Cisco Secure Access Control System 5.3 移行ガイド

2011 年 10 月

Text Part Number: OL-24202-01-J

【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。

Cisco Secure Access Control System 5.3 移行ガイド

CONTENTS

はじめに

このマニュアルでは、Cisco Secure Access Control System（ACS）リリース 3.x および 4.x から ACS 5.3 へのデータ移行プロセスについて説明します。ACS 5.3 には多くの新機能が備えられています。

ACS 3.x および 4.x プラットフォームと ACS 5.3 プラットフォームにはいくつかの違いがあります。ACS 5.3 に移行する前に、それらの違いを明確に理解する必要があります。このマニュアルでは、それらの違いを明確にし、ACS 3.x および 4.x の設定を ACS 5.3 に移行する方法について説明します。

このマニュアルの情報を理解するだけでなく、ACS 5.x プラットフォームの詳しい評価を実行することをお勧めします。

対象読者

このマニュアルは ACS 5.3 プラットフォームに移行する管理者を対象としています。

マニュアルの構成

この文書は、次の項で構成されています。

タイトル	説明
第 1 章「ACS 5.3 展開の概要」	ACS 3.x および 4.x と比較した ACS 5.3 展開モデルの概要を説明します。
第 2 章「ACS 5.3 の設定について」	ACS 3.x および 4.x と比較した ACS 5.3 の設定領域について説明し、古い設定を ACS 5.3 に変換する方法を理解するために役立ちます。
第 3 章「ACS 5.3 の設定の移行方法」	既存のシステムから ACS 5.3 に設定を移行するさまざまな方法を説明します。
第 4 章「ACS 5.3 移行ユーティリティのサポート」	移行ユーティリティを使用した移行の範囲について説明します。
第 5 章「移行ユーティリティのセットアップとインストール」	システム要件、インストール前の考慮事項、移行ユーティリティへのアクセス方法について説明します。
第 6 章「移行ユーティリティを使用した、ACS 4.x から ACS 5.3 へのデータ移行」	移行ユーティリティを使用したさまざまなフェーズのデータ移行プロセスについて説明します。
付録 A「移行ユーティリティでの ACS 5.3 属性サポート」	ACS 4.x から ACS 5.3 への属性の移行について説明します。

タイトル	説明
付録 B「ACS 3.x および 4.x から ACS 5.3 への設定マッピング」	ACS 3.x および 4.x から ACS 5.3 への設定のマッピングを示します。
付録 C「ACS 3.x および 4.x と ACS 5.3 の機能比較」	ACS 3.x および 4.x から ACS 5.3 の詳細な機能の比較を示します。
付録 D「移行ユーティリティのトラブルシューティング」	移行ユーティリティのトラブルシューティング方法について説明します。

このマニュアルの使用方法

次の章と付録で、以前のリリースから ACS 5.3 へ移行するための手順を説明します。

- 付録 C「ACS 3.x および 4.x と ACS 5.3 の機能比較」を参照して、展開のすべての重要な機能が ACS 5.3 で満たされていることを確認します。
- 第 1 章「ACS 5.3 展開の概要」を参照して、プラットフォームのサポート、分散展開モデル、システム インターフェイスなどの ACS 5.3 のシステム レベルの詳細を理解します。
- 第 2 章「ACS 5.3 の設定について」を参照して、ACS 5.3 の重要な機能と設定の違い、特定の設定の推奨事項と例を理解します。
- 第 3 章「ACS 5.3 の設定の移行方法」を参照して、既存の設定の移行の方法を理解します。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	用途
太字フォント	コマンド、キーワード、ユーザ入力テキストは**太字**で表示しています。
*イタリック体*フォント	ドキュメント名、新規用語または強調する用語、値を指定するための引数は、*イタリック体*フォントで示しています。
[ ]	角カッコは次のいずれかを示します。 • オプションの要素 • システム プロンプトへのデフォルトの応答
{ x | y | z }	必ずいずれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	いずれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
`courier` フォント	システムが表示するターミナル セッションおよび情報は、`courier` フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注） 「*注釈*」です。役立つ情報や、このマニュアル以外の参考資料などを紹介しています。

マニュアルの最新情報

表 1 に、『*Cisco Secure Access Control System 5.3 移行ガイド*』の更新内容を示します。

表 1　『Cisco Secure Access Control System 5.3 移行ガイド』の更新内容

日付	説明
2011/10/04	Cisco Secure Access Control System, Release 5.3。

製品マニュアル

（注） 初版発行後、印刷物または電子マニュアルのアップデートを行う場合があります。マニュアルのアップデートについては、Cisco.com で確認してください。

表 2 に ACS 5.3 で利用可能な製品マニュアルを示しています。Cisco.com ですべての製品のエンド ユーザ マニュアルを検索するには、次のサイトにアクセスしてください。http://www.cisco.com/go/techdocs

[Network Management and Automation] > [Security and Identity Management] > [Cisco Secure Access Control Server Products] > [Cisco Secure Access Control System] を選択します。

表 2　　製品マニュアル

参照先	ご利用形式
『*License and Documentation Guide for the Cisco Secure Access Control System 5.3*』	http://www.cisco.com/en/US/products/ps9911/products_documentation_roadmaps_list.html
『*Release Notes for the Cisco Secure Access Control System 5.3*』	http://www.cisco.com/en/US/products/ps9911/prod_release_notes_list.html
『*User Guide for the Cisco Secure Access Control System 5.3*』	http://www.cisco.com/en/US/products/ps9911/products_user_guide_list.html
『*CLI Reference Guide for the Cisco Secure Access Control System 5.3*』	http://www.cisco.com/en/US/products/ps9911/prod_command_reference_list.html
『*Supported and Interoperable Devices and Softwares for the Cisco Secure Access Control System 5.3*』	http://www.cisco.com/en/US/products/ps9911/products_device_support_tables_list.html
『*Installation and Upgrade Guide for the Cisco Secure Access Control System 5.3*』	http://www.cisco.com/en/US/products/ps9911/prod_installation_guides_list.html
『*Software Developer's Guide for the Cisco Secure Access Control System 5.3*』	http://www.cisco.com/en/US/products/ps9911/products_programming_reference_guides_list.html
『*Regulatory Compliance and Safety Information for Cisco Identity Services Engine, Cisco 1121 Secure Access Control System, Cisco NAC Appliance, Cisco NAC Guest Server, and Cisco NAC Profiler*』	http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/regulatory/compliance/csacsrcsi.html

関連資料

（注） 初版発行後、印刷物または電子マニュアルのアップデートを行う場合があります。マニュアルのアップデートについては、Cisco.com で確認してください。

表 3 に ACS 4.x で利用可能な関連資料を示しています。

表 3　　関連資料

参照先	ご利用形式
『*Installation Guide for Cisco Secure ACS for Windows 4.0*』	http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_installation_guides_list.html
『*User Guide for the Cisco Secure Access Control Server for Windows 4.0*』	http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_user_guide_list.html
『*Installation Guide for the Cisco Secure ACS for Windows 4.x*』	http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_installation_guides_list.html

表 3　　関連資料 （続き）

参照先	ご利用形式
『*User Guide for the Cisco Secure Access Control Server for Windows 4.1*』	http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_user_guide_list.html
『*Installation Guide for the Cisco Secure ACS for Windows 4.2*』	http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_installation_guides_list.html
『*User Guide for the Cisco Secure Access Control Server for Windows 4.2*』	http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_user_guide_list.html

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダーアプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

CHAPTER 1

ACS 5.3 展開の概要

ACS 5.3 展開モデルは ACS 4.x と似ており、単一のプライマリ ACS サーバと複数のセカンダリ ACS サーバから構成され、設定の変更はプライマリ ACS サーバで行います。これらの設定はセカンダリ ACS サーバに複製されます。

すべてのプライマリおよびセカンダリ ACS サーバで AAA 要求を処理できます。プライマリ ACS サーバは Monitoring and Report Viewer のデフォルトのログ コレクタでもありますが、任意の ACS サーバをログ コレクタに設定することができます。

1 台の ACS サーバで管理できますが、複数の ACS サーバを使用して、AAA 要求の処理の冗長性を備えることをお勧めします。ACS 5.3 は外部ログ用の syslog のサポートと、自動およびバッチ設定プロビジョニング用のインターフェイスを備えています。

ACS 展開は、セカンダリ サーバを追加することによって、AAA 要求の処理容量の増加に合わせて拡大できます。大規模な展開では、セカンダリ サーバを特定機能専用にすることができます。たとえば、プライマリ ACS サーバを設定の変更専用に使用し、AAA 要求の処理に使用しないようにすることもできます。セカンダリ ACS サーバをログ コレクタとしてのみ指定することができます。

大規模環境では、ロード バランサを使用して、展開内の ACS サーバ間で AAA 要求を分散し、AAA クライアント管理を簡単にして、高可用性を実現できます。

ACS サーバは一般にデータセンターや地域のサイトなどのユーザ クラスタの近くに配置します。

その他の展開情報については、『*Installation and Upgrade Guide for the Cisco Secure Access Control System 5.3*』の「Understanding the ACS Server Deployment」を参照してください。

表 1-1 にさまざまな ACS サーバの役割について説明します。

表 1-1　　ACS サーバの役割

ACS サーバの役割	役割の説明
プライマリ	プライマリ ACS サーバで実行した設定の変更は、展開内のすべてのセカンダリ ACS サーバに複製されます。プライマリ サーバとして使用できる ACS サーバは一度に 1 台だけです。
セカンダリ	ACS プライマリ サーバからの設定の変更を受け取るすべての ACS サーバはセカンダリ サーバです。
ログ コレクタ	Monitoring and Report Viewer のログ コレクタでもある ACS プライマリまたはセカンダリ サーバ。展開に配置できるログ コレクタは 1 台だけです。 他の ACS 展開（この展開と同期されないサーバ）は ACS ログをこのサーバに送信できません。

次の項では、ACS 4.x と ACS 5.3 の展開の違い、および ACS 5.3 を展開する場合のいくつかの考慮事項について説明します。

Windows と Linux ベースのアプリケーション

ACS 3.x および 4.x リリースは Windows サーバ プラットフォームにインストール可能な Windows ベースのアプリケーションとして使用できます。これらのアプリケーションは ACS Solution Engine と呼ばれるアプライアンスでも使用できます。このアプライアンスは ACS と Windows オペレーティング システムが事前ロードされているハードウェア プラットフォームです。

ACS 5.3 は Linux フレーバーのアプリケーションで Linux オペレーティング システムにパッケージされています。アプリケーションとオペレーティング システム パッケージはアプライアンスに同梱されており、VMware ESX Server 上の仮想マシンにもインストールできます。

ACS for Windows と ACS Solution Engine には機能と展開の違いがありますが、ACS 5.3 ハードウェア アプライアンスと仮想マシンにインストールされた ACS 5.3 には機能の違いがありません。ACS 5.3 ハードウェア アプライアンスと ACS 5.3 仮想マシンから構成される展開もサポートされます。

レプリケーション

ACS 3.x および 4.x は緩いレプリケーション モデルを提供します。ACS 3.x および 4.x レプリケーション モデルの特性を次に示します。

- 設定ブロックは ACS 設定の論理領域を表します。たとえば、ユーザとユーザグループ、ユーザグループのみ、ネットワーク デバイス、配布テーブル、インターフェイス設定、インターフェイス セキュリティ設定、パスワード検証設定、EAP-FAST 設定、ネットワーク アクセス プロファイル、ログ設定などです。
- プライマリ サーバからセカンダリ サーバに 1 つ以上の設定ブロックを複製するオプション。
- 設定の変更のサイズに関係なく、ブロック全体が複製されます。
- カスケード レプリケーション。これは、セカンダリ ACS サーバがレプリケーションの更新を別の ACS サーバにプッシュする機能です。
- レプリケーションは手動またはスケジュールに従って起動できます。
- TACACS+ パスワードの更新は、プライマリ サーバでのみ受け取ります。

この緩いレプリケーション モデルでは、プライマリ サーバとセカンダリ サーバ間で複製されたブロックが同期されますが、設定の他の部分は異なることがあり、ローカル環境に合わせてカスタマイズできます。

ACS 5.3 のレプリケーション モデルは単純で効率的かつ堅牢です。ACS 5.3 レプリケーション モデルの特性を次に示します。

- プライマリ サーバとセカンダリ サーバ間の完全同期。
- 透過的で即座のレプリケーション。
- 設定の変更のみが複製されます。
- 設定の変更はプライマリ サーバでのみ実行できます。
- カスケード レプリケーションはありません。
- 欠落した更新の自動リカバリ。
- セカンダリ サーバをプライマリ サーバにプロモートする機能。
- TACACS+ パスワードの更新は任意の ACS インスタンスで受け取ることができます。

ACS 5.3 ネットワーク アクセス ポリシー設定で地域固有のアクセス ポリシーを実装する必要があります。これは、ACS 5.3 の設定がプライマリ サーバとセカンダリ サーバで完全に同期され、直接セカンダリ サーバに対して設定を変更することができないためです。

ID ストア

ACS 3.x および 4.x と 5.3 の ID ストアのサポートに関する主な違いは、ACS 5.3 では、データベースへの認証に ODBC がサポートされないことと、TACACS+ 要求のプロキシ転送がサポートされないことです。ACS 5.3 では、認証に次の ID ストアがサポートされます。

- ACS 内部ストア
- Active Directory
- LDAP ディレクトリ
- 次を使用したワンタイム パスワード サーバ
  - RSA SecurID インターフェイス
  - RADIUS インターフェイス
- RADIUS による他のストアへのプロキシ転送（RADIUS プロキシ）

ロギング

ACS 5.3 では、Monitoring and Report Viewer 機能が ACS に含まれます。ACS 5.3 展開では、ACS サーバがレポートおよび監視機能のログ コレクタとして指定されます。その他のすべての ACS サーバは指定されたログ コレクタにログ メッセージを送信します。

ACS は外部サーバへのログ用に syslog をサポートしています。

ACS 5.3 は Monitoring and Report Viewer からユーザ認証情報を取得するための Cisco Wireless Control System（WCS）の Web サービス インターフェイスを備えています。

設定

ACS 5.3 では、設定のプライマリ モードは Web ベースのユーザ インターフェイスです。ACS 5.3 にはシステム タスクとファイルベースの設定の更新を実行できるコマンドライン インターフェイス（CLI）もあります。

CLI には、コンソール ポート、キーボード、ビデオ、マウス（KVM）、SSH からアクセスできます。内部 ACS ユーザ向けにパスワード変更アプリケーションを開発するための Web サービス インターフェイスが提供されています。

表 1-2 に ACS でサポートされる内部ユーザとネットワーク デバイスの数を示します。ユーザとネットワーク デバイスは一般的に使われ、広く読み込まれる ACS オブジェクトです。

表 1-2　内部ユーザとデバイスの設定の容量

ACS オブジェクト	設定の容量
内部ユーザ	300,000
ネットワーク デバイス	50,000

ライセンス

ACS の 3.x および 4.x リリースには、キーまたはライセンス ファイルを適用する必要がありませんでした。しかし、5.x リリースにはライセンス ファイルの適用が必要です。ACS 5.3 ライセンスは、http://cisco.com/go/license で入手できます。

表 1-3 に使用可能な ACS 5.3 ライセンスを示します。

表 1-3　使用可能な ACS 5.3 ライセンス

ライセンス	説明
Base Server	各 ACS インスタンスに 1 つ。
Large Deployment	ACS のネットワーク デバイス数（IP アドレスに基づく）が 500 を超える場合、各 ACS 展開に 1 つ。 Default Network Device を設定すると、デバイス数に影響します。

サーバの展開の推奨事項

表 1-4 に ACS 3.x および 4.x から ACS 5.3 へのコンポーネントのマッピングを示します。

表 1-4　　コンポーネントのマッピング

ACS 3.x および 4.x コンポーネント	ACS 5.3 コンポーネント	変更点
ACS for Windows	VMware ESX の VM または 1120/1121 アプライアンス	ACS 5.3 Windows オプションはありません。ACS 5.3 は VMWare またはサポート対象のアプライアンスで実行できるアプリケーションです。
ACS Solution Engine（1111、1112、1113）	VMware ESX の VM または 1120 または 1121 アプライアンス	ACS 1111、1112、および 1113 プラットフォームは ACS 5.3 をサポートしていません。ACS 4.2 は 1120 で実行できます。
ACS Remote Agent	該当なし	ACS 5.3 では Remote Agent は必要ありません
ACS View 4.0	VMware ESX の VM または 1120/1121 アプライアンス	ACS 5.3 には ACS View 機能が組み込まれています。

ACS 5.3 の展開のガイドライン

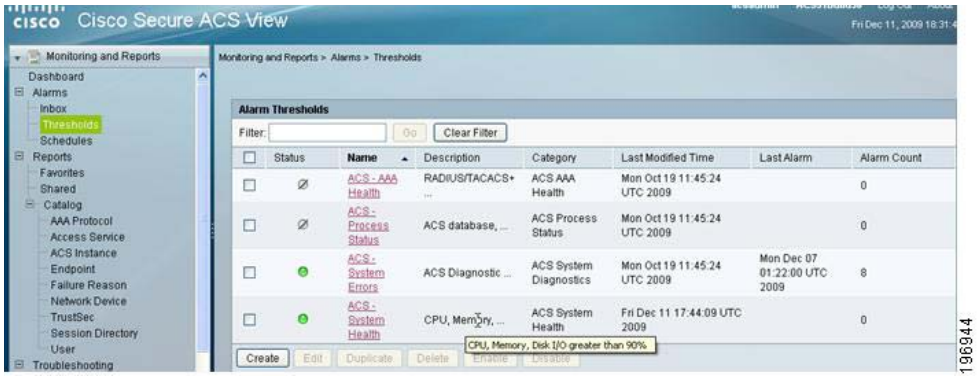
- ほとんどの場合に、1 対 1 の ACS サーバ置換が適切です。

  ACS 5.3 の認証パフォーマンスは以前のバージョンと同じです。
- 冗長性を提供するために、少なくとも 2 つの ACS インスタンスを展開します。
- 認証パフォーマンスを拡張するには、ACS サーバを追加します。

  1 台の ACS サーバでその AAA クライアントと、バックアップ AAA サーバとしてそれに依存するすべての AAA クライアントのピークの認証レートを処理できることを確認します。
- 展開環境を拡大するために、AAA 要求のみを処理するセカンダリ ACS サーバを使用することができます。プライマリは設定の更新とログの収集にのみ使用します。

  ログ コレクタには最も強力なハードウェアを使用します。たとえば、1120 アプライアンスよりも 1121 アプライアンスを使用します。
- ロード バランサを使用して、AAA 要求を受け取り、AAA クライアントの管理を簡単にし、耐障害性を向上して、ACS 認証容量を有効に利用します。
- 実行中のリソースの使用状況を監視します。これは、図 1-1 に示すように、Monitoring and Report Viewer の ACS システム健全性アラームしきい値を有効にすることによって実行できます。

図 1-1　ACS 5.3 のアラームしきい値



パフォーマンス

ログ コレクタとして動作しない単一の ACS 5.3 サーバは 1 秒あたり 100 を超える認証を処理できます。AAA 要求を処理する単一の ACS サーバでピーク時間の負荷を管理できることを確認する必要があります。ピーク時間は、一般にユーザの始業時やネットワーク機器の再起動時に発生します。これにより、大量の認証要求が作成されます。

たとえば、15 分間に 50,000 人の社員がネットワークに均等にログインします。これは、ピーク認証レートとして、1 秒あたり約 56 の認証に換算されます。この場合、ログ コレクタとして動作しない単一の ACS サーバでこのピーク認証レートをサポートできます。

表 1-5 に、最小レートが 1 秒あたり 100 認証として、さまざまな期間での 1 台の ACS サーバでサポートできる認証数を示します。

表 1-5　さまざまな期間での認証

1 秒	100 認証
60 秒	6,000 認証
5 分	30,000 認証
15 分	90,000 認証
1 時間	360,000 認証

ACS 認証パフォーマンスに影響する要因は、設定サイズ、ポリシーの複雑さ、外部サーバとの通信、認証プロトコルの複雑さなどたくさんあります。

表 1-6 にさまざまな認証環境での ACS のパフォーマンスを示します。このパフォーマンス データは、複雑な設定を使用する ACS をテストした場合に観察された低い範囲の認証レートを示しています。簡単な設定の場合はパフォーマンスが高くなります。

表 1-6　低い範囲の ACS 5.3 認証パフォーマンス（認証数/秒）

認証タイプ	ID ストア		
	内部	AD	LDAP
PAP	500	100	800
CHAP	500	500	該当なし
TACACS+	400	160	1200
MSCHAP	500	300	該当なし
PEAP-MSCHAP	200	100	該当なし
PEAP-GTC	200	100	300
EAP-TLS	200	180	270
LEAP	330	280	該当なし
FAST-MSCHAP	120	120	該当なし
FAST-GTC	130	110	190
MAC 認証バイパス	750	該当なし	2000

（注）　上の数値は、該当する EAP モジュールに高速再接続およびセッション再開が使用されていることを前提としています。

ACS サーバを Monitoring and Report Viewer のログ コレクタとしても使用する場合、認証パフォーマンスは約 50 % 低下します。

CSACS 1121 アプライアンスでは、表 1-6 に示す数値よりもパフォーマンスが約 10 % ～ 15 % 向上します。

仮想マシンでのパフォーマンスは、仮想マシンのオーバーヘッドのため、実際の 1120 アプライアンスよりも低くなります。CPU リソースを増やすと、仮想マシンのパフォーマンスが向上します。

仮想マシン環境での最小要件は 1121 アプライアンスと似ています。仮想マシン環境の詳細については、『*Installation and Upgrade Guide for the Cisco Secure Access Control System 5.3*』を参照してください。

CHAPTER 2

ACS 5.3 の設定について

ACS 5.3 の設定

この章では、既存の 3.x および 4.x の設定を 5.3 の設定に変換するにあたって、ACS 3.x、4.x と ACS 5.3 の設定の違いについて説明します。

この章は、次の内容で構成されています。

表 2-1 では、ACS 5.3 の主な設定領域について説明します。

:

表 2-1　ACS 5.3 の主な設定領域

設定領域	設定対象
ネットワーク リソース	AAA クライアント、クライアントのグループ化、および RADIUS プロキシ サーバ。
ユーザおよび ID ストア	内部ユーザ、内部ホスト、Active Directory、LDAP ディレクトリ、ワンタイム パスワード サーバ、RADIUS ID ストア、証明書認証情報、および ID ストア順序。
ポリシー要素	ネットワーク アクセス ポリシーの条件および認可プロファイル。
アクセス サービス	さまざまなアクセス シナリオに対処するネットワーク アクセス ポリシー。
モニタリングとレポート	タスクの ACS モニタリング、レポート、トラブルシューティング タスク。
システム管理	ACS システム管理タスク。

ネットワーク リソース

AAA クライアントおよび RADIUS プロキシ サーバは [Network Resources] ドローアで定義および編成されます。

次のコンポーネントは [Network Resources] で設定されます。

- 「ネットワーク デバイス グループ」（P.2-2）
- 「ネットワーク デバイス」（P.2-5）
- 「外部 RADIUS サーバ」（P.2-6）

ネットワーク デバイス グループ

ACS 5.3 の主な変更は次のとおりです。

- 1 つのデバイスが複数のグループに属することができます（ネットワーク デバイス グループ階層）。
- デバイス グループ レベルの共有秘密は使用できません。
- デバイス グループは AAA サーバ定義のコンテナではありません。

ネットワーク デバイス グループでは場所、タイプ、およびその他のグループ化に基づいてデバイスをグループ化できます。これは、これらのグループ化に基づいたネットワーク アクセス ポリシーを適用する場合に特に重要となります。たとえば、West Coast のファイアウォール管理者は West Coast のファイアウォールだけにアクセスできるように制限します。

ネットワーク デバイスを ACS 5.3 に移行する場合、デバイスのインポートまたは設定を行う前にデバイスのグループ化を計画することをお勧めします。これにより、デバイスが ACS 5.3 で作成されるときにデバイスにグループを割り当てることができます。

ACS 3.x および 4.x は平面的なグループ化モデルであるため、1 つのデバイスは 1 つのデバイス グループにだけ属することができます。このモデルは、デバイスを複数の方法でグループ化しようとするときに、グループの増加の原因となります。場所を階層型でグループ化することがよくあります。

たとえば、大陸、地域、国でグループ化します。ACS 3.x および 4.x のグループの例を次に示します。

- アフリカ - 南 - 南アフリカ
- アフリカ - 南 - ナミビア
- アフリカ - 南 - ボツワナ

多くの場合、デバイスはタイプでグループ化されます。上記の例を組み込みタイプのグループ化に拡張するとグループは次のようになります。

- アフリカ - 南 - 南アフリカ - ファイアウォール
- アフリカ - 南 - 南アフリカ - スイッチ
- アフリカ - 南 - 南アフリカ - ルータ
- アフリカ - 南 - ナミビア - ファイアウォール
- アフリカ - 南 - ナミビア - スイッチ
- アフリカ - 南 - ナミビア - ルータ
- アフリカ - 南 - ボツワナ - ファイアウォール
- アフリカ - 南 - ボツワナ - スイッチ
- アフリカ - 南 - ボツワナ - ルータ

デバイスのタイプ、ベンダーなどのその他のパラメータが追加されると、グループの数は増加します。

ACS 5.3 ではこのデバイス グループの増加の問題に、ネットワーク デバイス グループ階層を使用して対応しています。さまざまなグループを表す複数の階層が存在する場合があります。デバイスは各階層の 1 つのノードに属します。図 2-1、図 2-2、および図 2-3 は 3 つの異なるネットワーク デバイス グループ階層を表示しています。

図 2-1　　ネットワーク デバイス グループ階層

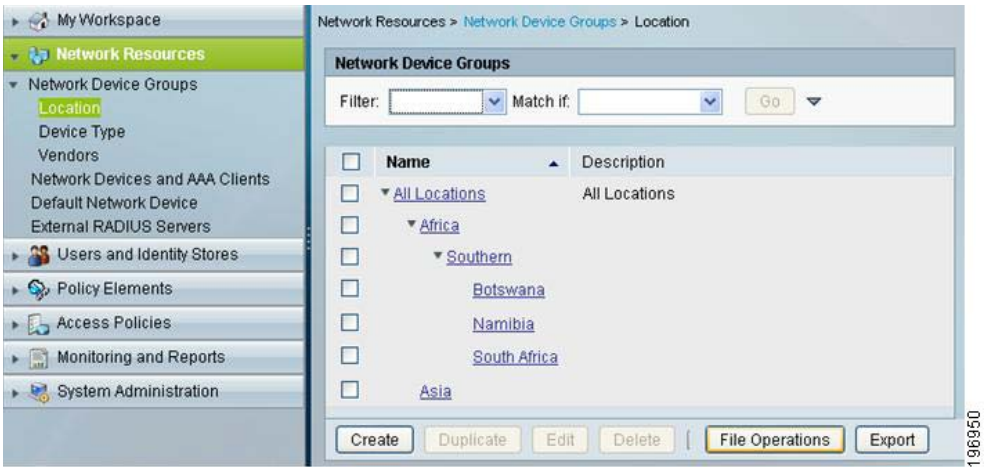


図 2-2　　ネットワーク デバイス グループ階層

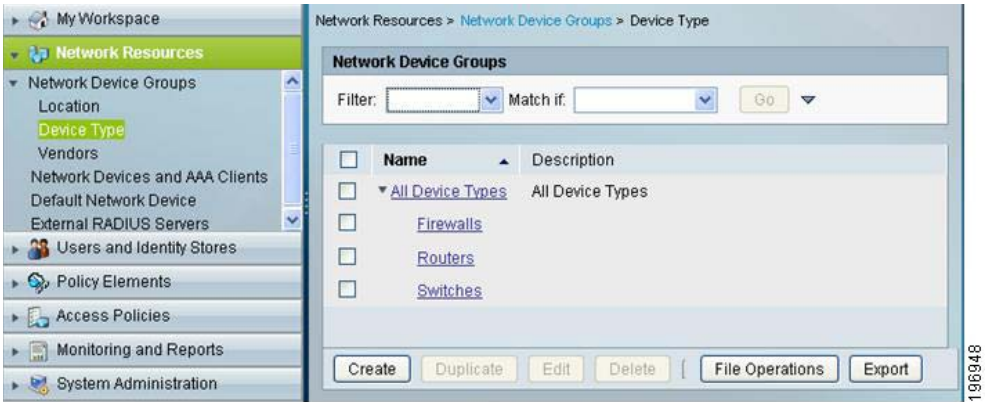
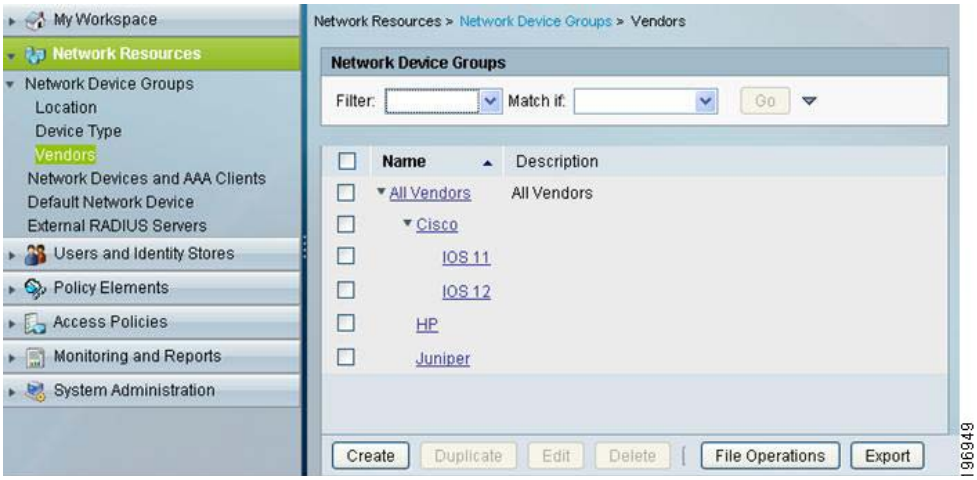
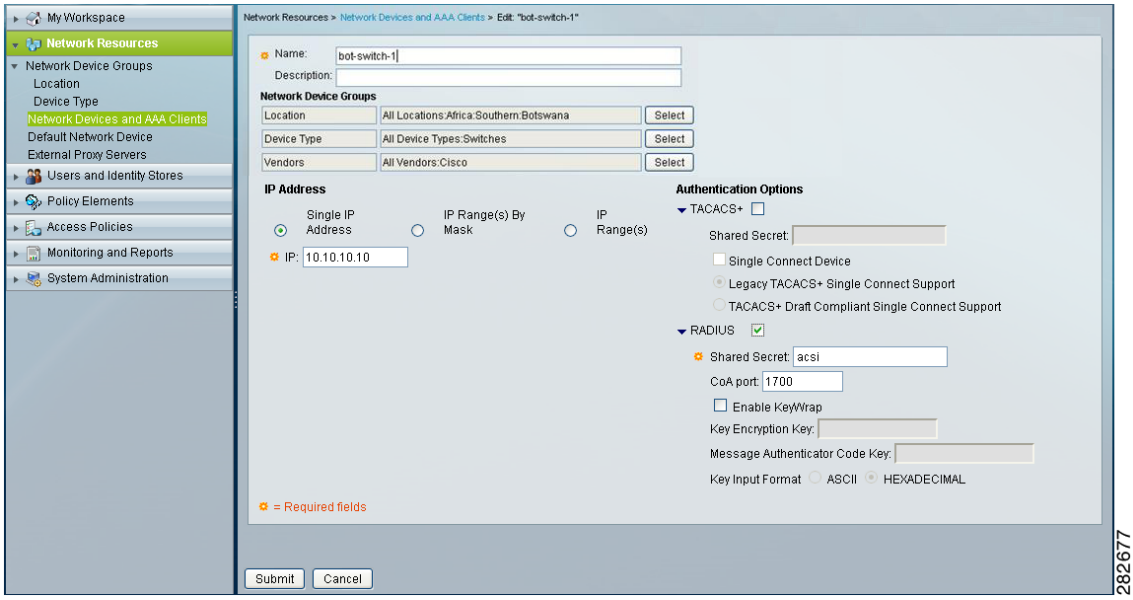


図 2-3　ネットワーク デバイス グループ階層



任意のデバイスを各階層の 1 つのノードに割り当てることができます。図 2-4 に、ボツワナにある Cisco スイッチ デバイスを示します。

図 2-4　ボツワナにある Cisco スイッチ デバイスの例



デバイス グループ階層の各ノードはネットワーク アクセス ポリシーで使用可能な属性になります。複数の階層でノードを参照することで、複数の階層の共通部分にあたるデバイスを簡単に表すことができます。

ナミビアの Cisco ファイアウォールに適用される条件を含む規則の例を次の表に示します。

状態			結果
NDG：場所	NDG：デバイス タイプ	NDG：ベンダー	
ナミビア	ファイアウォール	Cisco	…

移行メモ

- ACS 5.3 で、より自然な階層型グループを活用できるように、デバイスのグループ化の手法を計画してください。
- ACS 5.3 では、ACS 3.x および 4.x で使用できるデバイス グループごとの共有秘密をサポートしていません。ACS 5.3 では、共有秘密をデバイスの定義ごとに定義する必要があります。

ネットワーク デバイス

ACS 5.3 の主な変更は次のとおりです。

- クライアントが TACACS+ および RADIUS の両方をサポートする場合、AAA のデバイス定義は 1 つだけです。個別の定義は必要ありません。
- マスクベース IP アドレス。
- TACACS+ および RADIUS の両方に対するデフォルトのデバイス定義。

図 2-5 に、ACS 5.3 ネットワーク デバイス設定を示します。

図 2-5　　ACS 5.3 ネットワーク デバイス設定

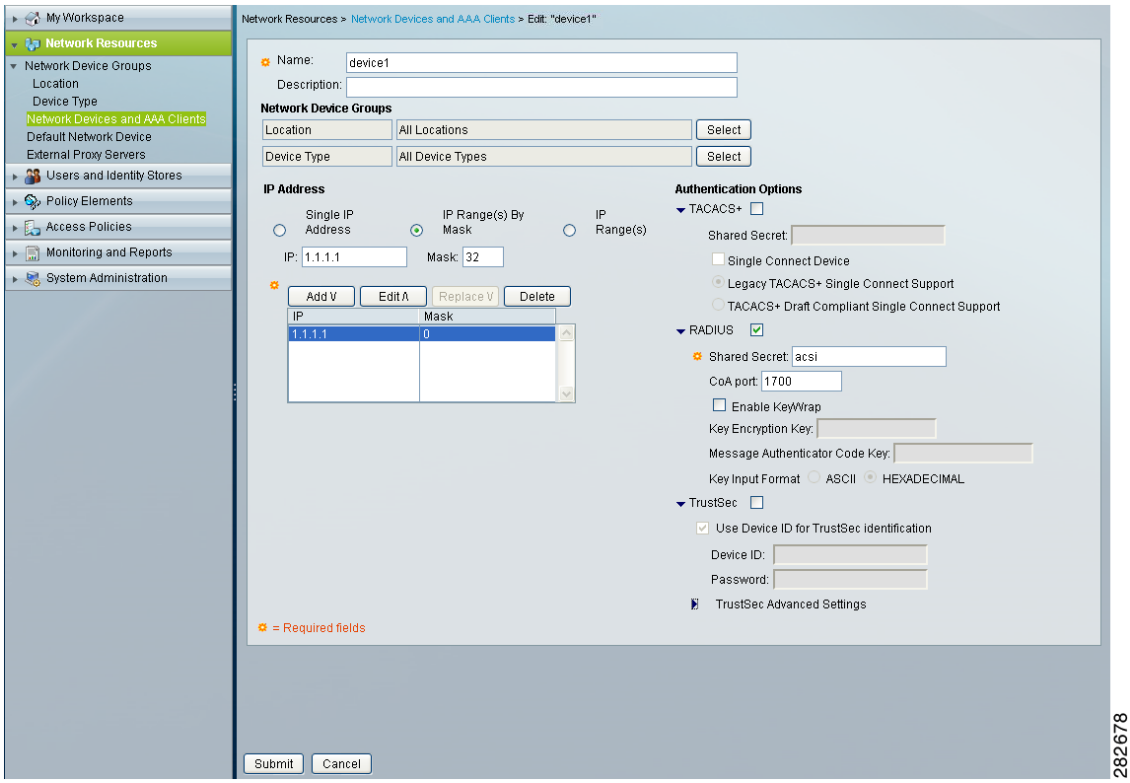
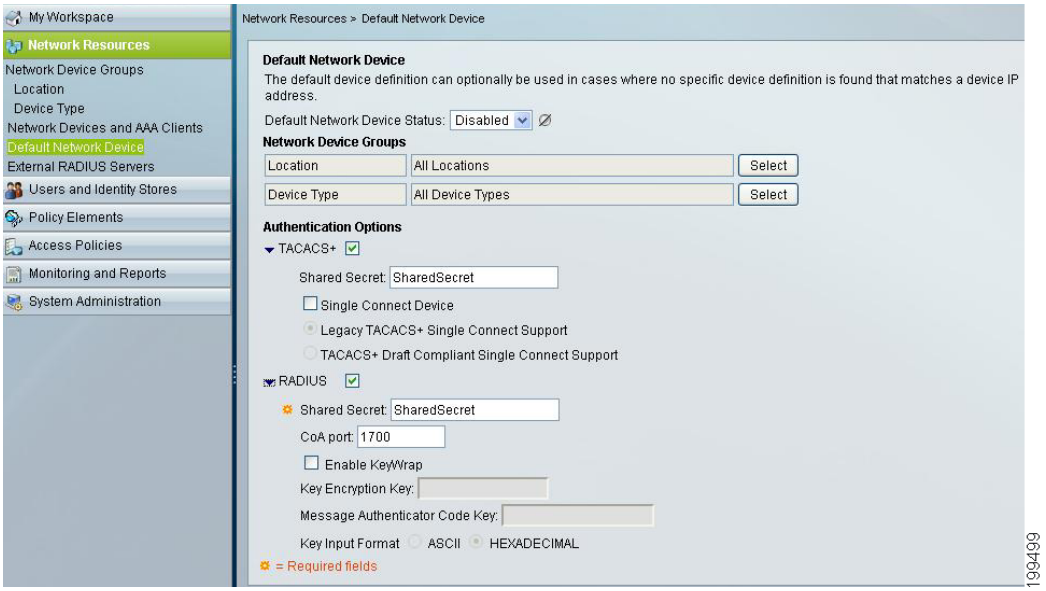


