ベスト プラクティス：サーバー セキュリティの強化

以下のセクションで、セキュリティ上の弱点を個別に排除または制御して、サーバーセキュリティを高める方法について説明します。

セキュアでないサービスの無効化

使用する予定のない、セキュアでないサービスは無効化する必要があります。たとえば、TFTP および FTP はセキュアなプロトコルではありません。これらのサービスは、通常、ネットワーク デバイスと Prime Infrastructure の間でファームウェアやソフトウェアのイメージを転送するために使用されます。また、システムバックアップを外部ストレージに転送するためにも使用されます。このようなサービスにはセキュアなプロトコル（SFTP または SCP など）を使用することを推奨します。

FTP および TFTP サービスを無効にするには、次の手順に従います。

ステップ 1 管理者権限を持つユーザー ID を使用して Prime Infrastructure にログインします。

ステップ 2 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [一般（General）] > [サーバー（Server）]** の順に選択します。

ステップ 3 [FTP] および [TFTP] に対して、[無効化（Disable）] ボタンを選択します。

ステップ 4 Cisco Prime Infrastructure を再起動して、設定の更新を適用します。

root アクセスの無効化

管理ユーザーは、トラブルシューティングの目的で基盤となるオペレーティング システムに対する root シェル アクセスを有効化できます。このアクセスは、シスコ サポート チームが製品関連の運用上の問題をデバッグするために使用されます。このアクセスは無効な状態のままにし、必要な場合にのみを有効化することを推奨します。root アクセスを無効化するには、コマンド ラインから root_disable コマンドを実行します（CLI から接続する方法を参照）。

インストール時に、Prime Infrastructure は Web root ユーザー アカウントも作成し、このアカウントに使われるパスワードを入力するようインストール担当者に促します。Prime Infrastructure サーバーとその Web ユーザー インターフェイスに初めてログインする際には、Web root アカウントが必要です。通常の動作にこのアカウントを使用しないことを推奨します。このアカウントの用途は、日常的な運用およびネットワーク管理を行うための適切な権限を持つユーザー ID と、Prime Infrastructure 自体を管理するための管理ユーザー ID を作成することです。これらのユーザー アカウントを作成したら、インストール時に作成されたデフォルトの「Web root」アカウントを無効化し、その後は、管理ユーザー ID を使用してユーザー アカウントを作成します。

シェル パスワードを忘れた場合は、管理者パスワードを復元するための以下の手順に従って、シェル パスワードを復元（およびリセット）できます。「仮想アプライアンスの管理者パスワードの回復」を参照してください。管理者パスワードを復旧した場合 Prime Infrastructure サーバーを再起動する必要が生じるため、システムが 20 分程度ダウンする可能性があります。

root アカウントを無効にするには、次の手順に従います。

ステップ 1 Prime Infrastructure サーバーとの CLI セッションを開きます（CLI から接続する方法を参照）。「端末設定」モードは開始しないでください。

ステップ 2 次のコマンドを入力して、Web root アカウントを無効化します。

PIServer/admin# **ncs webroot disable**

Prime Infrastructure により Web root アカウントが無効化されます。

ステップ 3 プロンプトで次のコマンドを入力して、root シェル アカウントを無効化します。

PIServer/admin# **shell disable**

root シェル アカウントのパスワードを入力するよう Prime Infrastructure から求められます。パスワードを入力すると、root シェル アカウントの無効化が完了します。

SNMPv2 の代わりに SNMPv3 を使用する

SNMPv3 は、SNMPv2 よりもセキュリティ機能が高いプロトコルです。SNMPv2 の代わりに SNMPv3 を使用して管理が行われるように管理対象デバイスの設定にすることにより、ネットワーク デバイスと Prime Infrastructure サーバー間の通信のセキュリティを強化できます。

新しいデバイスの追加時、デバイスの一括インポート時、またはデバイス検出の一環として、SNMPv3 の有効化を選択できます。それぞれの作業の実行手順については、「関連項目」を参照してください。

関連トピック

SNMPv3 を使用したデバイスの追加 （3 ページ）
SNMPv3 を使用したデバイスのインポート （3 ページ）
SNMPv3 を使用した検出の実行 （4 ページ）

