移行ユーティリティでの ACS 5.5 属性サポート

この章の内容は、次のとおりです。

概要

この章では、ACS 4.x から ACS 5.5 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 5.5 の基準を満たす必要があります。要素の一部の属性が ACS 5.5 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 5.5 に移行できます。

たとえば ACS 5.5 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 5.5 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 5.5 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 5.5 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 5.5 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 5.5 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 5.5 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 5.5 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 5.5 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 5.5 のポリシー関連の認可データは、ACS 5.5 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 5.5 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 5.5 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 5.5 では、デフォルトの特権レベルが最大特権レベルよりも大きくなることはできません。 • ACS 5.5 では、数値（1 ～ 15）による特権レベルがサポートされます。
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 5.5 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 5.5 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 5.5 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 5.5 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 5.5 では、数値（1 ～ 15）による特権レベルがサポートされます。 • ACS 5.5 では、デフォルトの特権レベルが最大特権レベルよりも大きくなることはできません。
TACACS+ Shell（exec）カスタム属性	ACS 5.5 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 5.5 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。

ACS 4.x はグループ ベースのアクセス コントロール システムですが、ACS 5.x 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。移行ユーティリティを使用して ACS 4.x から 5.x に移行した場合、カスタム属性は移行されません。その結果、すべての認証と許可が ACS 5.x で失敗することがあります。したがって、シェル プロファイルでカスタム属性を手動設定し、それをアクセス ポリシーで各ユーザにマッピングする必要があります。

カスタム属性を手動で設定する方法については、http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.5/user/guide/pol_elem.html #wp1053110 を参照してください。

ポリシー条件でカスタム属性をマッピングする方法については、http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.5/user/guide/access_policies.html を参照してください。

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 5.5 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 5.5 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 認証バイパス MAB（ホスト）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 コンテンツおよびネットワーク アクセス フィルタ（NAF）ID の組のリストで構成されます。ACS 4.x の 1 つの DACL を ACS 5.5 の複数の DACL に移行できます。ACS 5.5 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 5.5 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 5.5 情報モデル オブジェクト（IMO）に移行されます。

共有 RAC

ACS 4.x では、RADIUS 認可コンポーネント（RAC）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 5.5 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 5.5 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 5.5 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 5.5 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 5.5 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 5.5 の不足した属性の識別を反復して行います。ACS 5.5 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 5.5 ディクショナリにベンダーが存在する場合、ACS 5.5 で定義されていない属性だけが移行されます。

最大ユーザ セッション

ACS 4.*x* では、[Maximum User Sessions] 設定をユーザ レベル、グループ レベル、およびグローバルに設定できます。最大ユーザ セッションの設定は、4. *x* から 5.5 に移行する場合に移行されます。