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。

- 「ネットワーク リソース」（P.2-2）
- 「ユーザおよび ID ストア」（P.2-7）
- 「ポリシー要素」（P.2-11）
- 「システム管理」（P.2-15）

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

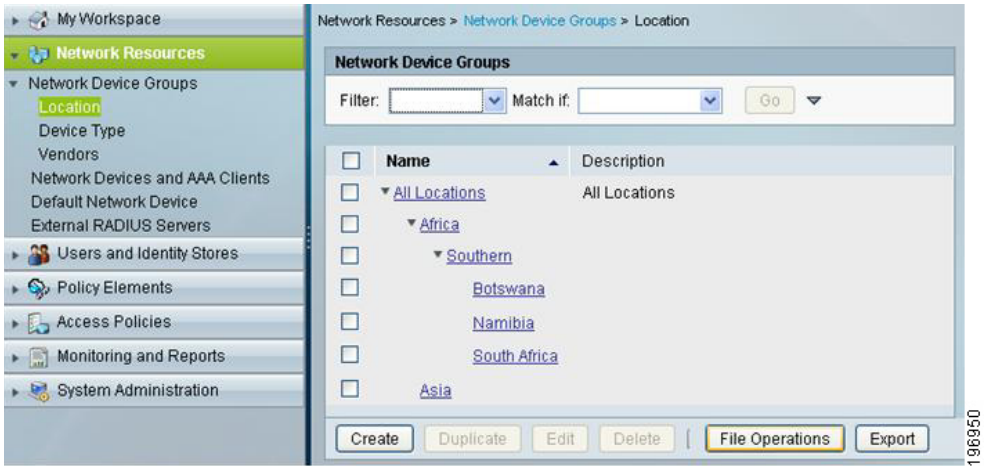
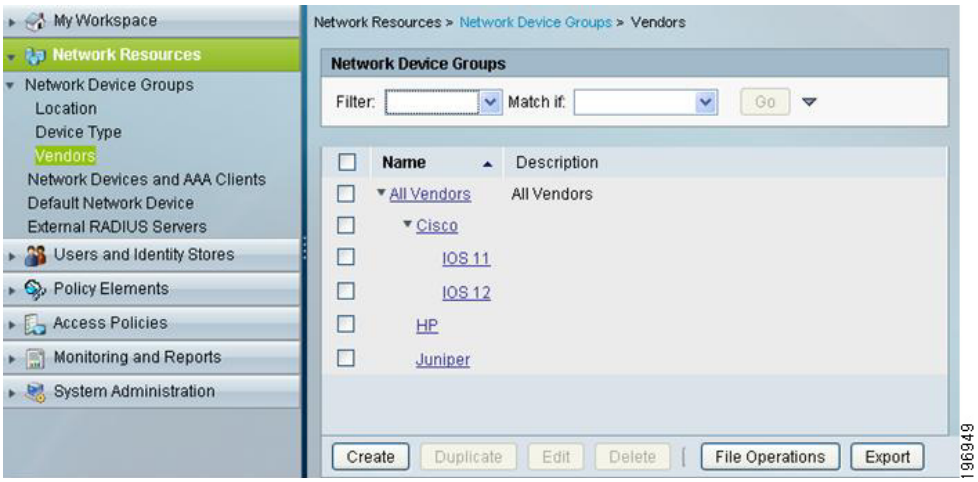


