監査およびログ

ユーザーによって行われる変更の監査（変更の監査）

Cisco EPN Manager では、以下の方法で、変更の監査データの管理がサポートされています。

変更監査通知の有効化および syslog レシーバの設定

必要に応じて、システムに変更が加えられると Cisco EPN Manager が変更監査通知を送信するように設定できます。これらの変更には、デバイス インベントリと設定の変更、設定テンプレートおよびモニタリングテンプレートの操作、ユーザー操作（ログイン、ログアウト、ユーザー アカウントの変更など）が含まれます。

次の動作を行うように Cisco EPN Manager を設定できます。

- 変更監査通知として変更を Java メッセージ サーバー（JMS）に転送する
- これらのメッセージを特定の syslog レシーバに送信する

syslog レシーバを設定しても syslog を受信しない場合は、宛先 syslog レシーバでのウイルス対策またはファイアウォールの設定を変更して、syslog メッセージの受信を許可するようにしなければならない可能性があります。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** の順に選択し、**[メールと通知（Mail and Notification）] > [監査通知の変更（Change Audit Notification）]** を選択します。

ステップ 2 [監査の変更通知の有効化（Enable Change Audit Notification）] チェックボックスをオンにして通知を有効にします。

ステップ 3 メッセージを特定の syslog レシーバに送信するには、次の手順に従います。

a) [追加（Add）] ボタン（+）をクリックして、Syslog レシーバを指定します。

b) [syslogレシーバ（Syslog Receiver）] 領域で、syslog レシーバの IP アドレス、プロトコル、およびポート番号を入力します。

さらに追加の syslog レシーバを指定するには、必要に応じてこの手順を繰り返します。

ステップ 4 [保存（Save）] をクリックします。

（注） レコードをセキュアな tls ログに反映するために Cisco EPN Manager サーバーの再起動をお勧めします。

監査の変更の詳細表示

ステップ 1 Cisco EPN Manager に管理者としてログインします。

ステップ 2 **[モニター（Monitor）] > [ツール（Tools）] > [変更監査ダッシュボード（Change Audit Dashboard）]** を選択します。

[変更監査ダッシュボード（Change Audit Dashboard）] に次の監査データが表示されます。

- デバイス管理
- ユーザー管理
- 設定テンプレートの管理（Configuration template management）
- デバイス コミュニティとクレデンシャルの変更
- デバイスのインベントリ変更（Inventory changes of devices）
- サービスディスカバリ
- アラーム、RESTConf
- ジョブ管理アシュアランス

[監査レポートの変更（Change Audit report）] と [監査の変更（Change Audit）] ダッシュボードには、ログインしている仮想ドメインに関係なく詳細が表示されます。

[変更監査ダッシュボード（Change Audit Dashboard）] 画面には、IP アドレス、監査の説明、ユーザー名、監査名、クライアントの IP アドレスなどの詳細とは別に、デバイス名も表示されます。[IP アドレス（IP Address）] フィールドの横にある [i] アイコンをクリックしてデバイス 360 の詳細を表示します。

（注） ルートユーザーとしてログインしている場合は、すべての監査変更を表示できます。非ルートユーザーとしてログインしている場合は、自分が実行した監査変更のみを表示できます。

OS ログをリモートシステムに転送する

EPNM によるリモートシステムへの OS CLI ログの転送や、ログレベルの設定を有効にするには、コンフィギュレーション モードで下記の logging コマンドを使用します。

（注） ログを転送するリモートシステムは 1 つだけ設定できます。

logging {ip-address | hostname} {loglevel level}

それぞれの説明は次のとおりです。

構文	説明
ip-address	ログを転送するリモートシステムの IP アドレス。最大 32 文字の英数字。
hostname	ログを転送するリモートシステムのホスト名。最大 32 文字の英数字。
loglevel	logging コマンドのログ レベルを設定するコマンド。
level	ログ メッセージを設定する希望のプライオリティ レベルの番号。プライオリティ レベルは以下のとおりです（キーワードの番号を入力）。 • 0 - emerg—Emergencies：システム使用不可 • 1 - alert—Alerts：ただちに処置が必要 • 2 - crit—Critical：重大な状態 • 3 - err—Error：エラー状態 • 4 - warn—Warning：警告状態 • 5 - notif—Notifications：正常ではあるが注意を要する状態