図 2-5 に、サブネット 10.10.20.0 および 10.10.30.0 のクライアントを表すデバイス定義を示します。デバイス設定で TACACS+ または RADIUS のどちらもイネーブルになっているため、これらのクライアントは両方の要求を送信できます。

図 2-6 に、デフォルトのネットワーク デバイスを示します。

図 2-6　　デフォルトのネットワーク デバイス



デフォルトのネットワーク デバイスによって、ACS 3.x および 4.x のデフォルトの TACACS+ デバイス、0.0.0.0 が置換されます。これは、RADIUS 要求のデフォルトのデバイスとして動作することもできます。

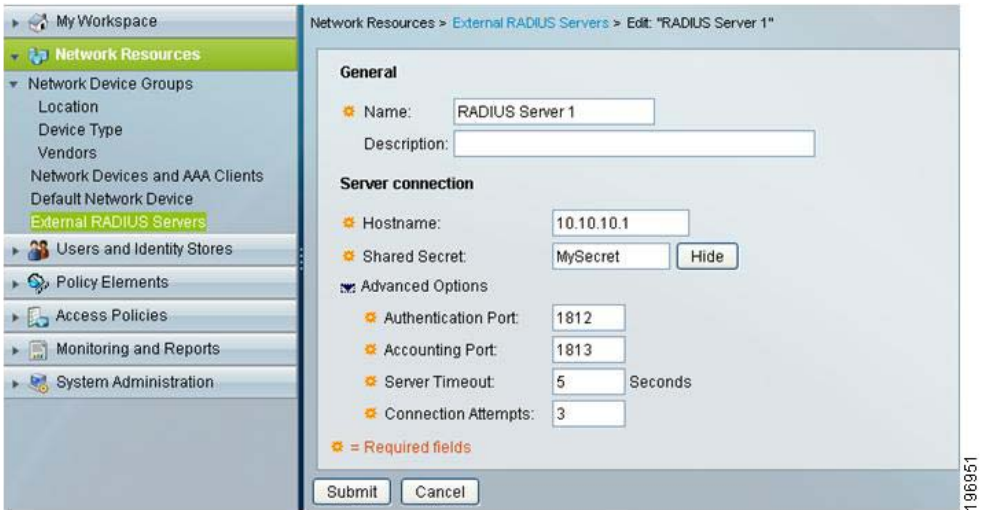
移行メモ

- ACS 3.x および 4.x での TACACS+ および RADIUS の二重のデバイス定義は、ACS 5.3 では 1 つのデバイス定義に統合されます。
- ACS 5.3 は IP アドレス定義にサブネット マスクを使用しています。IP 範囲およびワイルドカードを使用して、ACS 5.3 のサブネット マスク範囲に ACS 3.x および 4.x の設定をマッピングします。
- デフォルトのネットワーク デバイスは、ACS 5.3 への迅速な移行を可能にする便利なツールです。ACS 5.3 が AAA 要求の受信を開始すると同時に、より詳細なデバイス定義が作成されます。

外部 RADIUS サーバ

[Network Resources] ドローアの最後の設定領域は外部 RADIUS サーバです。このオプションでは、ACS のプロキシの対象となる RADIUS サーバを定義できます。図 2-7 に、ACS 5.3 の外部 RADIUS サーバ設定を示します。

図 2-7　　ACS 5.3 RADIUS サーバ設定



移行メモ

- ACS 5.3 では、その他の AAA サーバに認証要求を送信するプロキシの配布テーブルはありません。
- RADIUS プロキシには、RADIUS プロキシ アクセス サービスを設定します。

ユーザおよび ID ストア

次のコンポーネントは、[Users and Identity Stores] で設定されます。

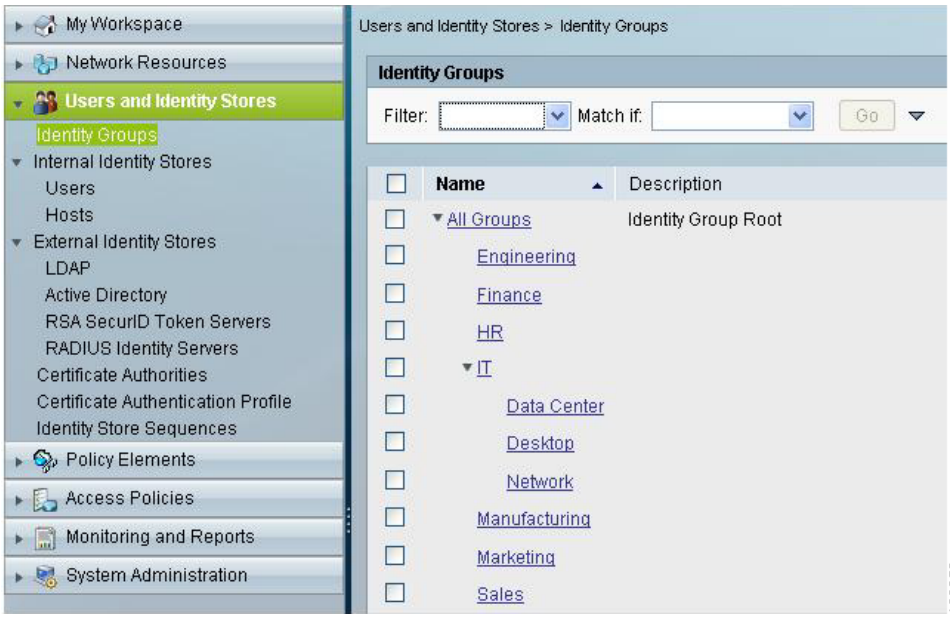
- 「ID グループ」（P.2-7）
- 「内部 ID ストア」（P.2-9）
- 「外部 ID ストア」（P.2-10）
- 「信頼できる認証局および証明書認証プロファイル」（P.2-10）
- 「ID ストア順序」（P.2-11）

ID グループ

ACS 5.3 の主な変更は次のとおりです。

- ACS 5.3 ID グループには、ACS 3.x および 4.x ユーザ グループのようなアクセス ポリシー権限がありません。
- ユーザを ACS グループに関連付ける必要はありません。
- 外部グループを ACS グループにマッピングする必要はありません。
- ID グループによって階層型のグループ化を実現しています。図 2-8 に、ACS 5.3 の ID グループの階層を示します。

図 2-8　ACS 5.3 の ID グループ



ACS 3.x および 4.x では、ACS は ACS ユーザ グループを使用してユーザにネットワーク アクセス ポリシーを適用します。ACS により認証されたすべての内部および外部ユーザは 1 つの ACS ユーザ グループだけにマッピングされます。ACS 5.3 では、ネットワーク アクセス ポリシーはグループを通じて適用されるのではなく、アクセス サービスを通じて適用されます。

アクセス サービスに含まれる規則は、ユーザに適用されるポリシーを管理する条件で構成されます。ユーザのグループ メンバシップは、これらの条件を構成するために使用される多くの属性の 1 つです。ポリシーはグループを通じて適用されないため、ACS 5.3 ではグループの関連付けは必要ありません。

ACS 3.x および 4.x では、Active Directory または LDAP ディレクトリなどの外部 ID ストアがユーザ認証に使用される場合や、ユーザのディレクトリ グループ メンバシップがそれらのネットワーク アクセスに関連する場合は、ユーザの外部グループ メンバシップを ACS グループにマッピングするためにグループのマッピングが必要です。これは、適切なネットワーク アクセス ポリシーを適用するために必要です。

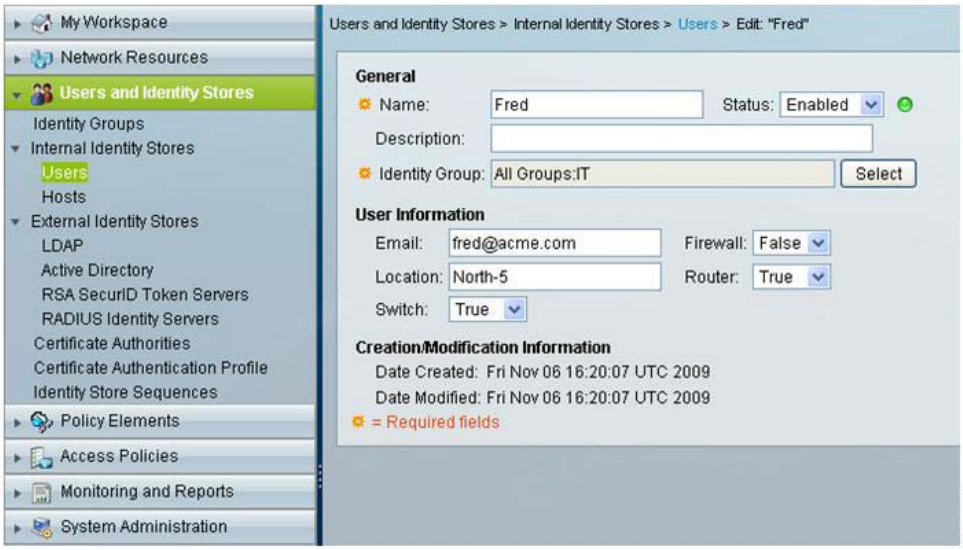
ACS 5.3 では、外部グループ メンバシップはネットワーク アクセス ポリシーを作成する場合に直接使用できる属性です。したがって、グループのマッピングを使用する必要はありません。

移行メモ

- ACS 5.3 で本当に ID グループが必要かどうかを検討してください。ID グループが必要になるのは、ACS 内のユーザを管理するときだけです。
- ID グループの階層構造を活用してください。
- ユーザ グループの一部である ACS 3.x および 4.x 認可は [Policy Elements] および [Access Services] ドローアで設定されます。
- 複数のグループに所属するユーザを表す組み合わせグループを作成する代わりに、内部 ID ストアスキーマを拡張してこれらのさまざまなグループを指定することを検討してください。

  図 2-9 の例では、場所で分類された IT グループのユーザ Fred が、スイッチ、ファイアウォール、ルータにアクセスできるかどうかを示しています。

図 2-9　　ACS 5.3 の内部 ID ストア



内部 ID ストア

ACS 5.3 の主な変更は次のとおりです。

- ユーザ ストアに加えて、ACS 5.3 には MAC アドレスをホストするホスト ストアがあります。
- アクセス ポリシー権限にはユーザ レコードが含まれません。
- ユーザ フィールドを追加してユーザ スキーマをカスタマイズできます。
- カスタム ユーザ フィールドには、アクセス ポリシーに利用できるユーザ固有の値を格納することができます。

ポリシー コンポーネントが ACS 5.3 のポリシー要素とアクセス サービスに移動したため、ACS 5.3 のユーザ ストアは ACS 3.x および 4.x と比べると単純です。名、性、場所、E メールなどのユーザ固有の情報を格納するようにスキーマをカスタマイズできるため、ACS 5.3 のユーザ ストアは外部ストアと似ています。

これらのフィールドを、アクセス ポリシーで使用できる属性にすることもできます。たとえば、ユーザの場所を条件として使用したり、IP アドレスの値を RADIUS の戻り値として使用したりできます。

ACS 5.3 では、エージェントレス ホストのシナリオの MAC アドレス データベースを管理するための個別のホスト ストアを使用できます（MAC 認証バイパス）。ユーザ ストアと同様に、アクセス ポリシーで使用するホスト レコードにカスタム フィールドを追加できます。

移行メモ

- ID ストア順序をアクセス サービス ID ポリシーと組み合わせて使用して、ユーザ レコードからパスワード認証方式を選択する ACS 3.x/4x の機能を実装できます。
- ユーザ パスワード ポリシーは [System Administration] > [Users] > [Authentication Settings] の下にあるセットです。

外部 ID ストア

ACS 5.3 の主な変更は次のとおりです。

- ACS 5.3 は Active Directory（AD）に直接参加し、ドメイン参加の Windows Server に依存しません。ACS Remote Agent は必要ありません。
- ODBC データベースは ACS 5.3 ではサポートされていませんが、LDAP ディレクトリやワンタイム パスワード サーバなどの、その他の ID ストアはサポートされています。
- ACS 5.3 は、RADIUS ベースのワンタイム パスワード サーバや、プロキシ応答属性がアクセス ポリシーで必要となる RADIUS プロキシに、RADIUS ID ストアを追加します。
- ACS 5.3 では、AD および LDAP ユーザ属性をユーザ グループのメンバシップに加えてアクセス ポリシーでも使用できるように、機能が追加されました。
- ACS 3.x および 4.x で、未知のユーザ ポリシーによって提供された ID ストアのリストは、ACS 5.3 では ID ストア順序を使用して設定されます。ACS 5.3 ではダイナミック ユーザの概念はありません。

外部 ID ストアの設定は ACS 3.x および 4.x の外部ユーザ データベースと同様です。ACS 5.3 では、外部 ID ストアが設定され、ACS がそれらと通信して、認証と認可を行います。

Active Directory では、ACS 5.3 は ACS 3.x および 4.x と同様に、基盤となる Windows オペレーティング システムを利用せずに AD ドメインに参加します。ACS 5.3 は、ACS 3.x および 4.x と同様に、ドメイン間の信頼関係によってドメイン間の認証を行います。

ACS 5.3 の設定では、ACS が AD ドメインに参加して通信するためのユーザ名とパスワードの資格情報を入力する必要があります。資格情報には、コンピュータ オブジェクトを作成できる権限が必要です。アクセス ポリシーにユーザの AD グループ メンバシップおよび属性情報が必要な場合、それらの情報は AD の設定で最初に選択される必要があります。

LDAP ディレクトリ設定は、ACS 3.x および 4.x と同様です。ACS 3.x および 4.x と同様に、ACS 5.3 では複数の LDAP ディレクトリを定義できます。LDAP ディレクトリ設定では、アクセス ポリシーで使用するグループおよび属性を選択できます。

ワンタイム パスワード認証では、ACS 5.3 は RSA SecurID トークン サーバを設定して、RSA SecurID ネイティブ インターフェイスをサポートします。RSA 以外のワンタイム パスワード サーバでは、RADIUS ID サーバ オプションを使用して、RADIUS のやり取りを設定できます。

移行メモ

RSA SecurID プロンプトを設定するには、[System Administration] > [Configuration] > [Global System Options] > [RSA SecurID Prompts] を参照してください。

信頼できる認証局および証明書認証プロファイル

ACS 5.3 の主な変更は次のとおりです。

- 証明書認証プロファイルでは、さまざまな証明書プロファイルの認証をカスタマイズできます。
- 証明書ベースの認証では、ID ストア認証は任意です。
- ルート CA 証明書をインポートする必要があります。

[Users and Identity Stores] の証明書の設定オプションの下に、信頼できる証明書認証局が定義されています。ここで、さまざまな証明書プロファイルの認証の特性を指定することもできます。

証明書認証プロファイルはアクセス サービス ID ポリシーで参照され、次を指定することができます。

- プリンシパル ユーザ名として使用する必要がある証明書フィールド。
- 証明書のバイナリ比較を実行する必要があるかどうか。

移行メモ

- PEM または DER 形式の X.509 証明書をインポートして、信頼できる CA のリストを作成することができます。
- ACS 5.3 では証明書のオーナーがディレクトリに存在するかどうかが確認されませんが、アクセス サービス認可ポリシーでユーザ属性の存在を確認できます。

ID ストア順序

ACS 5.3 の主な変更は次のとおりです。

- さまざまな ID ストアを認証と認可に使用できる
- 認証と認可の両方の ID ストアのリストを設定できる

ほとんどの展開では、ユーザの認証と認可に 1 つの ID ストアが使用されます。多くの展開では、ネットワーク アクセスは複数の ID ストアに依存しています。

ACS 5.3 の ID ストア順序はこの要件に対応しており、アクセス サービス ID ポリシーの ID ストアの代わりに参照することができます。ID ストア順序では、認証 ID サーバの 1 つのリストを指定し、認可で別のリストを指定することができます。

たとえば、ワンタイム パスワード ユーザはワンタイム パスワード サーバに対してユーザの認証を行う必要がありますが、グループやメンバシップなどのその他の認可情報はディレクトリ内でだけ使用できます。

移行メモ

ID ストア順序を使用して ACS 3.x および 4.x の未知のユーザ ポリシーで提供された機能を置き換えることができます。

ポリシー要素

アクセス ポリシーのプライマリ コンポーネントは、ID ポリシーおよび認可ポリシーです。どちらのポリシーも、ACS 5.3 アクセス サービスの個別の規則テーブルで表されます。規則テーブルの各規則は条件と結果で構成されます。

[Policy Elements] 設定領域で条件を作成してカスタマイズできます。認可結果はこの領域で作成されます。

次のコンポーネントは [Policy Elements] で設定されます。

- 「セッション条件」（P.2-12）
- 「認可および権限」（P.2-12）
- 「アクセス ポリシー」（P.2-12）

セッション条件

ACS 5.3 の主な変更は次のとおりです。

- 以前はネットワーク アクセスの制限（NAR）と呼ばれていたネットワーク条件は、この設定領域で定義されます。
- アクセス サービス規則の条件を作成するときは、次の属性を使用できます。
  - システム ディクショナリ属性
  - RADIUS 属性と TACACS+ 属性
  - ネットワーク デバイス グループ（NDG）
  - ユーザ属性とグループ メンバシップ
  - 証明書属性
- セッション条件の下に次の追加の条件を定義できます。
  - 日付と時刻の条件を使用して日時の範囲を定義します。
  - カスタム条件を使用すると、既存の属性の名前を変更し、ポリシーを簡素化して表すことができます。
  - ネットワーク条件を使用すると、ACS 3.x および 4.x に対応する NAR を定義できます。

移行メモ

ACS 3.x および 4.x のユーザ、ユーザ グループ、または共有プロファイル コンポーネントで設定されたアクセス ポリシー条件は、セッション条件で設定する必要があります。

認可および権限

ACS 5.3 の主な変更は次のとおりです。

- すべてのアクセス ポリシー認可はこの設定領域で定義される必要があります。
- さまざまなタイプのネットワーク認可を次に示します。
  - TACACS+ シェル特権およびコマンド セットを使用するデバイス管理の認可。
  - RADIUS を使用するネットワーク アクセス認可。
  - 一般的にリモート アクセス認可に使用されるダウンロード可能 ACL。

移行メモ

以前に ACS 3.x および 4.x のユーザ、ユーザ グループ、または共有プロファイル コンポーネントで設定されていたアクセス ポリシー認可は、[Authorizations and Permissions] で設定されます。

アクセス ポリシー

ACS 5.3 の主な変更は次のとおりです。

- ACS 5.3 では、[Access Policies] がネットワーク アクセス ポリシーの中心です。
- RADIUS および TACACS+ 認証や認可要求のすべてのネットワーク アクセス ポリシーはここで設定されます。

ACS 5.3 のすべての認証要求および認可要求は、アクセス サービスで処理する必要があります。アクセス サービスは認証ポリシーおよび認可ポリシーを定義します。ACS 5.3 は、さまざまなネットワーク アクセス シナリオの複数のアクセス サービスをサポートします。

アクセス サービスによって、さまざまなネットワーク アクセス ポリシーを論理的に分離することができます。たとえば、組織がデバイス管理ポリシー用にアクセス サービスを実装し、リモート VPN アクセス用に別のアクセス サービスを実装することがあります。

いずれかのアクセス サービス内のポリシーを簡素化するために、追加のアクセス サービスを設定することもできます。たとえば、すべての 802.1X ネットワーク アクセスを扱う 1 つのアクセス サービスを設定する代わりに、複数のアクセス サービスを使用して、有線、無線、マシン、802.1X アクセスのホスト用のポリシーに対処できます。

アクセス サービスに加えて、サービス セレクション ポリシーの設定も必要です。サービス セレクション ポリシーは、適切なアクセス サービスに認証要求および認可要求を送信する方法を ACS に指示します。

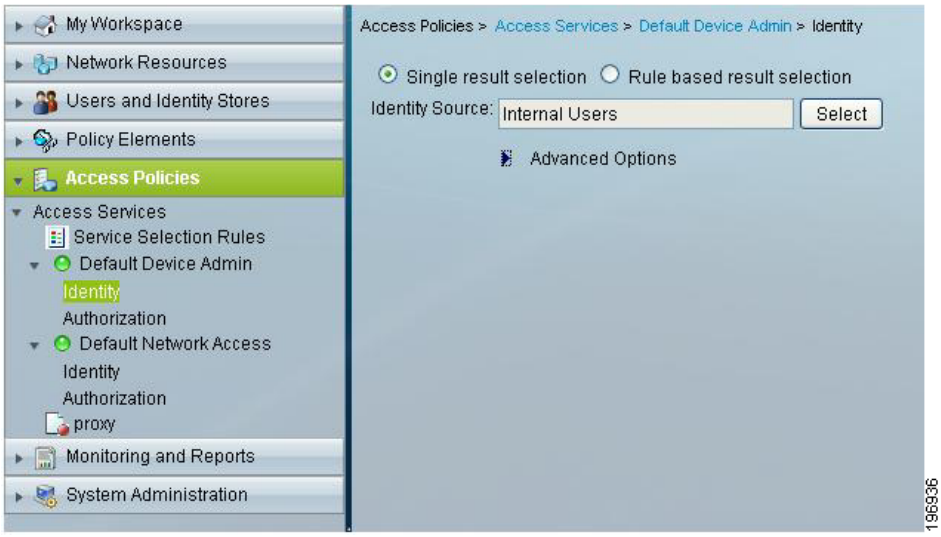
アクセス ポリシーの詳細については、『*User Guide for the Cisco Secure Access Control System*』を参照してください。

移行メモ

- TACACS+ を使用したデバイス管理シナリオでは、事前に設定されたデフォルトのデバイス管理アクセス サービスを更新できます。
  - 内部ユーザのデフォルトの設定が適切でない場合は、ID ポリシーを修正して、ワンタイム パスワードなどの別の ID ストアを使用します。
  - ユーザの認証および認可に複数の ID ストアが必要な場合は、図 2-10 に示すように、ID ストア順序を選択します。

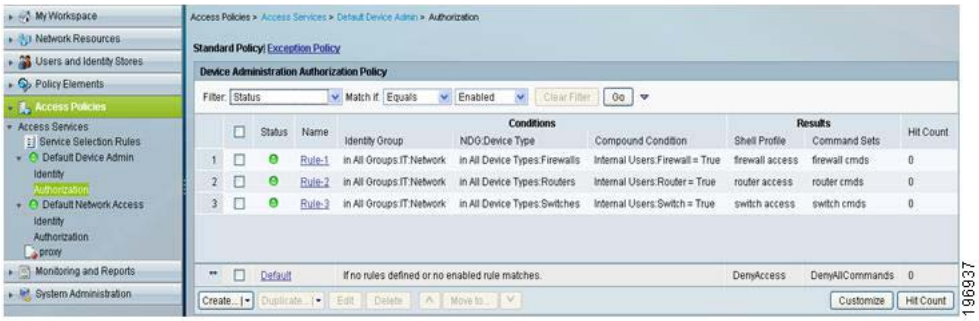
    たとえば、ユーザはワンタイム パスワード サーバに認証されますが、認可のためのユーザ属性の取得に ACS 内部ユーザ ストアが必要なことがあります。場合によっては、ACS は ACS 内部ユーザ ストアおよび Active Directory の両方を確認して、認証対象のユーザを検索する必要があります。

図 2-10　ID ストア順序



- 図 2-11 に示すように、新しいユーザおよびネットワーク デバイス グループ化を利用して認可ポリシーを作成できます。

図 2-11　認可ポリシー

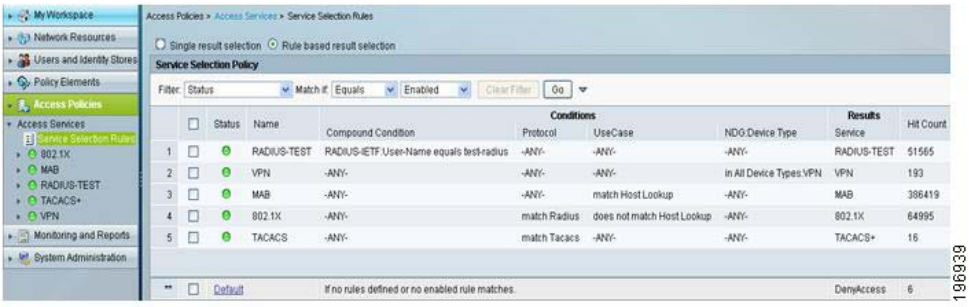


- RADIUS ベースのデバイス管理では、さまざまなアクセス サービスを作成して、サービス セレクション ポリシーのネットワーク アクセス サービスと、これらの認証要求および認可要求を区別します。図 2-12 にサービス セレクション ポリシーを示します。

図 2-12　サービス セレクション ポリシー

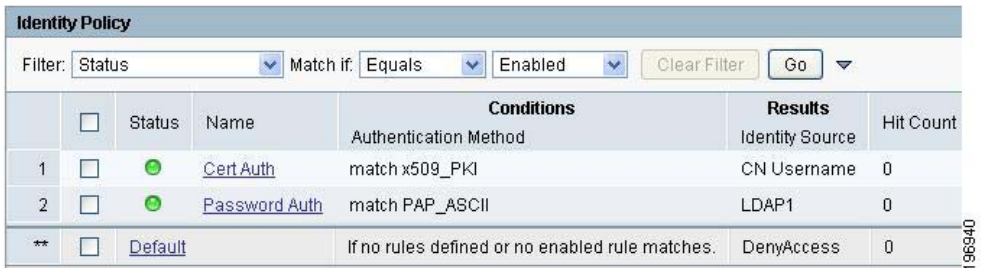
- 単純なネットワーク アクセス シナリオでは、事前に設定されたネットワーク アクセス サービスを更新できます。より複雑なネットワーク アクセス シナリオに対応できるように、図 2-13 に示す追加のアクセス サービスが導入されています。

図 2-13　ネットワーク アクセス サービス規則



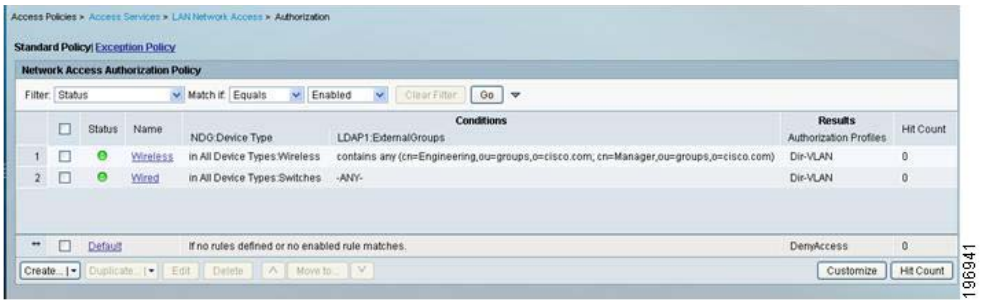
- 証明書ベースおよびパスワードベースの両方の認証に対応するアクセス サービスを作成する場合に使用します。たとえば、証明書ベースのマシン認証、パスワードベースのユーザ認証、規則ベースの ID ポリシーが必要な場合があります（図 2-14 を参照）。

図 2-14　ACS 5.3 の規則ベースの ID ポリシー



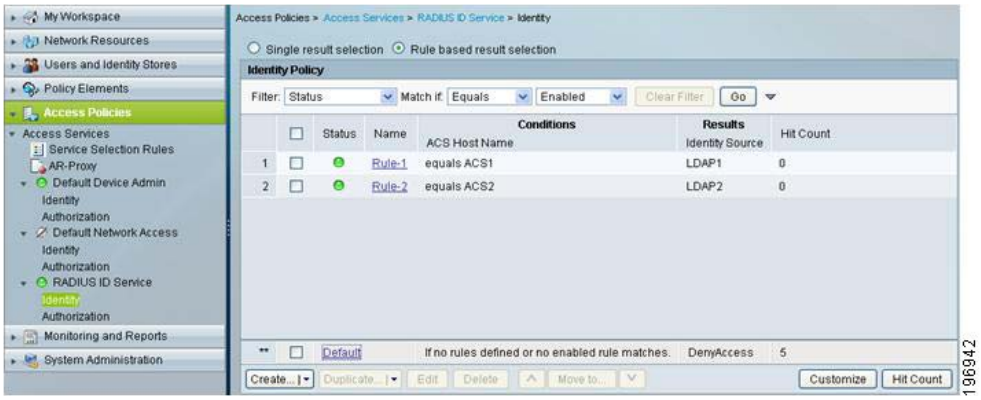
- 最初に ACS グループに外部グループをマッピングするのではなく、認可ポリシーで直接外部グループを使用します。

図 2-15　認可ポリシーで直接外部グループを使用する



- ACS 3.x および 4.x でのサーバ固有の設定を、ACS 5 のサーバベースのポリシーに変換します。図 2-16 に、システム条件の使用方法と、さまざまな LDAP ディレクトリへ要求を送信する ACS ホスト名を示します。

図 2-16　システム条件および ACS ホスト名



システム管理

ACS 5.3 の主な変更として、ACS 5.3 ではシステム管理タスク用に次のような設定領域があります。

- 「管理者」（P.2-16）
- 「ユーザ」（P.2-16）
- 「操作」（P.2-16）
- 「設定」（P.2-16）

- 「ダウンロード」（P.2-16）

管理者

ACS 5.3 の主な変更として、ACS 管理者には、管理者権限を管理する事前定義済みのロールを 10 まで割り当てることができます。

ユーザ

ACS 5.3 の主な変更は次のとおりです。

- 拡張されたパスワード ポリシーを ACS 内部ユーザに適用できます。次の内容が含まれています。
  - さらに複雑なパスワード規則
  - パスワード履歴
- パスワード ライフタイム ポリシーは経過時間だけに基づきます。

操作

ACS 5.3 の主な変更は次のとおりです。

- ACS サーバ ロールをプライマリまたはセカンダリ サーバに割り当てる機能。
- ローカルおよびグローバルのソフトウェア更新を実行する機能。

設定

ACS 5.3 の主な変更は次のとおりです。

- この設定領域は認証プロトコル設定、AAA ディクショナリ、内部ユーザ スキーマの変更、ACS 証明書管理、ロギングの設定、および ACS ライセンス管理に対応しています。次の内容が含まれています。
  - 編集可能な AAA プロトコル ディクショナリ
  - 編集可能な内部ユーザ/ホスト スキーマ
- ACS View のログ コレクタとして ACS を割り当てる機能。

ダウンロード

ACS 5.3 の主な変更は次のとおりです。

- ACS 5.3 は、ACS 4.2 の設定の一部を移行する場合に役立つ移行ツールを提供しています。
- ACS 内部ユーザのパスワード変更アプリケーションを作成する Web サービス インターフェイス。

設定領域では、パスワード変更アプリケーションを作成できるように、ACS 5.3 の移行ユーティリティおよび Web サービス ファイルをダウンロードできるリンクが含まれています。

CHAPTER 3

ACS 5.3 の設定の移行方法

この章では ACS 4.x から 5.3 の移行について説明し、次の項で構成されています。

移行方法

ACS 5.3 設定モデルは ACS 3.x および 4.x と異なります。ACS 3.x および 4.x から ACS 5.3 に直接データと設定を移行することはできません。ACS 5.3 の移行には、手動の再設定が必要になります。ACS 5.3 では、移行プロセス用に次のツールを提供しています。

移行ユーティリティ

移行ユーティリティは ACS 4.x Windows マシンで実行するツールです。このツールを使用して、ACS 4.x バックアップ ファイルをインポートしたり、データを分析したり、データを ACS 5.3 にインポートする前に必要な変更を行ったりすることができます。

移行ユーティリティは、表 3-1 に示す移行をサポートしています。移行ユーティリティは、[System Configuration] > [Downloads] の、ACS 5.3 Web インターフェイスからダウンロードできます。

移行ユーティリティによって、ACS 4.x Windows マシンから ACS 5.3 マシンにデータを移行します。このプロセスは、ACS のバージョン 3.x から 4.x または任意の 4.x アップグレードのアップグレード プロセスと異なります。

アップグレード プロセスでは、ACS 4.x システムは管理サポートを必要とせずに、同じように機能します。移行プロセスでは、ACS 5.3 にデータをインポートする前に、データを統合し、手動で解決する管理サポートが必要となる場合があります。

ACS 5.3 の移行ユーティリティでは、展開内のすべての ACS 4.x サーバを ACS 5.3 に移行する複数インスタンス移行がサポートされています。複数の ACS 4.x インスタンスを区別するため、プレフィクスを追加できます。プレフィクスを使用して、データ要素のサーバ固有 ID を保持し、異なるサーバのオブジェクト名の重複を避けます。

ACS 4.x 展開の移行は、複雑なプロセスで、十分に計画する必要があります。移行を実行する前に、ACS 4.x レプリケーション階層を考慮する必要があります。

たとえば、ある ACS 4.x サーバに、別の ACS 4.x サーバから複製されたデータがある場合、データは同じであるため、これらの両方の ACS サーバから同じデータ セットを移行する必要はありません。そのため、展開内の ACS インスタンスの移行の順序は十分に考慮する必要があります。

CSV インポート ツール

ACS 5.3 では、表 3-1 に示すように、カンマ区切り値（CSV）テキスト ファイルからデータ オブジェクトの一部をインポートできます。Web インターフェイスを使用して、ACS 5.3 のすべてのデータ オブジェクトを手動で設定しない場合は、CSV テキスト ファイルで設定を作成し、設定をインポートできます。

多くのインスタンスで、デバイスやユーザ情報などの ACS 設定データは ACS の外部に保存されています。このデータをテキスト形式でエクスポートして、ACS 5.3 にインポートできます。

CSV インポート ツールの詳細については、『*Software Developer's Guide for the Cisco Secure Access Control System 5.3*』の「Using the Scripting Interface」の章を参照してください。

表 3-1　ACS 5.3 移行ユーティリティとインポート ツールのオプション

ACS 5.3 設定領域	ACS 5.3 移行ユーティリティのサポート	ACS 5.3 インポート ツール
NDG	Yes	Yes
ネットワーク デバイス	Yes	Yes
RADIUS プロキシ サーバ	No	No
内部ユーザ/ホスト	Yes	Yes
ID グループ	Yes	Yes
外部 ID ストア	No	No
ポリシー要素	共有コマンド セット、RAC、共有 DACL	共有コマンド セット、共有 DACL
アクセス ポリシー	No	No
モニタリングとレポート	No	No
システム管理	FAST マスター キー、VSA	No

移行に関する推奨事項

- 小規模の ACS 設定の場合は、手動の設定と CSV インポートを組み合わせて使用します。これは次のような場合です。
  - ユーザを ACS で管理していない
  - ネットワーク デバイス ワイルドカードを使用している
  - ユーザとネットワーク デバイスの情報が CSV テキスト形式で使用できる
- その他の設定では、手動の設定と CSV インポートに加えて ACS 5.3 移行ユーティリティを使用します。

移行ユーティリティについて

移行ユーティリティを使用して、さまざまなタイプのデータを ACS 4.x から ACS 5.3 に移行します。ACS 4.x Windows ソース マシンに加えて、ACS 4.x 移行マシンと ACS 5.3 ターゲット マシンを展開する必要があります。

移行プロセスには次の 2 つのフェーズがあります。

- 分析およびエクスポート
- インポート

移行ユーティリティを ACS 4.x 移行マシンで実行します。移行マシンは ACS 4.x を実行する Windows プラットフォームです。分析フェーズとエクスポート フェーズを別々に複数回実行して、データがインポート フェーズに適切かどうかを確認できます。

分析フェーズに合格したデータはエクスポートして、ACS 5.3 にインポートできます。ACS 5.3 ポリシーの詳細については、『*User Guide for the Cisco Secure Access Control System* 5.3』を参照してください。

リモート デスクトップを使用して、移行マシンに接続し、移行ユーティリティを実行することはできません。移行ユーティリティは移行マシンで実行するか、VNC を使用して移行マシンに接続する必要があります。

（注）　ACS 5.3 移行ユーティリティは、Windows 2008 64 ビットではサポートされません。

移行ユーティリティは ACS 4.x データ要素のサブセットをサポートします。完全なリストについては、表 4-1（P.4-3）の「移行プロセスでサポートされるすべての ACS 要素」を参照してください。

ACS 4.x から 5.3 への移行

ここでは、ACS 4.x から ACS 5.3 の移行に使用する手法について説明します。ここでは、次の内容について説明します。

複数インスタンスの移行

ACS 5.3 には、すべての ACS 4.x インスタンスのデータを保持する 1 つのプライマリ データベースがあります。このプライマリ データベースに各 ACS 4.x インスタンスのデータが移行されます。ACS 4.x では、システム設定全体の個別のサブセットを別々の ACS インスタンスで管理できるように、選択したデータのレプリケーションを定義できます。

ACS 5.3 には、すべての ACS インスタンスに複製される統合データベースが含まれています。統合データベースには、各 ACS 4.x インスタンスのすべてのローカル設定定義が格納されます。

ACS 5.3 の移行フェーズ

ACS 5.3 は 2 フェーズの移行方式に従います。

- 「分析フェーズ」（P.3-4）
- 「移行フェーズ」（P.3-4）

分析フェーズ

このフェーズでは、既存の ACS 4.x 設定の分析が実行されます。可能性のある移行の問題が報告され、解決方法があれば推奨されます。移行ユーティリティを実行する前に、移行マシンに ACS 4.x をインストールし、データを復元する必要があります。

ACS 4.x サーバのバックアップから復元されたデータに対して分析ツールを実行できます。分析ツールを複数回実行して、必要に応じて、移行マシンの ACS 4.x 設定を変更できます。

（注）　分析フェーズとエクスポート フェーズは、移行プロセスの 1 つのフェーズとして実装されます。分析レポートには、分析とエクスポートの両方の情報が含まれます。

移行フェーズ

このフェーズでは、移行ユーティリティは ACS 4.x サーバから設定データを抽出し、ACS 5.3 サーバにインポート可能な形式で移行されるようにデータを準備します。移行ツールには、次のような 1 つ以上のカテゴリでデータを移行するオプションがあります。

- インベントリ データ移行（ユーザ、ネットワーク デバイス、MAC）
- ポリシー データ移行（ネットワーク デバイス グループ、ID グループ、コマンド セット、RAC、VSA、DACL）

