Cisco NAC のポリシーのインポート、エクスポート（PIE）を実行するベスト プラクティス

目次

概要

このドキュメントの目的は、Cisco NAC のポリシー インポート エクスポート（PIE）機能の正常な実行を確保するためのベスト プラクティス ガイドラインを強調することです。

前提条件

要件

Cisco NAC Manager（Clean Access Manager）Web インターフェイス、および一般的に設定されるポリシーに関する知識が必要です。 PIE でサポートされているものやサポートされていないものについては、Cisco NAC リリース 4.5 のリリース ノートを参照してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco NAC ソフトウェア 4.5.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

PIE のベスト プラクティスの推奨事項

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

設定

CAM のポリシー インポート エクスポート（PIE）機能を正常に実装するため、次の推奨事項に従ってください。

1. ポリシーの同期を実行する前に、すべての NACM に同じ Cisco Updates がインストールされていることを確認するため、マスターおよびレシーバ NACM の両方に同じ自動更新設定を行う（[Device Management] > [Clean Access] > [Updates]> [Update]）ことを推奨します。 これは、異なる自動更新設定を持つレシーバ NACM に Cisco Updates をインストールして、ポリシーの同期を実行すると、マスターの現在のチェックがレシーバのすべてのチェックを上書きするためです。
2. OOB NACM と IB のみのライセンスをもつレガシー NACM がある場合、OOB NACM をマスター NACM として使用し、レガシー NACM をレシーバとして使用してください。
3. マスターとレシーバ間の特定のコンポーネントで PIE が有効になると、レシーバ テーブルや情報はマスターからプッシュされた情報ですべて置き換えられます。 これはレシーバ側で蓄積できません。 たとえば、レシーバが mcafee.com へのアクセスを許可するトラフィック ルールを持っていて、マスターが cisco.com および abc.com へのアクセスを許可するトラフィック ルールを持つ一方、mcafee.com へのルールを持っていない場合、同期が実行されると、レシーバとマスターは同一のルール： cisco.com および abc.com を持つようになります。 マスターには mcafee.com のルールがなかったため、同期後にはレシーバに mcafee.com のトラフィック ルールがなくなることに注意してください。 ベスト プラクティスは、マスター NACM を希望通りに設定する一方、レシーバのポリシー設定を修正しないことです。
4. サポートされるレシーバの最大数は 10 です。 レシーバの数に技術的制約はありませんが、ベスト プラクティスの推奨事項は、これをサポートされる数（10 以下）にしておくことです。**注:** NACM HA ペアでは、スタンバイ NACM のポリシー同期設定は無効になります。
5. マスターとレシーバでは、Cisco NAC（4.5 以降）リリースの同じバージョンを実行する必要があります。
6. 両方の NAC Manager が認証局（CA）署名証明書を持ち、マスターとレシーバの両方が互いの証明書を信頼していることを確認します。 証明書は、マスターとレシーバ間の同期の安全を保証する鍵です。 マスターはレシーバが提示する証明書を信頼する必要があり、またその逆も必要です。 このためそれぞれが、信頼できる CA リストに、ピア証明書のルート CA（仲介が含まれる場合フル チェーン）を持っていることが必要です。 実稼働環境でのベスト プラクティスは、NAC Manager の自己署名証明書を CA 署名証明書に置き換えることです。 つまり、PIE を実装する前に、NAC Manager の SSL 証明書のベスト プラクティスに従っていることを確認します。
7. 自動または手動でポリシーの同期を実行するには、完全制御の管理ユーザとして、マスター NAC Manager にログインする必要があります。
8. 自動同期では、自動ポリシー同期を *X* 日（最低 1 日）毎にスケジュールすることができま

す。 PIE に自動同期を使用する場合、NAC Manager 間の自動同期を有効にする前に、手動同期を実行し、その同期が正常に動作することを確認するよう強く推奨します。

確認

現在、この設定に使用できる確認手順はありません。

関連情報

- テクニカルサポートとドキュメント - Cisco Systems