構文	説明
	• 6 - inform：（デフォルト）Informational（情報提供）メッセージ • 7 - debug：デバッグメッセージ

この機能をディセーブルにするには、このコマンドの no 形式を使用します。

このコマンドには **IP address** または **hostname** または **loglevel** キーワードが必要です。これらの引数を複数入力すると、エラーが発生します。

例 1：

```
ncs/admin(config)# logging 209.165.200.225
ncs/admin(config)#
```

例 2：

```
ncs/admin(config)# logging loglevel 0
ncs/admin(config)#
```

システム ログ

Cisco EPN Manager は、**[管理（Administration）]** > **[設定（Settings）]** > **[ロギング（Logging）]** を選択して制御される 3 つのクラスのログを提供しています。

ログの種類	説明	次を参照してください。
一般	システムでのアクションに関する情報を取得します。	一般的なシステム ログを表示して管理する （4 ページ）
Syslog	Cisco EPN Manager 監査ログを（syslog として）他の受信者に転送します。	Syslog としてのシステム監査ログの転送 （7 ページ）

一般的なシステム ログを表示して管理する

システム ログは、ローカル サーバーにダウンロード後に表示することができます。

特定のジョブのログを表示する

ステップ 1 **[管理（Administration）]** > **[ダッシュボード（Dashboards）]** > **[ジョブ ダッシュボード（Job Dashboard）]** を選択します。

ステップ 2 [ジョブ（Jobs）]ペインからジョブタイプを選択し、[ジョブ（Jobs）] ウィンドウからジョブインスタンス リンクをクリックします。

ステップ 3 [ジョブインスタンス（Job instance）] ウィンドウの左上にある [ログファイル（Log file）] を見つけ、[ダウンロード（Download）] をクリックします。

（注） 設定アーカイブソフトウェア、設定ロールバック、設定上書き、設定展開のジョブタイプのログのみをダウンロードできます。

ステップ 4 必要に応じてファイルを開くか保存します。

一般的なログ ファイルの設定とデフォルト サイズの調整

デフォルトでは、Cisco EPN Manager は、すべての管理対象デバイスで生成されたすべてのエラー、情報、およびトレース メッセージをログに記録します。

また、受信したすべての SNMP メッセージと Syslog もログに記録します。

これらの設定を調整して、デバッグ目的のログ レベルを変更することができます。

操作の目的：	**[管理（Administration）] > [設定（Settings）] > [ロギング（Logging）]** での操作：
ログのサイズ、保存するログの数、ファイル圧縮のオプションを変更する	ログ ファイルの設定を調整します。 （注） システムへの影響を避けるため、これらの設定は慎重に変更してください。 Log4j MaxBackupIndex ごとに、メインファイルが 1 つ存在し、バックアップファイルのセット数が伴います。たとえば、ログファイルの数が 3 に設定されている場合は、1 つのメインファイル（.log）と 3 つのバックアップファイル（.log.1、.log.2、.log.3）が存在します。 [ファイルの数（Number of files）] を以前に設定した値よりも小さい値に変更した場合、ログファイルの設定は新しく生成されたファイルにのみ適用されます。たとえば、設定済みの値が 5 の場合、ここで 2 に変更すると、設定は .log ファイル .log.1 および .log.2 にのみ適用されます。files.log.3、.log.4、および .log.5 に変更はありません。 **[圧縮（Zip）（Compression (Zip)）]** オプションを選択すると、ログファイルが圧縮され、プロセスの **`./logs/backup/[logging_module]`** フォルダにアーカイブされます。圧縮されたログファイルの保持は、次の基準に従います。 • [ストレージ（MB）（Storage (MB)）]：フォルダの最大サイズ（MB） • [日数（Number of Days）]：ログファイルの最大経過時間 いずれかの条件が満たされると、消去が開始されます。 必要に応じて、[外部ロケーションへのバックアップ（Backup to external location）] が有効になっている場合、クリーンアップ対象としてマークされたログファイルは、削除前に指定された外部リポジトリにコピーされます。