SNMPv3 を使用したデバイスの追加

新規デバイスを追加する際に SNMPv3 を指定するには、次の手順に従います。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）] を選択します。

ステップ 2 [デバイスの追加（Add Device）] を選択します。

ステップ 3 [SNMP パラメータ（SNMP Parameters）] エリアの [バージョン（Version）] で、[v3] を選択します。

ステップ 4 他のフィールドに適宜入力してから、[追加（Add）] をクリックします。

関連トピック

SNMPv3 を使用したデバイスのインポート （3 ページ）
SNMPv3 を使用した検出の実行 （4 ページ）
SNMPv2 の代わりに SNMPv3 を使用する （3 ページ）

SNMPv3 を使用したデバイスのインポート

デバイスを一括インポートする際に、SNMPv3 の使用を指定するには、次の手順に従います。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）] を選択します。

ステップ 2 [一括インポート（Bulk Import）] を選択します。[一括インポート（Bulk Import）] ページが表示されます。

ステップ 3 デバイス追加サンプル テンプレートを [Bulk Import] ページの [here] リンクからダウンロードします。

ステップ 4 任意の CSV 互換アプリケーションを使用してテンプレート ファイルを編集します。CSV インポート ファイル内で、デバイスを表す各行ごとに次の手順を実行します。

a) [snmp version] 列に 3 と入力します。
b) [snmpv3_user_name]、[snmpv3_auth_type]、[snmpv3_auth_password]、[snmpv3_privacy_type]、および [snmpv3_privacy_password] の各列に適切な値を入力します。
c) 使用するデバイスに合わせて、適宜他の列に入力します。

ステップ 5 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）] を選択し、[一括インポート（Bulk Import）] をクリックして、変更した CSV ファイルをインポートします。

関連トピック

SNMPv3 を使用したデバイスの追加 （3 ページ）
SNMPv3 を使用した検出の実行 （4 ページ）
SNMPv2 の代わりに SNMPv3 を使用する （3 ページ）

SNMPv3 を使用した検出の実行

SNMPv3 をデバイス検出の一部として指定するには、次の手順に従います。

ステップ 1 [Inventory] > [Device Management] > [Discovery] の順に選択します。[検出ジョブ（Discovery Jobs）] ページが表示されます。
ステップ 2 ページの右上隅にある [検出設定（Discovery Settings）] リンクをクリックします。[検出設定（Discovery Settings）] ページが表示されます。
ステップ 3 [New] をクリックして、新しい SNMP v3 クレデンシャルを追加します。
ステップ 4 必要に応じてフィールドに入力します。
ステップ 5 [保存（Save）] をクリックして、SNMPv3 の設定を保存し、使用を開始します。

関連トピック

SNMPv3 を使用したデバイスの追加 （3 ページ）
SNMPv3 を使用したデバイスのインポート （3 ページ）
SNMPv2 の代わりに SNMPv3 を使用する （3 ページ）

外部 AAA による認証

ユーザー アカウントとパスワードを RADIUS や TACACS+ などのセキュアな認証プロトコルを実行する専用のリモート認証サーバーにより一元管理すると、管理がより安全になります。

外部 AAA サーバーを使用してユーザーを認証するように Prime Infrastructure を設定できます。Prime Infrastructure グラフィック ユーザー インターフェイス（GUI）から外部認証をセットアップするには、[管理（Administration）]>[ユーザー（Users）]>[ユーザー、ロール、および AAA（Users, Roles & AAA）] ページにアクセスする必要があります。コマンドライン インターフェ

イス（CLI）から外部認証をセットアップすることもできます。それぞれの手法による AAA のセットアップ手順については、「関連項目」を参照してください。

関連トピック

GUI からの外部 AAA の設定 （5 ページ）
CLI からの外部 AAA の設定 （5 ページ）

GUI からの外部 AAA の設定

リモート ユーザー認証を GUI から設定するには、次の手順に従います。

ステップ 1 管理者権限を持つユーザー ID を使用して Prime Infrastructure にログインします。

ステップ 2 [管理（Administration）] > [ユーザー（Users）] > [ユーザー、ロール、および AAA（Users, Roles & AAA）] > [TACACS+] または [管理（Administration）] > [ユーザー（Users）] > [ユーザー、ロール、および AAA（Users, Roles & AAA）] > [RADIUS] を選択します。

