拡張セキュリティ モードと FIPS モード用の CLI コマンド

- 拡張セキュリティ モード用の CLI コマンド，1 ページ
- FIPS モード用の CLI コマンド，2 ページ
- CLI とインターフェイス上でのユーザ アカウントとサインインの試行，4 ページ
- プラットフォーム ログのリモート監査ロギングの設定，5 ページ
- 拡張セキュリティ モードのセキュリティ用のプラットフォーム CLI コマンド，6 ページ

拡張セキュリティ モード用の CLI コマンド

拡張セキュリティ モードでは、次の CLI コマンドを使用します。

- **admin:utils EnhancedSecurityMode**
- **utils EnhancedSecurityMode disable**
- **utils EnhancedSecurityMode enable**
- **utils EnhancedSecurityMode status**

拡張セキュリティ モードの設定

管理者は、Cisco Prime Collaboration Deployment 上で次の手順を使用して拡張セキュリティ モードを設定できます。このモードが有効になっている場合は、次のシステム拡張機能が自動的に更新されます。

- パスワード変更に関するより厳密なクレデンシャル ポリシーが実装される
- TCP がリモート監査ロギング用のデフォルト プロトコルになる
- FIPS モードが有効になる

手順

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 2 **utils EnhancedSecurityMode status** コマンドを実行し、拡張セキュリティ モードが有効になっているかどうかを確認します。

ステップ 3 拡張セキュリティ モードを設定するには、ノード上で次のコマンドのいずれかを実行します。

- このモードを有効にするには、**utils EnhancedSecurityMode enable** コマンドを実行します。
- このモードを無効にするには、**utils EnhancedSecurityMode disable** コマンドを実行します。

FIPS モード用の CLI コマンド

Cisco Prime Collaboration Deployment 上の FIPS モードでは、次の CLI コマンドを使用します。

- **utils fips enable**：FIPS モードを有効にします。詳細については、FIPS モードの有効化, （2 ページ）の手順を参照してください。
- **utils fips disable**：FIPS モードを無効にします。詳細については、FIPS モードの無効化, （3 ページ）の手順を参照してください。
- **utils fips status**：サーバ上で FIPS モードが有効になっているか無効になっているかの詳細を提供します。

（注） ディザスタ リカバリ システム CLI コマンドは FIPS モードでサポートされます。これらのコマンドの詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html で『*Cisco Prime Collaboration Deployment Administration Guide*』の「CLI Commands and Disaster Recovery System」の章を参照してください。

FIPS モードの有効化

CLI 経由で FIPS モードを有効にできます。

注意 FIPS モードを有効にする前に、システムバックアップを実行することを強く推奨します。FIPS のチェックが起動時に失敗した場合は、システムが停止し、復元するにはリカバリ CD が必要になります。

手順

ステップ 1 CLI セッションを開始します。

ステップ 2 CLI で次のコマンドを入力します。 **utils fips enable**
次のプロンプトが表示されます。

```
admin:utils fips disable

Security Warning : The operation will regenerate certificates for

1)Tomcat
2)IPsec

Any third party CA signed certificates that have been uploaded for the
above
components will need to be re-uploaded.
******************************************************************************
This will change the system to FIPS mode and will reboot.
******************************************************************************

Do you want to continue (yes/no) ?
```

ステップ 3 yes と入力します。
次のメッセージが表示されます。

```
Generating certificates...Setting FIPS mode in operating system.
FIPS mode enabled successfully.
********************************************************
It is highly recommended that after your system restarts
that a system backup is performed.
********************************************************
The system will reboot in a few minutes.
```

Cisco Prime Collaboration Deployment が自動的にリブートします。

FIPS モードの無効化

次の手順を使用して、CLI 経由で FIPS モードを無効にできます。

手順

ステップ 1 CLI セッションを開始します。

ステップ 2 CLI で次のコマンドを入力します。 **utils fips disable**
次のプロンプトが表示されます。

```
admin:utils fips disable

Security Warning : The operation will regenerate certificates for

1)Tomcat
2)IPsec

Any third party CA signed certificates that have been uploaded for the
above
components will need to be re-uploaded.
**********************************************************************
This will change the system to NON-FIPS mode and will reboot.
**********************************************************************

Do you want to continue (yes/no) ?
```

ステップ 3 yes と入力します。
Cisco Prime Collaboration Deployment がリブートして、非 FIPS モードに戻ります。

（注） 証明書および SSH キーは、FIPS 要件に応じて、自動的に再生成されます。

CLI とインターフェイス上でのユーザ アカウントとサインインの試行

次の表に、ユーザが Cisco Prime Collaboration Deployment アプリケーションまたは CLI にサインインするシナリオとサインイン試行の結果を示します。