データ モデル編成

ACS 5.3 は、ポリシーベースのアクセス コントロール システムです。ACS 5.3 での*ポリシー モデル*という用語は、ポリシー管理者のポリシー要素、ポリシー オブジェクト、およびポリシー規則を表しています。ACS 5.3 では、以前のバージョンで使用されていたグループベースのモデルの代わりに、規則ベース ポリシー モデルが使用されています。

規則ベース ポリシー モデルを使用すると、以前のグループベースの手法よりも強力で柔軟なアクセス コントロールを実現できます。ポリシー モデルの詳細については、『*User Guide for Cisco Secure Access Control System 5.3*』を参照してください。

次に、ACS 5.3 の 3 つの主なデータ モデル関連ポイントを示します。

- 「モデル編成」（P.3-5）
- 「モデル ストレージ」（P.3-5）
- 「レプリケーション モデル」（P.3-5）

モデル編成

ACS 5.3 ではネットワーク アクセス プロファイル（NAP）関連機能が、RADIUS と TACACS+ の両方の完全なポリシーベースの認証、認可、アカウンティング（AAA）ソリューションに拡張されています。

一連の RADIUS 属性などの特定のポリシーと認証情報は、ACS 4.x のように、ユーザまたはグループ レコード内に保存されません。代わりに、返された認証データのすべてのセットが選択されます。

モデル ストレージ

移行プロセスでは、次の基準を満たす ACS 4.x データが対象になります。

- ACS 5.3 モデルに変換できる
- ダイナミックユーザなどの実行時の操作中に生成されないデータから構成される

レプリケーション モデル

ACS 5.3 では、ACS 4.x の複数のデータベース インスタンスを組み合わせて、1 つのデータベースに移行されます。ACS 4.x では、システム設定全体の個別のサブセットを別々の ACS インスタンスで管理できるように、選択したデータのレプリケーションを定義できます。

ACS 5.3 には、すべての ACS インスタンスに複製される統合データベースが含まれています。この統合データベースには、各 ACS 4.x インスタンスのすべてのローカル設定定義が格納されます。

ACS 5.3 データ モデルは、ACS 4.x データ モデルよりはるかに統一性があります。ACS 5.3 データ モデルには、単一のマスター インスタンスが含まれ、ここですべての設定変更が行われます。内在するすべてのセカンダリ インスタンスは、設定の完全なコピーを保持し、設定のすべての変更の更新を受け取ります。

複数インスタンスの移行のサポート

ACS 4.x の複数のインスタンスを ACS 5.3 に移行するには、次の手順を実行します。

ステップ 1　移行する ACS 4.x インスタンスを選択します。

プライマリ ACS 4.x インスタンス（展開に存在する場合）を最初に移行する必要があります。選択した ACS 4.x インスタンスをバックアップします。

ステップ 2　バックアップした ACS 4.x インスタンスを移行マシンに復元します。

ステップ 3　移行プロセスを実行します。

ステップ 4　1 つの ACS 4.x インスタンスの移行プロセスが完了したら、別のインスタンスに進むか、プロセスを終了します。

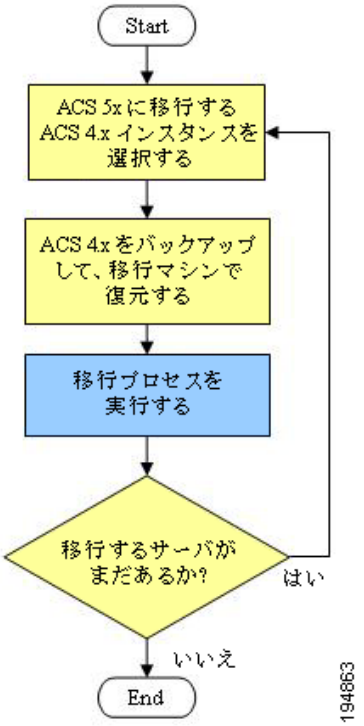
ACS 4.x のインスタンスを復元すると、以前の ACS 4.x インスタンス データが削除されます。

分析およびエクスポート フェーズでは、複数インスタンスに関して変更は行われません。

たとえば、移行ユーティリティは異なる ACS 4.x インスタンス間で重複したオブジェクトを検出しません。複数の ACS 4.x インスタンスに存在する重複した矛盾するデータ オブジェクトは、移行のインポート フェーズで検出され、報告されます。

図 3-1 に複数インスタンスの移行プロセスを示します。

図 3-1　　複数インスタンスの移行プロセス



データの移行

移行プロセスでは、ソース ACS 4.x サーバからデータがエクスポートされ、対応するデータ エンティティがターゲット ACS 5.3 サーバにインポートされます。エクスポート プロセスは稼動中の 4.x サーバでは実行しません。代わりに、ACS 4.x ソース サーバからデータベースをバックアップし、追加の ACS 4.x 移行マシンにデータを復元し、そこで移行ユーティリティを実行する必要があります。

（注）　移行プロセスを開始する前に、ACS 4.x ソース マシンで完全なデータベース バックアップを実行する必要があります。バックアップしたデータを追加の ACS 4.x 移行マシンに復元し、データを ACS 5.3 マシンにインポートする前に問題を修正します。

ACS 4.x データベースのパスワードは 37 文字以内にする必要があります。

データを移行するには、次の手順を実行します。

ステップ 1　ACS 4.x データに対して分析とエクスポートを実行し、AnalyzeAndExport 要約レポートと Analyze and Export 完全レポートを確認します。

「ACS 4.x データの分析およびエクスポート」（P.6-36）を参照してください。このフェーズでは、次の手順を実行します。

- 移行できないデータの問題を特定し、手動の移行の考慮事項を確認します。「移行の問題の解決」（P.D-3）を参照してください。
- 移行の前に修正する問題を特定します。
- 統合するデータを特定します。詳細は「データの統合」（P.6-37）を参照してください。

分析およびエクスポート フェーズに合格したデータのみをエクスポートし、後で ACS 5.3 にインポートできます。

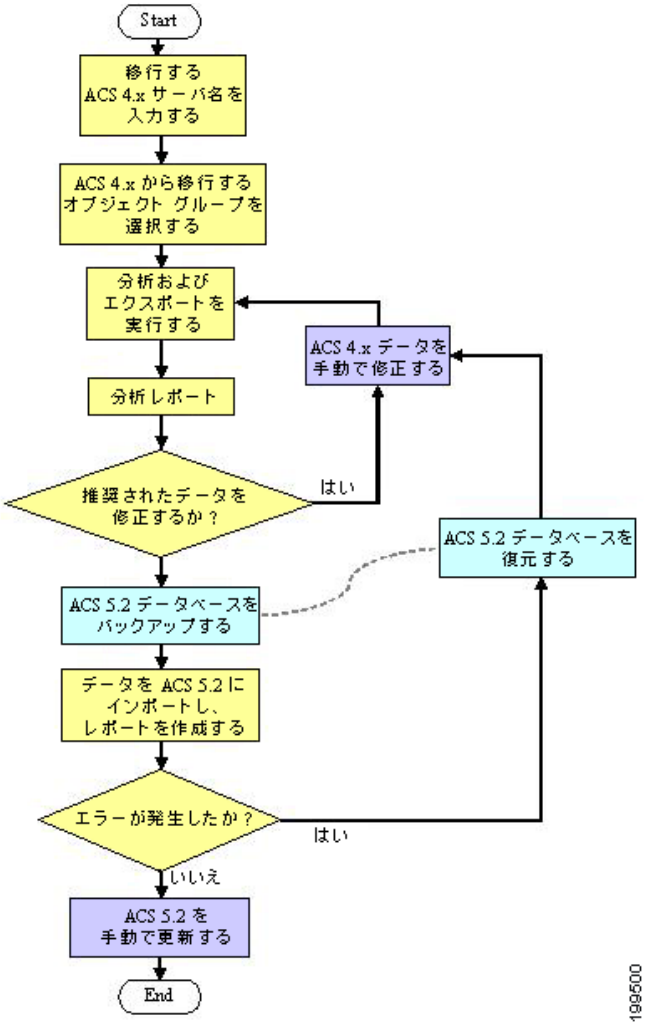
ステップ 2　ACS 5.3 ターゲット マシン データベースをバックアップします。

ステップ 3　ACS 4.x データを ACS 5.3 にインポートし、インポート要約レポートを確認します。

「ACS 5.3 への ACS 4.x データのインポート」（P.6-37）を参照してください。

図 3-2 に移行プロセスを示します。

図 3-2　移行プロセス



オブジェクト グループの選択

完全移行または部分移行の実行を選択できます。部分移行では、移行するオブジェクト グループを選択する必要があります。

オブジェクト グループは、オブジェクト間の依存関係に従って定義されます。アプリケーションでサポートされるオブジェクト タイプのグループか、またはサポートされるすべてのオブジェクト タイプを移行できます。次のオブジェクトのグループから選択できます。

- すべてのオブジェクト：移行プロセスでサポートされているすべての ACS オブジェクト
- すべてのユーザ オブジェクト：ID グループおよびユーザから抽出されたすべてのオブジェクト
- すべてのデバイス オブジェクト：ネットワーク デバイスと NDG
- 共有コマンド セット
- 共有ダウンロード可能アクセス コントロール リスト（DACL）

- マスター キー：Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）マスター キー
- 共有 RADIUS Authorization Components（RAC; RADIUS 認可コンポーネント）および Vendor Specific Attributes（VSA; ベンダー固有属性）

分析およびエクスポート

ACS 4.x の既存の設定を分析し、データ移行の実行の成功に影響する可能性のある移行の問題を特定する必要があります。

このフェーズでは、次のことを特定します。

- 移行できないデータの問題。移行前にこのデータを修正する機会もあります。
- 移行前に修正する問題。
- 統合するデータ。詳細は「データの統合」（P.6-37）を参照してください。

（注）　分析フェーズに合格したデータのみがエクスポートでき、後で ACS 5.3 にインポートされます。

エクスポート プロセスでは、ACS 4.x データの選択した一連のオブジェクトが、インポート プロセス時に処理される外部データ ファイルにエクスポートされます。

エクスポート プロセスでは次の問題が報告されます。

- エクスポートされなかったデータとその理由。
- エクスポートされたデータと統計情報。

インポート

ACS 4.x からのデータ エクスポート ファイルは ACS 5.3 にインポートされます。

インポートは完全なデータベースに対して実行できます。ACS 5.3 データベースを手動でバックアップすることをお勧めします。データのインポート プロセス中に予期しないエラーが発生した場合、データベースのバックアップ バージョンを使用して、システムを復元できます。

複数インスタンスのサポート

複数インスタンスの移行では、すべてのインスタンスが同じ移行マシンに復元され、すべてのインスタンスの結果が保持されます。複数インスタンスのサポートに関連する各データ タイプの特定の変更の詳細については、「ACS 4.x オブジェクトの移行」（P.6-9）を参照してください。

ACS 5.3 の複数インスタンスのサポートには、次の主な機能があります。

- 「重複オブジェクトの報告」（P.3-10）
- 「インスタンスごとのオブジェクト名プレフィクス」（P.3-10）
- 「共有オブジェクトの処理」（P.3-10）

重複オブジェクトの報告

複数の ACS 4.x インスタンスの重複データ オブジェクトはインポート フェーズで検出されます。ほとんどのデータ タイプでは、名前で重複を識別できます。さらに、インポート レポートで、重複オブジェクトに関する情報が報告されます。「ACS 4.x オブジェクトの移行」（P.6-9）を参照してください。

インスタンスごとのオブジェクト名プレフィクス

各 ACS 4.x インスタンスに異なる名前プレフィクスを定義できます。プレフィクスを使用して、データ要素のサーバ固有 ID を保持し、異なるサーバのオブジェクトの名前の重複を避けます。（ACS 4.x インスタンスごとの）移行ユーティリティの各実行の始めに名前のプレフィクスを変更できます。

インスタンス固有のプレフィクスを指定できるため、ACS 4.x インスタンス間の重複に関係なくすべてのデータをインポートできます。グローバル名プレフィクスまたはオブジェクトタイプごとの名前プレフィクスを設定できます。これにより、共有オブジェクト間の関連付けを維持できます。「ACS 4.x オブジェクトの移行」（P.6-9）を参照してください。

共有オブジェクトの処理

NDG、ユーザ属性定義、ユーザ グループなどの ACS 4.x インスタンス間の共有オブジェクトは 1 回だけ移行されます。ただし、複数インスタンスの関連付けのサポートのため、ACS 5.3 データのステータスに従ってオブジェクトの関連付けが作成されます。詳細については、「ACS 4.x オブジェクトの移行」（P.6-9）を参照してください。

たとえば、ユーザ *A* がグループ *BB* に関連づけられており、ユーザもグループも移行されなかった場合、ACS 5.3 で両方のオブジェクトが作成され、関連付けられます。

CHAPTER 4

ACS 5.3 移行ユーティリティのサポート

この章では、次の内容について説明します。

ACS 4.x から 5.3 への移行のバージョンのサポート

次の ACS 4.x バージョンを移行できます。

- ACS 4.1.1.24
- ACS 4.1.4
- ACS 4.2.0.124
- ACS 4.2.1

ACS 4.0 の移行のサポート

データを ACS 5.3 に移行するには、ACS for Windows Server 4.0 を ACS for Windows Server 4.1.1.24 にアップグレードする必要があります。詳細については、『*Installation Guide for Cisco Secure ACS for Windows 4.1*』を参照してください。

ACS 4.x アプライアンスのサポート

Windows ソフトウェア上の ACS 4.x からのみデータを移行できます。ACS 4.x アプライアンスを使用している場合、ACS 4.x 設定をバックアップし、それを復元して、ACS for Windows Server 4.1.1.24 にアップグレードする必要があります。

- アプライアンスのバージョンが ACS 4.1.1.24 の場合、Windows サーバに対応する ACS 4.x バージョンをインストールしてから、アプライアンスのデータを復元する必要があります。
- ACS バージョン 4.1.1.24 以上を使用している場合は、アップグレードする必要はありません。詳細については、『*Installation Guide for Cisco Secure ACS for Windows 4.1*』を参照してください。

CSACS-1120 シリーズ アプライアンスのサポート

CSACS-1120 アプライアンスを使用して、ACS 4.2 または ACS 5.0 をインストールできます。このアプライアンスで ACS 5.3 を実行することもできます。現在 CSACS-1120 アプライアンスに ACS 4.2 がインストールされていて、同じアプライアンスに ACS 5.3 をインストールする場合、ACS 5.3 のインストールに進む前に、まず ACS 4.2 データをバックアップする必要があります。

CSACS-1120 シリーズ アプライアンスで ACS 4.2 から ACS 5.3 にデータを移行するには、次の手順を実行します。

ステップ 1　アプライアンスの ACS 4.2 データをバックアップします。

ステップ 2　中間移行マシンに ACS 4.2 データを復元します。

ステップ 3　アプライアンスに ACS 5.3 をインストールします。

ステップ 4　中間移行マシンから ACS 4.2 オブジェクトを、アプライアンス上にインストールされている ACS 5.3 に移行します。

リモート デスクトップのサポート

移行ユーティリティはリモート デスクトップ接続をサポートしていません。移行ユーティリティは移行マシンで実行するか、VNC を使用して移行マシンに接続する必要があります。

複数インスタンスのサポート

ACS 5.3 では、複数の個別のデータベース インスタンス（4.x）が、1 つの統合データベースに組み合わされます。ACS 4.x では、システム設定全体の個別のサブセットを別々の ACS インスタンスで管理できるように、選択したデータのレプリケーションを定義できますが、ACS 5.3 では、単一の統合データベースが展開内のすべての ACS インスタンスに複製されます。

その結果、プライマリ データベースには、各 ACS 4.x インスタンスのすべてのローカル設定定義が格納されます。

移行プロセスでサポートされているすべての ACS 4.x 要素

表 4-1 に移行ユーティリティでサポートする ACS 4.x 要素および対応する ACS 5.3 要素を示します。

表 4-1　移行プロセスでサポートされるすべての ACS 要素

ACS 4.x 要素	ACS 5.3 要素
AAA クライアント/ネットワーク デバイス	ネットワーク デバイス 詳細は「AAA クライアント/ネットワーク デバイス」（P.6-10）を参照してください。
内部ユーザ	内部ユーザ。詳細は「内部ユーザ」（P.6-16）を参照してください。
ユーザ定義フィールド（Interface Configuration セクション）	ID 属性/内部ユーザ。詳細は「ユーザ グループ」（P.6-23）を参照してください。
ユーザ グループ	ID グループ。詳細は「ユーザ グループ」（P.6-23）を参照してください。
共有シェル コマンド認可セット	コマンド セット。詳細は「共有シェル コマンド認可セット」（P.6-28）を参照してください。
ユーザの T+ Shell Exec 属性	ID 属性/内部ユーザ。詳細は「ユーザ グループ」（P.6-23）を参照してください。
グループの T+ Shell Exec 属性	シェル プロファイル。詳細は「ユーザ グループ ポリシーのコンポーネント」（P.6-25）を参照してください。
ユーザの T+ コマンド認可セット	コマンド セット。詳細は「ユーザ グループ」（P.6-23）を参照してください。
MAC 認証バイパス（MAB）アドレス設定	内部ホスト データベース。詳細は「MAC アドレスと内部ホスト」（P.6-27）を参照してください。
共有ダウンロード可能アクセス コントロール リスト（DACL）	ダウンロード可能 ACL。詳細は「共有 DACL オブジェクト」（P.6-29）を参照してください。
EAP-FAST マスター キー	EAP-FAST マスター キー。詳細は「EAP-Fast マスター キーおよび認証局 ID」（P.6-34）を参照してください。
共有 RADIUS 認可コンポーネント	認可プロファイル。詳細は「共有 RAC」（P.A-5）を参照してください。
顧客のベンダー固有属性	顧客の VSA。詳細は「カスタマー VSA」（P.A-5）を参照してください。

（注）　共有オブジェクトから、またはユーザまたはグループ定義内から、コマンド セットを移行します。シェル プロファイルは、グループ定義内の shell exec パラメータから作成されます。ただし、ユーザ レコードに保存された shell exec パラメータは各ユーザに関連付けられている ID 属性として移行されます。

移行プロセスでサポートされない ACS 4.x 要素

移行ユーティリティは次をサポートしていません。

- グループの DACL
- グループの RADIUS 属性
- Active Directory（AD）設定
- AD グループ マッピング
- Admin アカウント
- 管理ユーザ
- 機関の証明書
- 証明書信頼リスト（CTL）
- 証明書失効リスト（CRL）
- 日付と時刻
- 外部データベース設定
- Generic Lightweight Directory Access Protocol（LDAP）設定
- グループのシェル カスタム属性
- グループの Private Internet Exchange、Adaptive Security Appliance（ASA）、シェル コマンド認可セット
- グループの Network Access Restrictions（NAR; ネットワーク アクセス制限）
- 内部 ID パスワードの適用：Sarbanes-Oxley Act（SOX; サーベンス オクスリー法）
- LDAP グループ マッピング
- ロギングの設定
- マシン アクセス制限（MAR）
- ネットワーク アクセス プロファイル（NAP）
- プロトコル設定（システムおよびグローバル認証）
- プロキシ RADIUS および T+（外部アクセス コントロール サーバの資格情報のみを移行します）
- TACACS+ ディレクトリ
- RADIUS ワンタイム パスワード（OTP）
- RSA OTP
- 共有 NAR
- サーバの証明書
- 共有ネットワーク アクセス フィルタリング（NAF）
- 共有 PIX および ASA コマンド認可セット
- Time-of-Day アクセス設定
- ユーザの PIX/ASA シェル コマンド認可
- ユーザの DACL
- ユーザの NAR
- ユーザの RADIUS 属性

- IP プール
- 最大ユーザ セッション
- ダイヤル イン サポート

移行しない属性の詳細については、『*User Guide for Cisco Secure Access Control Server 4.2*』を参照してください。

ユーザ インターフェイス

ここでは、ACS 5.3 移行ユーティリティのエンド ユーザ インターフェイスについて説明します。

CLI ベースの移行ユーティリティ

ACS 5.3 は CLI ベースの移行ユーティリティをサポートします。移行設定の詳細については、「移行ユーティリティの実行」（P.6-2）を参照してください。

CLI ベースの移行ユーティリティのフェーズ

CLI ベースの移行ユーティリティは次の部分から構成されます。

- 「設定」（P.4-5）
- 「オブジェクト グループの選択」（P.4-5）
- 「操作の選択」（P.4-6）

設定

移行ユーティリティでは、永続的に保存可能なオペレータが設定した設定が使われます。移行ユーティリティを起動するたびに、以前に定義された値を使用するか、新しい値を選択するか求められます。移行設定の詳細については、「移行ユーティリティの実行」（P.6-2）を参照してください。

設定には次の 2 つのタイプがあります。

- ACS 5.3 ID および資格情報 : データの移行先の ACS 5.3 サーバの IP アドレスまたはホスト名。ACS 5.3 サーバにデータをインポートするために使用する管理者ユーザ名とパスワードも指定します。

  移行操作の一意の管理者を定義して、設定レコードの参照中にそれらを識別しやすくすることをお勧めします。移行ユーティリティの実行中は、ACS 5.3 のデフォルトのスーパー管理者アカウント *acsadmin* だけを使用する必要があります。
- 設定オプション：特定のオブジェクト タイプの移行と関連付けられます。設定の適用後、その後のユーティリティの起動時に使用するデフォルトとしてそれらを保存するかどうかを確認するように求められます。

オブジェクト グループの選択

移行ユーティリティでサポートされるオブジェクト タイプのグループか、またはサポートされるすべてのオブジェクト タイプを移行できます。移行手順のさまざまなフェーズの詳細および各オブジェクト タイプの影響と考慮事項については、「ACS 4.x オブジェクトの移行」（P.6-9）を参照してください。

使用可能なオプションを選択する詳細な手順については、「移行ユーティリティの実行」（P.6-2）を参照してください。

次のオブジェクトのグループから選択できます。

- すべてのオブジェクト：すべての ACS オブジェクト
- すべてのユーザ オブジェクト：ID グループおよびユーザから抽出されたすべてのオブジェクト
- すべてのデバイス オブジェクト：ネットワーク デバイスと NDG
- 共有コマンド セット
- 共有 DACL
- マスター キー：EAP-FAST マスター キー
- 共有 RAC および VSA

操作の選択

一連のオブジェクト タイプを選択したら、実行する移行フェーズを選択する必要があります。次のオプションを使用できます。

- 分析およびエクスポート
- インポート

オプションの選択後、対応するプロセスが実行され、関連レポートが画面に表示されます。各操作について、2 つのタイプのレポートが表示されます。

- 要約
- 詳細

移行のさまざまなフェーズで生成されるレポートの詳細については、「レポートの印刷とレポート タイプ」（P.6-40）を参照してください。

CHAPTER 5

移行ユーティリティのセットアップとインストール

この章は、移行プロセスにおける各マシンの移行の考慮事項について説明し、次の項で構成されています。

移行のインストール前の考慮事項

始める前に、移行のための環境が設定されていることを確認します。ACS 4.x Windows ソース マシンに加えて、ACS 4.x 移行マシンと ACS 5.3 ターゲット マシンを展開する必要があります。次の考慮事項に注意します。

- ACS 4.x データベースにデータベース破損の問題が発生していないことを確認します。
- ACS 4.x 移行マシンを単一の IP アドレスで設定していることを確認します。1 つのインターフェイスに複数の IP アドレス エイリアスを持つ移行マシンでは移行が失敗します。
- ACS 4.x Windows ソース マシンで完全なデータベースのバックアップを実行します。このマシンを使用して、ACS 4.x データを保持します。バックアップ データを追加の ACS 4.x 移行マシンに復元して、データを ACS 5.3 マシンにインポートする前に問題を修正します。

  データベースのバックアップ手順については、『*Installation Guide for Cisco Secure ACS for Windows 4.1*』を参照してください。
- 移行マシンはソース マシンと同じ 4.x バージョンを使用している必要があります。4.x Windows ソース マシン上で移行する ACS 4.x バージョンをバックアップし、移行マシンで同じ 4.x バージョンを復元する必要があります。移行マシンがソース マシンと同じ 4.x バージョンを使用していない場合、復元が失敗します。

  『*Installation Guide for Cisco Secure ACS for Windows 4.1*』を参照してください。
- ACS 4.x Windows ソース マシンからデータを移行マシンに復元します。移行マシンは ACS 4.x を実行する Windows プラットフォームです。このマシンは移行目的のみに使用してください。移行マシンにはアプライアンス マシンを指定できません。

（注）　ACS 4.x データを変更する場合、移行マシンを使用します。

- ACS 5.3 ターゲット マシンで完全なデータベースのバックアップを実行します。このマシンを使用して、インポートされたデータを処理します。データベースのバックアップ手順については、『*Command Line Interface Reference Guide for the Cisco Secure Access Control System 5.3*』を参照してください。
- 次のことを確認します。
  - ターゲット マシンに ACS 5.3 をインストールしている。
  - 互換性のある ACS 5.3 ライセンスを使用している。
  - 移行マシンと ACS 5.3 サーバ間にネットワーク接続を確立している。
- インポート フェーズを実行する前に、ACS 5.3 データベースをバックアップします。
- ACS 5.3 サーバで移行インターフェイスをイネーブルにします。移行インターフェイスをイネーブルにし、移行ユーティリティを実行する方法の詳細については、第 6 章「移行ユーティリティを使用した、ACS 4.x から ACS 5.3 へのデータ移行」を参照してください。

システム要件

ACS マシンは表 5-1 に説明するシステム要件を満たしている必要があります。すべてのマニュアルは Cisco.com で入手できます。

表 5-1　移行マシンのシステム要件

プラットフォーム	要件
ACS 4.x ソース マシン	『*Installation Guide for Cisco Secure ACS for Windows 4.1*』を参照してください。
ACS 4.x 移行マシン	『*Installation Guide for Cisco Secure ACS for Windows 4.1*』を参照してください。 マシンには 2 GB のメモリが必要です。 ACS 4.x 移行マシンを単一の IP アドレスで設定していることを確認します。1 つのインターフェイスに複数の IP アドレス エイリアスを持つ移行マシンでは移行が失敗します。
ACS 5.3 ターゲット マシン	次を参照してください。 • 『*Installation and Setup Guide for ACS 5.3*』 • 『*Cisco Application Deployment Engine (ADE) 1010 and 2120 Series Appliance Hardware Installation Guide*』 • 『*Cisco Application Deployment Engine (ADE) 2130 and 2140 Series Appliance Hardware Installation Guide*』

ACS ソフトウェア アクセサリ キット DVD

表 5-2 に ACS ソフトウェア アクセサリ キット DVD について説明します。

表 5-2　ACS ソフトウェア アクセサリ キット DVD

DVD	説明	部品番号
Cisco Secure Access Control System - Installation and Recovery DVD, Version 5.3	この DVD を使用して、次のことを行います。 • ACS 5.3_ISO イメージ • アプリケーション アップグレード バンドル • VMware のインストール。 • ACS 5.3 アプライアンスの復旧 • パスワードのリセット	80-10127-01
Cisco Secure Access Control System - Upgrade and Migration DVD, Version 5.3	この DVD を使用して、次のことを行います。 • ACS 5.1 アップグレード パッケージ（5.0 から 5.1 へのアップグレード） • ACS 5.3 アップグレード バンドル（5.1/5.2 から 5.3 へのアップグレード） • 次のいずれかの ACS バージョンを実行している場合に移行ユーティリティをインストールする。 – 4.1.1.24 – 4.1.4 – 4.2 • 移行の前にサーバを ACS 4.1.1 にアップグレードする。 • マニュアル – ACS 5.3 CLI Reference Guide.pdf – ACS 5.3 Installation and Upgrade Guide.pdf – ACS 5.3 License and Documentation Guide.pdf – ACS 5.3 Migration Guide.pdf – ACS 5.3 RCSI.pdf – ACS 5.3 Software Developer's Guide.pdf – ACS 5.3 User Guide.pdf	80-10128-01

ACS 4.x から ACS 5.x への移行は、ソフトウェア バージョン ACS 4.x だけからサポートされます。

ACS 4.x アプライアンス バージョンから移行するには、次の手順を実行します。

ステップ 1　ACS 4.x アプライアンスのサポートされるいずれかのバージョンからバックアップを作成します。

ステップ 2　サポートされている同じ ACS4.x ソフトウェア バージョンでアプライアンス バックアップを復旧します。

ステップ 3　移行ユーティリティを実行します。

セキュリティ上の留意事項

移行プロセスのエクスポート フェーズでは、インポート プロセスの入力として使用されるデータ ファイルが作成されます。データ ファイルの内容は暗号化され、直接読み取ることはできません。

データを ACS 5.3 にインポートするには、ACS 管理者ユーザ名およびパスワードが必要です。インポート ユーティリティによって作成されたレコードを監査ログ内で識別できるように、予約済みユーザ名を使用する必要があります。

移行ユーティリティへのアクセス

移行ユーティリティにアクセスするには、ACS 5.3 Web インターフェイスからダウンロードします。

移行アプリケーション ファイルをダウンロードするには、次の手順を実行します。

ステップ 1　[System Administration] > [Downloads] > [Migration Utility] を選択します。

[Migration from 4.x] ページが表示されます。

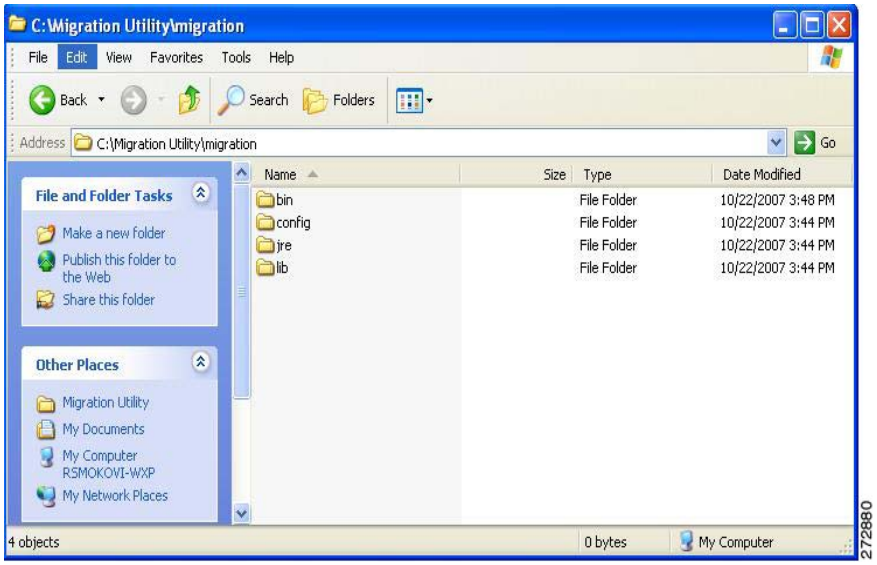
ステップ 2　[Migration application files] をクリックして、移行ユーティリティを実行する場合に使用するアプリケーション ファイルが格納されている *migration.zip* をダウンロードします。

移行ソフトウェア アクセサリ キットから入手できる Cisco Secure Access Control System - Installation and Recovery DVD, Version 5.3 を使用して、*migration.zip* ファイルをダウンロードすることもできます。

移行ユーティリティのパッケージ

zip ファイル *migration.zip* には移行ユーティリティ ファイルが格納されています。このファイルを移行ディレクトリに解凍します。このマニュアルでは、図 5-1 に示す移行ディレクトリ構造を使用しています。

図 5-1　移行ユーティリティ ディレクトリ構造



データの移行および展開のシナリオ

移行ユーティリティによって、ACS 4.x オブジェクトが ACS 5.3 に移行されます。単一の ACS アプライアンスのデータ移行のプロセスは、分散環境での ACS アプライアンスの移行と異なります。ここでは、次の内容について説明します。

- 「単一の ACS サーバでのデータ移行のガイドライン」（P.5-5）
- 「分散環境におけるデータ移行のガイドライン」（P.5-5）

単一の ACS サーバでのデータ移行のガイドライン

環境内に単一の ACS アプライアンスがある（または複数の ACS アプライアンスがあるが、分散されたセットアップでない）場合、このガイドで説明するように、ACS アプライアンスに対して移行ユーティリティを実行します。

移行が完了したことを確認する手順については、「インポートの検証」（P.6-45）を参照してください。

分散環境におけるデータ移行のガイドライン

分散環境（たとえば、1 台のプライマリ ACS アプライアンスと、プライマリ ACS と相互運用する 1 台以上のセカンダリ ACS アプライアンス）で ACS を実行する場合、次の手順を実行する必要があります。

ステップ 1　プライマリ ACS アプライアンスをバックアップし、移行マシンにそれを復元します。

ステップ 2　プライマリ ACS アプライアンスに対して移行ユーティリティを実行します。

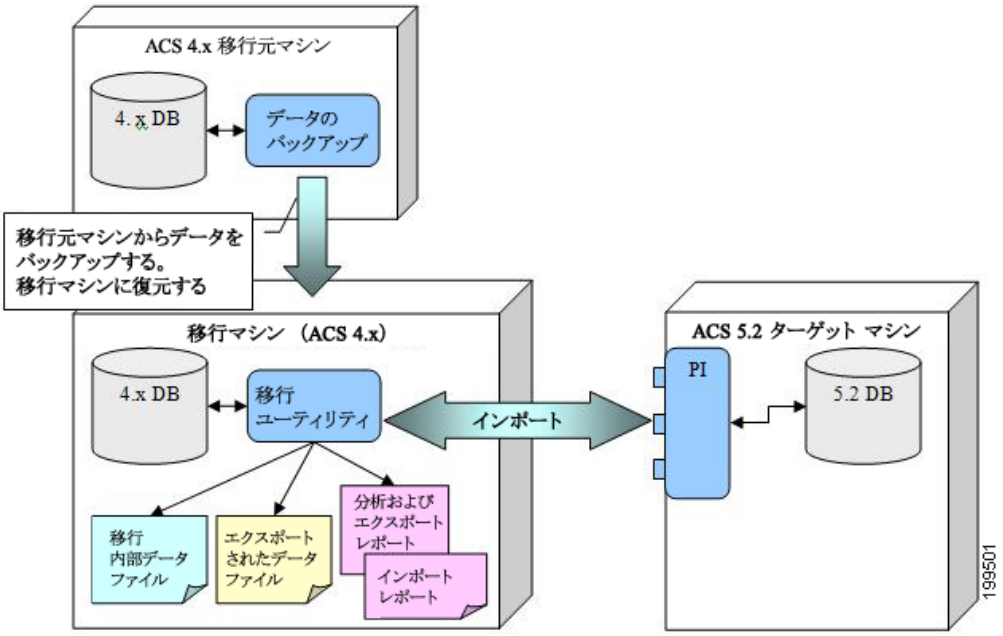
大規模な内部データベースがある場合、ACS 4.x からの移行は、複数のセカンダリ アプライアンスに接続されている ACS 5.3 プライマリ サーバではなく、スタンドアロンのプライマリ サーバに対して実行することをお勧めします。移行プロセスの完了後に、すべてのセカンダリを登録できます。

移行ユーティリティは 300,000 ユーザ、50,000 デバイス、および 50,000 MAB の移行に約 15 時間かかります。ACS 5.3 を再起動すると、起動プロセスは ACS 5.3 が使用できるようになるまでに、約 15 分かかります。400,000 ユーザと 200,000 デバイスを超えるデータ移行の ACS 5.3 の動作は不明です。

プラットフォーム間のデータ移行

図 5-2 にプラットフォーム間のデータ移行を示します。第 6 章「移行ユーティリティを使用した、ACS 4.x から ACS 5.3 へのデータ移行」を参照してください。

図 5-2　　プラットフォーム間の移行フロー



CHAPTER 6

移行ユーティリティを使用した、ACS 4.x から ACS 5.3 へのデータ移行

この章では、ACS 4.x から ACS 5.3 にデータを移行する方法を説明します。

概要

この章では、ACS 4.x から ACS 5.3 にデータを移行する方法を説明します。開始する前に、第 5 章「移行ユーティリティのセットアップとインストール」に記載されているセットアップ、バックアップ、インストールの手順に従う必要があります。

移行を開始する前に、ACS 5.3 サーバで移行インターフェイスがイネーブルになっていることを確認してください。

コマンドライン インターフェイスから、次のように入力します。

```
acs config-web-interface migration enable
```

ACS 5.3 サーバで移行インターフェイスがイネーブルになっていることを確認するには、コマンドライン インターフェイスから次のように入力します。

```
show acs-config-web-interface
```

詳細については、『*Command Line Interface Reference Guide for the Cisco Secure Access Control System 5.3*』を参照してください。