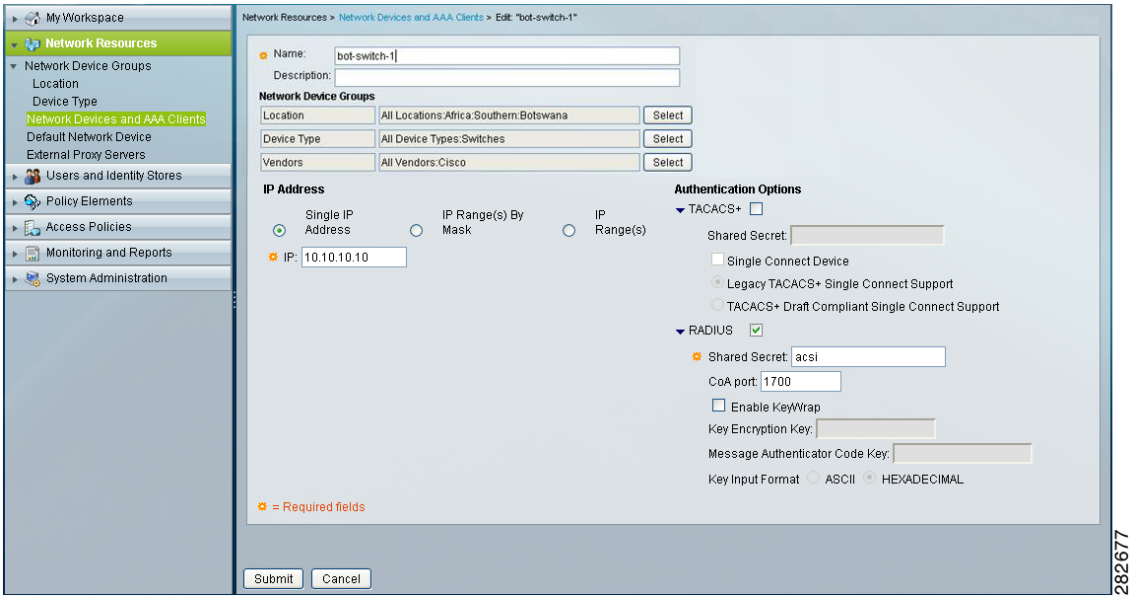
図 2-2　　ネットワーク デバイス グループ階層

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

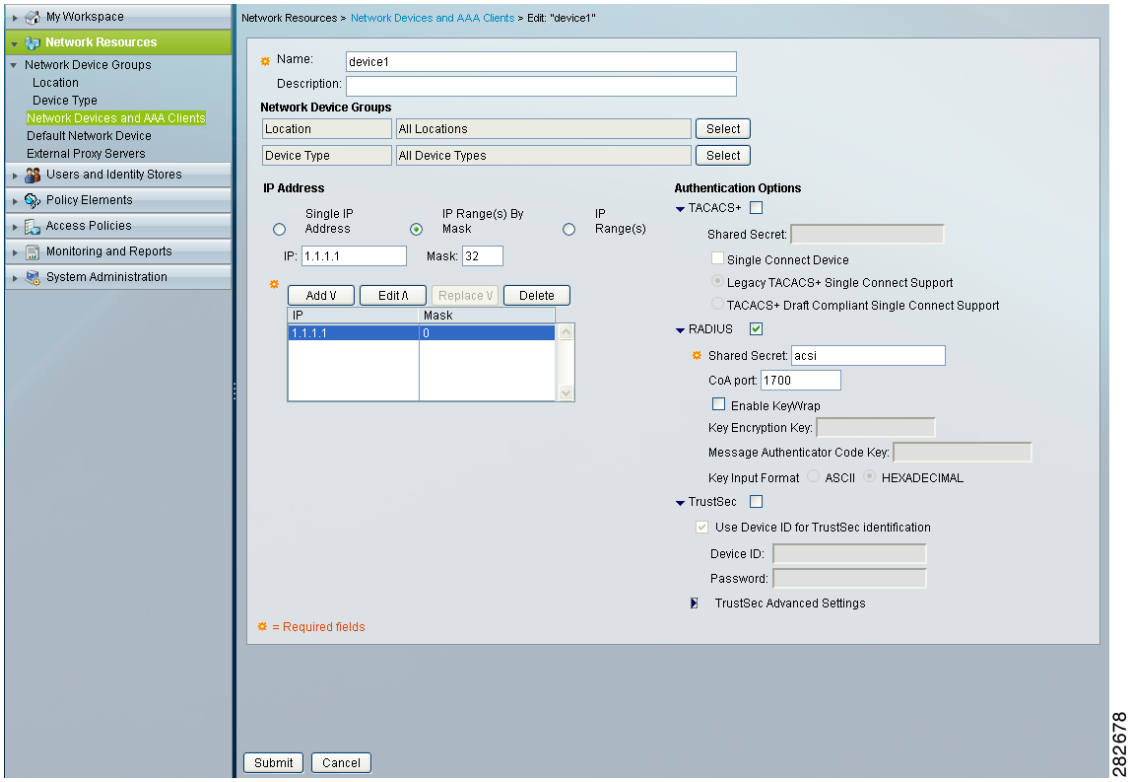