ユーザ サインイン シナリオ	サインイン試行の結果
有効なクレデンシャルを使用したサインイン	サインインが成功し、アプリケーションのホーム ページにアクセスできる
無効なクレデンシャルを使用したサインイン	サインインが失敗する
アプリケーション上での試行回数超過後のサインイン	試行が 3 回連続で失敗した場合にアカウントがロックされる
CLI 上での試行回数超過後のサインイン	ユーザが正しいパスワードを入力した場合でもアカウントがロックされているために CLI サインインが失敗する
ロックアウト期間経過後のアプリケーションへのサインイン	5 分間のロックアウト期間の後に、アプリケーションがサインインを許可する

ユーザ サインイン シナリオ	サインイン試行の結果
ロックアウト期間経過後のCLIへのサインイン	5 分間のロックアウト期間の後に、アカウントがロック解除され、CLI にサインインできるようになる
非活動が原因でアカウントがロックされた状態でのアプリケーションへのサインイン	セッションの非活動が原因でアカウントがロックされる
非活動が原因でアカウントがロックアウトされた後のアプリケーションへのサインインが解決される	サインインが成功する

プラットフォーム ログのリモート監査ロギングの設定

次のタスクを実行して、プラットフォーム監査ログ、リモート サポート ログ、および CSV ファイルに対するリモート監査ロギング サポートを追加します。この種のログには、FileBeat クライアントと Logstash サーバが使用されます。

はじめる前に

外部 Logstash サーバがセットアップされていることを確認します。

手順

ステップ 1 IP アドレス、ポート、ファイル タイプなどの外部 Logstash サーバの詳細で FileBeat クライアントを設定します。手順については、Logstash サーバ情報の設定, （5 ページ）を参照してください。

ステップ 2 リモート監査ロギングに対して Filebeat クライアントを有効にします。手順については、FileBeat クライアントの設定, （6 ページ）を参照してください。

Logstash サーバ情報の設定

次の手順を使用して、IP アドレス、ポート番号、ダウンロード可能なファイル タイプなどの外部 Logstash サーバ情報で FileBeat クライアントを設定します。

はじめる前に

外部 Logstash サーバがセットアップされていることを確認します。

手順

ステップ 1　コマンドライン インターフェイスにログインします。
ステップ 2　**utils FileBeat configure** コマンドを実行します。
ステップ 3　画面上の指示に従って、Logstash サーバの詳細を設定します。

FileBeat クライアントの設定

次の手順を使用して、Filebeat クライアントによるプラットフォーム監査ログ、リモート サポート ログ、および CSV ファイルのアップロードを有効または無効にします。

手順

ステップ 1　コマンドライン インターフェイスにログインします。
ステップ 2　**utils FileBeat status** コマンドを実行し、Filebeat クライアントが有効になっているかどうかを確認します。
ステップ 3　次のコマンドの 1 つを実行します。

- クライアントを有効にするには、**utils FileBeat enable** コマンドを実行します。
- クライアントを無効にするには、**utils FileBeat disable** コマンドを実行します。

ステップ 4　各ノードでこの手順を繰り返します。
（注）　これらのコマンドをすべてのノードで同時に実行しないでください。

拡張セキュリティ モードのセキュリティ用のプラットフォーム CLI コマンド

拡張セキュリティ モードを有効にすると、管理者は、不正アクセスを防止するために以下のオプションを制限できます。

- 監査ログの表示
- 監査ログのダウンロード
- 監査ログの削除
- 監査デーモンの有効化または無効化

管理者は、次のプラットフォーム CLI コマンドを実行することにより、上記オプションを制限できます。

- **file view activelog**<audit log file name>
- **file get activelog** <audit log file name>
- **file delete activelog**<audit log file name>
- **file dump activelog**<audit log file name>
- **file tail activelog** <audit log file name>
- **file search activelog**<audit log file name><search string>
- **file view inactivelog** <audit log file name>
- **file get inactivelog** <audit log file name>
- **file delete inactivelog** <audit log file name>
- **file dump inactivelog** <audit log file name>
- **file tail inactivelog** <audit log file name>
- **file search inactivelog** <audit log file name><search string>
- **utils auditd enable**
- **utils auditd disable**
- **utils auditd status**

ここで、<audit log file name> は以下の監査ログ ファイルのいずれかにすることができます。

- `/var/log/active/audit/AuditApp`
- `/var/log/active/audit/vos`
- `/var/log/inactive/audit/AuditApp`
- `/var/log/inactive/audit/vos`

（注） 非拡張セキュリティ モードでは、権限が 640 のときにグループ所有権が ccmsyslog になります。ただし、拡張セキュリティ モード要件の一部として、ファイル権限が、root がファイル グループ所有権を持つ 600 に変更されます。そのため、デフォルトで、`/var/log/active/syslog` の場所に保存されたファイルは、root が所有権を持つ 600 の権限に変更されます。