移行ユーティリティの実行

移行ユーティリティを実行するには、次の手順を実行します。

ステップ 1　コマンド プロンプトを開き、ディレクトリを `C:\Migration Utility\migration\bin` に変更します。

移行ユーティリティをインストールするディレクトリを指定できます。この例では、移行ユーティリティをルート ディレクトリとして使用します。

ステップ 2　コマンド プロンプトに、`migration.bat` と入力します。

例 6-1 に、移行ユーティリティの実行時に表示されるプロンプトを示します。

例 6-1　　移行スクリプト（ユーザ入力）

```
Copyright (c) 2008-2009 Cisco Systems, Inc.
All rights reserved.
--------------------------------------------------------------------------------
This utility migrates data from ACS 4.x to ACS 5. You can migrate directly from the
following ACS versions:

- ACS 4.1.1.24
- ACS 4.1.4
- ACS 4.2.0.124
- ACS 4.2.1

Data migration involves the following:
a. The migration utility analyzes the ACS 4.x data, exports any data from ACS 4.x that can
be migrated automatically, and imports the data into ACS 5.
b. Before the import stage, you can manually consolidate and resolve data according to the
analysis report, to maximize the amount of data that the utility can migrate.
c. After migration, use the imported data to recreate your policies in ACS 5.
--------------------------------------------------------------------------------

Make sure that the database is running.
Enter ACS 5 IP address or hostname:[nn.nn.nnn.nnn]
Enter ACS 5 administrator username:[test]
Enter ACS 5 password:
Change user preferences?[no]
yes

User Groups
--------------------------------------------------------------------------------
Existing user groups will be migrated to the Identity Group.
Enter new Root name:[Migrated Group]

Network Device Groups
--------------------------------------------------------------------------------

Existing network device groups will be migrated to the Network Device Group.
Enter new Root name:[Migrated NDGs]

Consolidation Prefix
--------------------------------------------------------------------------------
Identical objects found will be consolidated into one object.
Enter a prefix to add to the consolidated object:[cons]

Users
--------------------------------------------------------------------------------
```

```
ACS 5 supports authentication for internal users against the internal database only.
ACS 4.x users who were configured to use an external database for authentication will be
migrated with a default authentication password.
Specify a default password.

Disabled Group Users
--------------------------------------------------------------------------------
ACS 4.x users and hosts that are associated with disabled groups will be migrated as
disabled:[yes]


Configure these users as disabled in ACS 5, or ask for a change of password on a user's
first attempt to access ACS 5.
Select the option:
1 - DisableExternalUser
2 - SetPasswordChange
Selected option:[2]
2

Network Devices
--------------------------------------------------------------------------------
TACACS+ and RADIUS network devices with same IP address will be unified.
Select a name to be used for unified devices.
1 - RADIUSName
2 - TACACSName
3 - CombinedName
Selected option:[3]

DACL name construction
--------------------------------------------------------------------------------
Existing downloadable ACL will be migrated.
Select a name to be used for the migrated DACL
1 - DaclName_AclName
2 - AclName
Selected option:[1]

Save user defaults? [yes]
yes

Enter ACS 4.x Server ID:
acs1

Add server-specific migration prefixes?[no]
yes

You can add a global prefix to all migrated objects from this server.
Enter a global prefix:[]
s1

Use special prefixes for specific object types?[no]
yes

** To input an empty prefix, enter the keyword EMPTY.

User Attributes Prefix: You can add an additional prefix to the user attributes.
Enter a prefix to add to these objects:[s1]

Network Device Prefix: You can add an additional prefix to the network devices names.
Enter a prefix to add to these objects:[s1]

Users Command Set Prefix: Extracted command sets are migrated to a shared named object
with an optional prefix.
Enter a prefix to add to these objects:[s1]
```

```
Groups Command Set Prefix: Extracted command sets will be given the group name with an
optional prefix.
Enter a prefix to add to these objects:[s1]

Groups Shell Exec Prefix: Extracted shell profile will be given the group name with an
optional prefix.
Enter a prefix to add to these objects:[s1]

Shared Command Sets Prefix: Extracted command sets are migrated to a shared named object
with an optional prefix.
Enter a prefix to add to these objects:[s1]

Shared Downloadable ACL Prefix: Extracted Downloadable ACL will be given a name with an
optional prefix.
Enter the prefix to add to such objects:[s1]

RAC Prefix: Existing RAC will be migrated with an optional prefix.
Enter the prefix to add to such objects:[s1]

User Groups Root Prefix: You can add a prefix to the user groups root.
Enter a prefix to add to the user groups root:[s1

Network Device Groups Root Prefix: You can add a prefix to the network device groups root.
Enter a prefix to add to the network device groups root:[s1]

Save server migration prefixes?[yes]
yes

Show full report on screen?[yes]
yes

--------------------------------------------------------------------------------

Select the ACS 4.x Configuration groups to be migrated:[1]
1 - ALLObjects
2 - AllUsersObjects
3 - AllDevicesObjects
4 - SharedCommandSet
5 - SharedDACLObject
6 - MasterKeys
7 - SharedRACObjectWithVSA
--------------------------------------------------------------------------------

6
--------------------------------------------------------------------------------

The following object types will be extracted:
--------------------------------------------------------------------------------

EAP FAST - Master Keys
--------------------------------------------------------------------------------

Choose one of the following:
1 - AnalyzeAndExport
2 - Import
3 - CreateReportFiles
4 - Exit
--------------------------------------------------------------------------------

4
--------------------------------------------------------------------------------
```

```
Would you like to migrate another ACS4.x server? [no]
yes

--------------------------------------------------------------------------------
Enter ACS 4.x Sever ID:
```

移行スクリプト セクション

移行スクリプトは、次のセクションで構成されます。

- 移行環境情報。表 6-1（P.6-5）を参照してください。
- 移行ユーザ プリファレンス。表 6-2（P.6-6）を参照してください。
- 移行グループ。表 6-3（P.6-8）を参照してください。
- 移行フェーズ。表 6-4（P.6-9）を参照してください。

表 6-1　移行スクリプト環境情報。

スクリプトの要素	説明
`Use saved user defaults?[yes]`	このプロンプトは、移行ユーティリティを再実行して複数のインスタンスを移行する場合に表示されます。デフォルトは yes です。ACS 5.3 ターゲット マシンに別の IP アドレスおよび資格情報を入力する場合は、**no** と入力します。
`Make sure that the database is running.`	情報メッセージ。次の内容を確認してください。 • ACS 4.x サービスがアクティブになっていること。 • ACS 4.x 移行元マシンでデータベースをバックアップしていること。 • IP アドレス接続を設定していること。 • ACS 4.x 移行マシンから ACS 5.3 ターゲット マシンにアクセスできること。Web インターフェイスにアクセスして、ACS 5.3 マシンが使用可能であることを確認してください。 次のコマンドの実行後に移行インターフェイスがイネーブルになっていること `acs config-web-interface migration enable`
`Enter ACS 5 IP address or hostname:[nn.nn.nnn.nnn]`	ACS 5.3 ターゲット マシンの IP アドレスまたはホスト名を入力します。ACS 4.x データを ACS 5.3 ターゲット マシンに移行します。
`Enter ACS 5 administrator username:[test]`	ACS 5.3 ターゲット マシンのユーザ名を入力します。ACS 5.3 では、管理ユーザだけがサポートされます。 ACS 5.3 では、デフォルトのスーパー管理者アカウント *acsadmin* だけがサポートされ、手動によるユーザの介入はサポートされません。
`Enter ACS 5 password:`	ACS 5.3 ターゲット マシンのパスワードを入力します。
`Change user preferences?[no]` `yes`	デフォルト値は **no** です。 • 定義済みの値を保持するには、**no** と入力します。移行ユーティリティを再実行する場合、これらは UseDefaults 値になります。 • ユーザ プリファレンスを変更するには、**yes** と入力します。

表 6-2　移行スクリプト ユーザ プリファレンス

スクリプトの要素	説明
User Groups Existing user groups will be migrated to the Identity Group Enter new Root name:[Migrated Group]	ID グループのデフォルト名は *Migrated Group* です。たとえば、ユーザ *acs_3* は ID グループ *All Groups:Migrated Group:ACS_Migrate 2* に属しています。新しい名前を入力して、**Enter** を押すと、デフォルト名が変更されます。
Network Device Groups Existing network device groups will be migrated to the Network Device Group. Enter new Root name:[Migrated NDGs]	ネットワーク デバイス グループ（NDG）のデフォルト名は *Migrated NDGs* です。新しい名前を入力して、**Enter** を押すと、デフォルト名が変更されます。
Consolidation Prefix Identical objects found will be consolidated into one object. Enter a prefix to add to the consolidated object:[cons]	統合されたオブジェクトに追加するプレフィクスを入力します。
Users ACS 5 supports authentication for internal users against the internal database only. ACS 4.x users who were configured to use an external database for authentication will be migrated with a default authentication password. Specify a default password.	ユーザ オブジェクトの外部ユーザのデフォルト パスワードです。新しいパスワードを入力して、**Enter** を押すと、デフォルトのパスワードが変更されます。 ACS 5.3 では、内部データベースに対してだけ、内部ユーザの認証がサポートされます。認証に外部データベースを使用していた ACS 4.x ユーザは、デフォルトの認証パスワードで移行されます。 ACS 5.3 では、デフォルトのパスワードを設定することができます。
Disabled Group Users ACS 4.x users and hosts that are associated with disabled group will be migrated as disabled:[yes]	ディセーブルになっているユーザ グループに関連付けられたユーザおよびホストは、1 つのグループの下にディセーブルとして移行されます。
Configure these users as disabled in ACS 5, or ask for a change of password on a user's first attempt to access ACS 5. Select the option: 1 - DisableExternalUser 2 - SetPasswordChange Selected option:[2]	外部データベースで認証された ACS 4.x ユーザは、スタティック パスワードの内部ユーザとして移行されます。 • 外部ユーザをディセーブルにするには、オプション 1 を選択します。 • 移行された外部ユーザのパスワードを変更するには、オプション 2 を選択します。
Network Devices TACACS+ and RADIUS network devices with same IP address will be unified. Select the name to be used for unified devices. 1 - RADIUSName 2 - TACACSName 3 - CombinedName Selected option:[3]	同じ IP アドレスの TACACS+ および RADIUS ネットワーク デバイスを組み合わせて 1 つの名前にします。 たとえば、TACACS+ ネットワーク デバイス名が *MyTacacsDev* で、RADIUS ネットワーク デバイスが *RadiusDev* の場合、組み合わせた名前 *MyTacacsDev_MyRadiusDev* を作成するには、オプション 3 を選択します。
DACL name construction Existing downloadable ACL will be migrated. Select the name to be used for the migrated DACL 1 - DaclName_AclName 2 - AclName Selected option:[1]	移行された ACS 4.x DACL に使用する命名規則を選択します。 1：DACL_ACL 名 2：ACL 名
Save user deafults?[yes]	デフォルト値は **yes** です。このセッションで使用した設定を保持しない場合は、**no** と入力します。

表 6-2　移行スクリプト ユーザ プリファレンス （続き）

スクリプトの要素	説明
`Enter ACS 4.x Server ID:`	データの移行元の ACS 4.x サーバ ID を入力します。
`Add server specific migration prefixes?[no]`	デフォルトは **no** です。**yes** と入力して、各 4.x サーバ名にプレフィクスを追加します。

`You can add a global prefix to all migrated objects from this server.`
`Enter a global prefix:[]`
`s1`
	特定のサーバから移行されるすべてのオブジェクトに追加するプレフィクスを入力します。

`Use special prefixes for specific object types?[no]`
`yes`
`** To input an empty prefix, enter the keyword EMPTY.`
	デフォルトは **no** です。これによって、移行されるすべてのオブジェクト タイプにグローバル プレフィクスが追加されます。移行する特定のオブジェクト タイプに特定のプレフィクスを追加する場合は、**yes** と入力します。

`User Attributes Prefix: You can add an additional prefix to the user attributes.` `Enter a prefix to add to these objects:[s1]`	デフォルトはグローバル プレフィクスに入力される値です。移行するすべてのユーザ属性に特別なプレフィクスを追加する場合は、プレフィクスを入力します。
`Network Device Prefix: You can add an additional prefix to the network devices names.` `Enter a prefix to add to these objects:[s1]`	デフォルトはグローバル プレフィクスに入力される値です。移行するすべてのネットワーク デバイスに特別なプレフィクスを追加する場合は、プレフィクスを入力します。
`Users Command Set Prefix: Extracted command sets are migrated to a shared named object with an optional prefix.` `Enter a prefix to add to these objects:[s1]`	デフォルトはグローバル プレフィクスに入力される値です。移行するすべてのユーザ コマンド セットに特別なプレフィクスを追加する場合は、プレフィクスを入力します。
`Groups Command Set Prefix: Extracted command sets will be given the group name with an optional prefix.` `Enter a prefix to add to these objects:[s1]`	デフォルトはグローバル プレフィクスに入力される値です。移行するすべてのグループ コマンド セットに特別なプレフィクスを追加する場合は、プレフィクスを入力します。
`Groups Shell Exec Prefix: Extracted shell profile will be given the group name with an optional prefix.` `Enter a prefix to add to these objects:[s1]`	デフォルトはグローバル プレフィクスに入力される値です。移行するすべてのグループ Shell Exec に特別なプレフィクスを追加する場合は、プレフィクスを入力します。
`Shared Command Sets Prefix: Extracted command sets are migrated to a shared named object with an optional prefix.` `Enter a prefix to add to these objects:[s1]`	デフォルトはグローバル プレフィクスに入力される値です。移行するすべての共有コマンド セットに特別なプレフィクスを追加する場合は、プレフィクスを入力します。
`Shared Downloadable ACL Prefix: Extracted Downloadable ACL will be given a name with an optional prefix.` `Enter the prefix to add to such objects:[s1]`	デフォルトはグローバル プレフィクスに入力される値です。移行するすべての共有ダウンロード可能 ACL に特別なプレフィクスを追加する場合は、プレフィクスを入力します。
`RAC Prefix: Existing RAC will be migrated with an optional prefix.` `Enter the prefix to add to such objects:[s1]`	デフォルトはグローバル プレフィクスに入力される値です。移行するすべての RAC に特別なプレフィクスを追加する場合は、プレフィクスを入力します。
`User Groups Root Prefix: You can add a prefix to the user groups root.` `Enter a prefix to add to the user groups root:[s1]`	デフォルトはグローバル プレフィクスに入力される値です。移行するすべてのユーザ グループ ルートに特別なプレフィクスを追加する場合は、プレフィクスを入力します。
`Network Device Groups Root Prefix: You can add a prefix to the network device groups root.` `Enter a prefix to add to the network device groups root:[s1]`	デフォルトはグローバル プレフィクスに入力される値です。移行するすべてのネットワーク デバイス グループ ルートに特別なプレフィクスを追加する場合は、プレフィクスを入力します。
`Save server migration prefixes?[yes]`	デフォルトは **yes** です。サーバ移行プレフィクスを保存しない場合は、**no** と入力します。

表 6-2　移行スクリプト ユーザ プリファレンス （続き）

スクリプトの要素	説明
`Show full report on screen?[yes]`	デフォルト値は **yes** です。画面上にログ情報を表示しない場合は、**no** と入力します。
`Update RADIUS dictionary cache?[no]`	現在の ACS 5.3 RADIUS ディレクトリをキャッシュするために使用されます。すでに ACS 5.3 に移行されて削除されたベンダーを移行する場合、RADIUS ディレクトリ キャッシュを更新する必要があります。 更新しないと、そのベンダーが移行されずに拒否され、すでに存在していることを示すメッセージが表示されます。

表 6-3　移行スクリプト オブジェクト グループ

スクリプトの要素	説明

`Select the ACS 4.x Configuration groups to be migrated:`
`1 - ALLObjects`
`2 - AllUsersObjects`
`3 - AllDevicesObjects`
`4 - SharedCommandSet`
`5 - SharedDACLObject`
`6 - MasterKeys`
`7 - SharedRACObjectsWithVSA`
 	
`The following object types will be extracted:`
 	
`User Attributes`
`User Attribute Values`
`Network Device Groups`
`User Groups`
`Groups Shell Exec`
`Groups Command Set`
`Users Shell Exec`
`Users Command Set`
`Shared Command Sets`
`Network Devices`
`Users`
`Shared Downloadable ACL`
`EAP FAST - Master Keys`
`MAB`
`RAC`
`VSA Vendors`
`VSA`
	移行する ACS 要素。次のいずれかのオプションを選択して、移行する ACS 4.x 要素に対して各フェーズを実行します。
	1. ALLObjects。サポートされる ACS オブジェクトに対して各移行フェーズを実行できます。
	2. AllUsersObjects。ユーザ オブジェクトに対して各移行フェーズを実行できます。
	3. AllDevicesObjects。デバイス オブジェクトに対して各移行フェーズを実行できます。
	4. SharedCommandSet。共有コマンド セット オブジェクトに対して各移行フェーズを実行できます。
	5. SharedDACLObject。共有 DACL オブジェクトに対して各移行フェーズを実行できます。
	6. MasterKeys。マスターキー オブジェクトに対して各移行フェーズを実行できます。
	7. SharedRACObjectsWithVSA。共有 RAC オブジェクトおよび VSA に対して各移行フェーズを実行できます。

表 6-4　移行スクリプト フェーズ

スクリプトの要素	説明

`Choose one of the following:`
`1 - AnalyzeAndExport`
`2 - Import`
`3 - CreateReportFiles`
`4 - Exit`
	移行ユーティリティ オプションは次のとおりです。
	• AnalyzeAndExport：ACS 4.x データを分析してエクスポートするには、オプション 1 を選択します。これは反復的なプロセスです。データを分析し、修正し、分析フェーズを再実行して、結果を確認することができます。
	データが分析フェーズに合格した場合、後でエクスポートして ACS 5.3 にインポートできます。「ACS 4.x オブジェクトの移行」（P.6-9）を参照してください。
	必ず ACS 5.3 データベースをバックアップしてください。
	• Import：外部データ ファイルから ACS 4.x データをインポートするには、オプション 2 を選択します。移行プロセスでデータ エクスポート ファイルが作成された後、データが ACS 5.3 にインポートされます。「ACS 5.3 への ACS 4.x データのインポート」（P.6-37）を参照してください。
	• CreateReportFiles：各フェーズのフル レポートと要約レポートが含まれるカンマ区切り形式（CSV）ファイルを作成するには、オプション 3 を選択します。CSV ファイルを Excel スプレッドシートまたは CSV ファイルをサポートするその他のエディタにアップロードできます。
	移行ディレクトリ内の *config* フォルダに、フル レポートと要約レポートが保存されます。「レポートの印刷とレポート タイプ」（P.6-40）を参照してください。
	• Exit：移行ユーティリティを終了するか、別の ACS 4.x インスタンスを移行する場合、オプション 4 を選択します。

`Would you like to migrate another ACS 4.x server? [no]`	デフォルト値は **no** です。別の ACS 4.x インスタンスを移行するには、**yes** と入力します。

ACS 4.x オブジェクトの移行

以下の項では、移行手順のさまざまなフェーズと、各オブジェクト タイプの影響と考慮事項について詳しく説明します。

ここで説明する内容は次のとおりです。

- 「EAP-Fast マスター キーおよび認証局 ID」（P.6-34）

AAA クライアント/ネットワーク デバイス

ACS 4.x では、[Network Configuration] オプションに AAA サーバまたは AAA クライアントを順に含めることができる NDG があります。AAA クライアントの定義は ACS 5.3 の [Network Devices and AAA Clients] オプションで移行および保存されます。

ここでは、次の内容について説明します。

- 「データ マッピング」（P.6-10）
- 「分析およびエクスポート」（P.6-11）
- 「インポート」（P.6-13）
- 「複数インスタンスのサポート」（P.6-14）

データ マッピング

表 6-5 に、ACS 4.x と ACS 5.3 の AAA クライアントまたはネットワーク デバイスのデータ マッピングについて示します。

表 6-5　AAA クライアントまたはネットワーク デバイスのデータ マッピング

4.x 属性名	5.3 属性名	コメント
AAA Client Hostname	Name	—
—	Description	ACS 4.x から取得される説明はありません。「*Migrated*」で事前に定義された説明は、移行されるすべてのデバイスに対して使用されます。
Shared Secret	Shared Secret	ACS 5.3 レコードには RADIUS と TACACS+ の共有秘密のそれぞれのフィールドが含まれます。ACS 5.3 レコードで設定される特定のフィールドは、[Authentication using] フィールドの設定に応じて異なります。
Network Device Group	All migrated NDGs の下の Network device group	—
Authentication using	RADIUS オプションまたは TACACS+ オプションで選択される内容	ACS 4.x には、サポートされるすべての RADIUS ベンダーのリストがあります。この情報は ACS 5.3 では保持されません。RADIUS ベンダーが選択される場合、「Authenticating using RADIUS」とマークされます。
AAA Client IP Address	IP	表示される内容はさまざまです。
Single Connect TACACS+ AAA Client（障害時にレコードのアカウンティングが停止される）	Single Connect Device	—
Legacy TACACS+ Single Connect support for this AAA client	Legacy TACACS+ Single Connect Support	4.2 累積パッチ 1 および 4.1.4.13 パッチ 10 以上でのみ使用可能です。
TACACS+ Draft compliant Single Connect support for this AAA client	TACACS+ Draft Compliant Single Connect Support	ACS 4.2 累積パッチ 1 および ACS 4.1.4.13 パッチ 10 以上でのみ使用可能です。

表 6-5　AAA クライアントまたはネットワーク デバイスのデータ マッピング （続き）

4.x 属性名	5.3 属性名	コメント
• Log Update/Watchdog Packets from this AAA Client（サーバに対する唯一のオプション） • Log RADIUS Tunneling Packets from this AAA Client • Replace RADIUS Port info with Username from this AAA Client • Match Framed-IP-Address with user IP address for accounting packets from this AAA Client	—	ACS 5.3 ではサポートされません。
Key Encryption Key	keyEncryptionKey	キーの長さは、次の表示タイプによって異なります。 • HEX：キーの長さは 32 文字です • ASCII：キーの長さは 16 文字です
Message Authenticator Code Key	messageAuthenticatorCodeKey	キーの長さは、次の表示タイプによって異なります。 • HEX：キーの長さは 40 文字です • ASCII：キーの長さは 20 文字です
Key Input Format	Key Input Format	ブール

（注）　グループの Single Connect フラグによって、デバイスの Single Connect フラグが上書きされます。

分析およびエクスポート

AAA クライアント（ACS 4.x）とネットワーク デバイス（ACS 5.3）の定義には、主に次の 3 つの相違点があります。

- ACS 5.3 では、RADIUS と TACACS+ の両方を処理する 1 つのネットワーク デバイスを定義できますが、ACS 4.x では、2 つの AAA クライアントが必要です。
- ACS 5.3 では、IP アドレスが IP アドレスとマスクからなるペアとして定義され、ACS 4.1 では IP アドレスが正規表現を使用して定義されます。
- ACS 5.3 では、各ネットワーク デバイス定義で保存できる IP アドレスが 40 個に制限されます。ACS 4.x では、41 以上の IP アドレスを定義できます。

ここでは、次の内容について説明します。

- 「デバイス名でサポートされない文字」（P.6-12）
- 「IP アドレスのオーバーラップ」（P.6-12）
- 「IP アドレス変換」（P.6-12）
- 「IP サブネットの制限」（P.6-12）

デバイス名でサポートされない文字

エクスポート時は、デバイス名に一部の特殊文字を使用できません。次の文字がデバイス名に使用されている場合は、分析中にエラー メッセージが表示され、エクスポートは処理されません。

{} " '

IP アドレスのオーバーラップ

ACS 4.x では、ネットワーク デバイスの一部として、IP アドレスがオーバーラップした定義を作成でき、最初の IP アドレスが TACACS+ を利用し、2 番目の IP アドレスが RADIUS を利用します。

ACS 5.3 では、TACACS+ と RADIUS が 1 つのネットワーク デバイス定義に統合されます。ただし、TACACS+ と RADIUS が ACS 4.x のそれぞれ別個の NDG の一部である場合は、統合することができません。

移行分析フェーズでは、ネットワーク グループおよび IP アドレスのオーバーラップが識別されて管理者に報告されるため、ACS 5.3 の要件に準拠するようにこれらの定義を変更できます。

例を示します。

`Network device AA: IP address` = *23.8.23.*, 45.67.*.8*, `protocol` = *RADIUS*, `group` = *HR*

`Network device BB: IP address` = *45.*.6.8, 1.2.3.4*, `protocol` = *TACACS*, `group` = *Admin*

この例では、*AA* ネットワーク デバイス リストの 2 番目の IP アドレスが *BB* ネットワーク デバイス リストの最初の IP アドレスとオーバーラップし、各ネットワーク デバイスがそれぞれ別個の NDG の一部です。

この例では、RADIUS ネットワーク デバイスと TACACS+ ネットワーク デバイスのそれぞれのエントリの統合は、IP アドレスが同一で、両方のネットワーク デバイスが同じ NDG の一部である場合にのみ可能です。すべての統合が分析レポートで報告されます。

IP アドレス変換

ACS 5.3 では、ワイルドカードおよび範囲をサポートします。ACS 4.x と同様に IP アドレスを指定する場合、ACS 4.x のすべての既存の IP アドレスが ACS 5.3 に移行されます。

たとえば、次の IP アドレス パターンを変換できます。

- 1.*.*.10 ～ 15
- 1.2.3.13 ～ 17

IP サブネットの制限

移行分析プロセスでは、41 以上の IP サブネットがあるネットワーク デバイスが識別され、これらのデバイスを移行できないことが報告されます。移行を可能にするには、ACS 5.3 形式に準拠するように、サブネット マスクに変更するか、または複数のネットワーク デバイス定義に分割します。表 6-6 では、ACS 5.3 の制限に準拠するように変更できる ACS 4.x 属性について説明しています。

キー ラップ属性

次の文字が含まれるキーは、分析フェーズで識別されます。

- 27 HEX
- 22 HEX

次のいずれかの文字がネットワーク デバイスのキー暗号キーまたはメッセージ オーセンティケータ コード キーに見つかった場合、分析フェーズでエラー メッセージが表示され、エクスポートは処理されません。

' "

表 6-6 では、ACS 5.3 の制限に準拠するように変更できる ACS 4.x 属性について説明しています。

表 6-6　　属性の変更

4.x の属性名	コメント
Authentication using	特定の RADIUS ベンダーの選択内容が *Authenticate Using RADIUS* に変換されます。たとえば、RADIUS（Cisco Aironet）は RADIUS に変換されます。
AAA Client IP Address	ACS 5.3 では、ワイルドカードおよび範囲をサポートします。ACS 4.x と同様に IP アドレスを指定する場合、ACS 4.x のすべての既存の IP アドレスが ACS 5.3 に移行されます。
Shared Secret	NDG に共有秘密情報が含まれる NDG に属しているデバイス。 ネットワーク デバイス定義の共有秘密情報の代わりに NDG の共有秘密情報が抽出されてネットワーク デバイス定義に含まれます。
Key Encryption Key	NDG にキー暗号キーが含まれる NDG に属しているデバイス。 ネットワーク デバイス定義のキー暗号キーで定義される代わりに NDG のキー暗号キーが抽出されてネットワーク デバイス定義に含まれます。
Message Authenticator Code Key	NDG にメッセージ オーセンティケータ コード キーが含まれる NDG に属しているデバイス。 NDG のメッセージ オーセンティケータ コード キーが抽出され、ネットワーク デバイス定義のメッセージ オーセンティケータ コード キーで定義される代わりにネットワーク デバイス定義に組み込まれます。

インポート

[Unified Device Name] 設定はネットワーク デバイスのインポート時に使用されます。1 つのネットワーク デバイス定義に統合できる ACS 4.x の個別の RADIUS デバイスや TACACS+ デバイスがある場合、ACS 5.3 では、ACS 5.3 の新しいデバイスの名前を決定するための設定オプションを使用可能です。ACS 5.3 では、次のオプションを使用できます。

- RADIUS デバイスの名前
- TACACS+ デバイスの名前

ACS 4.x には、ネットワーク デバイスと NDG の間の単一レベルの階層が含まれています。定義済みの各ネットワーク デバイス（AAA クライアント）をいずれかの NDG に含める必要があります。ネットワーク デバイスと NDG の間のこの関連付けを維持するには、ACS 5.3 で最初に NDG をエクスポートしてインポートし、次に NDG に関連付けられたネットワーク デバイスをエクスポートしてインポートします。NDG とネットワーク デバイスは 1 つのオブジェクト グループとして処理されます。

ACS 5.3 に新しいレコードがインポートされると、デフォルトの説明フィールド [Migrated] が作成されます。

複数インスタンスのサポート

ACS 5.3 では、IP アドレスがオーバーラップした複数のネットワーク デバイスを定義できます。ネットワーク デバイス名に特定の（またはグローバル）プレフィクスを定義して、重複を避けることができます。ただし、IP アドレスがオーバーラップしたデバイスは、名前が一意であっても、重複して移行されないと報告されます。また、このような 2 つのインスタンス間の移行はサポートされません。

例を示します。

`Instance` = *X*, `network device` = *AA*, `IP address` = *23.8.23.12*, `protocol` = *RADIUS*, `group` = *HR*

`Instance` = *Y*, `network device` = *BB*, `IP address` = *23.8.23.12*, `protocol` = *TACACS+*, `group` = *HR*

この例では、ネットワーク デバイス *AA* がインスタンス X にあり、ネットワーク デバイス *BB* がインスタンス Y にあるため、統合されたデバイスを作成できません。TACACS+ デバイスと RADIUS デバイスが同じインスタンスにある場合、統合デバイスの作成がサポートされます。

以前の移行インスタンスでインポートされた NDG に関連付けられたデバイスは、ACS 5.3 にすでに存在している NDG に関連付けられます。

NDG

ACS 4.x の NDG 定義の移行を利用するには、ACS 5.3 で追加の NDG 階層が作成されます。

移行プロセスで、ACS 4.x NDG 定義を保存する階層のルートの名前を入力することを要求するプロンプトが表示されます。プロンプトに、移行される NDG のデフォルト名が表示されます。必要に応じて、この名前を変更できます。

ACS 4.x には、どのグループにも属していないすべてのデバイスのための「Not Assigned NDG」という名前の保存されていないグループが含まれています。「Not Assigned NDG」グループは ACS 5.3 へのエクスポート後に作成されます。

ACS 4.x では、NDG に AAA クライアントの共有秘密や Legacy TACACS+ Single Connect Support などの属性が含まれます。ただし、ACS 5.3 では、NDG はネットワーク デバイス定義に添付できるラベルであり、データが含まれていません。値が ACS 4.x の NDG の共有秘密に設定されている場合、グループに関連付けられる各ネットワーク デバイスの値を設定するためにこの値が抽出されます。

ここでは、次の内容について説明します。

- 「データ マッピング」（P.6-15）
- 「分析およびエクスポート」（P.6-15）
- 「インポート」（P.6-16）
- 「複数インスタンスのサポート」（P.6-16）

データ マッピング

表 6-7 に、ACS 4.x および ACS 5.3 間の NDG のデータのマッピングについて示します。

表 6-7　NDG のデータ マッピング

4.x 属性名	5.3 属性名	コメント
Network Device Group Name	Name	—
—	Description	ACS 4.x から取得される説明は ありません。「*Migrated*」で事前に定義された説明は、移行されるすべてのデバイスに対して使用されます。
Shared Secret	—	グループで定義された値が抽出され、グループに関連付けられた各ネットワーク デバイスに定義されます。
Encryption Key	—	ACS 5.3 ではサポートされません。
Message Authenticator Code Key	—	ACS 5.3 ではサポートされません。
Key Encryption Key	keyEncryptionKey	キーの長さは、次の表示タイプによって異なります。 • HEX：キーの長さは 32 文字です • ASCII：キーの長さは 16 文字です
Message Authenticator Code Key	messageAuthenticatorCodeKey	キーの長さは、次の表示タイプによって異なります。 • HEX：キーの長さは 40 文字です • ASCII：キーの長さは 20 文字です
Key Input Format	Key Input Format	ブール

分析およびエクスポート

次の項目は、分析フェーズで報告されます。

- NDG 名の特殊文字：一部の特殊文字は、エクスポート時に NDG 名に使用できません。次の文字が NDG 名に使用されている場合は、分析中にエラー メッセージが表示され、エクスポートは処理されません。

  {} | " = ' :

- 共有秘密の定義が含まれる NDG：共有秘密の定義によってデバイス レベルで定義された値が上書きされることを示すメッセージ。
- キー暗号キーまたはメッセージ オーセンティケータ コード キーのいずれかの定義が含まれる NDG：キー暗号キーまたはメッセージ オーセンティケータ コード キーの定義によってデバイス レベルで定義された値が上書きされることを示すメッセージ。
- ネットワーク デバイスのキー暗号キーまたはメッセージ オーセンティケータ コード キーの特殊文字：次のいずれかの文字がネットワーク デバイスのキー暗号キーまたはメッセージ オーセンティケータ コード キーに見つかった場合、分析フェーズでエラー メッセージが表示され、エクスポートは処理されません。

  ' "

エクスポート フェーズでは同様の情報が表示されません。

インポート

インポート フェーズで、[User Preferences] で名前が定義された新しい NDG 階層が作成されます。[User Preferences] で名前が付けられ、*All* というプレフィクスが付いたルート ノードも作成されます。移行されたすべての NDG がこのルート ノードの下に作成されます。

複数インスタンスのサポート

ACS 5.3 では、階層ルート 1 つに同じ名前の 2 つの NDG（階層ノード）を定義できません。ただし異なる階層であれば定義できます。たとえば *Engineers* という名前の 2 つのグループをルート *SJ* とルート *NY* にそれぞれ定義できます。複数インスタンスをサポートすることで、NDG を移行するために次のいずれかを実行できます。

- インスタンスごとに別のルートを定義し、インスタンスのルートにそのインスタンスのすべての NDG をインポートします。
- 移行されるすべての NDG のための 1 つのルートを定義します。ただし、移行ユーティリティでは、固有の NDG のみがそのルートに追加されます。すでに存在する NDG は、重複していると報告され、インポートされません。ただし、この場合、すでに存在する NDG の ID は、関連付けのために取得されます。

いずれかのオプションを選択するには、[Preferences] > [User Interface] に移動します。選択ごとに、NDG とネットワーク デバイスの間の関連付けが選択のロジックに従って維持されます。

たとえば、NDG *SJ* に関連付けられたデバイス *ABC*（一意の名前と IP アドレスがある）が最初の ACS 4.x インスタンスから移行されます。上記の 2 つのオプションのいずれかを選択する場合、*ABC* は NDG の *SJ* に関連付けられますが、*SJ* はルート *All* または指定したルート *Engineers* のいずれかに定義できます。

内部ユーザ

ACS 5.3 では、ポリシーのコンポーネントは、ポリシーの結果として選択できる再利用可能なオブジェクトです。

内部ユーザに関連する移行アクティビティは、次の内容で構成されます。

- 「基本ユーザ定義」（P.6-16）
- 「複数インスタンスのサポート」（P.6-18）
- 「ユーザ データ設定およびユーザ マッピング」（P.6-18）
- 「ユーザ シェル コマンド認可」（P.6-20）
- 「Shell exec パラメータ」（P.6-22）

ACS 4.x にはダイナミック ユーザを含めることができます。LDAP などの外部データベースはダイナミック ユーザ、その ID、関連するその他のプロパティを管理できます。

ダイナミック ユーザは、外部ソースに対して正常に認証された後で、ACS 内部データベースで作成されます。ダイナミック ユーザは最適化のために作成され、削除しても ACS の機能は影響を受けません。ダイナミック ユーザは移行ユーティリティで無視され、処理されません。

基本ユーザ定義

各ユーザに対して、基本定義にはユーザ名、パスワード、ディセーブルまたはイネーブルのステータス、ID グループが含まれます。

ここでは、次の内容について説明します。

データ マッピング

表 6-8 に、ACS 4.x と ACS 5.3 の内部ユーザのユーザ インターフェイスのデータ マッピングについて示します。

表 6-8　内部ユーザのデータ マッピング

4.x 属性名	5.3 属性名	コメント
User Name	Name	—
Account Disabled	Status: • Enabled • Disabled	—
—	Description	ACS 4.x から取得される説明はありません。ACS 5.3 で使用される説明は、次のような定義されるユーザの種類に応じて異なります。 • 移行される内部ユーザ • 外部認証の移行されるユーザ
Password	Password	—
Group to which the user is assigned	Identity Group	最初にユーザ グループを移行する必要があります。移行された ID グループとの関連付けは維持されます。
Separate TACACS+ Enable Password	Enable Password	—

分析およびエクスポート

エクスポート時は、ユーザ名に一部の特殊文字と「スペース」を使用できません。次の文字をユーザ名で使用すると、分析レポートで報告されます。

<> " * ?{ }

デフォルトでは、外部パスワード タイプの内部ユーザが、そのパスワード タイプの内部ユーザとして移行されます。内部パスワード タイプのユーザが分析レポートで報告されます。

パスワードが 4 文字未満のユーザはエクスポートされません。

（注） アポストロフィ（'）が含まれるユーザのユーザ コマンド セットは移行されません。

次のオプションは、内部ユーザのパスワード定義には使用できます。

- [Internal]：パスワードは ACS 内部に保存されます。
- [External Database]：パスワードは外部データベースに保存され、認証はこのデータベースに対して実行されます。

- [Empty Password]：VoIP ユーザは [This is a Voice-over-IP (VoIP) group -] 設定および [all users of this group are VoIP users] 設定が選択されているグループに関連付けると定義できます。この場合、ユーザにパスワードが定義されません。

インポート

ACS 5.3 では、外部認証ユーザはサポートされません。このようなユーザのインポートを定義するために、次の設定オプションを使用できます。

- [Default authentication password]：すべての外部認証ユーザにこのパスワードが割り当てられます。
- [Disabled or Change password]：このようなユーザが ACS 5.3 でディセーブルとして定義されるか、または次のログイン時にパスワードの変更が必要かを選択できます。

多数のユーザが存在する可能性があるため、このようなユーザには分析の警告が表示されません。

（注）　VoIP は ACS 5.3 ではサポートされません。VoIP がイネーブルになっているユーザ グループに関連付けられたユーザは分析の一部として報告され、エクスポートされません。

複数インスタンスのサポート

複数の ACS 4.x インスタンスに存在している重複した ID のユーザは、ユーザ名に基づいて、インポート レポートで報告されます。一意のユーザのみが移行されます。複数の ACS 4.x インスタンスに存在しているユーザのデータ間の名前のプレフィクスまたは移行はサポートされません。

たとえば、ユーザ *Jeff* が複数の ACS 4.x インスタンスに存在し、最初に移行されなかったインスタンスだけにイネーブル パスワードが存在している場合、*Jeff* にイネーブル パスワードを追加することはできません。

一意のユーザ名を持ち、ユーザ グループに関連付けられたユーザは、ユーザ グループ自体がユーザまたは以前のインスタンスと同じインスタンスで移行される場合でも移行され、関連付けは維持されます。

（注）　また、ユーザが移行をパスしない場合、TACACS+ 属性値や Shell 属性値およびそのユーザから生成されたコマンド セットなどのユーザ属性値やポリシー コンポーネントは、有効な場合でも移行されません。

ユーザ データ設定およびユーザ マッピング

ACS 4.x には、ユーザ レコードに含めるように選択できる最大 5 つのユーザ定義フィールドがあります。各フィールドに、対応するフィールド名を定義できます。ACS 5.3 では、対応するユーザ属性を作成して各ユーザに対して読み込めるように、これらのフィールドを移行します。

これらのフィールドを設定するには、[Interface Configuration] > [User Data Configuration] を選択します。5 つのフィールドのそれぞれに対して、設定を繰り返す必要があります。

ここでは、次の内容について説明します。

- 「データ マッピング」（P.6-19）
- 「分析およびエクスポート」（P.6-19）
- 「インポート」（P.6-19）
- 「複数インスタンスのサポート」（P.6-19）