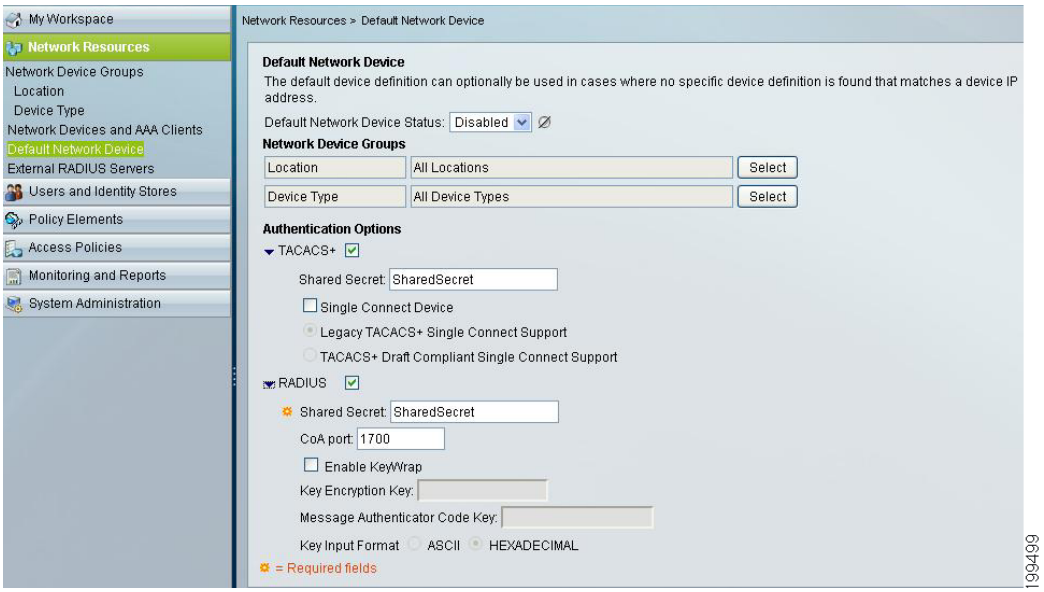


図 2-5 に、サブネット 10.10.20.0 および 10.10.30.0 のクライアントを表すデバイス定義を示します。デバイス設定で TACACS+ または RADIUS のどちらもイネーブルになっているため、これらのクライアントは両方の要求を送信できます。

