EnhancedSecurityMode および FIPS モード用の CLI コマンド

EnhancedSecurityMode の CLI コマンド

EnhancedSecurityMode には、次の CLI コマンドを使用します。

- **admin: ユーティリティ EnhancedSecurityMode**
- **utils EnhancedSecurityMode disable**
- **utils EnhancedSecurityMode enable**
- **utils EnhancedSecurityMode status**

EnhancedSecurityMode の設定

管理者は、Cisco Prime Collaboration の導入時にこの手順を使用して EnhancedSecurityMode を設定できます。このモードを有効にすると、次のシステム拡張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、強化されたセキュリティ モードが有効であ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、ノードで次のいずれかのコマンドを実行します。

- 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 展開では、FIPS モードで次の CLI コマンドを使用します。

- **ユーティリティ fips 有効化**: 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）を参照してください。
- **ユーティリティ 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）を参照してください。
- [ユーティリティ (ユーティリティ)] [**fips ステータス (fips status)**]: fips モードがサーバで有効か無効かを示します。

（注） ディザスタリカバリシステムの CLI コマンドは、FIPS モードでサポートされています。これらのコマンドの詳細については、にあるhttp://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html『 *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 を使用して FIPS モードを有効にすることができます。

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、を入力します。**utils fips enable**

次のプロンプトが表示されます。

```
admin: ユーティリティ fips enable セキュリティ警告: 操作によって1の証明書が再生成されます) tomcat 2) IPsec 上記のコンポーネント用にアップロードされたサードパーティの CA 署名付き証明書を再アップロードする必要があります。これにより、システムが FIPS モードに変更され、再起動します。
******************************************************************************
 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。

```
証明書を生成しています...オペレーティングシステムで FIPS モードを設定しています。FIPS mode enabled successfully. システムのバックアップが実行されると、システムを再起動した後に、これを強くお勧めします。システムは数分で再起動します。
```

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

FIPS モードの無効化

CLI を使用して FIPS モードを無効にするには、次の手順を実行します。

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、を入力します。**utils fips disable**

次のプロンプトが表示されます。

```
admin: ユーティリティの fips 無効化セキュリティ警告: 操作によって1の証明書が再生成されます) tomcat 2) IPsec 上記のコンポーネント用にアップロードされたサードパーティの CA 署名付き証明書を再アップロードする必要があります。これにより、システムが FIPS 以外のモードに変更され、再起動します。
******************************************************************************
 Do you want to continue (yes/no) ?
```

ステップ 3 **yes** と入力します。

Cisco Prime Collaboration 展開がリブートし、FIPS 以外のモードに復元されます。

（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 導入アプリケーションまたは CLI にサインインする場合のシナリオと、サインイン試行の結果を示します。

ユーザログインシナリオ	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可能
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
アプリケーションの試行回数を超過した後のサインイン	3回連続して失敗した場合、アカウントはロックされます
CLI での試行回数を超過した後のサインイン	ユーザが正しいパスワードを入力した場合でも、ロックされたアカウントが原因で CLI サインインが失敗する
ロックアウト期間が経過した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が経過すると、アプリケーションがサインインできるようになります。
ロックアウト期間が経過した後の CLI へのサインイン	5分間のロックアウト期間が経過すると、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ります。
非アクティブのためにアカウントがロックされた場合のアプリケーションへのサインイン	セッションが非アクティブになったため、アカウントがロックされました
非アクティブ状態が原因で発生したアカウントロックアウト後のアプリケーションへのサインインが解決された場合	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

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するには、次のタスクを実行します。これらのタイプのログでは、FileBeat クライアントと logstash サーバが使用されます。

始める前に

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Logstash サーバ情報の設定 （5 ページ）は、を参照してください。

ステップ 2 リモート監査ロギング用の 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 （5 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。

始める前に

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。

EnhancedSecurityMode でのセキュリティのためのプラットフォーム CLI コマンド

EnhancedSecurityMode が有効になっている場合、管理者は次のオプションを制限して不正アクセスを防止できます。

- 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
- 監査デーモンを有効または無効にします。

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で、上記の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 >**
- **ユーティリティ auditd 有効**
- **ユーティリティ auditd 無効化**
- **ユーティリティ auditd ステータス**

ここで、**< audit log file name >**には、次のいずれかの監査ログファイルを指定できます。

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

（注） 非 EnhancedSecurityMode では、権限が640の場合、グループ所有権は ccmsyslog になります。ただし、EnhancedSecurityMode 要件の一部として、ファイルの権限は、ルートによってファイルグループの所有権を持つ600に変更されます。したがって、デフォルトでは、/var/log/active/syslogの場所に保存されたファイルは、所有権が root になる600の権限に変更されます。

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。