データ マッピング

表 6-9 に、ACS 4.x と ACS 5.3 のユーザ データ設定およびユーザ マッピングのユーザ インターフェイス データ マッピングについて示します。

表 6-9　ユーザ データ設定およびユーザ マッピングのデータ マッピング

4.x 属性名	5.3 属性名	コメント
Display	—	イネーブルの場合、対応するフィールド名が抽出されます。そうでない場合は無視されます。
Field Name	Attribute	—
—	Description	ACS 4.x から取得される説明はありません。「*Attribute added as part of the migration process*」で事前に定義された説明は、すべての属性に使用されます。

分析およびエクスポート

次のことを確認するために、フィールド名に対して分析が実行されます。

- フィールドの長さが 32 文字を超えていないこと。
- フィールドに次の特殊文字が含まれていないこと。

  { } ' "

インポート

ACS 4.x では、同じ名前の複数のフィールド名を定義できます。ただし、ACS 5.3 では、ユーザ定義の属性の名前を一意にする必要があります。複数の属性の名前が同じである場合、最初に検出された属性だけに元の名前が維持されます。その後に検出された属性については、サフィクス「_1」が追加されます。

たとえば、ACS 4.x の 3 つの属性の名前が *ACS* である場合、ACS 5.3 へのインポート後、属性名は次のようになります。

- 最初の属性：ACS
- 2 番目の属性：ACS_1
- 3 番目の属性：ACS_2

複数インスタンスのサポート

ACS 5.3 では、ID ディクショナリに同じ名前の 2 つのユーザ属性を定義できません。ただし、ACS 4.x インスタンスごとに名前のプレフィクスを作成することで、各インスタンスに属性を追加することができます。

次のオプションのいずれかを選択して、ユーザ属性を移行できます。

- インスタンスごとに異なる名前プレフィクスを定義して、異なる名前のすべてのユーザ属性をインポートします。
- プレフィクスを定義しないでください。これによって、一意の属性だけが移行されます。すでに存在している属性は重複として報告されます。この場合、既存のユーザ属性の ID は、関連付けのために維持されます。

1 つの ACS 4.x インスタンスだけからすべてのユーザのユーザ データが取得されます。同じユーザが別の ACS 4.x インスタンスに存在する場合、そのユーザはインポートされませんが、ユーザ属性はヌル値で移行されます。すべてのユーザに適用される内部ユーザ属性は、1 組あります。

たとえば、最初の ACS 4.x インスタンスからユーザ属性 *A*、値 *x*、ユーザ属性 *B*、値 *y* のユーザ *user1* を移行します。次に、2 番目の ACS 4.x インスタンスから、ユーザ属性 *C*、値 *z*、ユーザ属性 *D*、値 w の同じユーザ *user1* を移行します。

ここで、2 番目のインスタンスのユーザ *user1* は移行されませんが、ユーザ属性 *C* と *D* はヌル値で移行されます。ACS 5.3 のユーザ *user1* には次の属性が含まれています。

- *A*、値 *x*
- *B*、値 *y*
- *C*、2 番目のインスタンスのヌル値。
- *D*、2 番目のインスタンスのヌル値。

同じユーザに 2 番目のインスタンスの属性を含めることはできますが、属性値を含めることはできません。複数の ACS 4.x インスタンスからユーザ属性を移行することはできません。

たとえば、ユーザが ACS 5.3 にすでに存在している（別の ACS 4.x インスタンスから移行された）場合、属性 *Real Name: Jeffrey* だけをユーザ *jeff* に追加することはできません。また、属性 *Real Name: Jeffrey* は現在の ACS 4.x インスタンスだけに存在します。

ユーザ属性の定義が移行されるときは、現在または以前の移行の実行に関係なく、ユーザとユーザ属性の関連付けが維持されます。ACS 5.3 にすでに存在している（以前の移行の実行で移行された）ユーザ属性に関連付けられた固有のユーザ名を持つ（現在の実行で追加できる）ユーザは、既存のユーザ属性に関連付けられます。

ACS 5.3 では、ディクショナリに追加されるすべての ID 属性が、値が空白の場合でも、すべてのユーザにも追加されます。

たとえば、ACS 4.x の最初のインスタンスでユーザ *User1* を作成し、移行ユーティリティを開始します。最初のインスタンス サーバ ID を入力し、サーバに固有の移行プレフィクス *global1* を追加します。ユーザ *User1* をユーザ属性「city」、「real name」、「description」とともに移行します。

ACS 4.x の 2 番目のインスタンスでユーザ *User2* を作成し、移行ユーティリティを開始します。2 番目のインスタンス サーバ ID を入力し、サーバに固有の移行プレフィクス *global2* を追加します。ユーザ *User2* をユーザ属性「city」、「country」および「state」とともに移行します。

ACS 5.3 に移行した後、*user1* には属性「*global1_city*」、「*global1_Description*」、「*global1_Real Name*」、「*global2_city*」、「*global2_country*」および「*global2_state*」が含まれます。

User2 には属性「*global1_city*」、「*global1_Description*」、「*global1_Real Name*」、「*global2_city*」、「*global2_country*」および「*global2_state*」が含まれます。

ここで、プレフィクス *global1* の属性は *User1* に使用され、プレフィクス *global2* の属性は *User2* に使用されます。

ユーザ シェル コマンド認可

ACS 4.x では、シェル コマンド セットをユーザ レコードに組み込むことができます。移行機能の一部として、このコマンド セットが抽出され、共有オブジェクトとして定義されます。ユーザ属性には、ユーザ レコードから取得したユーザに関連付けられたコマンド名が含まれます。

ユーザ コマンド セットは、ユーザが移行される場合にのみ共有コマンド セットに移行されます。ユーザ名から名前が生成されます。

共有コマンド セットは、対応するユーザが移行された場合にのみ抽出されます。

ここでは、次の内容について説明します。

- 「データ マッピング」（P.6-21）
- 「分析およびエクスポート」（P.6-21）

- 「インポート」（P.6-21）
- 「複数インスタンスのサポート」（P.6-22）

データ マッピング

表 6-10 に、ACS 4.x と ACS 5.3 のユーザ シェル コマンド認可のユーザ インターフェイス データ マッピングについて示します。

表 6-10　ユーザ シェル コマンド認可のデータ マッピング

4.x 属性名	5.3 属性名	コメント
一致しない Cisco IOS コマンド（Permit / Deny）	コマンドのリストに表示されないコマンドを許可します。	—
コマンド、およびそれに続く引数のリスト（次の形式）： `permit / deny < arguments >`	次の形式のコマンドのリスト： `permit / deny <command> <arguments>`	—
—	Description	ACS 4.x から取得される説明はありません。「*Attribute added as part of migration process*」で事前に定義された説明は、すべての属性に使用されます。
リストに表示されない引数（Permit / Deny）	特定コマンドで引数の各リストに続く追加のエントリ（次の形式）： `permit / deny <command>`	—

分析およびエクスポート

ACS 4.x では、ユーザ レコードにデバイス グループ名とコマンド セット名の組み合わせが含まれる場合、NDG ごとにシェル コマンド認可セットを割り当てることができます。ACS 5.3 ではこれに相当する機能がサポートされず、分析中にメッセージが表示されます。

インポート

各ユーザ コマンド セットのインポート時は、次のユーザ設定が使用されます。

- コマンド セット名形式のオプション：Add Prefix | User Name のみ。
- プレフィクスのテキスト。
- 以前のプレフィクスに加え、統合オブジェクトで追加されるプレフィクス：デフォルトは空白の文字列。

ユーザ属性 *cmd-set* は、ユーザ定義から移行される ACS 5.3 コマンド セットの名前を保存するために使用されます。

ユーザ コマンド セットをインポートするには、次の手順を実行します。

ステップ 1　*cmd-set* ユーザ属性を作成します。

ステップ 2　コマンド セットのユーザごとの定義を持つユーザの場合：

a.　コマンド セットが別のレコードに統合されている場合は、次のユーザに進みます。

b.　ユーザ名と定義されたプレフィクスの組み合わせとしてコマンド セットの名前を指定します。

c.　移行したコマンド セットを作成します。

ステップ 3　ユーザの *cmd-set* ユーザ属性に、移行されたコマンド セットの名前を設定します。

複数インスタンスのサポート

ACS 5.3 では、同じ名前のコマンド セット 2 つを定義できません。ただし、ACS 4.x インスタンスごとの名前プレフィクスを使用してコマンド セットを作成し、ACS 4.x インスタンスごとにコマンド セットを移行できます。

したがって、次のオプションのいずれかを選択して、コマンド セットを移行できます。

- インスタンスごとに異なる名前プレフィクスを定義して、異なる名前のすべてのコマンド セットをインポートします。
- プレフィクスを定義しないでください。一意のコマンド セットのみが移行されます。（以前のインスタンスで移行した）既存のコマンドセットは、重複していると報告されます。

Shell exec パラメータ

ACS 4.x では、ユーザ レコードに shell（exec）TACACS+ 設定が含まれます。これらの設定はユーザ レコードの属性として ACS 5.3 に移行されます。これらの属性のいずれかが、移行されたユーザ レコードのいずれかに使用される場合、ユーザ属性として作成されます。移行されるユーザ定義で対応する属性に値が設定されます。

ユーザ シェル属性値は、ユーザが移行される場合にだけ移行されます。

ここでは、次の内容について説明します。

- 「データ マッピング」（P.6-22）
- 「分析およびエクスポート」（P.6-23）
- 「インポート」（P.6-23）
- 「複数インスタンスのサポート」（P.6-23）

データ マッピング

表 6-11 に、ACS 4.x と ACS 5.3 のユーザ シェル属性のデータ マッピングについて示します。Max Privilege 属性以外のすべての属性は、TACACS+ shell（exec）設定から取得されます。

表 6-11　ユーザ シェル属性のデータ マッピング

4.x 属性名	5.3 属性名	コメント
TACACS+ Enable Control：任意の AAA クライアントの Max Privilege	Max_priv_lvl（Unsigned Integer 32）	—
Access control list	ACL（文字列）	—
Auto command	Autocmd（文字列）	—
Callback line	Callback-line（文字列）	—
Callback rotary	Callback-rotary（文字列）	—
Idle time	Idle time（Unsigned Integer 32）	—
No callback verify	No callback-verify（ブール）	—
No escape	No escape（ブール）	—
No hangup	No hangup（ブール）	—

表 6-11　ユーザ シェル属性のデータ マッピング （続き）

4.x 属性名	5.3 属性名	コメント
Privilege level	Priv_lvl（Unsigned Integer 32）	—
Timeout	Conn-timeout（Unsigned Integer 32）	—

分析およびエクスポート

ACS 5.3 では、数値（0 ～ 9999）による特権レベルをサポートします。ACS 4.x の特権レベルは文字列フィールドですが、有効性のチェックは行われません。特権レベルが有効な範囲にない場合は、管理者に報告されます。

このチェックは、特権レベルを有効リストから選択するイネーブル パスワードには適用されません。ただし、shell exec 設定の特権レベルが最大イネーブル特権を超えていないかどうかが追加の分析で確認されます。ACS 5.3 では、shell exec で定義されるカスタム パラメータがサポートされません。無効なアイドル時間およびタイムアウトの値は、分析レポートで報告されます。

インポート

全ユーザを対象とした shell exec パラメータが収集されます。移行されるユーザ 1 人以上に対して存在するパラメータは、ユーザ属性として移行されます。ACS 4.x で移行される各ユーザに対して shell exec 値が設定されている場合、ACS 5.3 では ACS 5.3 のユーザと関連付けられたユーザ属性にその値が設定されます。属性が ACS 4.x で定義されていない場合、ACS 5.3 ではブランクになります。

複数インスタンスのサポート

シェル属性には、固定名があります。ACS 4.x インスタンスごとの名前プレフィクスを使用してシェル属性を作成することはできません。また、複数の ACS 4.x インスタンスからシェル属性データ（値）をマージすることもできません。

たとえばユーザ *jeff* が ACS 5.3 に存在していて、シェル属性 *Timeout:123* がこのユーザで定義されていない場合、この属性のみをこのユーザに追加することはできません。

シェル属性の定義が移行されるときは、現在または以前の移行の実行に関係なく、ユーザとシェル属性の関連付けが維持されます。

固有のユーザ名を持つユーザ（現在の実行で追加）は、ACS 5.3 ID ディクショナリ内にすでに存在するシェル属性（移行の以前の実行で移行）と関連付けられ、既存のシェル属性に関連付けられます。

同じユーザが別の ACS 4.x インスタンスに存在する場合、そのユーザはインポートされませんが、ユーザ シェル属性はヌル値で移行されます。すべてのユーザに適用される内部ユーザ シェル属性は、1 組あります。ACS 5.3 では、ディクショナリに追加されるユーザ シェル属性のそれぞれがすべてのユーザにも追加されます。

ユーザ グループ

ACS 5.3 では、ID グループはユーザ グループと同等です。ただし ID グループは、規則条件でポリシーの処理と選択を行うために、一連のユーザをグループ化する純粋な論理コンテナです。

ユーザ グループ名は、ID グループ階層に移行およびマージされます。ID 階層のルート ノードの下に新しいノードが作成され、そのノードの下に移行されるすべてのユーザ グループが同一階層に配置されます。このノードの名前を定義するように求められます。デフォルトの名前も表示されます。

ACS 4.x ではデフォルトで 500 ユーザ グループが作成され、管理者はこれらのグループを編集できます。ACS 5.3 では、利用していてユーザまたは MAC 定義から参照されているユーザ グループのみが移行されます。

ユーザとユーザ グループ（ID グループ）との関連付けを維持するには、先にユーザ グループ、次にそれらのユーザ グループと関連付けられている内部ユーザをエクスポート（およびインポート）する必要があります。

ここでは、次の内容について説明します。

分析およびエクスポート

内部ユーザまたは MAC 定義を含まないユーザ グループはエクスポートされません。そのようなユーザ グループは移行されなかったことが管理者に報告されます。またエクスポート時は、グループ名に一部の特殊文字を使用できません。次の文字がグループ名に使用されている場合は、分析レポートで報告され、エクスポートは処理されません。

{ } | ' " = :

インポート

インポート時は、新しい ID グループ ノードが ID グループ階層のルート ノードに作成され、[User Preferences] で定義された名前が付けられます。デフォルトの名前は *Migrated Group* です。移行されるすべてのユーザ グループは、この新しく作成されたノードの下に同一階層で作成されます。

ACS 4.x では、各ユーザが 1 つのグループに関連付けられていました。ユーザとユーザ グループ（ID グループ）との関連付けを維持するには、先にユーザ グループ、次にそのユーザ グループと関連付けられている内部ユーザをインポートします。

複数インスタンスのサポート

ACS 5.3 では、階層ルート 1 つに同じ名前の ID グループ 2 つを定義できません。ただし異なる階層であれば定義できます。

たとえば *Engineers* という名前の 2 つのグループをルート *NY* とルート *SJ* にそれぞれ定義できます。複数インスタンスをサポートすることで、グループを移行するときに次のいずれかのオプションを選択できます。

- インスタンスごとに別のルートを定義し、インスタンスのルートにそのインスタンスのユーザ グループすべてをインポートします。
- 移行されるすべてのグループに対してルート 1 つを定義します。移行ユーティリティでは、固有のグループのみがそのルートに追加されます。すでに存在するグループは、重複していると報告され、インポートされません。ただし、すでに存在するユーザ グループの ID は、関連付けのために取得されます。

いずれかのオプションを選択するには、[User Preferences] に移動します。ユーザ グループとユーザとの関連付けは、選択したロジックに従って維持されます。

たとえばユーザ *john*（固有のユーザ名）が ACS 4.x インスタンスの前回の実行から移行されたグループ *Management* に関連付けられているとします。いずれのオプションを選択しても、*john* はグループ *Management* に関連付けられますが、*Management* はルート *All* で定義されるか、特定のルート *Engineers* で定義されます。

ユーザ グループ ポリシーのコンポーネント

ACS 4.x ではポリシー関連の認可データのほとんどがユーザ グループ定義に埋め込まれますが、ACS 5.3 では共有オブジェクトとして定義されます。

データは、使用中のグループからのみ移行されます。グループ データから抽出されるデータは次のとおりです。

- TACACS+ シェル コマンド認可セットは、コマンド セットに移行されます。
- TACACS+ shell exec（および最大特権レベル）は、シェル プロファイルに移行されます。

ここでは、次の内容について説明します。

- 「グループ コマンド セット」（P.6-25）
- 「グループ Shell Exec」（P.6-25）
- 「MAC アドレスと内部ホスト」（P.6-27）
- 「共有シェル コマンド認可セット」（P.6-28）

グループ コマンド セット

ユーザから抽出されるコマンド セットの名前は、ユーザ属性に格納されます。データがユーザ グループから抽出されるときは、このようなアクションは実行されません。グループのコマンド セットに対する複数インスタンスのサポートは、ユーザのコマンド セットの場合と同様です。

（注）　グループ コマンド セットは、グループの移行時のみ移行されます。

グループ Shell Exec

ここでは、次の内容について説明します。

- 「データ マッピング」（P.6-25）
- 「分析およびエクスポート」（P.6-26）
- 「インポート」（P.6-26）
- 「複数インスタンスのサポート」（P.6-26）

データ マッピング

表 6-12 に、グループ データの属性からシェル プロファイルでの属性へのマッピングについて説明します。シェル プロファイルの各フィールドには、プロファイルにそのフィールドが存在するかどうかを示すフラグがあります。グループ レコードでフィールドがイネーブルではない場合、そのフィールドはシェル プロファイルで存在しないとマークされます。

表 6-12　グループ Shell Exec のデータ マッピング

4.x 属性名	5.3 属性名	コメント
イネーブル オプション：任意の AAA クライアントの Max Privilege	Maximum Privilege Level	—
Access control list	Access Control List	—
Auto command	Auto Command	—
Callback line	Callback Line	—

表 6-12　グループ Shell Exec のデータ マッピング （続き）

4.x 属性名	5.3 属性名	コメント
Callback rotary	Callback Rotary	—
Idle time	Idle time	—
No callback verify	No Callback Verify	—
No escape	No Escape	—
No hangup	No Hang Up	—
Privilege level	Default Privilege Level	—
Timeout	Timeout	—

分析およびエクスポート

分析は、使用中であると判断されたすべてのグループ、およびユーザまたは MAC アドレスと関連付けられているすべてのグループに対して実行されます。分析では、ACS 4.x で入力された次の値が対応する ACS 5.3 オブジェクトで有効な値であることを検証します。

- Timeout : 0 ～ 9999
- Idle Time : 0 ～ 9999
- Privilege Level : 0 ～ 15

ACS 5.3 では、MAC アドレスにワイルドカードを含めることができますが、ワイルドカードを使用できるのは特定の OID、たとえば「00-00-00-*」で使用する場合だけです。ワイルドカード形式 11-11-11-11-11-* はサポートされていません。

分析では、新しい Default Privilege Level 値が最大値よりも大きくないことも検証します。移行されるグループで定義されたカスタム属性は、ACS 5.3 に移行されず、警告が表示されます。

インポート

グループ shell exec のインポート時は、次のユーザ設定が使用されます。

- シェル プロファイル名の形式。次のオプションがあります。
  - プレフィクスを追加
  - グループ名のみ
- プレフィクスのテキスト。
- 上記のプレフィクスに加え、統合オブジェクトで追加されるプレフィクス。デフォルトは空の文字列です。

インポート プロセスは、別のオブジェクトに統合されていない各 shell exec で実行されます。ACS 5.3 オブジェクトの名前は、ユーザ設定および作成されるシェル プロファイルに基づいて決まります。

（注）　グループ シェル属性は、グループの移行時のみ移行されます。

複数インスタンスのサポート

グループ シェル属性は、共有シェル プロファイルに移行され、名前はグループ名から生成されます。

ACS 5.3 では、同じ名前のシェル プロファイル 2 つを定義できません。ただし、ACS 4.x インスタンスごとの名前プレフィクスを使用してシェル プロファイルを作成できるため、インスタンスごとにシェル プロファイルを追加できます。複数インスタンスをサポートすることで、シェル プロファイルを移行するときに次のいずれかのオプションを選択できます。

- インスタンスごとに異なる名前プレフィクスを定義して、異なる名前のシェル プロファイルをすべてインポートします。
- プレフィクスを定義しないでください。その結果、固有の名前が付いたシェル プロファイルが移行されます。すでに存在するシェル プロファイルは、重複していると報告されます。

MAC アドレスと内部ホスト

ACS 4.x では、MAC アドレスに基づく認証を次のようにサポートしています。

- MAC アドレスを内部ユーザ名、およびユーザ名と同一のパスワード認証プロトコル（PAP）パスワードとして定義します。ユーザは内部ユーザ データベースに移行され、MAC アドレスの追加サポートは必要ありません。
- 認証ポリシーの一環として NAP テーブルに MAC アドレスを定義します。認証ポリシーでは、ACS 内部データベースを使用して MAC アドレスを認証するように設定できます。その後、MAC アドレスと対応する ID のリストを提供できます。MAC アドレスは、内部ホストのデータベースで対応するレコードに移行されます。

ACS 5.3 では、ユーザに対する場合と同様に、ホストと関連付けられた追加の属性を定義できます。一方、ACS 4.x では MAC 定義と関連付けられた追加データはなく、移行に追加された属性は必要ありません。ただし ID グループの関連付けは維持されます。

ここでは、次の内容について説明します。

- 「データ マッピング」（P.6-27）
- 「分析およびエクスポート」（P.6-27）
- 「複数インスタンスのサポート」（P.6-28）

データ マッピング

表 6-13 に、ACS 4.x と ACS 5.3 の MAC アドレスと内部ホストのデータ マッピングについて示します。

表 6-13　MAC アドレスと内部ホストのデータ マッピング

4.x 属性名	5.3 属性名	コメント
NAP の認証セクションに保管された MAC Addresses	MAC Address	アドレスのリストが含まれることがあります。内部ホスト定義は、定義されたアドレスごとに作成されます。
—	Status	移行されたすべてのエントリはイネーブルであると設定されます。
—	Description	ACS 4.x から取得される説明はありません。「*Migrated From ACS* 4.x」で事前に定義された説明は、すべての定義に対して使用されます。
User Group	Identity Group	ACS 5.3 ID グループ階層内にある同じ ID グループを参照するように設定されます。

分析およびエクスポート

MAC アドレスは複数の形式で入力できますが、常に *12-34-56-78-90-AB* という形式で保管されます。ただし ACS 4.x では、アドレスでワイルドカードを使用できます。たとえば *12-34-56-78** です。

ACS 5.3 では、MAC アドレスにワイルドカードを含めることができます。MAC アドレスの最初の 3 オクテットよりも後だけにワイルドカードが指定されたホストを、関連付けられたユーザ グループと組み合わせて移行できます。ワイルドカードなしのホストも移行できます。

例を示します。

NAP A には次の MAC アドレスがあります：1-2-3-4-5-6 Group 10

NAP B には次の MAC アドレスがあります：1-2-4-* Group 24

ここで、NAP A の MAC アドレス 1-2-3-4-5-6 は、グループ 10 に関連付けられて移行されます。また、NAP B の MAC アドレス 1-2-4-* はグループ 24 との組み合わせで移行されます。

複数インスタンスのサポート

ACS 4.x では、重複した MAC は MAC アドレスに基づいて認識され、インポート レポートで報告されます。固有の MAC アドレスのみが移行されます。名前プレフィクスはサポートされません。ユーザ グループに関連付けられた固有の MAC アドレスが移行されます。

関連付けは維持されます。ユーザ グループ自体が MAC アドレスと同じインスタンス、または以前のインスタンスで移行されたかどうかは関係ありません。

共有シェル コマンド認可セット

ACS 4.x のシェル コマンド認可セットは、デバイスの管理時に共有オブジェクトとして定義できます。そのようなオブジェクトは、コマンド セットへ移行されます。各オブジェクトの名前と説明は、ACS 4.x と同じです。

ここでは、次の内容について説明します。

- 「データ マッピング」（P.6-28）
- 「分析およびエクスポート」（P.6-29）
- 「複数インスタンスのサポート」（P.6-29）

データ マッピング

表 6-14 に、ACS 4.x と ACS 5.3 のシェル コマンド認可セットのデータ マッピングについて示します。

表 6-14　共有シェル コマンド認可セットのデータ マッピング

4.x 属性名	5.3 属性名	コメント
Name	Name	—
Description	Description	—
一致しないコマンド • Permit • Deny	[*Permit any command that is not in the table*] というラベルの付いたチェックボックス	—
コマンド、およびそれに続く引数のリスト（次の形式）： `permit / deny <arguments>`	コマンド テーブル内のエントリ： • Grant: Permit / Deny • コマンド • 引数	—
リストでない引数 • Permit • Deny	特定コマンドで引数の各リストに続く追加のエントリ（次の形式）： `permit / deny <command>`	—

分析およびエクスポート

エクスポート時は、シェル コマンド認可セットに一部の特殊文字を使用できません。デバイス名に次の文字が使用される場合は、分析レポートで報告されます。

{ } ' "

複数インスタンスのサポート

ACS 5.3 では、同じ名前のコマンド セット 2 つを定義できません。ただし、ACS 4.x インスタンスごとの名前プレフィクスを使用して作成できるため、コマンド セットごとにシェル プロファイルを追加できます。従って複数インスタンスをサポートすることで、共有コマンド セットを移行するときに次のいずれかのオプションを選択できます。

- ACS 4.x インスタンスごとに異なる名前プレフィクスを定義して、異なる名前のコマンド セットをすべてインポートします。
- プレフィクスを定義しません。その結果、固有の名前が付いたコマンド セットが移行されます。すでに存在するコマンド セットは、重複していると報告されます。

共有 DACL オブジェクト

ACS 4.x では、共有ダウンロード可能アクセス コントロール リスト（DACL）は、アプリケーションから参照される共有オブジェクトとして定義されます。共有 DACL は、一連の ACL コンテンツで構成されます。各 ACL は、特定の Network Access Filtering（NAF; ネットワーク アクセス フィルタリング）選択と関連付けられています。オブジェクトが参照されると、最初に一致する NAF の条件によって使用される実際の ACL が異なります。

ACS 5.3 には、認可プロファイルからの DACL の選択の結果となる認可ポリシーが含まれます。したがって、ACS 4.x 共有 DACL に含まれる各 ACL は ACS 5.3 の別の DACL にマッピングされます。

ここでは、次の内容について説明します。

- 「データ マッピング」（P.6-29）
- 「分析およびエクスポート」（P.6-30）
- 「インポート」（P.6-30）
- 「複数インスタンスのサポート」（P.6-30）

データ マッピング

表 6-15 に、ACS 4.x および ACS 5.3 間の共有 DACL のデータのマッピングについて示します。

表 6-15　共有 DACL オブジェクトのデータのマッピング

4.x 属性名	5.3 属性名	コメント
Name	Name	名前に使用される値を決定する設定オプションです。
Description	Description	—
ACL Definitions	Downloadable ACL Content	—
	GenId	この属性は GUI で表示されませんが、ACL 定義の各アップデートでアップデートされます。オブジェクト作成の時間に設定されます。ACL 内の変更を検出するデバイスで使用します。

分析およびエクスポート

次の設定オプションが使用でき、分析およびインポート動作に影響を与えます。

- 各 ACL に作成されたオブジェクト名は DACL 名および ACL 名または ACL 名だけの組み合わせになります。
- 以前に説明した名前に加えて、プレフィクスを追加することもできます。

作成されたオブジェクト名は分析され、次の分析の問題がある場合は報告されます。

- オブジェクト名が 32 文字を超える場合には、オブジェクト名の最後の部分が 32 文字に切り詰められることを示すレポートが表示されます。
- 無効な文字を含むすべてのオブジェクト名を次に示します。

  { }' "

  無効な文字は、名前の共有 DACL 部分または ACL 部分から取得されることがあります。DACL 名に無効な文字が含まれる場合、レポートはすべての ACL の組み合わせを表示します。

ヒント　ACL 名が使用されていると、ACS 5.3 に同じ名前の複数の ACL レコードが作成されることがあります。ACL 名が一意であることや、重複する ACL が存在するが 1 つだけインポートすることを確認している場合のみ、このオプションを使用できます。

ACL 定義に分析は必要ありません。

インポート

同じ名前の複数の DACL を作成することはできません。作成すると、インポート レポートに報告されます。これは、DACL 名に ACL オプションを使用して同じ ACL を含む複数の共有 ACL を移行する場合に起こります。

複数インスタンスのサポート

ACS 5.3 では、同じ名前の 2 つの DACL を定義できません。ただし、ACS 4.x インスタンスごとに名前のプレフィクスのある DACL を作成することで各インスタンスに DACL を追加できます。複数インスタンスをサポートすることで、DACL を移行するときに次のいずれかのオプションを選択できます。

- インスタンスごとに異なる名前プレフィクスを定義して、異なる名前の DACL をすべてインポートします。
- プレフィクスを定義しないでください。固有の名前の DACL だけが移行されます。すでに存在する DACL は重複として報告されます。

共有 RAC

ACS 4.x では、RADIUS 認可コンポーネント（RAC）を含む共有プロファイル コンポーネントの定義および RADIUS 属性のセットと認可応答で返される値を定義することができます。これらの共有オブジェクトは ACS 5.3 で定義される認可プロファイルへの方向をマッピングします。

ACS 4.x では、属性はベンダー名と属性名の組み合わせとして GUI で識別されます。ACS 5.3 では、ディクショナリと属性名の組み合わせとして定義されます。内部では、ベンダーまたはディクショナリと属性は RADIUS 応答を作成する間に使用される ID で識別されます。

ここでは、次の内容について説明します。

データ マッピング

表 6-16 に、ACS 4.x および ACS 5.3 間の共有 RACs のデータのマッピングについて示します。

表 6-16　共有 RADIUS 認可コンポーネントのデータ マッピング

4.x 属性名	5.3 属性名	コメント
Name	Name	名前に使用される値を決定する設定オプションです。
Description	Description	—
List of vendor / attribute / value triplets	List of dictionary / attribute / value	[Authorization Profile] の [RADIUS Attributes] タブのセクションに手動で入力した属性のリストが表示されます。

分析およびエクスポート

エクスポート時は、共有 RAC に一部の特殊文字を使用できません。共有 RAC に次の文字が使用される場合は、分析レポートで報告されます。

{ } ' "

ACS 4.x では、Microsoft ベンダー属性を RAC に含めることができますが、値はセットできず、<*Value set by ACS*> という固定の文字列が表示されます。次の Microsoft ベンダー属性を選択できます。

- MS-CHAP-MPPE-Keys (12)
- MS-MPPE-Send-Key (16)
- MS-MPPE-Recv-Key (17)

ACS 5.3 では、これらの属性は設定できませんが、実行する認証のタイプや対応する必要な応答によっては、必要に応じてプロファイルに追加できます。これらの属性が ACS 4.x で定義されると、属性を含む RAC が移行されているが、属性が移行されていないことが分析レポートに記載されます。

インポート

すべての移行された RAC の名前に、追加する予定のプレフィクスを任意で設定することができます。ACS 5.3 では、属性は認可プロファイルに含まれます（該当するプロパティの次の条件に一致する場合）。

- Direction：OUT または BOTH
- Available：TRUE

これらの条件を検証するインポート プロセスはプロファイルに含まれるすべての属性に当てはまります。インポート レポートの矛盾はすべて報告されます。

複数インスタンスのサポート

ACS 5.3 では、同じ名前の 2 つの RAC を定義できません。ただし、ACS 4.x インスタンスごとに名前のプレフィクスのある RAC を作成することで各インスタンスに RAC を追加できます。複数インスタンスをサポートすることで、RAC を移行するときに次のいずれかのオプションを選択できます。

- インスタンスごとに異なる名前プレフィクスを定義して、異なる名前の RAC をすべてインポートします。
- プレフィクスを定義しないでください。固有の名前の RAC だけが移行されます。すでに存在する RAC は重複として報告されます。

RADIUS VSA

ディクショナリとそのコンテンツ（属性定義）は ACS 4.x の重要な中心となる部分です。ディクショナリは RADIUS プロトコルの IETF によって指定された属性を定義し、さまざまなデバイス ベンダーによって定義されたベンダー固有属性（VSA）によって増加します。IETF 属性（属性 26）の 1 つの値にある構造化された名前空間が VSA に割り当てられます。

使用される属性の大部分が ACS と一緒に出荷されたディクショナリに事前に定義されています。ただし、ベンダーがデバイスの機能を拡張すると、新しい VSA が追加されます。

ACS の次のリリースよりも前にアップデートされたディクショナリを取得する場合には、コマンド ライン ユーティリティを使用して新しいベンダーの新しいディクショナリ スロットの定義を行い、ディクショナリの既存の属性を追加したり、またはすでに定義された VSA（たとえば、追加の列挙値など）を更新することができます。

移行時には、ディクショナリは各ベンダーの ACS 5.3 の不足した属性の識別を反復して行います。識別プロセスの間に、次の 2 つの状況が起こることがあります。

- ACS 5.3 ディクショナリにベンダーが存在しない場合、すべてのベンダー属性が移行されます。
- ACS 5.3 ディクショナリにベンダーが存在する場合、ACS 5.3 で定義されていない属性だけが移行されます。

Cisco Airespace 属性 Aire-QoS-Level(2) の場合、列挙値の詳細は ACS 4.1.x および ACS 5 で異なります。数値は移行されているため、この属性を含む RAC を使用して送信した応答には違いがなく、同じ数値が応答に送信されます。ただし、この値に対して ACS の GUI で表示される文字列は異なります。

たとえば、ACS 4.1.x では 1 の値が「*Silver*」と表示され、ACS 5.3 では「*Gold*」と表示されます。

表 6-17 に、ACS 4.1.x および ACS 5.3 間の Aire-QoS-Level (2) 値のマッピングを示します。

表 6-17　ACS 4.1.x および ACS 5.3 での Aire-QoS-Level (2) 値

ACS 4.1.x での値	ACS 5.3 での値
Bronze (0)	Silver (0)
Silver (1)	Gold (1)
Gold (2)	Platinum (2)
Platinum (3)	Bronze (3)
Uranium (4)	Uranium (4)

ACS 4.2 および ACS 5.3 間の Cisco Airespace 属性 Aire-QoS-Level(2) の列挙値の詳細は同じです。

ここでは、次の内容について説明します。

- 「データ マッピング」（P.6-33）

- 「分析およびエクスポート」（P.6-34）
- 「インポート」（P.6-34）

データ マッピング

表 6-18 に、ACS 4.x および ACS 5.3 間の RADIUS ベンダーのデータ フィールドのマッピングについて示します。

表 6-18　RADIUS ベンダーのデータ マッピング

4.x 属性名	5.3 属性名	コメント
Vendor Name	Name	—
—	Description	移行時に生成されます。
Vendor ID	Vendor ID	次のキーのサブキーを列挙する間に、キーのパスにある重要性の低い装置を検査して ACS 4.x のベンダー ID が抽出されます。 CiscoACS\Dictionaries\002\026

表 6-19 に、ACS 4.x および ACS 5.3 間の RADIUS VSA のデータ フィールドのマッピングについて示します。

表 6-19　RADIUS VSA のデータ マッピング

4.x 属性名	5.3 属性名	コメント
Name	Name	ACS 5.3 の名前の最大長は非常に短いです。
—	Description	移行時に生成されます。
Attribute Number	Attribute Number	ベンダー キーのサブキーを列挙する間に、キーのパスにある重要性の低い装置を検査して ACS 4.x の属性番号が抽出されます。
Profile	Direction	IN：1（インバウンド） OUT：2（アウトバウンド） IN OUT：3（両方）
Type	ValueType	構文 ID がマッピングされています。

分析およびエクスポート

RADIUS VSA の分析フェーズでは ACS 4.x のディクショナリ コンテンツの ACS 5.3 のディクショナリ コンテンツへのマージを中心に取り上げます。分析には次の 2 つの例があります

- 一般的に、ACS 4.x をサポートするベンダーにとって、ACS 5.3 のディクショナリはより最新のものとなります。ただし、新しい VSA を含めたり、既存の VSA を修正するために一部の ACS 4.x ベンダー ディクショナリを修正していることがあります（たとえば、新しい列挙値など）。移行動作は次のようになります。
  - ACS 5.3 で定義された属性は移行の間は変更されません。そのような属性に対しては警告が表示されます。
  - ACS 5.3 で定義されていないが、ACS 4.x に存在する属性は移行されます。
- ACS 4.x にインポートされたが、ACS 5.3 に存在しないベンダーは分析の警告が出ることなく移行されます。

（注）　ACS 4.x および ACS 5.3 VSA 属性（プロファイル、名前、タイプ）の違いが分析レポートに報告されます。

インポート

エクスポートされたすべての VSA が ACS 5.3 にインポートされます。

EAP-Fast マスター キーおよび認証局 ID

ACS 5.3 では、ACS 4.x で認証されたすべてのオブジェクト（ユーザまたはデバイス）に対するサポートを保存できます。したがって、すべてのマスター キーおよび ACS 4.x からの認証局 ID が移行されます。

ACS 4.x のマスター キーは ACS 5.3 のスキーマとは異なるスキーマを持ち、さまざまな IM オブジェクトに移行されます。ACS 4.x は認証局 ID をノード単位で保存し、ACS 5.3 は認証局 ID をプライマリ データベースの中だけで保存して、展開全体に適用します。

ここでは、次の内容について説明します。

データ マッピング

表 6-20 に、ACS 4.x および ACS 5.3 間の EAP-FAST マスター キーおよび認証局 ID のデータのマッピングについて示します。

表 6-20　EAP-Fast マスター キーおよび認証局 ID へのデータ マッピング

4.x 属性名	5.3 属性名	コメント
Master Key ID	Identifier	ACS 4.x 内部 ID
Encryption key	EncriptionKey	32 バイト

表 6-20　EAP-Fast マスター キーおよび認証局 ID へのデータ マッピング （続き）

4.x 属性名	5.3 属性名	コメント
Authentication key	AuthenticationKey	32 バイト
Cipher suite	Cipher	—
Creation Time	—	—
Expiration Time (TTL)	Expiration Time	有効期限は、現在の時刻と非アクティブなマスター キー TTL を追加して計算されます。