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。

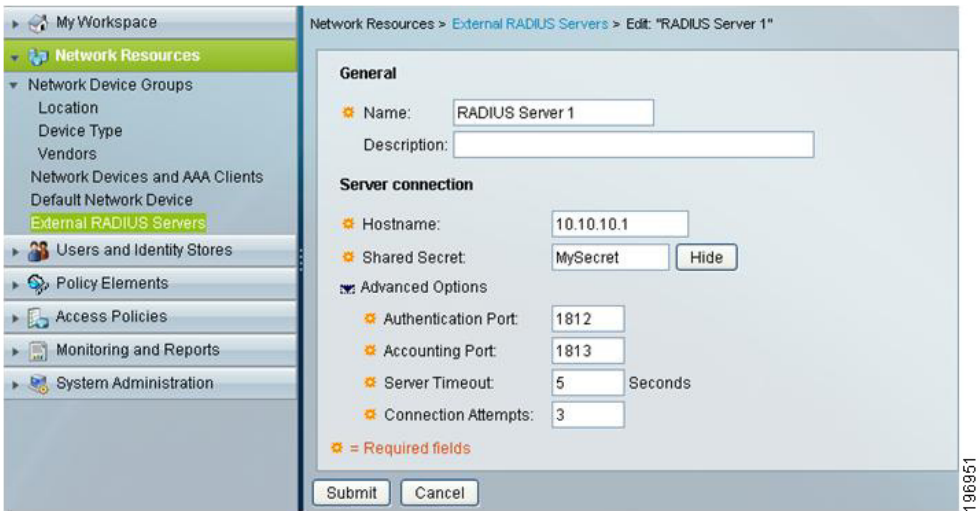
移行メモ

- 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。

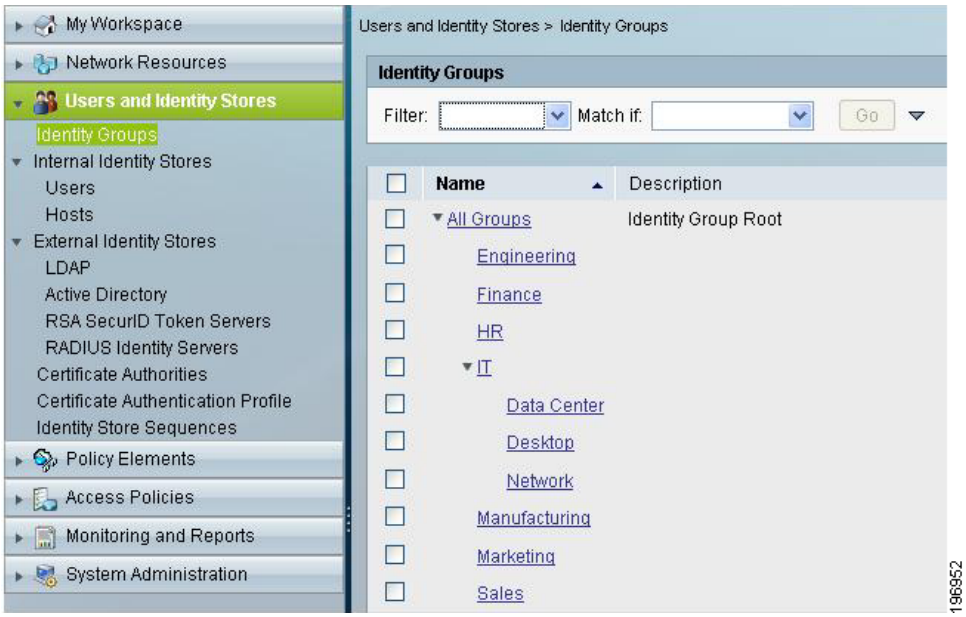
- 「ID グループ」（P.2-7）
- 「内部 ID ストア」（P.2-9）
- 「外部 ID ストア」（P.2-10）
- 「信頼できる認証局および証明書認証プロファイル」（P.2-10）
- 「ID ストア順序」（P.2-11）