ステップ 3 該当するフィールドに TACACS+ または RADIUS サーバーの IP アドレスと共有秘密を入力します。

ステップ 4 [管理（Administration）] > [ユーザー（Users）] > [ユーザー、ロール、および AAA（Users, Roles & AAA）] > [AAA モードの設定（AAA Mode Settings）] の順に選択します。

ステップ 5 必要に応じて AAA モードを設定します。

関連トピック

外部 AAA による認証 （4 ページ）
CLI からの外部 AAA の設定 （5 ページ）

CLI からの外部 AAA の設定

リモート ユーザー認証を CLI から設定するには、次の手順に従います。

ステップ 1 CLI から接続する方法の説明に従って、コマンドラインを使用して Prime Infrastructure にログインします。必ず「端末設定」モードにしてください。

ステップ 2 プロンプトで次のコマンドを入力し、外部 TACACS+ サーバーをセットアップします。

PIServer/admin/terminal# aaa authentication tacacs+ server **tacacs**-ip key plain *shared-secret*

ここで、

- **tacacs**-ip はアクティブな TACACS+ サーバーの IP アドレスです。
- *shared-secret* はアクティブな TACACS+ サーバーのプレーンテキストの共有秘密です。

ステップ 3 プロンプトで次のコマンドを入力し、管理者権限を持つユーザーを作成します。このユーザーは上記の AAA サーバーによって認証されます。

PIServer/admin/terminal# **username** *username password* **remote role admin email** *emailID*

ここで、

- *username* はユーザー ID の名前です。
- *password* はユーザーのプレーンテキストのパスワードです。
- *emailID* はユーザーのメール アドレスです（オプション）。

関連トピック

外部 AAA による認証 （4 ページ）
GUI からの外部 AAA の設定 （5 ページ）

NTP 更新認証の有効化

Network Time Protocol（NTP）バージョン 4 は、サーバーの日付と時刻の更新を認証し、サーバー セキュリティを強化する重要な方法です。Prime Infrastructure では最大 3 台の NTP サーバーを設定できます。

認証された NTP 更新をセットアップするには、次の手順に従います。

ステップ 1 CLI から接続する方法の説明に従って、コマンドラインで Prime Infrastructure にログインします。必ず「端末設定」モードにしてください。

ステップ 2 プロンプトで次のコマンドを入力し、外部 NTPv4 サーバーをセットアップします。

PIServer/admin/terminal# ntp server serverIP userID plain password

ここで、

- serverIP は、使用する認証 NTPv4 サーバーの IP アドレスです。
- userID は、NTPv4 サーバーの MD5 キー ID です。
- password は NTPv4 サーバーに対応する md5 プレーン テキスト パスワードです。

  例：ntp server 10.81.254.131 20 plain MyPassword

ステップ 3 NTP 認証が適切に動作していることを確認するには、次のコマンドを実行してテストします。

- NTP 更新の詳細を確認する：sh run
- NTP 同期の詳細を確認する：sh ntp

Prime Infrastructure サーバー上の OCSP 設定の有効化

Online Certificate Status Protocol（OCSP）は、OCSP レスポンダを使用して Web クライアントの証明書ベース認証を可能にします。通常、OCSP レスポンダの URL は証明書の Authority Information Access（AIA）から読み取られます。フェールオーバー メカニズムとして、Prime Infrastructure サーバー上で同じ URL を設定できます。

OCSP レスポンダのカスタム URL をセットアップするには、次の手順に従います。

ステップ 1 CLI から接続する方法の説明に従って、コマンドラインを使用して、Prime Infrastructure サーバーにログインします。「端末設定」モードは開始しないでください。

ステップ 2 プロンプトで次のコマンドを入力し、クライアント証明書認証を有効化します。

PIServer/admin# **ocsp responder custom enable**

ステップ 3 プロンプトで次のコマンドを入力し、カスタム OCSP レスポンダ URL を設定します。

PIServer/admin# **ocsp responder set url** *Responder#URL*

ここで、

- *Responder#* は定義する OCSP レスポンダの数です（たとえば、1、2 など）。
- *URL* はクライアントの CA 証明書から取得される OCSP レスポンダ の URL です。