有効期限は次のように計算されます。

1. データベース内のキーのリストから最後のキーを確認して、それが期限切れであるかを判断します。
2. キーの作成時間が現在のキーの KeyCtime として保存されます。
3. Calling Time(NULL) によって現在の時刻が計算されます。
4. TTL は [AuthenConfig] > [EAP-FAST] に保存されたキーのために保存されます。
5. 有効期限は、現在の時刻と非アクティブなマスター キー TTL を追加して計算されます。

マスター キー TTL ユニットは次のように表されます。

分：1、時間：2、日：3、週：4、月：5、年：6

たとえば、アクティブなマスター キー TTL が 1 か月として選択された場合は、1 * 30 * 24 * 3600 と同じです。

分析およびエクスポート

分析は行われません。期限切れのキーは移行されません。

インポート

ACS 5.3 では、オブジェクトはマスター キーの表に追加され、GUI を使用して利用することができません。認証局 ID が EAP-FAST グローバル設定に移行されます。

複数インスタンスのサポート

ACS 5.3 では、同じ ID に 2 つのマスター キーを定義できません。一意のマスター キーだけが ACS 4.x の複数インスタンスから移行できます。

ACS 5.3 では、グローバルな EAP 設定として認証局 ID が保存されますが、ノード単位またはインスタンス単位では保存されません。したがって、1 つのインスタンスだけから移行することができます。

ACS 4.x データの分析およびエクスポート

移行ユーティリティのオプション 1 を選択して AnalyzeAndExport を実行します。例 6-1（P.6-2）を参照してください。分析およびエクスポート フェーズは ACS 4.x の移行元マシンのバックアップから復元したデータを使用して ACS 4.x 移行マシン上で実行されます。AnalyzeAndExport 要約レポートで次の総数をリストします。

- 検出されたオブジェクト。
- 各オブジェクトで報告された問題。
- 移行されたオブジェクト。
- 各オブジェクトの問題の情報。
- 統合するデータ。「データの統合」（P.6-37）を参照してください。

分析およびエクスポート フェーズを複数回実行して分析サイクル間の変更を設定できます。たとえば、ネットワーク デバイス用のオーバーラップする IP アドレスがあるとします。ACS 4.x アプリケーションを使用してこの問題を解決します。問題を解決して、分析およびエクスポート フェーズを再度実行し、インポート フェーズに進みます。「IP アドレスのオーバーラップ」（P.D-3）を参照してください。

ここでは、次の内容について説明します。

例 6-2 に、分析およびエクスポート フェーズの要約レポートの例を示します。この例では、移行ユーティリティで option 3- AllDevicesObjects を選択した場合に生成されるレポートを示しています。

例 6-2　AnalyzeAndExport 要約レポート

```
------------------------------------------------------------------------------
        Summary Report for phase AnalyzeAndExport
------------------------------------------------------------------------------
Network Device Groups
------------------------------------------------------------------------------
Total:3        Successful:3       Reported issues:0
------------------------------------------------------------------------------
------------------------------------------------------------------------------
Network Device
------------------------------------------------------------------------------
Total:5        Successful:5       Reported Issues:0
------------------------------------------------------------------------------
------------------------------------------------------------------------------
         Analysis and Export Report
------------------------------------------------------------------------------
------------------------------------------------------------------------------
        Network Device Group
------------------------------------------------------------------------------
------------------------------------------------------------------------------
INFO: The following objects are password_included
------------------------------------------------------------------------------
------------------------------------------------------------------------------
1. Name: NDG01 Comment: NDG has shared key password
2. Name: NDG02 Comment: NDG has shared key password
------------------------------------------------------------------------------
------------------------------------------------------------------------------
       Network Device
------------------------------------------------------------------------------
```

移行された属性のリストについては、付録 A「移行ユーティリティでの ACS 5.3 属性サポート」を参照してください。

データの統合

統合プロセスは分析およびエクスポート フェーズおよび次の場合に実行されます。

- 作成された共有オブジェクトを分析する。
- 同一のオブジェクトを識別する。
- 重複する ACS 4.x オブジェクトが ACS 5.3 に移行された 1 つのオブジェクトに縮小されていることを確認します。次に、このオブジェクトは ACS 5.3 ポリシーによって参照されます。

  たとえば、複数のコマンド セットが異なるように見えるが、実際には同じコマンド セットであると分析レポートに表示されることがあります。これは、*show* または *sho* のようなコマンド セットのショートカットのことです。ACS 5.3 では、移行したコマンド セットの情報を組み込むようなポリシーを定義することができます。ACS 5.3 のポリシーの詳細については、『*User Guide for Cisco Secure Access Control System 5.3*』を参照してください。
- 次の統合を行います。
  - ユーザおよびユーザ グループ コマンド セットをコマンド セット プロファイルに統合。
  - グループのシェル実行をシェル プロファイルに統合。

分析およびエクスポート フェーズの結果の問題

すべてのデータ エントリが ACS 4.x から ACS 5.3 へ移行できるわけではありません。分析およびエクスポート フェーズでは、ネットワーク デバイスの IP アドレスのオーバーラップなどの問題を表示します。

ACS 4.x IP アドレス ネットワーク デバイス定義の別の問題として、ワイルドカードおよび範囲が含まれます。ACS 5.3 は標準的なサブネット マスク表現を使用します。したがって、ネットワーク デバイス定義には互換性がありません。

分析およびエクスポートではこれらの問題の詳細を報告します。ACS 4.x アプリケーションのこれらの問題に対応して、あとで分析およびエクスポートを再度実行できます。このプロセスは必要に応じて何度でも再実行できます。これらの問題を解決した後に、エクスポートしたデータを ACS 5.3 マシンにインポートすることができます。

ACS 5.3 への ACS 4.x データのインポート

移行ユーティリティのオプション 2 を選択してインポートを実行します。例 6-1（P.6-2）を参照してください。このフェーズでは、エクスポート フェーズで作成した ACS 4.x データのエクスポート ファイルがインポートされます。

大規模なデータベースからデータを移行する場合に、インポート プロセスに時間がかかる場合があります。

（注）　ACS 5.3 のインポートが失敗した場合は、ACS 5.3 データベースを復元します。

例 6-3 に、インポート フェーズの進捗レポートの例を示します。このフェーズでは 2 つのレポートを生成します。

- 例 6-4 にインポート要約レポートを示します。
- 例 6-5 にインポート レポートを示します。

例 6-3　インポート フェーズの進捗レポートの例

```
3
Tue Jul 20 14:57:00 EST 2007 Network Device Group 1 / 3 (33%) complete.
Tue Jul 20 14:57:00 EST 2007 Network Device Group 2 / 3 (66%) complete.
Tue Jul 20 14:57:00 EST 2007 Network Device Group 3 / 3 (100%) complete.
Imported 3 items of type: Network Device Group
Imported 2 items of type: User Group
Tue Jul 20 14:57:02 EST 2007 Group Shell Exec 1 / 1 (100%) complete.
Imported 1 items of type: Group Shell Exec
Tue Jul 20 14:57:03 EST 2007 Group Command Set 1 / 1 (100%) complete.
Imported 1 items of type: Group Command Set
Imported 0 items of type: User Shell Exec
Imported 0 items of type: User Command Set
Tue Jul 20 14:57:06 EST 2007 Shared Command Set 1 / 2 (50%) complete.
Tue Jul 20 14:57:24 EST 2007 Shared Command Set 2 / 2 (100%) complete.
Imported 2 items of type: Shared Command Set
Tue Jul 20 14:57:25 EST 2007 User 1 / 5 (20%) complete.
Tue Jul 20 14:57:25 EST 2007 User 2 / 5 (40%) complete.
Tue Jul 20 14:57:25 EST 2007 User 3 / 5 (60%) complete.
Tue Jul 20 14:57:25 EST 2007 User 4 / 5 (80%) complete.
Tue Jul 20 14:57:26 EST 2007 User 5 / 5 (100%) complete.
Imported 5 items of type: User
Tue Jul 20 14:57:26 EST 2007 Network Device 1 / 6 (16%) complete.
Tue Jul 20 14:57:27 EST 2007 Network Device 2 / 6 (33%) complete.
Tue Jul 20 14:57:28 EST 2007 Network Device 3 / 6 (50%) complete.
Tue Jul 20 14:57:28 EST 2007 Network Device 4 / 6 (66%) complete.
Tue Jul 20 14:57:29 EST 2007 Network Device 5 / 6 (83%) complete.
Tue Jul 20 14:57:29 EST 2007 Network Device 6 / 6 (100%) complete.
```

例 6-4　インポート要約レポート

```
-------------------------------------------------------------------------------
        Summary Report for phase imported
-------------------------------------------------------------------------------
User Attributes
-------------------------------------------------------------------------------
Total:2         Successful:0    Reported issues:2
-------------------------------------------------------------------------------
Network Device Groups
-------------------------------------------------------------------------------
Total:3         Successful:2    Reported issues:1
-------------------------------------------------------------------------------
Groups Shell Exec
-------------------------------------------------------------------------------
Total:1         Successful:0    Reported issues:1
-------------------------------------------------------------------------------
Groups Command Set
-------------------------------------------------------------------------------
Total:1         Successful:1    Reported issues:0
-------------------------------------------------------------------------------
Users Shell Exec
-------------------------------------------------------------------------------
Total:0         Successful:0    Reported issues:0
-------------------------------------------------------------------------------
Users Command Set
-------------------------------------------------------------------------------
Total:0         Successful:0    Reported issues:0
-------------------------------------------------------------------------------
```

```
Shared Command Sets
--------------------------------------------------------------------------------
Total:2         Successful:2    Reported issues:0
--------------------------------------------------------------------------------
Network Devices
--------------------------------------------------------------------------------
Total:5         Successful:5    Reported issues:0
--------------------------------------------------------------------------------
Users
--------------------------------------------------------------------------------
Total:6         Successful:6    Reported issues:0
--------------------------------------------------------------------------------
Shared Downloadable ACL
--------------------------------------------------------------------------------
Total:6         Successful:6    Reported issues:0
--------------------------------------------------------------------------------
EAP FAST - Master Keys
--------------------------------------------------------------------------------
Total:6         Successful:6    Reported issues:0
--------------------------------------------------------------------------------
Mab
--------------------------------------------------------------------------------
Total:6         Successful:6    Reported issues:0
--------------------------------------------------------------------------------
```

例 6-5　　インポート レポート

```
--------------------------------------------------------------------------------------------
        Import Report
--------------------------------------------------------------------------------------------
The following User Attributes were not imported:
--------------------------------------------------------------------------------------------
1. Name: Real Name      Comment: Attribute cannot be added.
2. Name: Description    Comment: Attribute cannot be added.
The following Network Device Groups were not imported:
--------------------------------------------------------------------------------------------
1. Name: Not Assigned   Comment: Error 1: Failure to add object: Migrated NDGs:All
Migrated NDGs:Not Assigned in function: createGroup

The following User Groups were not imported:
--------------------------------------------------------------------------------------------
1. Name: IdentityGroup:All Groups:Migrated Group        Comment: Failure to add object:
IdentityGroup:All Groups:Migrated Group in function: createGroup

The following Group Shell Exec were not imported:
--------------------------------------------------------------------------------------------
1. Name: ACS_Migrate_Priv Comment: customError CRUDex002 Object already exist exception
The following Group Command Set failed on import:
--------------------------------------------------------------------------------------------
The following User Shell Exec were not imported:
--------------------------------------------------------------------------------------------
The following User Command Set were not imported:
--------------------------------------------------------------------------------------------
The following Shared Command Set were not imported:
--------------------------------------------------------------------------------------------
The following Network Devices were not imported:
--------------------------------------------------------------------------------------------
The following Users were not imported:
--------------------------------------------------------------------------------------------
The following Shared Downloadable ACL were not imported:
--------------------------------------------------------------------------------------------
The following EAP FAST - Master Keys were not imported:
```

```
-------------------------------------------------------------------------------------------
The following Mab were not imported:
-------------------------------------------------------------------------------------------
```

複数のインスタンスの移行

移行ユーティリティのオプション 4 を選択して、別の ACS 4.x インスタンスをインポートします。例 6-1（P.6-2）を参照してください。複数の ACS 4.x インスタンスを ACS 5.3 にインポートすることができます。例 6-6 に、複数のインスタンスを移行する場合に表示されるプロンプトを示します。

例 6-6　　複数のインスタンスのインポート

```
Choose one of the following:
1 - AnalyzeAndExport
2 - Import
3 - CreateReportFiles
4 - Exit
-----------------------------------------------------
4

Would you like to migrate another ACS4.x server? [no]
yes
Enter ACS 4.x Sever ID:
-----------------------------------------------------
```

別の ACS 4.x インスタンスのサーバ ID またはホスト名を入力した後、移行プロセス全体が再び開始されます。これにより、複数の ACS 4.x インスタンスを ACS 5.3 にインポートすることができます。

移行によるメモリおよびパフォーマンスへの影響

ACS 4.x 移行サーバからデータのエクスポートが実行されます。ACS 4.x 運用サーバまたはソースサーバから直接実行されることはありません。したがって、移行によって ACS 4.x 運用サーバのパフォーマンスが影響を受けることはありません。移行ユーティリティは標準的な PC 環境で実行できます。

移行されたデータのインポート中、ACS 5.3 サーバはアイドルになり、AAA 要求は処理されません。

レポートの印刷とレポート タイプ

移行ユーティリティのオプション 3 を選択して、フル レポートおよび要約レポートを CSV ファイル形式に出力します。例 6-1（P.6-2）を参照してください。移行ディレクトリ内の *config* フォルダに、移行ユーティリティ レポートが保存されます。*config* フォルダ内に、移行する ACS 4.x サーバごとにサーバ ID と同じ名前の新しいフォルダが作成されます。

たとえば、サーバ ID が *test1* の場合、*test1* が *config* フォルダの下に作成され、移行ユーティリティ レポートが保存されます。レポート名はサーバ ID と同じです。ここでは、次の内容について説明します。

- 「分析レポートとエクスポート要約レポート」（P.6-42）
- 「分析レポートとエクスポート フル レポート」（P.6-42）
- 「インポート要約レポート」（P.6-43）

- 「インポート フル レポート」（P.6-44）
- 「インポートの検証」（P.6-45）
- 「要約レポート」（P.6-46）
- 「フル レポート」（P.6-47）

表 6-21 に、移行フェーズと、各フェーズで生成されるレポートを示します。

表 6-21　移行時に生成されるレポート

移行フェーズ	生成されるレポート
分析およびエクスポート	• AnalyzeAndExport_*server ID*_Summary_report.csv • AnalyzeAndExport_*server ID*_full_report.csv
インポート	• ImportSummary_*server ID*_report.csv • Importfull_*server ID*_report.csv

表 6-22 で、移行ユーティリティ レポートについて説明します。

表 6-22　移行ユーティリティのレポート

移行レポート	説明
AnalyzeAndExport_Summary_report.csv	分析フェーズおよびエクスポート フェーズの要約レポート。移行できるオブジェクトの総数と関連する問題を示します。
AnalyzeAndExport_full_report.csv	分析フェーズおよびエクスポート フェーズのフル レポート。移行できるオブジェクトの総数と各オブジェクトの説明コメントを示します。
ImportSummary_report.csv	インポート フェーズの要約レポート。インポートされるオブジェクトの総数と関連する問題を示します。
Importfull_report.csv	インポート フェーズのフル レポート。インポートされるオブジェクトの総数と各オブジェクトの説明コメントを示します。
Full_report.csv	移行ユーティリティのすべてのレポートを 1 つのファイルに統合します。
Summary_report.csv	すべての移行フェーズについての要約情報を示します。

分析レポートとエクスポート要約レポート

図 6-1 に、分析レポートとエクスポート要約レポートを示します。表 6-23 に、分析レポートとエクスポート要約レポートのカラムの定義を示します。

図 6-1　　分析レポートとエクスポート要約レポート

	A	B	C	D	E	F	G
1	Server Id	Phase	Element Name	Total Elements	Total Migratable	Total with Issues	Comment
2	racbugobj	AnalyzeAndExport	User Attributes	2	2	0	
3	racbugobj	AnalyzeAndExport	Network Device Groups	1	1	0	
4	racbugobj	AnalyzeAndExport	User Groups	500	0	500	
5	racbugobj	AnalyzeAndExport	Groups Shell Exec	0	0	0	
6	racbugobj	AnalyzeAndExport	Users Shell Exec	0	0	0	
7	racbugobj	AnalyzeAndExport	Users	0	0	0	
8	racbugobj	AnalyzeAndExport	Shared Command Sets	0	0	0	
9	racbugobj	AnalyzeAndExport	Groups Command Set	0	0	0	
10	racbugobj	AnalyzeAndExport	Users Command Set	0	0	0	
11	racbugobj	AnalyzeAndExport	Network Device	12	12	0	
12	racbugobj	AnalyzeAndExport	Shared Downloadable ACL	0	0	0	
13	racbugobj	AnalyzeAndExport	EAP FAST - Master Keys	0	0	0	
14	racbugobj	AnalyzeAndExport	MAB	0	0	0	
15	racbugobj	AnalyzeAndExport	RAC	6	1	5	

194859

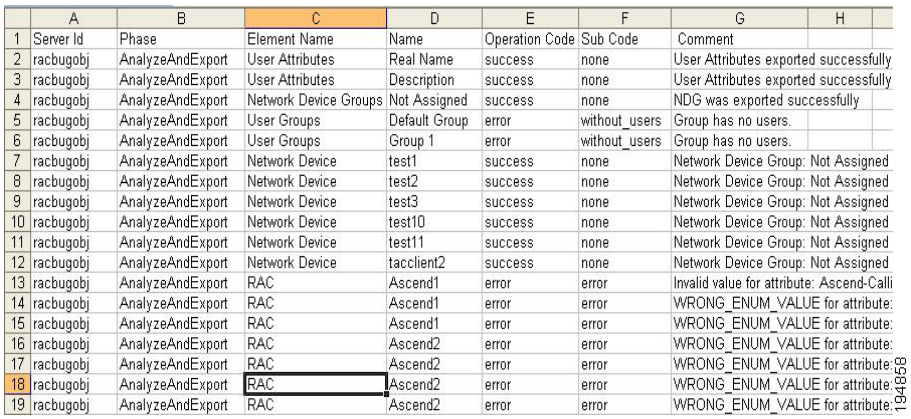
表 6-23　　分析レポートとエクスポート要約レポートのカラムの定義

カラム	説明
Server ID	サーバの名前。
Phase	移行フェーズの名前。
Element Name	移行する ACS オブジェクト タイプの名前。
Total Elements	要素の合計数。
Total Migratable	移行できる要素の合計数。
Total with Issues	問題がある要素の合計数。
Comment	ACS オブジェクトのステータスを示すメッセージ。

分析レポートとエクスポート フル レポート

図 6-2 に、分析レポートとエクスポート フル レポートを示します。表 6-24 に、分析レポートとエクスポート フル レポートのカラムの定義を示します。

図 6-2　　分析レポートとエクスポート フル レポート



	A	B	C	D	E	F	G	H
1	Server Id	Phase	Element Name	Name	Operation Code	Sub Code	Comment	
2	racbugobj	AnalyzeAndExport	User Attributes	Real Name	success	none	User Attributes exported successfully	
3	racbugobj	AnalyzeAndExport	User Attributes	Description	success	none	User Attributes exported successfully	
4	racbugobj	AnalyzeAndExport	Network Device Groups	Not Assigned	success	none	NDG was exported successfully	
5	racbugobj	AnalyzeAndExport	User Groups	Default Group	error	without_users	Group has no users.	
6	racbugobj	AnalyzeAndExport	User Groups	Group 1	error	without_users	Group has no users.	
7	racbugobj	AnalyzeAndExport	Network Device	test1	success	none	Network Device Group: Not Assigned	
8	racbugobj	AnalyzeAndExport	Network Device	test2	success	none	Network Device Group: Not Assigned	
9	racbugobj	AnalyzeAndExport	Network Device	test3	success	none	Network Device Group: Not Assigned	
10	racbugobj	AnalyzeAndExport	Network Device	test10	success	none	Network Device Group: Not Assigned	
11	racbugobj	AnalyzeAndExport	Network Device	test11	success	none	Network Device Group: Not Assigned	
12	racbugobj	AnalyzeAndExport	Network Device	tacclient2	success	none	Network Device Group: Not Assigned	
13	racbugobj	AnalyzeAndExport	RAC	Ascend1	error	error	Invalid value for attribute: Ascend-Calli	
14	racbugobj	AnalyzeAndExport	RAC	Ascend1	error	error	WRONG_ENUM_VALUE for attribute:	
15	racbugobj	AnalyzeAndExport	RAC	Ascend1	error	error	WRONG_ENUM_VALUE for attribute:	
16	racbugobj	AnalyzeAndExport	RAC	Ascend2	error	error	WRONG_ENUM_VALUE for attribute:	
17	racbugobj	AnalyzeAndExport	RAC	Ascend2	error	error	WRONG_ENUM_VALUE for attribute:	
18	racbugobj	AnalyzeAndExport	RAC	Ascend2	error	error	WRONG_ENUM_VALUE for attribute:	
19	racbugobj	AnalyzeAndExport	RAC	Ascend2	error	error	WRONG_ENUM_VALUE for attribute:	

194858

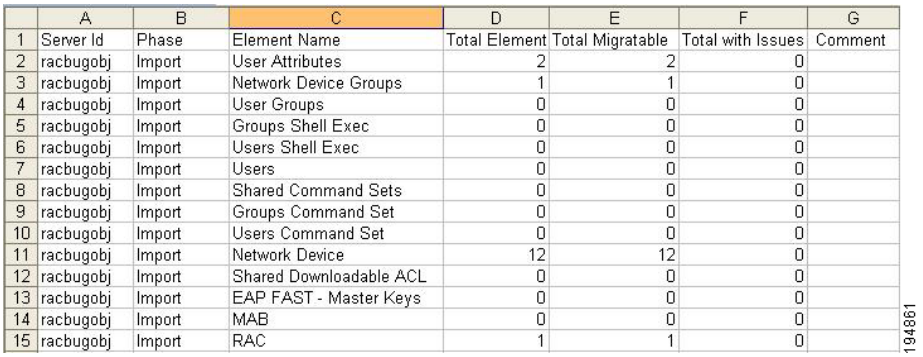
表 6-24　　分析レポートとエクスポート フル レポートのカラムの定義

カラム	説明
Server ID	サーバの名前。
Phase	移行フェーズの名前。
Element Name	抽出された ACS オブジェクト タイプの名前。
Name	移行する ACS オブジェクト タイプの名前。
Operation code	分析フェーズおよびエクスポート フェーズのステータス。有効な値は success、error、および info（情報メッセージ）。
Sub Code	動作のステータスに関連付けられたコード。
Comment	ACS オブジェクトのステータスを示すメッセージ。

インポート要約レポート

図 6-3 にインポート要約レポートを示します。表 6-25 に、インポート要約レポートのカラムの定義を示します。

図 6-3　　インポート要約レポート



	A	B	C	D	E	F	G
1	Server Id	Phase	Element Name	Total Element	Total Migratable	Total with Issues	Comment
2	racbugobj	Import	User Attributes	2	2	0	
3	racbugobj	Import	Network Device Groups	1	1	0	
4	racbugobj	Import	User Groups	0	0	0	
5	racbugobj	Import	Groups Shell Exec	0	0	0	
6	racbugobj	Import	Users Shell Exec	0	0	0	
7	racbugobj	Import	Users	0	0	0	
8	racbugobj	Import	Shared Command Sets	0	0	0	
9	racbugobj	Import	Groups Command Set	0	0	0	
10	racbugobj	Import	Users Command Set	0	0	0	
11	racbugobj	Import	Network Device	12	12	0	
12	racbugobj	Import	Shared Downloadable ACL	0	0	0	
13	racbugobj	Import	EAP FAST - Master Keys	0	0	0	
14	racbugobj	Import	MAB	0	0	0	
15	racbugobj	Import	RAC	1	1	0	

194861

表 6-25　インポート要約レポートのカラムの定義

カラム	説明
Server ID	サーバの名前。
Phase	移行フェーズの名前。
Element Name	移行する ACS オブジェクト タイプの名前。
Total Elements	要素の合計数。
Total Migratable	移行される要素の合計数。
Total with Issues	問題がある要素の合計数。
Comment	ACS オブジェクトのステータスを示すメッセージ。

インポート フル レポート

図 6-4 にインポート フル レポートを示します。表 6-26 に、インポート フル レポートのカラムの定義を示します。

図 6-4　インポート フル レポート

	Server Id	Phase	Element Name	Name	Operation Code	Sub Code	Comment
2	racbugobj	Import	User Attributes	Real Name	success	none	Attribute Successfully Imported
3	racbugobj	Import	User Attributes	Description	success	none	Attribute Successfully Imported
4	racbugobj	Import	Network Device Groups	Not Assigned	success	none	Imported Successfully
5	racbugobj	Import	Network Device	test1	success	none	Imported Successfully
6	racbugobj	Import	Network Device	test2	success	none	Imported Successfully
7	racbugobj	Import	Network Device	test3	success	none	Imported Successfully
8	racbugobj	Import	Network Device	test4	success	none	Imported Successfully
9	racbugobj	Import	Network Device	test5	success	none	Imported Successfully
10	racbugobj	Import	Network Device	test6	success	none	Imported Successfully
11	racbugobj	Import	Network Device	test7	success	none	Imported Successfully
12	racbugobj	Import	Network Device	test8	success	none	Imported Successfully
13	racbugobj	Import	Network Device	test9	success	none	Imported Successfully
14	racbugobj	Import	Network Device	test10	success	none	Imported Successfully
15	racbugobj	Import	Network Device	test11	success	none	Imported Successfully
16	racbugobj	Import	Network Device	tacclient2	success	none	Imported Successfully
17	racbugobj	Import	RAC	selvisameconf	success	none	Imported Successfully

表 6-26　インポート フル レポートのカラムの定義

カラム	説明
Server ID	サーバの名前。
Phase	移行フェーズの名前。
Element Name	移行する ACS オブジェクト タイプの名前。
Name	ユーザが指定した名前。
Operation code	動作が成功したかどうか、エラーが発生したかどうかを示します。
Sub Code	動作のステータスに関連付けられたコード。
Comment	ACS オブジェクトのステータスを示すメッセージ。

インポートの検証

インポート フェーズの完了後、インポート要約レポートを手動で分析する必要があります。これによって、次のリストが表示されます。

- 移行されるオブジェクトの合計数。
- 正常に移行されたオブジェクトの合計数。
- 移行に失敗したオブジェクトの合計数。

インポート フル レポートで、移行されなかったオブジェクトの情報を確認できます。これによって、次のリストが表示されます。

- オブジェクトの名前。
- オブジェクトのステータス。
- エラーの原因。

ACS 4.x オブジェクトのいずれかが移行されない場合、次の手順を実行する必要があります。

1. 移行されていないオブジェクトを手動で追加するか、または ACS 4.x アプリケーションでこれらの問題を解決します。
2. 分析フェーズおよびエクスポート フェーズを再実行します。
3. （インポートの前に）ACS 5.3 データベースを以前の状態に復元します。
4. インポート フェーズを再度実行します。

（注） 移行が完了したことを確認するには、インポート要約レポートを分析してください。レポートにすべてのオブジェクトが正常に移行されたと表示されている場合、移行は完了です。

要約レポート

図 6-5 に、すべての移行フェーズについての要約レポート情報を示します。表 6-27 に、要約レポートのカラムの定義を示します。

図 6-5　　要約レポート

	A	B	C	D	E	F	G
1	Server Id	Phase	Element Name	Total Elements	Total Migratable	Total with Issues	Comment
2	racbugobj	AnalyzeAndExport	User Attributes	2	2	0	
3	racbugobj	AnalyzeAndExport	Network Device Groups	1	1	0	
4	racbugobj	AnalyzeAndExport	User Groups	500	0	500	
5	racbugobj	AnalyzeAndExport	Groups Shell Exec	0	0	0	
6	racbugobj	AnalyzeAndExport	Users Shell Exec	0	0	0	
7	racbugobj	AnalyzeAndExport	Users	0	0	0	
8	racbugobj	AnalyzeAndExport	Shared Command Sets	0	0	0	
9	racbugobj	AnalyzeAndExport	Groups Command Set	0	0	0	
10	racbugobj	AnalyzeAndExport	Users Command Set	0	0	0	
11	racbugobj	AnalyzeAndExport	Network Device	12	12	0	
12	racbugobj	AnalyzeAndExport	Shared Downloadable ACL	0	0	0	
13	racbugobj	AnalyzeAndExport	EAP FAST - Master Keys	0	0	0	
14	racbugobj	AnalyzeAndExport	MAB	0	0	0	
15	racbugobj	AnalyzeAndExport	RAC	6	1	5	
16	racbugobj	Import	User Attributes	2	2	0	
17	racbugobj	Import	Network Device Groups	1	1	0	
18	racbugobj	Import	User Groups	0	0	0	
19	racbugobj	Import	Groups Shell Exec	0	0	0	
20	racbugobj	Import	Users Shell Exec	0	0	0	
21	racbugobj	Import	Users	0	0	0	
22	racbugobj	Import	Shared Command Sets	0	0	0	
23	racbugobj	Import	Groups Command Set	0	0	0	
24	racbugobj	Import	Users Command Set	0	0	0	
25	racbugobj	Import	Network Device	12	12	0	
26	racbugobj	Import	Shared Downloadable ACL	0	0	0	
27	racbugobj	Import	EAP FAST - Master Keys	0	0	0	
28	racbugobj	Import	MAB	0	0	0	
29	racbugobj	Import	RAC	1	1	0	

194864

表 6-27　　要約レポートのカラムの定義

カラム	説明
Server ID	サーバの名前。
Phase	移行フェーズの名前。
Element Name	移行された ACS オブジェクトの名前。
Total Elements	処理された ACS オブジェクトの合計数。
Total Migratable	移行された ACS オブジェクトの合計数。
Total with Issues	各 ACS オブジェクトの問題の合計数。
Comment	ACS オブジェクトのステータスを示すメッセージ。

フル レポート

図 6-6 に、すべての移行フェーズについてのフル レポート情報を示します。表 6-28 に、フル レポートのカラムの定義を示します。

図 6-6　　フル レポート

	A	B	C	D	E	F	G
1	Server Id	Phase	Element Name	Name	Operation Code	Sub Code	Comment
2	racbugobj	AnalyzeAndExport	Network Device	test9	success	none	Network Device Group: Not Assigned network devic
3	racbugobj	AnalyzeAndExport	Network Device	test10	success	none	Network Device Group: Not Assigned network devic
4	racbugobj	AnalyzeAndExport	Network Device	test11	success	none	Network Device Group: Not Assigned network devic
5	racbugobj	AnalyzeAndExport	Network Device	tacclient2	success	none	Network Device Group: Not Assigned network devic
6	racbugobj	AnalyzeAndExport	RAC	Ascend1	error	error	Invalid value for attribute: Ascend-Calling-Id-Present
7	racbugobj	AnalyzeAndExport	RAC	Ascend1	error	error	WRONG_ENUM_VALUE for attribute: Ascend-Num
8	racbugobj	AnalyzeAndExport	RAC	Ascend1	error	error	WRONG_ENUM_VALUE for attribute: Ascend-FR-L
9	racbugobj	AnalyzeAndExport	RAC	Ascend2	error	error	WRONG_ENUM_VALUE for attribute: Ascend-Appl
10	racbugobj	AnalyzeAndExport	RAC	Ascend2	error	error	WRONG_ENUM_VALUE for attribute: Ascend-Rout
11	racbugobj	AnalyzeAndExport	RAC	Ascend2	error	error	WRONG_ENUM_VALUE for attribute: Ascend-FR-L
12	racbugobj	AnalyzeAndExport	RAC	Ascend2	error	error	WRONG_ENUM_VALUE for attribute: Ascend-TS-Id
13	racbugobj	AnalyzeAndExport	RAC	Ascend2	error	error	WRONG_ENUM_VALUE for attribute: Ascend-CBC
14	racbugobj	AnalyzeAndExport	RAC	Ascend3	error	error	WRONG_ENUM_VALUE for attribute: Ascend-Requ
15	racbugobj	AnalyzeAndExport	RAC	Ascend3	error	error	WRONG_ENUM_VALUE for attribute: Ascend-PPP
16	racbugobj	AnalyzeAndExport	RAC	rj	error	unsupported_vendor	ACS 5 does not support this attribute.: (vid=9 att=2
17	racbugobj	AnalyzeAndExport	RAC	rj	error	error	WRONG_ENUM_VALUE for attribute: USR-Simplifi
18	racbugobj	AnalyzeAndExport	RAC	Ascend3	success	none	RAC exported successfully
19	racbugobj	AnalyzeAndExport	RAC	unique2	error	unsupported_vendor	ACS 5 does not support this attribute.: (vid=9 att=2
20	racbugobj	AnalyzeAndExport	RAC	unique2	error	error	WRONG_ENUM_VALUE for attribute: USR-Simplifi
21	racbugobj	Import	User Attributes	Real Name	success	none	Attribute Successfully Imported
22	racbugobj	Import	User Attributes	Description	success	none	Attribute Successfully Imported
23	racbugobj	Import	Network Device Groups	Not Assigned	success	none	Imported Successfully
24	racbugobj	Import	Network Device	test1	success	none	Imported Successfully
25	racbugobj	Import	Network Device	test2	success	none	Imported Successfully
26	racbugobj	Import	Network Device	test3	success	none	Imported Successfully
27	racbugobj	Import	Network Device	test4	success	none	Imported Successfully
28	racbugobj	Import	Network Device	test5	success	none	Imported Successfully
29	racbugobj	Import	Network Device	test6	success	none	Imported Successfully

276460

表 6-28　　フル レポートのカラムの定義

カラム	説明
Server ID	サーバの名前。
Phase	移行フェーズの名前。
Element Name	移行された ACS オブジェクトの名前。
Name	ユーザが指定した名前。
Operation Code	動作が成功したかどうか、エラーが発生したかどうかを示します。
Sub Code	動作のステータスに関連付けられたコード。
Comment	ACS オブジェクトのステータスを示すメッセージ。

エラーと例外の処理

分析フェーズとエクスポート フェーズまたはインポート フェーズで発生したエラー は、それぞれのレポートで報告されます。移行のエラーとその解決手順の詳細については、「移行の問題の解決」（P.D-3）を参照してください。

さまざまな ACS オブジェクトの移行時に表示される可能性のあるエラーおよび通知メッセージについては、「移行ユーティリティ メッセージ」（P.D-6）を参照してください。

移行の確認

ACS 5.3 ターゲット マシンにログインして、ACS 4.x の要素を正常に移行したことを確認します。移行フェーズで、ACS 4.x で定義された次の ACS 要素が ACS 5.3 に移行されます。

- ユーザ属性
- ユーザ属性値
- NDG
- ユーザ グループ
- グループ Shell Exec
- グループ コマンド セット
- ユーザ Shell Exec
- ユーザ コマンド セット
- 共有コマンド セット
- ネットワーク デバイス
- ユーザ
- 共有 DACL
- EAP-FAST マスター キー
- MAB
- 共有 RAC
- カスタマー VSA

ACS 4.x オブジェクトにアクセスするには、『*User Guide for Cisco Secure Access Control Server 4.2*』に記載されている手順に従います。ACS 5.3 オブジェクトにアクセスするには、『*User Guide for Cisco Secure Access Control System 5.3*』に記載されている手順に従います。

ここでは、移行の確認について説明します。

- 「ユーザおよびユーザ グループ」（P.6-49）
- 「コマンド シェルの移行」（P.6-50）
- 「コマンド セットの移行」（P.6-51）
- 「NDG の移行」（P.6-52）
- 「ネットワーク デバイスの移行」（P.6-53）
- 「DACL の移行」（P.6-54）
- 「MAB の移行」（P.6-55）
- 「共有 RAC」（P.6-56）
- 「RADIUS VSA」（P.6-57）
- 「KEK キーと MACK キー」（P.6-59）

ユーザおよびユーザ グループ

図 6-7 に、ACS 4.x のユーザとユーザ グループを示し、図 6-8 に ACS 5.3 に移行されたユーザとユーザ グループを示します。[Users and Identity Stores] > [Internal Identity Stores] > [Users] を選択して、移行されたユーザとユーザ グループにアクセスします。

図 6-7　　ACS 4.x で定義されたユーザとユーザ グループ

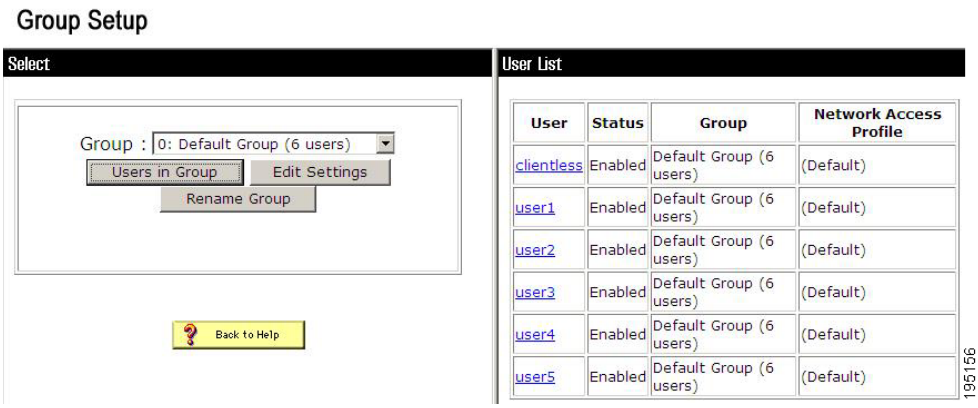
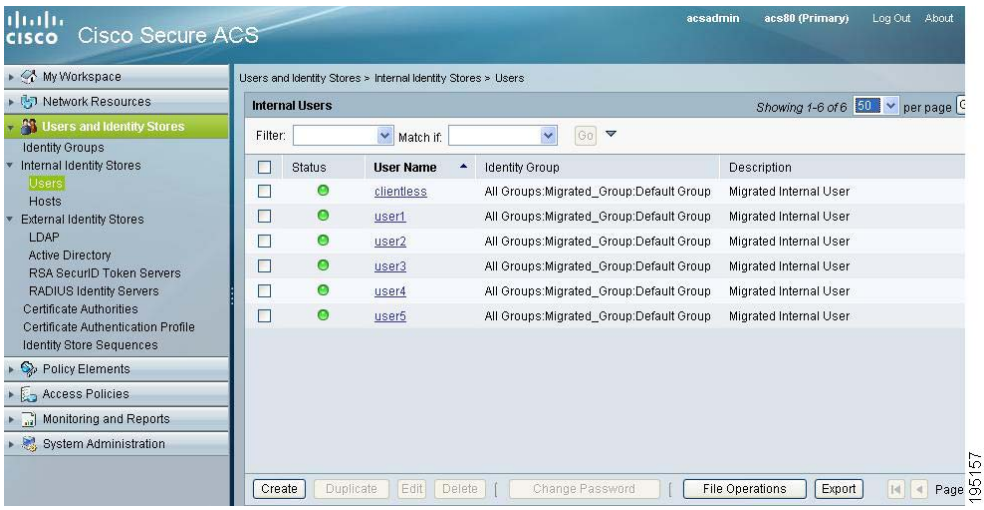