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。

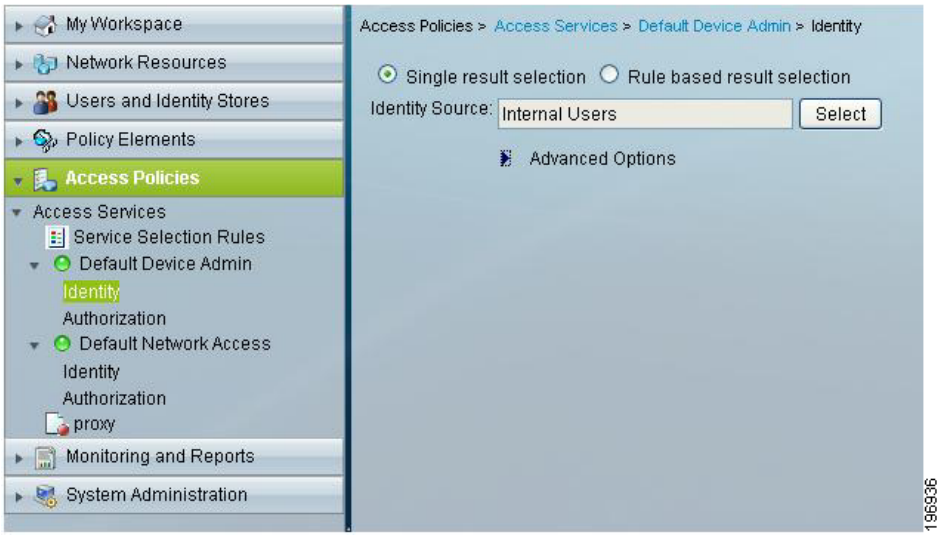
アクセス ポリシーの詳細については、『*User Guide for the Cisco Secure Access Control System*』を参照してください。

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。

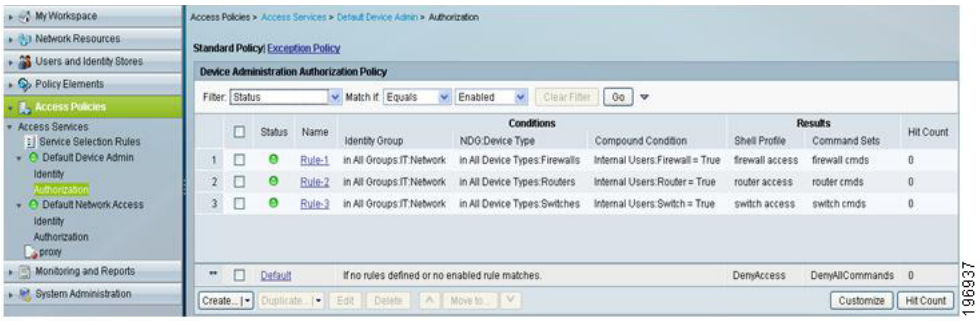
    たとえば、ユーザはワンタイム パスワード サーバに認証されますが、認可のためのユーザ属性の取得に ACS 内部ユーザ ストアが必要なことがあります。場合によっては、ACS は ACS 内部ユーザ ストアおよび Active Directory の両方を確認して、認証対象のユーザを検索する必要があります。

図 2-10　ID ストア順序



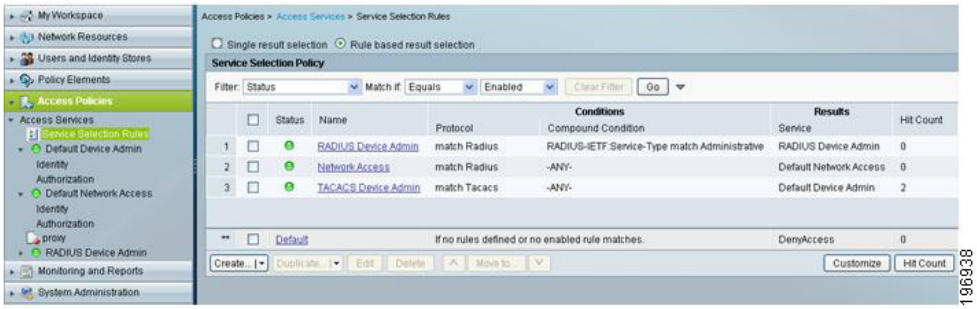
- 図 2-11 に示すように、新しいユーザおよびネットワーク デバイス グループ化を利用して認可ポリシーを作成できます。