  Responder# 値と *URL* 値の間にスペースを入れないことに注意してください。

ステップ 4 Prime Infrastructure サーバーで定義されている既存のカスタム OCSP レスポンダを削除するには、次のコマンドを使用します。

PIServer/admin# **ocsp responder clear url** *Responder#*

削除する OCSP レスポンダの数が不明な場合は、**show security-status** コマンドを使用して、サーバー上で現在設定されている OCSP レスポンダを確認します。詳細については、「サーバー セキュリティ ステータスの確認」を参照してください。

ローカル パスワード ポリシーの設定

Prime Infrastructure 独自の内部認証を使用してユーザーをローカルで認証する場合、強力なパスワードの選択ルールを適用することにより、システムのセキュリティを向上させることができます。

これらのポリシーは、ローカルの Prime Infrastructure ユーザー ID のパスワードにのみ影響します。集中型つまりリモート AAA サーバーで Prime Infrastructure ユーザーを認証している場合、AAA サーバーの機能を利用して、同様の保護を適用できます。

ローカル パスワード ポリシーを適用するには：

ステップ 1 管理者権限を持つユーザー ID を使用して Prime Infrastructure にログインします。

ステップ 2 [管理（Administration）] > [ユーザー（Users）] > [ユーザー、ロール、および AAA（Users, Roles, & AAA）] > [ローカル パスワード ポリシー（Local Password Policy）] の順に選択します。

ステップ 3 適用するパスワードポリシーの横にあるチェックボックスを選択します。パスワードポリシーには以下が含まれます。

- パスワードに含める必要がある最小文字数。
- パスワードにユーザ名または「cisco」（またはこれらの一般的な並べ替え）を使用しない。
- ルート パスワードに「public」を使用しない。
- どのパスワード文字についても連続する繰り返しは 3 回以下。
- パスワードには大文字、小文字、数字、特殊文字という文字クラスのうち 3 つから少なくとも 1 文字ずつを含める必要がある。
- パスワードは ASCII 文字のみを含む必要があるかどうか。
- パスワードを再利用するまでの最小経過日数。
- パスワードの有効期限。
- パスワード失効の事前警告。

パスワード ポリシー要件に応じて、次のパスワード ポリシーも指定できます。

- 最小パスワード長（文字の数）。
- パスワード再利用間の最小経過期間。
- パスワード有効期間。
- 将来のパスワード失効に関してユーザへの警告を開始する事前日数。

ステップ 4 [Save] をクリックします。

個々の TCP/UDP ポートの無効化

次の表に、Prime Infrastructure が使用する TCP および UDP ポート、これらのポート上で通信するサービスの名前、およびポート使用における製品の目的を示します。「安全」列は、Prime Infrastructure の機能に影響を与えることなくポートとサービスを無効化できるかどうかを示します。

ベスト プラクティス：サーバー セキュリティの強化

表 *1 : Prime Infrastructure* の *TCP/UDP* ポート

[ポート（Port）]	サービス名（Service Name）	目的	安全?
21/tcp	FTP	デバイスとサーバの間のファイル転送	Y
22/tcp	SSHD	システムへ、またシステムからのSCP、SFTP、およびSSH接続で使用される	N
69/udp	TFTP	デバイスとサーバの間のファイル転送	Y
80/tcp	HTTP	Nexusデバイスのプロビジョニング	Y
162/udp	SNMP-TRAP	SNMPトラップを受信する	N
443/tcp	HTTPS	製品へのプライマリWebインターフェイス	N
514/udp	SYSLOG	Syslogメッセージを受信する	N
1522/tcp	Oracle	Oracle/JDBCデータベース接続：これらは内部サーバ接続とハイ アベイラビリティ ピア サーバとの接続の両方を含みます。	N
8082/tcp	HTTPS	ヘルス モニタリング	N
8087/tcp	HTTPS	HAセカンダリ システムのソフトウェア アップデート	N
9991/udp	NETFLOW	Netflowストリームを受信する（保証ライセンスがインストールされている場合に有効）	N
9992/tcp	PI Tomcatプロセス	保証内のLyncモニタリング	N
61617/tcp	JMS（over SSL）	リモートのプラグ アンド プレイ ゲートウェイ サーバーとの対話用	あり

ベスト プラクティス：サーバー セキュリティの強化

翻訳について
このドキュメントは、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。