図 6-8　　ACS 5.3 に移行されるユーザとユーザ グループ



コマンド シェルの移行

図 6-9 に ACS 4.x のコマンド シェル属性を示し、図 6-10 に ACS 5.3 にシェル プロファイルとして移行されたグループ シェル属性を示します。

[Policy Elements] > [Authorization and Permissions] > [Device Administration] > [Shell Profiles] を選択してから、[Edit] をクリックして、移行されたグループ シェル属性にアクセスします。

[User and Identity Stores] > [Internal Identity Stores] > [Users] を選択し、いずれかのユーザをクリックして、移行されたユーザ シェル属性にアクセスします。図 6-11 に、ACS 5.3 に移行されるユーザ シェル属性を示します。

図 6-9　ACS 4.x で定義されたコマンド シェル属性

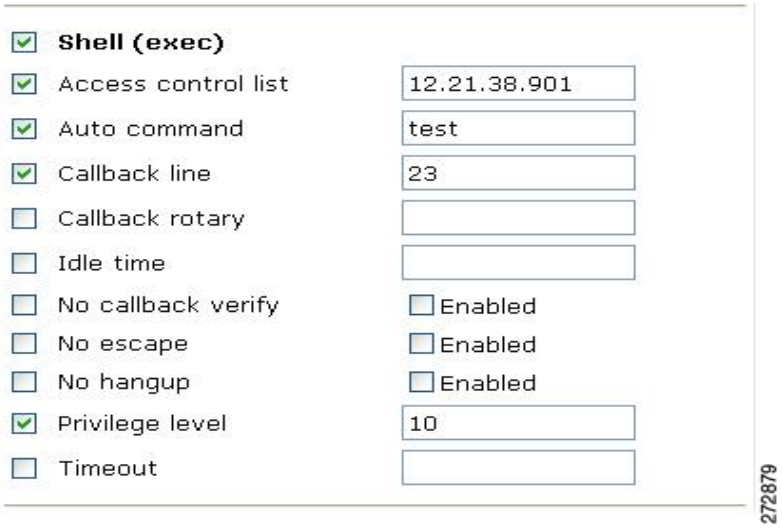


図 6-10　ACS 5.3 に移行されるグループ シェル属性

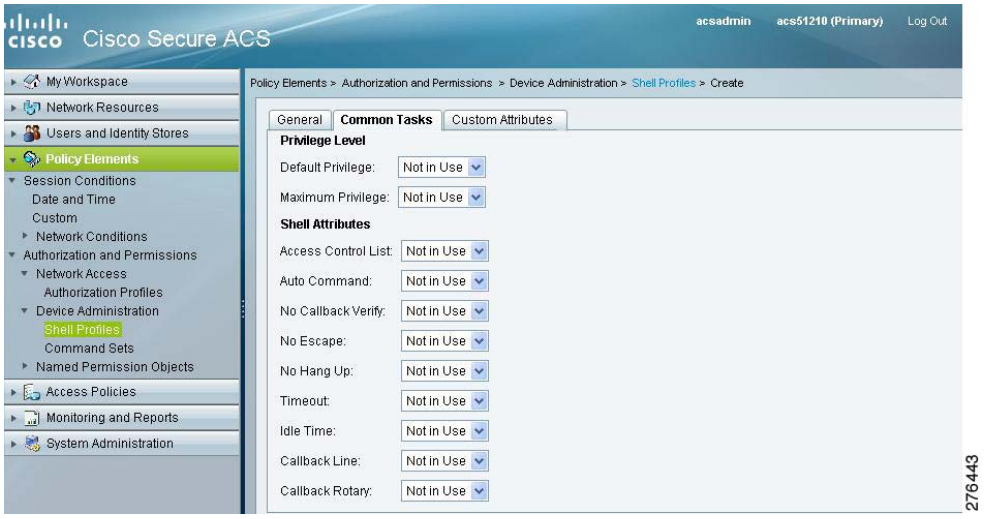


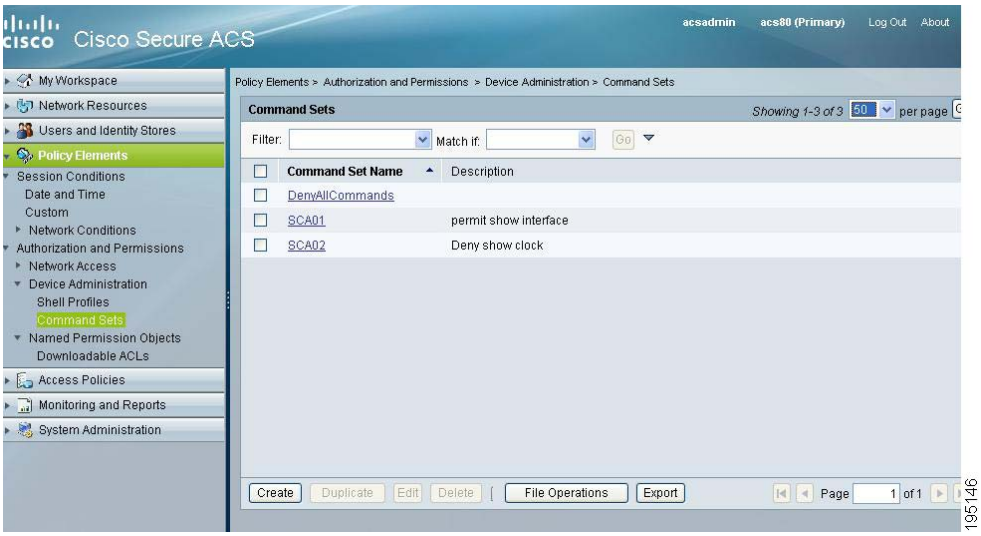
図 6-11　ACS 5.3 に移行されるユーザ シェル属性

コマンド セットの移行

図 6-12 に ACS 4.x のコマンド シェルを示し、図 6-13 に ACS 5.3 に移行されたコマンド セットを示します。[Policy Elements] > [Device Administration] > [Command Sets] を選択して、移行されたコマンド セット属性にアクセスします。

図 6-12　ACS 4.x で定義されたコマンド セット

図 6-13　ACS 5.3 に移行されたコマンド セット



NDG の移行

図 6-14 に ACS 4.x の NDG を示し、図 6-15 に ACS 5.3 に移行された NDG を示します。[Network Resources] > [Network Device Groups] を選択し、移行された NDG にアクセスします。

図 6-14　ACS 4.x で定義された NDG

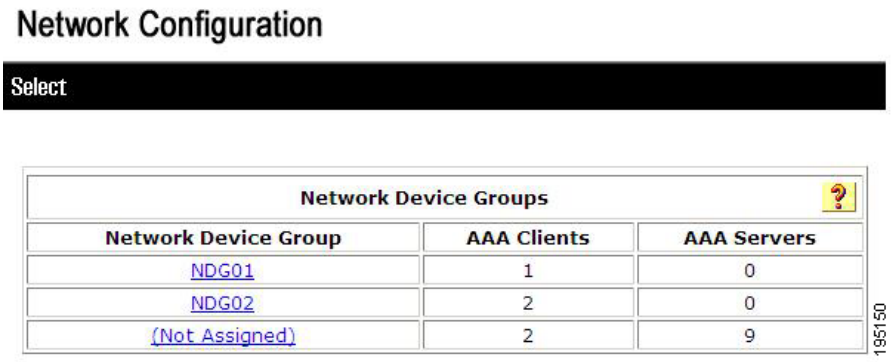
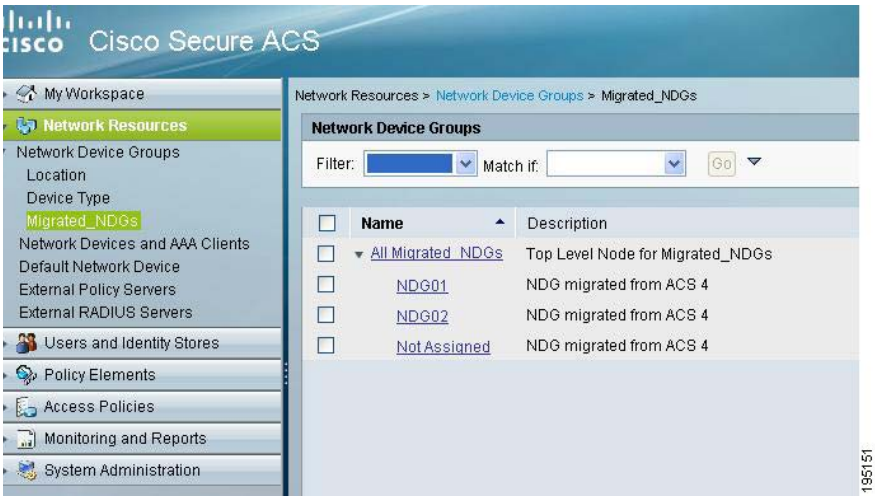


図 6-15　ACS 5.3 に移行された NDG



ネットワーク デバイスの移行

図 6-16 に ACS 4.x のネットワーク デバイスを示し、図 6-17 に ACS 5.3 に移行されたネットワーク デバイスを示します。[Network Resources] > [Network Devices and AAA Clients] を選択し、移行されたネットワーク デバイスにアクセスします。

図 6-16　ACS 4.x で定義されたネットワーク デバイス

NDG01 AAA Clients

AAA Client Hostname	AAA Client IP Address	Authenticate Using
10.77.242.83	10.77.242.83	RADIUS (IETF)

NDG02 AAA Clients

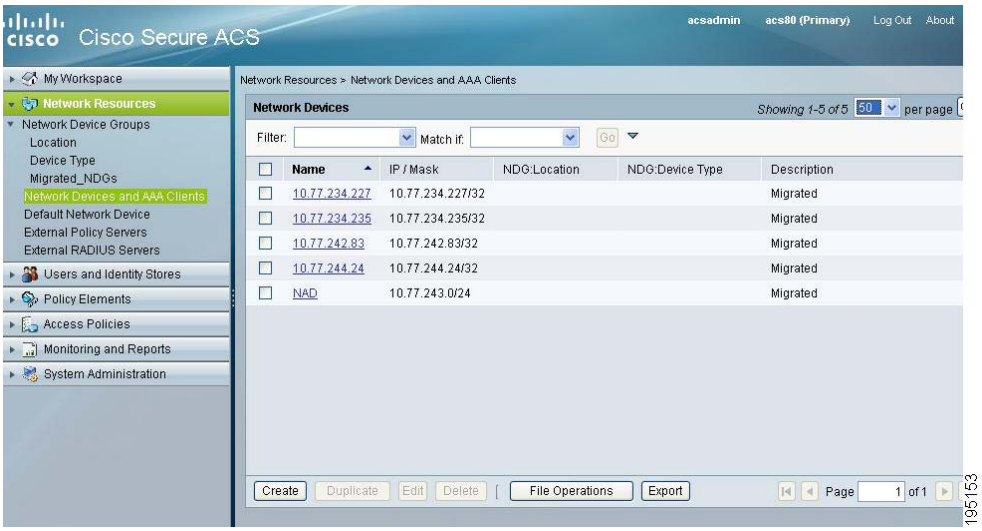
AAA Client Hostname	AAA Client IP Address	Authenticate Using
10.77.234.227	10.77.234.227	TACACS+ (Cisco IOS)
10.77.234.235	10.77.234.235	TACACS+ (Cisco IOS)

(Not Assigned) AAA Clients

AAA Client Hostname	AAA Client IP Address	Authenticate Using
10.77.244.24	10.77.244.24	RADIUS (Cisco IOS/PIX 6.0)
NAD	10.77.243.*	RADIUS (Cisco IOS/PIX 6.0)

195152

図 6-17　ACS 5.3 に移行されたネットワーク デバイス



DACL の移行

図 6-18 に ACS 4.x のダウンロード可能アクセス コントロール リスト（DACL）を示し、図 6-19 に ACS 5.3 に移行された DACL を示します。

[Policy Elements] > [Authorization and Permissions] > [Named Permission Objects] > [Downloadable ACLs] を選択し、移行された DACL にアクセスします。

図 6-18　ACS 4.x で定義された DACL

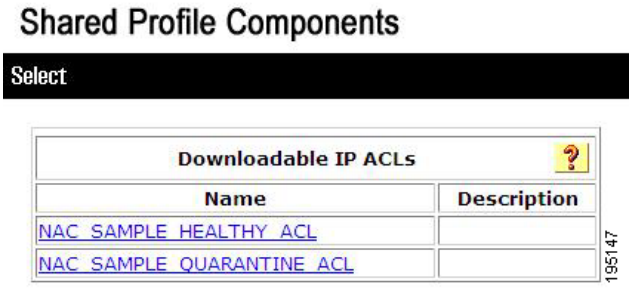
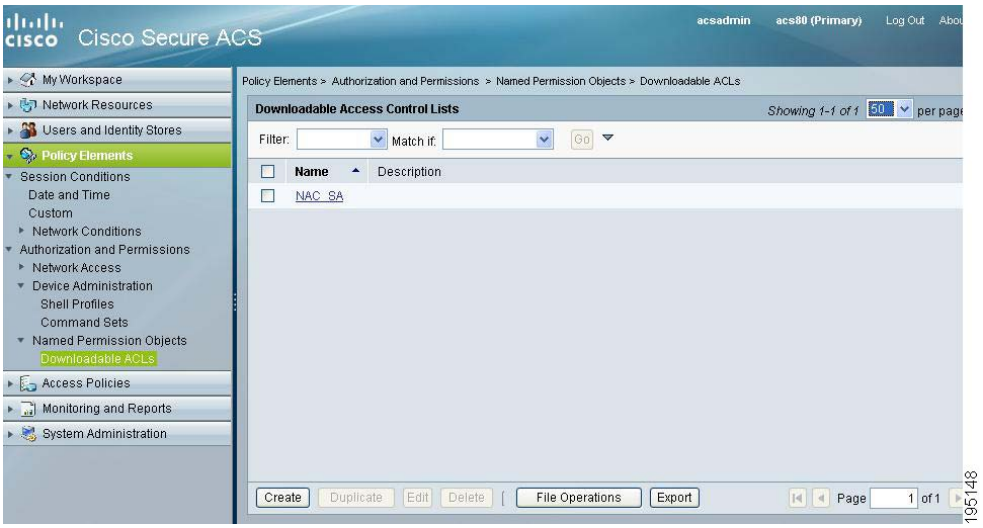


図 6-19　ACS 5.3 に移行された DACL



MAB の移行

図 6-20 に ACS 4.x で定義された MAC Authentication Bypass（MAB）を示し、図 6-21 に ACS 5.3 に移行された MAB を示します。

[Users and Identity Stores] > [Internal Identity Stores] > [Hosts] を選択して、[Create] をクリックし、移行された MAB にアクセスします。

図 6-20　ACS 4.x で定義された MAB

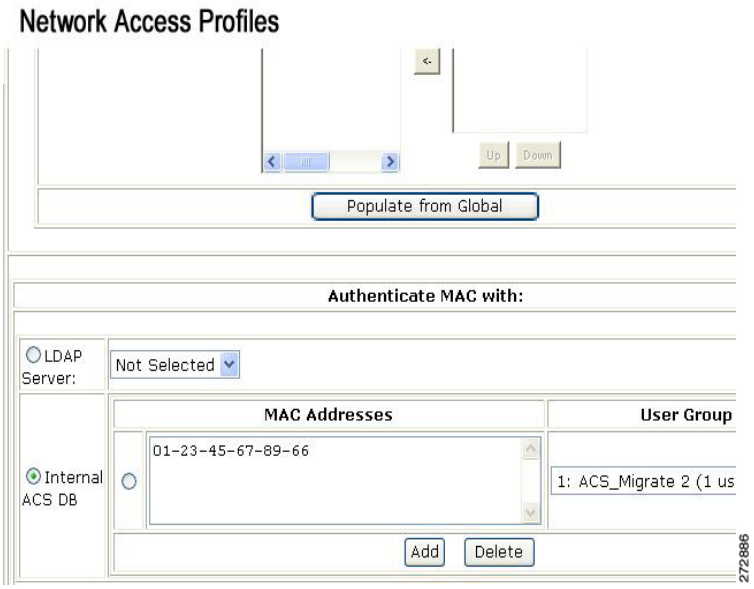
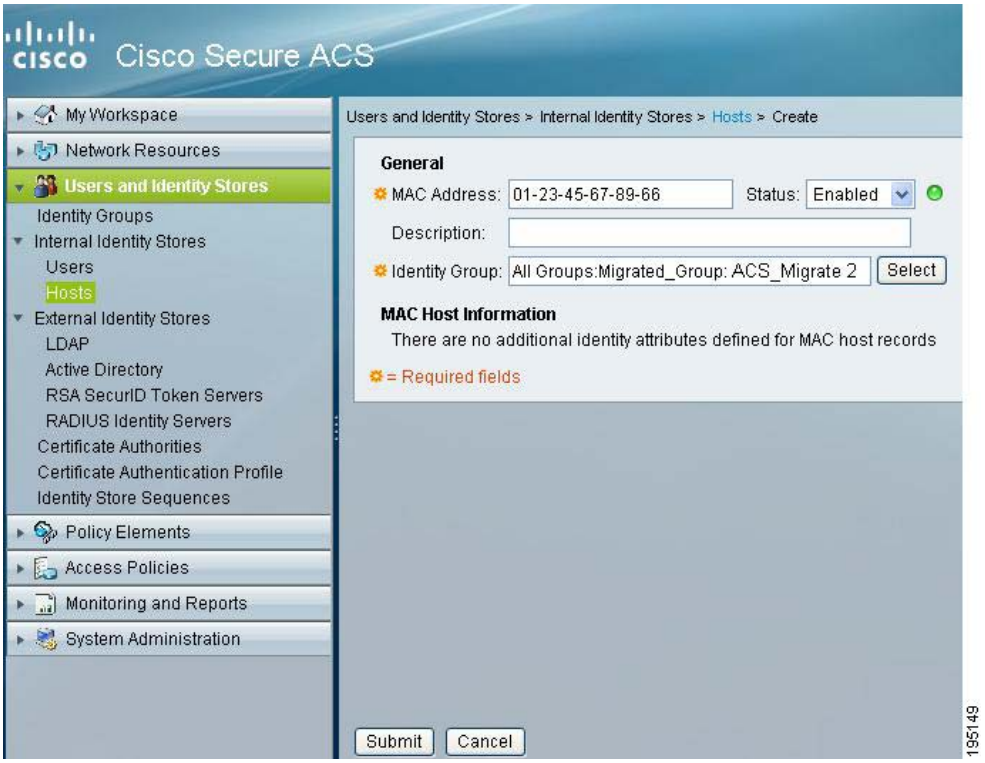


図 6-21　ACS 5.3 に移行された MAB



共有 RAC

図 6-22 に ACS 4.x で定義された共有 RADIUS Authorization Component（RAC; RADIUS 認可コンポーネント）を示し、図 6-23 に ACS 5.3 に移行された共有 RAC を示します。

[Policy Elements] > [Authorization and Permissions] > [Network Access] > [Authorization Profiles] を選択し、移行された RAC にアクセスします。

図 6-22　ACS 4.x で定義された共有 RAC

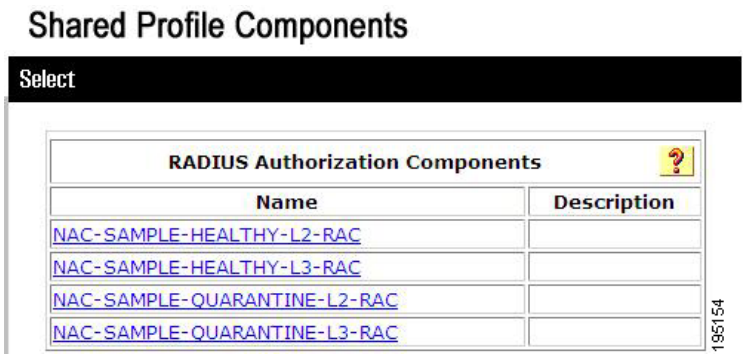
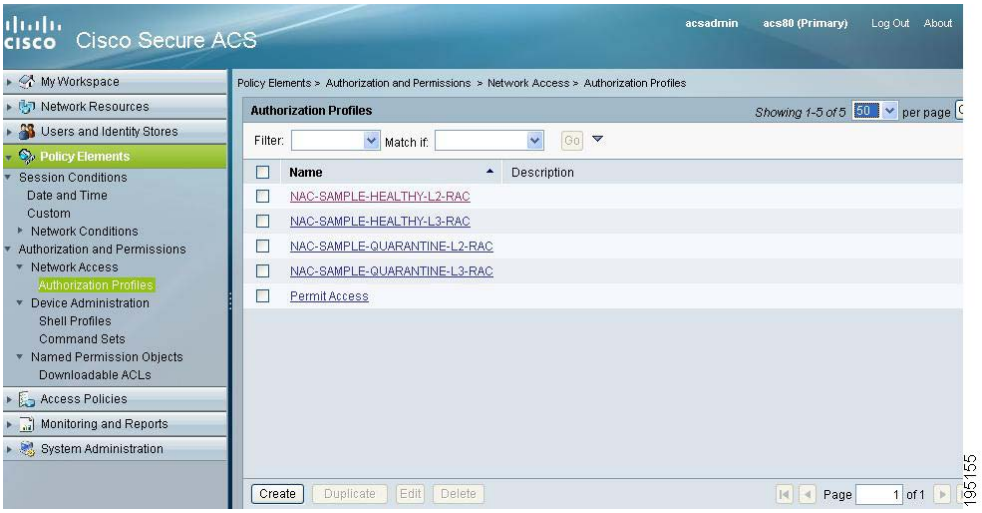


図 6-23　ACS 5.3 に移行された共有 RAC



RADIUS VSA

図 6-24 に ACS 4.x で定義された RADIUS VSA を示し、図 6-25 に ACS 5.3 に移行された RADIUS VSA を示します。

[System Administration] > [Configuration] > [Dictionaries] > [RADIUS] > [RADIUS VSA] を選択し、移行された RADIUS VSA にアクセスします。

図 6-24　ACS 4.x の RADIUS VSA

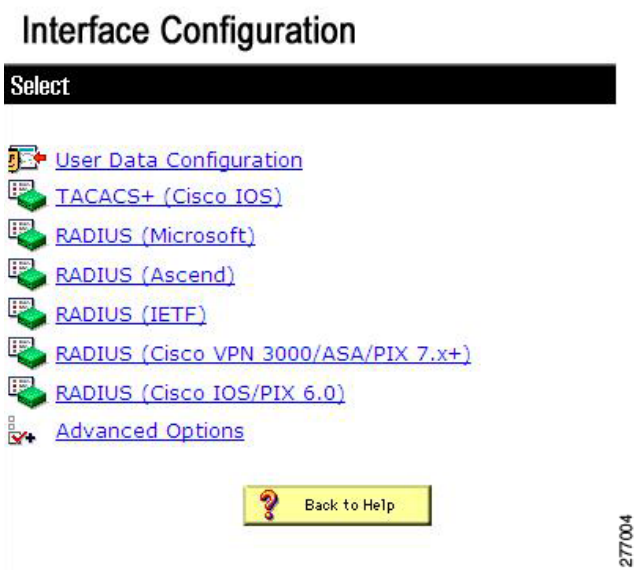
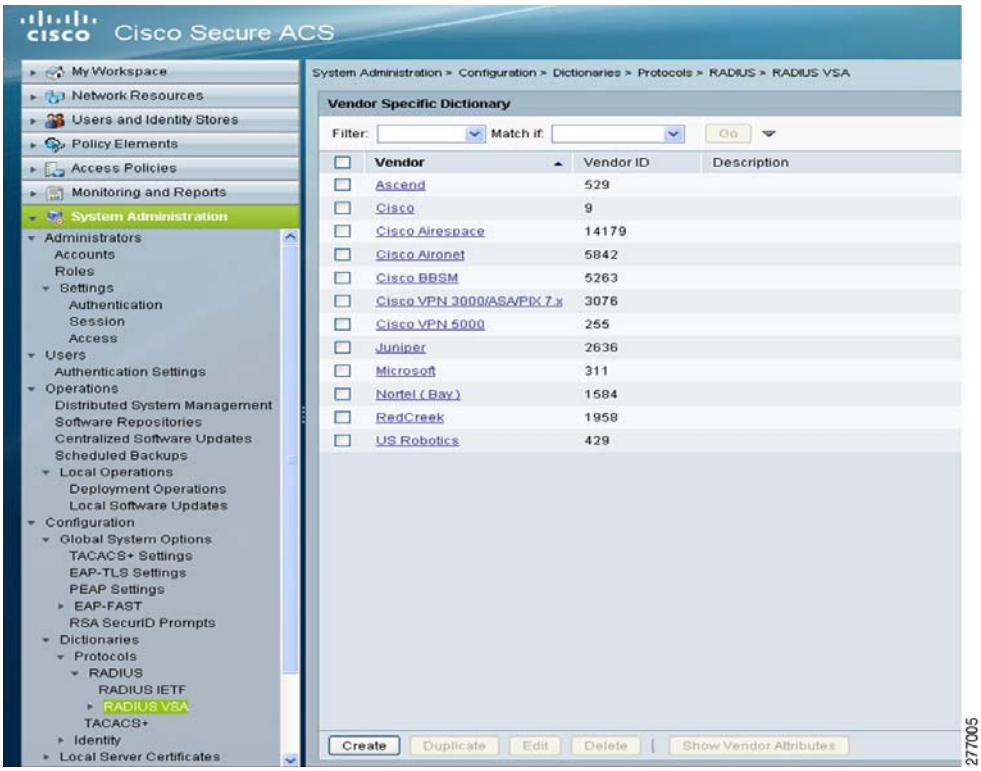


図 6-25　ACS 5.3 に移行された RADIUS VSA



KEK キーと MACK キー

図 6-26 に ACS 4.x で定義された KEK キーと MACK キーを示し、図 6-27 に ACS 5.3 に移行された KEK キーと MACK キーを示します。

[Network Devices] > [Network Devices and AAA Clients] を選択し、デバイスを選択して [Edit] をクリックし、移行された KEK キーと MACK キーにアクセスします。

図 6-26　ACS 4.x で定義された KEK キーと MACK キー

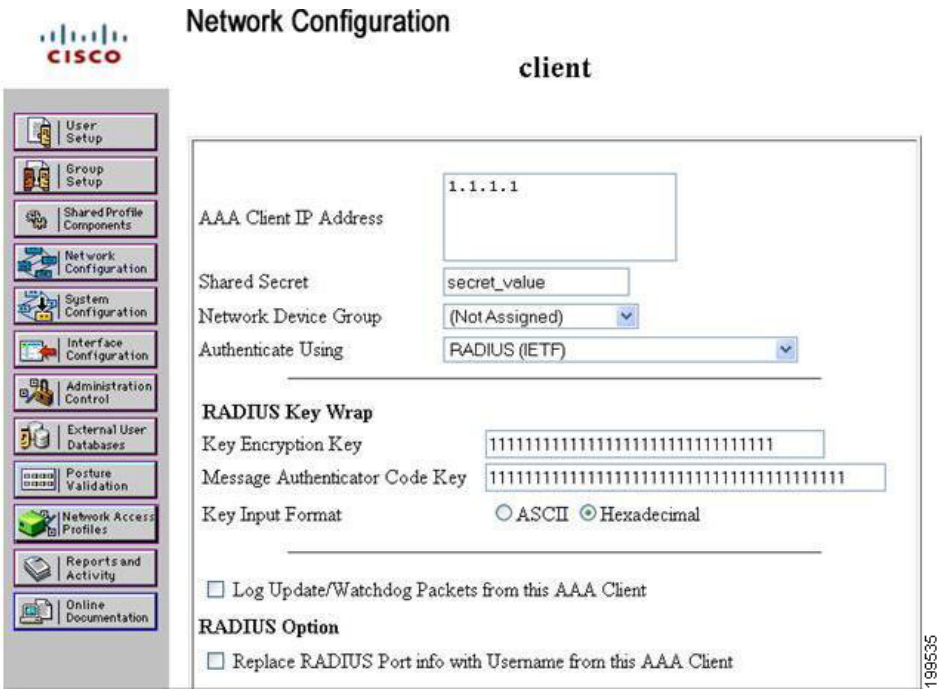
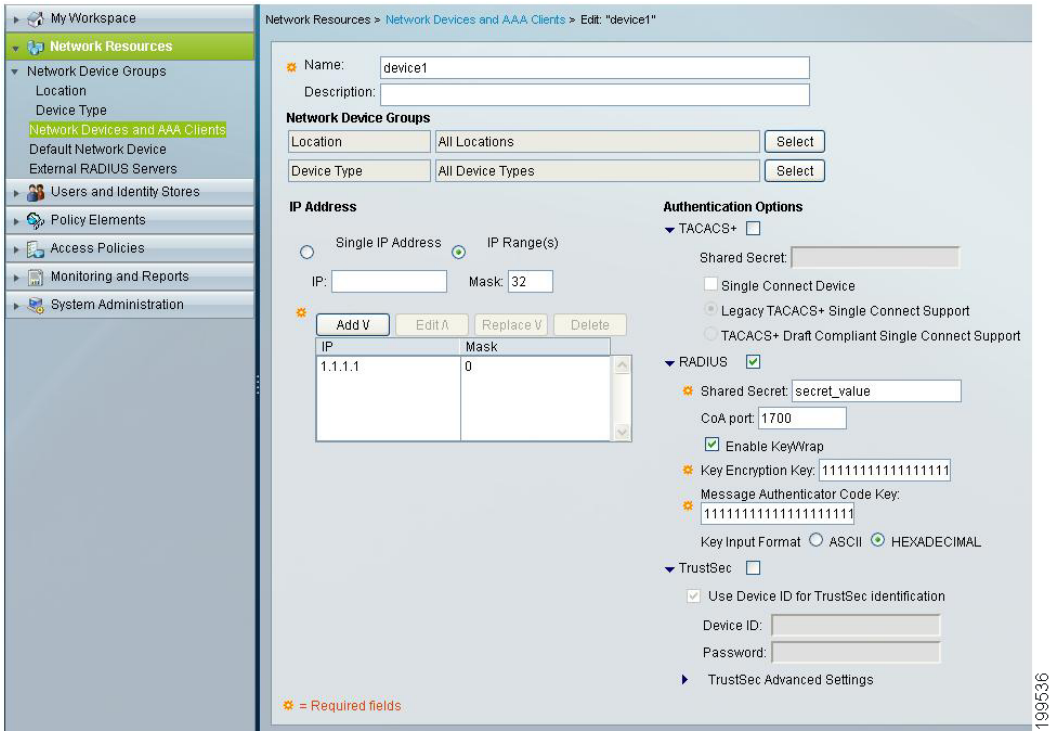


図 6-27　ACS 5.3 に移行される KEK キーと MACK キー



APPENDIX A

移行ユーティリティでの ACS 5.3 属性サポート

この章は、次の項で構成されています。

概要

この章では、ACS 4.x から ACS 5.3 への属性の移行について説明します。ACS 4.x 属性を移行するには、ACS 5.3 の基準を満たす必要があります。要素の一部の属性が ACS 5.3 に移行（または変換）されない場合でも、一部の ACS 4.x 要素を ACS 5.3 に移行できます。

たとえば ACS 5.3 では、数値 1 ～ 15 のユーザ shell exec 特権レベルをサポートします。ACS 4.x の User 要素の特権レベルが数値 1 ～ 15 ではない場合、User 要素は移行されますが、ユーザ shell exec 特権レベル属性は移行されません。

ACS 4.x から 5.3 への移行

次の項では、要素に関する情報について説明します。

AAA クライアント/ネットワーク デバイス

表 A-1 では、ACS 4.x のネットワーク デバイス定義と ACS 5.3 ネットワーク デバイス定義の違いについて説明します。

表 A-1　ACS ネットワーク デバイス定義

ACS 要素	ACS 4.x	ACS 5.3 ステータス
RADIUS および TACACS+	プロトコルごとに 1 つのネットワーク デバイスを定義します。たとえば RADIUS にネットワーク デバイス 1、TACACS+ にネットワーク デバイス 2。	RADIUS および TACACS+ に 1 つのネットワーク デバイスを定義します。「IP アドレスのオーバーラップ」（P.D-3）を参照してください。
IP Address	• 正規表現を使用して IP アドレスを定義します。 • 41 以上の IP アドレスを定義できます。 • ワイルドカードおよび範囲を使用できます。	• IP アドレスとマスク定義のペアとして IP アドレスを定義します。 • 40 個までの IP アドレスに制限されます。 • 定義は、サブネット マスクを使用した形式を使用します。「変換できない IP アドレス」（P.D-4）を参照してください。

（注）　ACS 5.3 では、ネットワーク デバイスの属性を使用した ACS 4.x 認証をサポートしません。ACS 5.3 では、RADIUS および TACACS+ のみをサポートします。特定のベンダーを定義することはできません。

NDG

ACS 5.3 では、NDG に対して ACS 4.x 共有キー パスワード属性をサポートしません。分析レポートでは、NDG レベルの共有キー パスワードにフラグを設定します。共有キー パスワードは、ネットワーク デバイス レベルでのみ使用できます。

NDG にキー暗号キーが含まれるような NDG に属するデバイスの場合、NDG のキー暗号キーが抽出され、ネットワーク デバイス定義のキー暗号キーで定義されたものに代わってネットワーク デバイス定義に含められます。

NDG にメッセージ オーセンティケータ コード キーが含まれるような NDG に属するデバイスの場合、NDG のメッセージ オーセンティケータ コード キーが抽出され、ネットワーク デバイス定義のメッセージ オーセンティケータ コード キーで定義されたものに代わってネットワーク デバイス定義に組み込まれます。

（注）　共有キー パスワードが NDG レベルで存在する場合、共有キー パスワードはその NDG に属するすべてのネットワーク デバイスへ移行されます。ネットワーク デバイスの共有キー パスワードは、NDG 共有キー パスワードが空の場合のみ移行されます。

内部ユーザ

ACS 5.3 では、ACS 4.x パスワード認証タイプがサポートされます。ACS 5.3 では、内部データベースと外部データベースの両方の認証がサポートされます。管理者が Windows または LDAP を使用する場合は、デフォルトの認証パスワードでユーザ オブジェクトを移行します。移行ユーティリティを実行する場合は別のパスワードを使用できます。「移行スクリプト ユーザ プリファレンス」を参照してください。

ユーザ ポリシーのコンポーネント

ACS 4.x では、ポリシー関連の認可データがユーザ定義内に埋め込まれています。ACS 5.3 のポリシー関連の認可データは、ACS 5.3 ポリシー テーブル内から参照される共有コンポーネント内に含まれています。表 A-2 に、ACS 4.x ユーザ ポリシー コンポーネントの属性を示し、ACS 5.3 でのステータスについて説明します。

表 A-2　　ユーザ ポリシー コンポーネントの属性

ACS 4.x 属性	ACS 5.3 ステータス
TACACS+ Shell（exec）特権レベル： 特権レベルは、有効性チェックが行われない文字列フィールドです。	• ACS 5.3 では、デフォルトの特権レベルが最大特権レベルより大きくなることはできません。 • ACS 5.3 では、数値（1 ～ 15）による特権レベルをサポートします。
TACACS+ Shell カスタム属性	フェーズ 2 では、特権レベルおよびシェル コマンドのカスタム属性をサポートしません。
TACACS+ シェル コマンド認可セット： 各属性の値を指定する必要はありません。	移行ではユーザ単位のコマンド認可のみサポートされ、次の属性はサポートされません。 • 任意のネットワーク デバイスへのシェル コマンド認可セットの割り当て。 • ネットワーク デバイス グループ単位でのシェル コマンド認可セットの割り当て。 各属性の値を指定する必要があります。

ユーザ グループ

ACS 4.x では、各ユーザが 1 つのグループに関連付けられていました。ユーザ グループ要素には、一般的な ID 属性とともにポリシー コンポーネント属性（shell exec や RADIUS 属性など）が含まれます。ACS 5.3 では ID グループがユーザ グループに相当します。ただし ID グループは、純粋な論理コンテナであり、ポリシー コンポーネントは含みません。

ユーザ グループ ポリシーのコンポーネント

ACS 4.x では、ポリシー認可データがユーザ グループ定義内に埋め込まれています。ACS 5.3 のポリシー認可データは、セッション認可プロファイルで定義されます。表 A-3 に、ACS 4.x ユーザ グループを示し、ACS 5.3 でのステータスについて説明します。

表 A-3　ユーザ グループ ポリシー コンポーネントの属性

ACS 4.x 属性	ACS 5.3 ステータス
TACACS+ Shell（exec）特権レベル： 特権レベルは、有効性チェックが行われない文字列フィールドです。	• ACS 5.3 では、数値（1 ～ 15）による特権レベルをサポートします。 • ACS 5.3 では、デフォルトの特権レベルが最大特権レベルより大きくなることはできません。
TACACS+ Shell（exec）カスタム属性	ACS 5.3 では、シェル コマンドのカスタム属性をサポートしません。
TACACS+ シェル コマンド認可セット 各属性の値を指定する必要はありません。	ACS 5.3 では、ユーザ単位のコマンド認可のみサポートされ、次の属性はサポートされません。 • 任意のネットワーク デバイスへのシェル コマンド認可セットの割り当て。 • ネットワーク デバイス グループ単位でのシェル コマンド認可セットの割り当て。 各属性の値を指定する必要があります。

共有シェル コマンド認可セット

失われる属性はありません。ACS 4.x のシェル コマンド認可セットは、デバイス管理に含まれる共有要素として定義されます。エクスポートおよびインポートのフェーズでは、これらの要素をコマンド セットに移行します。ACS 5.3 における各要素の名前と説明は、ACS 4.x と同じです。