図 2-11　認可ポリシー



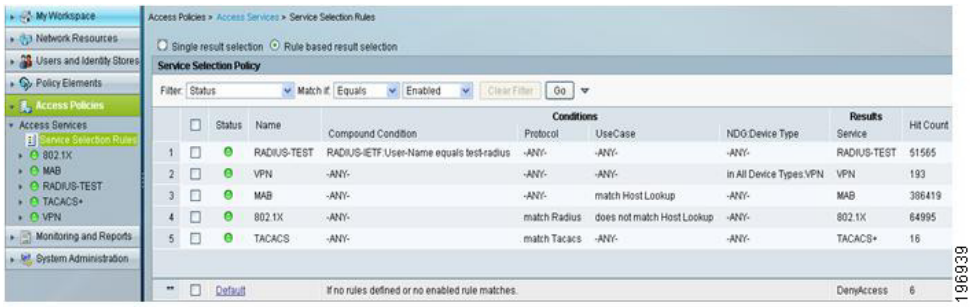
- RADIUS ベースのデバイス管理では、さまざまなアクセス サービスを作成して、サービス セレクション ポリシーのネットワーク アクセス サービスと、これらの認証要求および認可要求を区別します。図 2-12 にサービス セレクション ポリシーを示します。

図 2-12　サービス セレクション ポリシー



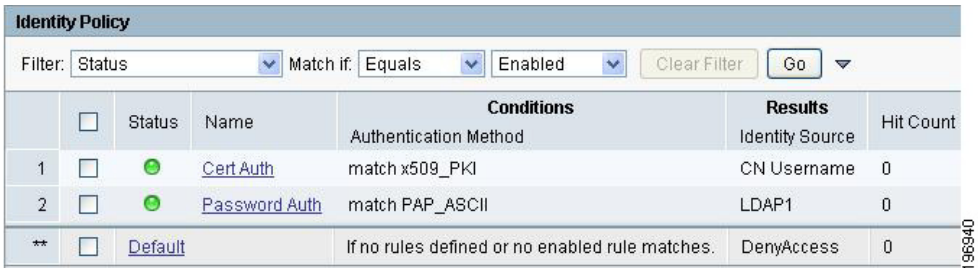
- 単純なネットワーク アクセス シナリオでは、事前に設定されたネットワーク アクセス サービスを更新できます。より複雑なネットワーク アクセス シナリオに対応できるように、図 2-13 に示す追加のアクセス サービスが導入されています。

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

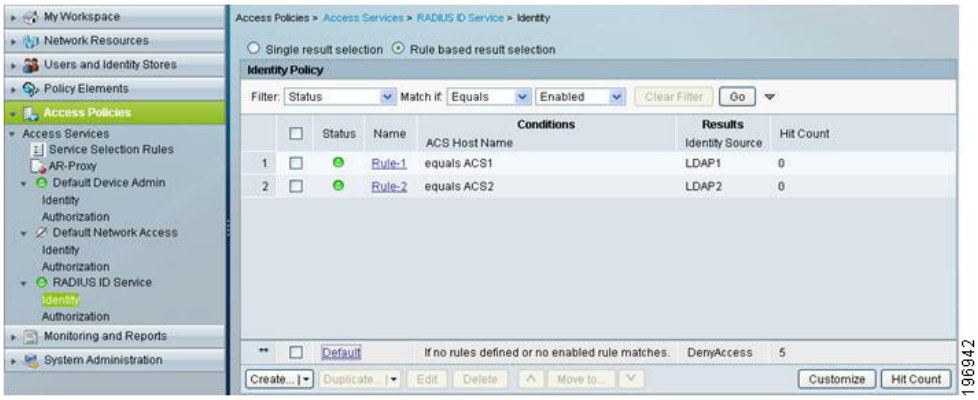


- 最初に ACS グループに外部グループをマッピングするのではなく、認可ポリシーで直接外部グループを使用します。

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。