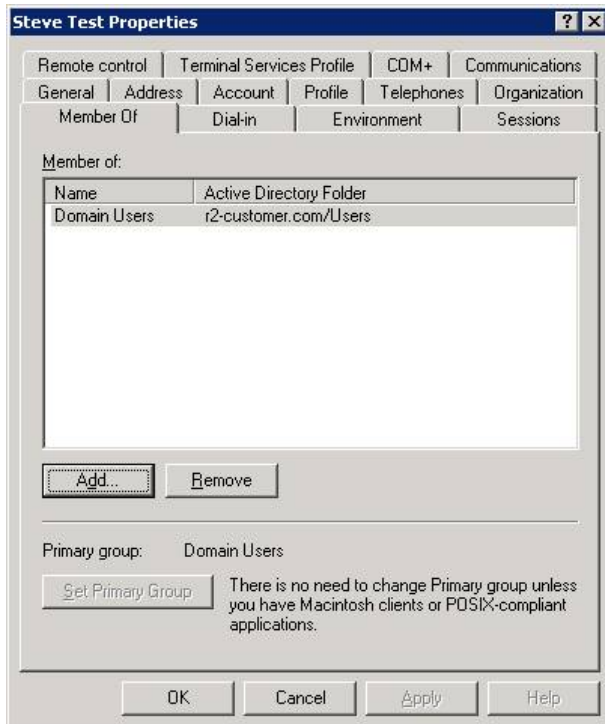
4. 次のようにフィールドを設定します。

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。

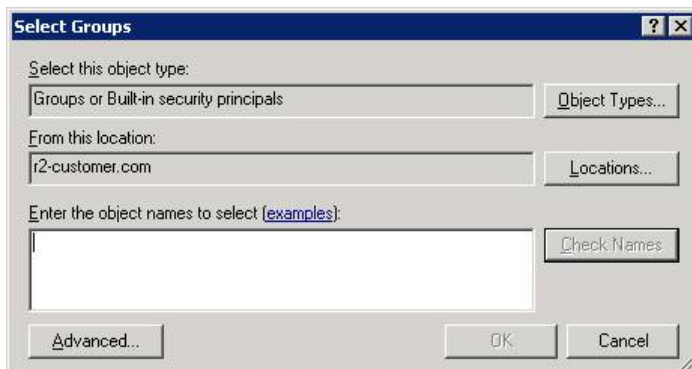
5. 読み取り専用アクセス用に第 2 のグループを作成します (例 : [グループ名 (Group name)] = VCS_admin_RO)
6. 監査アクセス用に第 3 のグループを作成します (例 : [グループ名 (Group name)] = VCS_auditor)
7. ユーザ アクセス用に第 4 のグループを作成します (例 : [グループ名 (Group name)] = VCS_User)

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。

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。

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. 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. (1005R)

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。

© 2012 Cisco Systems, Inc. All rights reserved.

©2008 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)

この資料の記載内容は2008年10月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



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/>