MAB

ACS 4.x では、NAP 設定時に [User] テーブルで MAC アドレスを定義できます。ACS 5.3 では、MAC ID が MacId オブジェクトとして移行されます。各 MacId オブジェクトは MAC Authentication Bypass（MAB）ID ストアに追加されます。

DACL

ACS 4.x の共有 DACL は、NAP テーブルに含まれる共有オブジェクトと、ユーザ オブジェクトおよびユーザ グループ オブジェクトとして定義されます。共有 DACL は、ACL コンテンツおよび Network Access Filter（NAF; ネットワーク アクセス フィルタ）ID の組のリストで構成されます。ACS 4.x の 1 つの DACL を ACS 5.3 の複数の DACL に移行できます。ACS 5.3 では NAF をサポートしないため、ACL コンテンツのみを移行できます。

EAP-FAST マスターキー

ACS 4.x のマスター キー定義には、ACS 5.3 スキーマとは異なるスキーマがあります。そのためマスター キーは、別の ACS 5.3 Information Model Object（IMO; 情報モデル オブジェクト）に移行されます。

共有 RAC

ACS 4.x では、RADIUS Authorization Component（RAC; RADIUS 認可コンポーネント）が含まれる共有プロファイル コンポーネントを定義したり、認可の応答で返される RADIUS 属性および値のセットを定義したりすることができます。ACS 5.3 の RAC は、共有認可プロファイルに定義されます。

表 A-4 に、ACS 4.x での RAC の属性を示し、ACS 5.3 でのステータスについて説明します。

表 A-4　共有 RADIUS 認可コンポーネントの属性

ACS 4.x 属性	ACS 5.3 ステータス
ACS 4.x では、次の属性を設定および修正できます。 • MS-CHAP-MPPE-Keys (12) • MS-MPPE-Send-Key (16) • MS-MPPE-Recv-Key (17)	ACS 5.3 では、これらの属性を設定できません。必要に応じてプロファイルに追加されます。
ACS 4.x では、Ascend 属性は、ベンダー ID 0 で内部的に保存されます。	ACS 5.3 では、Ascend ベンダー ID 529 を割り当てる必要があります。

カスタマー VSA

移行時には、ディクショナリは各ベンダーの ACS 5.3 の不足した属性の識別を反復して行います。ACS 5.3 ディクショナリにベンダーが存在しない場合、すべてのベンダー属性が移行されます。ACS 5.3 ディクショナリ内にベンダーが存在する場合は、ACS 5.3 で定義されていない属性のみが移行されます。

APPENDIX B

ACS 3.x および 4.x から ACS 5.3 への設定マッピング

表 B-1 に、ACS 3.x および 4.x の設定領域と ACS 5.3 における対応を示します。

表 B-1　ACS 3.x および 4.x から ACS 5.3 への設定マッピング

ACS 3.x および 4.x の設定領域	ACS 5.3 設定領域
ユーザ設定	ユーザおよび ID ストア、ポリシー要素、アクセス ポリシー、システム管理
グループ設定	ユーザおよび ID ストア、ポリシー要素、アクセス ポリシー
共有プロファイル コンポーネント	ポリシー要素
ネットワーク設定	ネットワーク リソース
システム設定	システム管理
インターフェイス設定	該当せず
管理コントロール	システム管理
外部ユーザ データベース	ユーザおよび ID ストア
ポスチャ検証	該当せず
ネットワーク アクセス プロファイル	アクセス ポリシー
レポートとアクティビティ	モニタリングとレポート

APPENDIX C

ACS 3.x および 4.x と ACS 5.3 の機能比較

表 C-1　機能比較リスト：ACS 3.x/4.x と ACS 5.3

機能	ACS 3.x と 4.x	ACS 5.3	注釈
プラットフォーム サポート			
1111	Yes	No	
1112	Yes	No	
1113	Yes	No	
1120	○（4.2）	Yes	ACS 5.0 出荷アプライアンス
1121	No	Yes	ACS 5.3 出荷アプライアンス
Windows Server	Yes	No	
仮想マシン	ESX 3.x	ESX 3.x/4.0	
コンポーネント			
ACS for Windows	Yes	No	ACS 5.3 では Windows Server はサポート対象外です
ACS Solution Engine	Yes	No	ACS 5.3 固有のアプライアンス オプションを提供します
ACS View 4.0	Yes	No	ACS 5.3 では表示機能を統合しました
ACS Remote Agent	Yes	No	5.3 では Remote Agent は必要ありません
ACS Express 5.0	No	No	
アプリケーション統合			
CiscoWorks Common Service（CSM/LMS 用）	Yes	No	
Cisco Wireless Control System（WCS）	Yes	Yes	
分散モデル			
単一プライマリ / 複数セカンダリ	Yes	Yes	
カスケード複製	Yes	No	
レプリケーション トリガー	手動またはスケジュールごと	設定変更時	

表 C-1　機能比較リスト：ACS 3.x/4.x と ACS 5.3 （続き）

機能	ACS 3.x と 4.x	ACS 5.3	注釈
レプリケーション ユニット	レプリケーション コンポーネント全体	delta 設定のみ	
同期	ゆるい	きつい	
自動停止再同期	No	Yes	
内部ユーザのパスワード更新	プライマリのみ	すべてのサーバ	
ロールベースのセカンダリをプライマリに昇格	No	Yes	
ID ストア サポート			
内部	Yes	Yes	
Active Directory	Yes	Yes	
LDAP	Yes	Yes	
RDBMS	Yes	No	
RSA SecurID	Yes	Yes	
その他のワンタイム パスワード サーバ	Yes	Yes	OTP サーバに RADIUS インターフェイスを使用
AAA プロキシ サポート			
RADIUS プロキシ	Yes	Yes	EAP プロキシを含む
TACACS+ プロキシ	Yes	Yes	
ロギングの宛先			
ACS View	Yes	Yes	
Syslog	Yes	Yes	
ODBC	Yes	No	ACS 5.3 は、View のログ データを外部データベースと同期して保存することができます。
クエリー / プロビジョニングの設定			
Web ベースの GUI	Yes	Yes	
CSV ベースの更新	Yes	Yes	
CSUtil	Yes	No	
RDBMS 同期化	Yes	No	
管理			
SNMP クエリー	○（アプライアンスのみ）	Yes	
SNMP トラップ	No	No	
アラーム表示	Yes	Yes	
GUI	Yes	Yes	
Cisco 標準のルック アンド フィール GUI	No	Yes	
CLI	○（アプライアンスのみに制限）	○（IOS と同様）	

表 C-1　機能比較リスト：ACS 3.x/4.x と ACS 5.3 （続き）

機能	ACS 3.x と 4.x	ACS 5.3	注釈
一部の設定を変更するとシステムが再起動します	Yes	No	
KVM コンソール アクセス	No	Yes	
ファイル転送ストレージ リポジトリの選択	No	Yes	
配置済みの、バージョンをまたぐアップグレードの手順	No	Yes	
リモート アップグレード/パッチ実行	部分的	Yes	
パスワード認証			
PAP	Yes	Yes	
CHAP	Yes	Yes	
MS-CHAPv1	Yes	Yes	
MS-CHAPv2	Yes	Yes	
EAP-MD5	Yes	Yes	
EAP-TLS	Yes	Yes	
PEAP-MSCHAPv2	Yes	Yes	
PEAP-GTC	Yes	Yes	
PEAP-TLS	Yes	No	
FAST-MSCHAPv2	Yes	Yes	
FAST-GTC	Yes	Yes	
FAST-TLS	Yes	No	
LEAP	Yes	Yes	
TACACS+			
コマンド認可	Yes	Yes	
アカウンティング	Yes	Yes	
単一接続	Yes	Yes	
パスワードの変更	Yes	Yes	
イネーブル処理	Yes	Yes	
カスタム サービス	Yes	Yes	
任意の属性	Yes	Yes	
CHAP/MSCHAP 認証	Yes	No	
属性の置換	Yes	No	
ACS パスワード ポリシー			
複雑度	Yes	○（強力）	
履歴	○（最後のみ）	○（複数）	
有効期限	○（日付、ログイン、最初のログインごと）	○（日付順）	
有効期限の警告	Yes	Yes	

表 C-1　機能比較リスト：ACS 3.x/4.x と ACS 5.3 （続き）

機能	ACS 3.x と 4.x	ACS 5.3	注釈
猶予期間	Yes	No	
アカウントのディセーブル化			
日付による	Yes	No	認可ポリシーを使用して実装できます
失敗した試行による	Yes	No	
非アクティブによる	No	No	
ネットワーク デバイス			
各 TACACS+/RADIUS エントリ	Yes	No	
階層型のスケーラブルなデバイスのグループ化	No	Yes	
デフォルト ネットワーク デバイス	TACACS+ のみ	RADIUS および TACACS+	
グループ レベルの共有秘密	Yes	No	
IP アドレスのワイルドカード	Yes	○（マスクベースのみ）	
アクセス ポリシー			
柔軟な、規則ベースのポリシーモデル	No	Yes	
必須 ACS グループ割り当て	Yes	No	
複数のグループ メンバシップ	No	Yes	
静的 IP アドレス割り当て	Yes	Yes	拡張スキーマ、ポリシー
最大セッション数	Yes	No	
グループのディセーブル化	Yes	Yes	ACS 5.3 ポリシーに実装
VOIP サポート	Yes	No	
ToD 設定	Yes	Yes	
コールバック	Yes	Yes	Windows のコールバック設定は ACS 5.3 では使用できません
ネットワーク アクセス制限	Yes	Yes	
クォータの使用状況	Yes	No	
オプションをイネーブルにする	Yes	Yes	ACS 5 ポリシーに実装
トークンのキャッシング	Yes	No	

表 C-1　機能比較リスト：ACS 3.x/4.x と ACS 5.3 （続き）

機能	ACS 3.x と 4.x	ACS 5.3	注釈
IP アドレスの割り当て	Yes	○（スタティックおよび AAA クライアント プールのみ）	スタティック IP アドレスの割り当ての場合、IP アドレス フィールドをユーザ スキーマに追加することで認可ポリシーに実装します。 AAA クライアント プールとは、ACS で VSA 属性「ip-pool-definition」を設定する機能のことです。プール自体はスイッチまたはルータ自体で定義されます。
ダウンロード可能 ACL	Yes	Yes	
ユーザの補足情報	Yes	Yes	
ポリシーの条件の使用および値の認証のための拡張 ACS ユーザ スキーマ	No	Yes	
ポリシーの条件や値の認証として利用可能なユーザ属性（内部、AD、LDAP）	No	Yes	
ACS 内部ユーザの拡張パスワード認証	Yes	Yes	ACS 5 では、パスワードの格納はアクセス サービス ID ポリシーで指定する必要があり、ユーザのレコードでは指定できません。
時間をバインドする別のグループ	Yes	Yes	ACS 5 では、その日の時間に基づいてさまざまな権限を指定する場合に、時間ベースの条件を使用します。
Windows ダイヤルイン サポート	Yes	No	
ACS 管理者			
ネットワークの制限	Yes	Yes	
権限付与レポート	Yes	Yes	
パスワードの複雑度	Yes	○（強力）	
パスワード エージング	Yes	Yes	
パスワード履歴	Yes	Yes	
パスワードは非アクティブ	Yes	Yes	
失敗した試行によるアカウントのディセーブル化	Yes	Yes	
非アクティブなアカウントによるアカウントのディセーブル化	Yes	Yes	
権限コントロール	Yes	○（ロールベース）	

表 C-1　機能比較リスト：ACS 3.x/4.x と ACS 5.3 （続き）

機能	ACS 3.x と 4.x	ACS 5.3	注釈
証明書ベースの認証 / 許可			
必須 AD 許可	Yes	No	
SAN/CN 比較	Yes	No	ユーザ属性の存在を確認することで ACS 5.3 に間接的に実装できます
証明書のバイナリ比較	Yes	Yes	

APPENDIX D

移行ユーティリティのトラブルシューティング

この章では、ACS 5.3 移行ユーティリティに関連する一般的な問題について説明します。

ACS 4.x データベースを移行マシンで復元できない

条件

ACS 4.x データベースを移行マシンで復元できません。

アクション

ACS 4.x 運用マシン（バックアップが作成された）および ACS 4.x 移行マシン（バックアップが復元された）が同じバージョンのシステム ソフトウェアを使用していることを確認します。この問題は、パッチのレベル不足が原因であることがあります。

リモート デスクトップ接続が移行ユーティリティでサポートされていない

条件

リモートデスクトップ接続（RDC）を使用して、移行ユーティリティを実行できません。

アクション

仮想ネットワーク コンピューティング（VNC）を使用して、移行マシンで移行ユーティリティを実行します。

大規模データベースの移行オブジェクト

大規模なデータベースからオブジェクトを移行する場合に、さまざまな問題が発生することがあります。

条件

ACS 4.x データベースから多数のオブジェクトを移行する場合に、パフォーマンスの問題が発生することがあります。

アクション

各オブジェクト グループに対して移行ユーティリティを実行することを推奨します。たとえば、移行ユーティリティで、2 と入力してオプション 2 の AllUsersObjects を選択します。この例では、ユーザオブジェクトに対して移行ユーティリティを実行するだけです。

インポート フェーズで一部のデータだけが追加される

条件

インポートを行うと、一部のデータだけが追加されます。

アクション

1. 次の内容を確認してください。
   - 移行インターフェイスが ACS 5.3 サーバでイネーブルであること
   - ネットワーク接続がイネーブルであること
   - ACS 5.3 サービスが起動し、実行していること
   - 互換性のある ACS 5.3 ライセンスを使用していること
2. ACS 5.3 データベースを前のバージョンに復元します。
3. 移行ユーティリティを再起動します。
4. インポート フェーズを再度実行します。

インポート後に ACS 5.3 マシンが応答しない

条件

インポート後に ACS 5.3 マシンが応答しません。

アクション

ACS 5.3 を再起動します。

移行の問題の解決

このセクションでは、手動で移行の問題を解決する方法について説明します。次の移行の問題について説明します。

IP アドレスのオーバーラップ

分析フェーズで、ACS 4.x のネットワーク デバイスの IP アドレスのオーバーラップがレポートされる場合があります。例 D-1 は、AA ネットワーク デバイスの IP アドレスが BB ネットワーク デバイスの IP アドレスにオーバーラップしており、各ネットワーク デバイスがさまざまな NDG に属していることを示しています。ACS 4.x 側から見ると、これらは 2 つの個別のオブジェクトです。

例 D-1　　IP アドレスのオーバーラップ

```
The following Network Devices are overlapped:
Network device: AA, IP Address = 23.8.23.*, 45.67.*.8, protocol =RADIUS, Group= HR
Network device: BB, IP Address = 45.*.6.8, 1.2.3.4, protocol =TACACS, Group = Admin
```

ただし、ACS 5.3 は TACACS+ および RADIUS を 1 つのオブジェクトとして定義します。

ソリューションとしては、ACS 4.x アプリケーションを使用して同じ IP アドレスを持つネットワーク デバイスの再定義を行い、それらが同じ NDG に属するようにします。例 D-2 にソリューションを示します。

例 D-2　　解決済みの IP アドレス

```
Network device: CC, IP Address = 1.2.3.*, protocol =RADIUS, Group= HR
Network device: DD, IP Address = 1.2.3.*, protocol =TACACS, Group = HR
```

この例では、IP アドレスが同一で、両方のネットワーク デバイスが同じ NDG に含まれる、RADIUS および TACACS+ ネットワーク デバイスを統合します。CC および DD を、CC+DD という名前の 1 つのオブジェクトとしてエクスポートできます。

変換できない IP アドレス

ACS 4.x の IP アドレスの定義ではワイルドカードや範囲を使用できます。ACS 5.3 では、IP アドレスの定義はサブネット マスク形式です。分析フェーズでは、変換できない IP アドレスのあるネットワーク グループを識別します。

ACS 4.x アプリケーションを使用して、IP アドレスの範囲を ACS 5.3 のサブネット マスク定義に変更できます。ただし、IP アドレスのすべての組み合わせを ACS 5.3 のサブネット マスク定義に変換できるわけではありません。例を示します。

```
Network device: AA, IP Address =23.8.23.12-221 protocol =RADIUS, Group= HR
```

この例では、IP アドレスに **12 ～ 221** の範囲が含まれており、サブネット マスク定義に変換できません。

ワイルドカード（*）または範囲（x ～ y）がアドレスの途中に含まれる場合、IP アドレスを移行できません。次のパターンの IP アドレスは移行できません。

- 1.*.2.*
- *.*.*.1
- *.*.*.*

次のパターンの IP アドレスは変換できます。

- 1.*.*.*
- 1.2.*.*
- 1.2.3.*
- 1.2.3.13 ～ 17

（注） 移行では、0 ～ 255 の IP 範囲がサポートされます。

41 以上の IP アドレスがあるネットワーク デバイス

条件

ACS 4.x のネットワーク デバイスには 41 以上の IP アドレスがあります。ACS 5.3 では 41 以上の IP アドレスのあるネットワーク デバイスを移行しません。

アクション

移行マシンの ACS 4.x アプリケーションを使用して、ネットワーク デバイス設定を編集します。次の手順に従います。

ステップ 1　[Network Configuration] を選択します。

ステップ 2　ネットワーク デバイスのある [NDG] を選択します。

ステップ 3　ネットワーク デバイスを選択します。

ステップ 4　[AAA Client IP Address] フィールドを編集します。AAA クライアントに 40 以下の IP アドレスがあることを確認します。

ステップ 5　[Submit + Apply] をクリックします。

移行ユーティリティを再実行します（分析およびエクスポート フェーズおよびインポート フェーズ）。

無効な TACACS+ シェル特権レベル

条件

TACACS+（T+）シェル特権レベルが 0 ～ 15 の範囲内にありません。

アクション

ACS 4.x アプリケーションを移行マシンで使用して、T+ 設定を編集します。T+ 特権レベルを 0 ～ 15 の間に設定します。

ユーザ レベルで T+ 設定を編集するには、次の手順を実行します。

ステップ 1　[User Setup] を選択します。

ステップ 2　ユーザを選択します。

[Edit] 画面が表示されます。

ステップ 3　[TACACS+ Settings] テーブルの [Privilege level] チェックボックスを確認して、0 ～ 15 の値を入力します。

ステップ 4　[Submit] をクリックします。

グループ レベルで T+ 設定を編集するには、次の手順を実行します。

ステップ 1　[Group Setup] を選択します。

ステップ 2　グループを選択して、[Edit Settings] をクリックします。

ステップ 3　[TACACS+ Settings] テーブルの [Privilege level] チェックボックスを確認して、0 ～ 15 の値を入力します。

ステップ 4　[Submit + Restart] をクリックします。

移行ユーティリティを再実行します（分析およびエクスポート フェーズおよびインポート フェーズ）。

TACACS+ カスタム属性が移行されない

条件

ACS 4.x では、T+ カスタム属性がユーザおよびグループに対して定義されています。ACS 5.3 は TACACS+ カスタム属性をサポートしていません。

アクション

何も実行する必要はありません。ユーザおよびグループに対して定義されているその他すべての T+ シェル実行属性は移行されません。T+ カスタム属性は削除されます。

シェル コマンド認可セットをユーザまたはグループに関連付けられない

条件

シェル コマンド認可セットは ACS 4.x のユーザまたはグループに関連付けられています。移行後は、シェル コマンド認可セットとユーザまたはグループ間の関連付けが失われます。

アクション

ACS 5.3 アプリケーションを使用して、次の手順を実行します。

1. 移行したコマンド セットにアクセスします。詳細については、「コマンド セットの移行」（P.6-51）を参照してください。
2. ユーザおよび ID グループのポリシーを作成します。

ポリシーの作成の詳細については、『*User Guide for the Cisco Secure Access Control System 5.3*』を参照してください。

手動で作成した Super Admin の移行が失敗する

条件

ACS 5.3 では、ユーザ *Admin1* は [System Administration] > [Administrators] > [Accounts] で、Super Admin のロールで作成されます。Admin1 を管理者のユーザ名に設定しようとしたときに移行が失敗しました。

アクション

何も実行する必要はありません。ACS 5.3 ではデフォルトのスーパー管理者 *acsadmin* だけをサポートし、手動入力のユーザをサポートしません。

移行ユーティリティ メッセージ

次の表で、さまざまな ACS オブジェクトの移行時に表示される可能性のあるエラーおよび通知メッセージについて説明します。ここでは、次の内容について説明します。

ダウンロード可能 ACL

表 D-1 で、ダウンロード可能な ACL の移行時に表示される可能性のあるエラーおよび通知メッセージの詳細を説明します。

表 D-1　ダウンロード可能な ACL のエラーおよび通知メッセージ

フェーズ	タイプ	エラー	診断
エクスポート	Information	Shared DACL name after migration has been changed to: *name after truncation.*	切り捨て
エクスポート	Error	Cannot migrate a shared DACL with a name that contains any of the following characters: *illegal characters for the object*.	名前エラー
インポート	Error	*Error from PI.*For example, object already exists in the ACS 5.3 database.	なし

MAB

表 D-2 で、MAB の移行時に表示される可能性のあるエラーおよび通知メッセージの詳細を説明します。

表 D-2　MAB のエラーおよび通知メッセージ

フェーズ	タイプ	エラー	診断
エクスポート	Information	MAB name after migration has been changed to: *name after truncation*.	切り捨て
エクスポート	Information	Cannot migrate a MAB with a name that contains any of the following characters: *illegal characters for the object*.	名前エラー
エクスポート	Information	Invalid MAC ID.	変換できない
インポート	Error	*Error from PI.*For example, Object already exists in the ACS 5.3 database.	なし
インポート	Error	Group ID: *group ID* referenced object was not imported.	参照インポートなし
インポート	Error	Group could not be found for: *MAB name* Group ID: *group ID*.	ログ エラー

NDG

表 D-3 で、NDG の移行時に表示される可能性のあるエラーおよび通知メッセージの詳細を説明します。

表 D-3　NDG のエラーおよび通知メッセージ

フェーズ	タイプ	エラー	診断
エクスポート	Information	Network device name after migration has been changed to: *name after truncation.*	切り捨て
エクスポート	Information	Cannot migrate an NDG with a name that contains any of the following characters: *illegal characters for the object.*	名前エラー
エクスポート	Information	NDG has a shared key password.	パスワードが含まれる
インポート	Error	*Error from PI.*For example, failed to add object: *NDG root name* in function: *method name.*	なし
インポート	Information	Object already exists in the ACS 5.3 database.	重複

マスター キー

表 D-4 で、マスター キーの移行時に表示される可能性のあるエラーおよび通知メッセージの詳細を説明します。

表 D-4　マスター キーのエラーおよび通知メッセージ

フェーズ	タイプ	エラー	診断
エクスポート	Information	Fatal Error: Authority ID is null - Import Failed.	なし
インポート	Error	*Error from PI.*For example, object already exists in the ACS 5.3 database.	なし

ネットワーク デバイス

表 D-5 で、ネットワーク デバイスの移行時に表示される可能性のあるエラーおよび通知メッセージの詳細を説明します。

表 D-5　ネットワーク デバイスのエラーおよび通知メッセージ

フェーズ	タイプ	エラー	診断
エクスポート	Information	Network device name after migration has been changed to: *name after truncation*.	切り捨て。
エクスポート	Information	Network Device has shared key password.	パスワードが含まれる。
エクスポート	Information	NDG *referenced NDG* unified with *Name of the Network device overlapped with* from NDG *NDG name*.	統合された NDG：*参照された NDG*。
エクスポート	Error	Cannot migrate an NDG with a name that contains any of the following characters: *Illegal characters for the object*.	名前エラー。
エクスポート	Error	NDG referenced object was not exported.	参照オブジェクトはエクスポートされませんでした。
エクスポート	Error	NDG: *referenced NDG* there are *number of subnets* subnets in the following IP address *IP address*.	サブネット制限を超えている。
エクスポート	Error	Unable to translate network device IP address.	変換できない NDG：*参照された NDG*。
エクスポート	Error	NDG *referenced NDG*: Network device IP address overlaps the same device.	オーバーラップする NDG：*参照された NDG*。
エクスポート	Error	Network device has been discarded as it is unified with: *unified NDG*.	統合されたパートナー NDG：*参照された NDG*。
エクスポート	Error	Network device IP is overlapping with other device.	オーバーラップする NDG：*参照された NDG*。
エクスポート	Error	Overlaps with: *Network device name* from NDG: *NDG name*.	オーバーラップする NDG：*参照された NDG* IP アドレス：*IP アドレス*。
インポート	Error	NDG referenced object was not imported.	参照インポートなし。
インポート	Error	*Error from PI.*For example, Object already exists in the ACS 5.x database.	なし。

RAC

表 D-6 で、RAC の移行時に表示される可能性のあるエラーおよび通知メッセージの詳細を説明します。

表 D-6　RAC のエラーおよび通知メッセージ

フェーズ	タイプ	エラー	診断
エクスポート	Information	RAC name after migration has been changed to: *name after truncation.*	切り捨て
エクスポート	Error	ACS 5.3 does not support this attribute: vid= *vendor ID*, att= *attribute value*.No other attributes in RAC will be migrated.	サポートされていないベンダー
エクスポート	Error	RAC does not contain any supported attributes.	値なし
エクスポート	Error	Cannot migrate an RAC with a name that contains any of the following characters: *Illegal characters for the object.*	名前エラー
エクスポート	Error	Wrong enum value for attribute: *attribute name.*No other attributes in RAC will be migrated.	エラー
エクスポート	Error	Invalid value for attribute: *VSA attribute name.*No other attributes in RAC will be migrated.	エラー
エクスポート	Information	The following attribute was not migrated: *attribute name.*	サポートされていないベンダー
エクスポート	Error	ACS 5.3 does not support this attribute: vid= *vendor ID*, att= *attribute value*, name= *attribute name.*No other attributes in RAC will be migrated.	サポートされていないベンダー
インポート	Error	RAC exception, for example, Invalid attribute number.	なし
インポート	Error	*Error from PI.*For example, Object already exists in the ACS 5.3 database.	なし
インポート	Fatal	An error occurred in createCapabilitiesAll(): *Exception details.*	ログ エラー

コマンド セット

表 D-7 で、コマンド セットの移行時に表示される可能性のあるエラーおよび通知メッセージの詳細を説明します。

表 D-7　コマンド セットのエラーおよび通知メッセージ

フェーズ	タイプ	エラー	診断
エクスポート	Information	Command set name after migration has been changed to: *name after truncation.*	切り捨て
エクスポート	Information	Identical objects cannot be migrated: *identical object name.*	統合
エクスポート	Information	*Command set value:* Invalid Command Set value.	変換できない
エクスポート	Information	Cannot migrate a command set with a name that contains any of the following characters: *Illegal characters for the object.*	名前エラー
エクスポート	Information	*Command set name* was not imported and shell exec and command set for this user/group were not imported.	名前エラー
エクスポート	Information	Shared command sets name cannot contain apostrophes or curly braces.	名前エラー
エクスポート	Information	*Command Set name* contains a duplicate argument.	引数が重複している
エクスポート	Information	The selected network device NDG is not supported.	サポートされていないオプション
エクスポート	Error	Translation failed.The argument does not start with Unmatched.	ログ エラー
エクスポート	Error	Translation failed.An equals sign (=) is missing after Unmatched	ログ エラー
エクスポート	Fatal	Translation failed since Unmatched is not set to permit or deny: *unmatched value.*	ログ エラー
エクスポート	Error	Group T+ shell command translation failed: *exception details*.	ログ エラー
エクスポート	Error	Group T+ shell command translation failed.The argument is not a prefix with permit/deny: *argument action value*.	ログ エラー
エクスポート	Error	*Command name* Group T+ command set translation failed: *exception details*.	ログ エラー
エクスポート	Error	*Command description, Exception details*.	ログ エラー
インポート	Error	Referenced object was not imported.	参照インポートなし
インポート	Error	*Error from PI.*For example, object already exists in the ACS 5.3 database.	エラー

Shell Exec

表 D-8 で、shell exec の移行時に表示される可能性のあるエラーおよび通知メッセージの詳細を説明します。

表 D-8　Shell Exec のエラーおよび通知メッセージ

フェーズ	タイプ	エラー	診断
エクスポート	Information	Command set name after migration has been changed to: *name after truncation.*	切り捨て
エクスポート	Information	Identical objects cannot be migrated: *identical object name.*	統合
エクスポート	Information	*Shell Exec value* Invalid shell exec value.No other T+ shell exec attributes will be migrated.	変換できない
エクスポート	Information	Parsing error.No other T+ shell exec attributes will be migrated.	変換できない
エクスポート	Information	Cannot migrate a command set with a name that contains any of the following characters: *Illegal characters for the object*.No other T+ shell exec attributes will be migrated.	名前エラー
エクスポート	Information	*Shell Exec name* was not imported and shell exec and command set for this user/group were not imported.No other T+ shell exec attributes will be migrated.	名前エラー
エクスポート	Information	ACS 5.3 does not support custom attributes present in T+ shell exec.No other T+ shell exec attributes will be migrated.	挿入
エクスポート	Information	T+ shell exec not defined for user or user group.No other T+ shell exec attributes will be migrated.	挿入
エクスポート	Information	Idle time for shell exec should be in the range of 0-9999.No other T+ shell exec attributes will be migrated.	無効なアイドル時間
エクスポート	Information	Time out for shell exec should be in the range of 0-9999.No other T+ shell exec attributes will be migrated.	無効なタイムアウト
エクスポート	Information	T+ shell priv-lvl is invalid *value*.No other T+ shell exec attributes will be migrated.	無効な特権レベル
エクスポート	Information	T+ shell priv-lvl *value* is higher than max-priv-lvl *max value*.No other T+ shell exec attributes will be migrated.	無効な特権レベル
エクスポート	Information	ACS 5.3 does not support custom attributes present in T+ shell exec.	サポートされていないオプション

表 D-8　Shell Exec のエラーおよび通知メッセージ （続き）

フェーズ	タイプ	エラー	診断
エクスポート	Error	Group T+ shell exec translation failed: *exception details*.	ログ エラー
エクスポート	Error	An error occurred while retrieving the max privilege: *exception details*.	ログ エラー
インポート	Error	Referenced object was not imported.	参照インポートなし
インポート	Error	*Error from PI*.For example, object already exists in the ACS 5.3 database.	エラー

ユーザ

表 D-9 で、ユーザの移行時に表示される可能性のあるエラーおよび通知メッセージの詳細を説明します。

表 D-9　ユーザのエラーおよび通知メッセージ

フェーズ	タイプ	エラー	診断
エクスポート	Information	User name after migration has been changed to: *name after truncation*.	切り捨て
エクスポート	Error	Cannot migrate users with names that contain any of the following characters: *Illegal characters for the object.*	名前エラー
エクスポート	Error	Cannot migrate users whose password does not conform to the ACS 5 password policy.Passwords should be between 4 and 32 characters in length.	パスワード エラー
エクスポート	Error	Cannot migrate users with empty password to ACS 5.3.	パスワードなし
エクスポート	Error	Cannot migrate VoIP users to ACS 5.3.	VoIP グループ
エクスポート	Error	A problem occurred while reading the expiry data for the user.	ログ エラー
インポート	Error	Referenced object was not imported.	参照インポートなし
インポート	Error	Group could not be found for: *MAB name* Group ID: *group ID*.	ログ エラー

ユーザ属性

表 D-10 で、ユーザ属性の移行時に表示される可能性のあるエラーおよび通知メッセージの詳細を説明します。

表 D-10　ユーザ属性のエラーおよび通知メッセージ

フェーズ	タイプ	エラー	診断
エクスポート	Information	User attribute after migration has been changed to: *name after truncation*.	切り捨て
エクスポート	Information	Cannot migrate a user attribute with a name that contains any of the following characters: *Illegal characters for the object.*	名前エラー
エクスポート	Information	*User attribute name* User-defined name is not unique.It will be disambiguated for import by appending a suffix.	反復
インポート	Information	Attribute added with warning: Object already exists in the ACS 5.3 database.	重複
インポート	Error	*Error from PI.*	エラー

ユーザ属性値

表 D-11 で、ユーザ属性値の移行時に表示される可能性のあるエラーおよび通知メッセージの詳細を説明します。

表 D-11　ユーザ属性値のエラーおよび通知メッセージ

フェーズ	タイプ	エラー	診断
エクスポート	Error	*User attribute value* was not imported and user attribute values for this user were not imported.	ログ エラー

ユーザ グループ

表 D-12 で、ユーザ グループの移行時に表示される可能性のあるエラーおよび通知メッセージの詳細を説明します。

表 D-12　ユーザ グループのエラーおよび通知メッセージ

フェーズ	タイプ	エラー	診断
エクスポート	Error	Group has no users.	ユーザなし
エクスポート	Error	Cannot migrate a user group with a name that contains any of the following characters: *Illegal characters for the object.*	名前エラー
インポート	Information	*Error from PI.*	重複
インポート	Error	*Error from PI.*	エラー

VSA ベンダー

表 D-13 で、VSA ベンダー ID の移行時に表示される可能性のあるエラーおよび通知メッセージの詳細を説明します。

表 D-13　VSA ベンダーのエラーおよび通知メッセージ

フェーズ	タイプ	エラー	診断
エクスポート	Error	Object already exists in the ACS 5.3 database.	重複
エクスポート	Information	Vendor name conflict.ACS 5.3 vendor name: *vendor name.*	名前エラー
インポート	Error	VSA vendor ID *vendor id* import failed.*Error from PI*:	Enum エラー

VSA

表 D-14 で、VSA の移行時に表示される可能性のあるエラーおよび通知メッセージの詳細を説明します。

表 D-14　VSA のエラーおよび通知メッセージ

フェーズ	タイプ	エラー	診断
エクスポート	Error	VSA ID *attribute id value* has attribute profile conflicts: In ACS 4.x, it is *name for the profile*, but in ACS 5.0, it is *direction value*.	プロファイル エラー
エクスポート	Error	VSA ID (attribute id) has attribute name conflicts: In ACS 4.x, it is *attribute name*, but in ACS 5.3, it is *attribute name*.	名前エラー

表 D-14　VSA のエラーおよび通知メッセージ （続き）

フェーズ	タイプ	エラー	診断
インポート	Error	VSA ID *attribute id* has attribute type conflicts: In ACS 4.x, it is *attribute type*, but in ACS 5.0, it is *ACS 5.3 attribute type value.*	タイプ エラー
エクスポート	Error	There is a problem with the VSA ID *attribute id* enum values (see log for details)	Enum エラー
エクスポート	Error	Object already exists in the ACS 5.3 database.	なし
インポート	Error	VSA *attribute id* enum import failed.*Error from PI:*	Enum エラー
インポート	Information	VSA *attribute ID* enabling log failed.	なし
インポート	Error	VSA *attribute ID* attribute import failed.*Error from PI.*	サポートされていない属性
インポート	Error	VSA *attribute ID* vendor ID *vendor ID* import failed.*Error from PI.*	参照インポートなし

Cisco TAC へのレポートの問題

Cisco TAC へ問題を報告する場合は、次の情報を含めてください。

- ACS 4.x データベース（.dmp ファイル）のバックアップ
- 移行のログファイル（...migration/bin/migration.log）
- config フォルダのすべてのレポート（...migration/config）
- ACS 5.3 ログファイル
- ACS 5.3 ビルド番号
- ACS 4.x ビルド番号

GLOSSARY

A

ACL Access Control List（アクセス コントロール リスト）。オブジェクトに付随する権限のリスト。

ACS Access Control System（アクセス コントロール システム）。

AD Active Directory。

C

CN Common Name（共通名）。

E

EAP Extensible Authentication Protocol。無線ネットワークとポイントツーポイント接続でよく使われる認証フレームワークです。

EAP-FAST Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling。EAP-FAST は IEEE 802.1X と IEEE 802.11i に準拠しています。すべての EAP タイプと同様に EAP-FAST は WPA ネットワークと WPA2 ネットワークで使用できます。

H

HTTPS Hypertext Transfer Protocol Secure。HTTP を使用してリソースにアクセスする場合に、通常使用される HTTP スキームと構文上同一の URL スキーム。URL に HTTPS: を使用することは、HTTP を使用しますが、HTTP と TCP 間で別のデフォルト ポート（443）と追加の暗号化 / 認証レイヤを使用することを示します。

J

JDBC JAVA Database Connectivity。クライアントのデータベースへのアクセス方法を定義する JAVA プログラミング言語の API。データベース内のデータを問い合わせ、更新するための方法を提供します。

L

LDAP Lightweight Directory Access Protocol。TCP/IP で実行するディレクトリ サービスを使用してデータを問い合わせ、変更するためのアプリケーション プロトコルです。

M

MAC アドレス Media Access Control（メディア アクセス コントロール）アドレス。識別用にほとんどのネットワーク アダプタやネットワーク インターフェイス カードに割り当てられる擬似固有識別子。

N

NAP Network Access Profile（ネットワーク アクセス プロファイル）。

NDG Network Device Group（ネットワーク デバイス グループ）。

P

PI Programmatic Interface（プログラマチック インターフェイス）。外部アプリケーションが ACS とやりとりするためのメカニズム。

R

RADIUS Remote Authentication Dial-In User Service。接続してネットワーク サービスを使用するコンピュータの認証、認可、アカウンティング（AAA）集中管理を提供するネットワーキング プロトコルです。

S

SOAP Simple Object Access Protocol。通常 HTTP を使用して、コンピュータ ネットワーク上で XML ベースのメッセージを交換するためのプロトコル。SOAP は Web サービス スタックの基礎レイヤを形成します。

SAN Subject Alternative Name。

T

TACACS Terminal Access Controller Access-Control System。UNIX ネットワークで一般的に使用される認証サーバと通信するために使用されるリモート認証プロトコルです。リモート アクセス サーバは、ユーザがネットワークへのアクセス権を持つかどうかを判断するために、TACACS を使用して、認証サーバと通信します。

V

VSA ベンダー固有属性（Vendor Specific Attribute）。標準 RADIUS 属性セットによって提供されない独自のプロパティまたは特性。VSA は、リモート アクセス サーバのベンダーによって、RADIUS をベンダー サーバ用にカスタマイズするために定義されます。

X

XML eXtensible Markup Language。

INDEX

A

M

あ

い

か

き

こ

さ

し

せ

た

て

と

ね

は

ふ

ゆ

よ

れ