操作の目的：	**[管理（Administration）] > [設定（Settings）] > [ロギング（Logging）]** での操作：
特定のモジュールのログ レベルを変更する	[一般的なログ設定（General Log Settings）] で、ファイルと必要なレベルを選択して **[Save]** をクリックします。たとえば、[メッセージレベル（Message Level）] ドロップダウンリストから、現在のログ レベルとして次のいずれかを選択します。 • [エラー（Error）]：システム上のエラーログをキャプチャします。 • [情報（Information）]：システム上の情報ログをキャプチャします。 • [トレース（Trace）]：詳細情報をログに記録するために、システムで管理対象デバイスの問題を再現します。 • [デバッグ（Debug）]：システムのデバッグログをキャプチャします。 Cisco EPN Manager を再起動すると、ログレベルが [Error] にリセットされます。
トラブルシューティングの目的でログファイルをダウンロードする	[グローバル設定（Global Settings）] タブで **Download** をクリックします。

Syslog としてのシステム監査ログの転送

始める前に

Syslog としてシステム監査ログを転送するには、ユーザーが監査の変更通知を有効化して syslog レシーバを設定する必要があります。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [ロギング（Logging）]** の順に選択してから、[Syslog] タブを選択し、[Syslog設定（Syslog Settings）] を表示します。

ステップ 2 システム ログの収集および処理を有効にするために、[Syslog の有効化（Enable Syslog）] チェックボックスをオンにします。

ステップ 3 [Syslogホスト（Syslog Host）] フィールドに、宛先サーバーの IP アドレスを入力します。

ステップ 4 [Syslogファシリティ（Syslog Facility）] ドロップダウンリストから、ローカル用途のファシリティのうち、Syslog メッセージを送信するために使用するファシリティを選択します。このローカル用途のファシリティは予約されておらず、一般的な用途で使用可能です。

ステップ 5 [保存（Save）] をクリックします。

（注） 管理 CLI を使用してリモートサーバーへのシステムログ転送を有効にすると、ログは ade.log ファイルに登録されません。

監査ログ

Cisco EPN Manager は、`audit.log` の **[モニター（Monitor）]** > **[ツール（Tools）]** > **[監査ダッシュボードの変更（Change Audit Dashboard）]**の下に表示される情報をログに記録します。デフォルトでは、ロギングはイネーブルです。この情報は、メッセージレベルかログモジュールの変更に関係なく記録されます。

デバイス固有のロギング

Cisco EPN Manager では、特定のデバイスのデバッグモードで XDE およびインベントリログを保存できます。SSH CLI からロギングを有効または無効にすることができます。（Cisco EPN Manager サーバーとの SSH セッションを確立する を参照）。

デバイス固有のロギングの有効化

重要 XDE またはインベントリログのデバイス固有のロギングを有効にする前に、次のコマンドを実行して、グローバルログレベルが INFO に設定されていることを確認します。

```
/opt/CSCOlumos/bin/setLogLevel.sh logName INFO
```

logName：必要に応じて xde または inventory と入力します。

デバイス固有のロギングを有効にするには、次のコマンドを実行します。

```
/opt/CSCOlumos/bin/setDeviceLevelDebug.sh logName DEBUG deviceIP
```

ここで、

- *logName*：必要に応じて xde または inventory と入力します。インベントリログのデバイス固有のロギングを有効にすると、ifm_inventory ログのロギングも有効になります。
- *deviceIP*：ロギングをイネーブルにするデバイスの IP アドレスを指定します。同じコマンドで複数の IP アドレスをカンマで区切って指定できます。

指定されたデバイスに対してのみ、デバッグモードでインベントリまたは XDE のログを保存します。他のデバイスの場合、情報ログのみが保存されます。同期中に生成されるログファイルは *xde.log.**、*inventory.log.**、および *ifm_inventory.log.** です。

Cisco EPN Manager は、このコマンドを実行するたびに、ユーザーが指定した IP アドレスを使用して、以前に指定された IP アドレスを上書きします。

例

インベントリログの場合：

```
/opt/CSCOlumos/bin/setDeviceLevelDebug.sh inventory DEBUG 1.2.3.4,5.6.7.8
```

XDE ログの場合：

```
/opt/CSCOlumos/bin/setDeviceLevelDebug.sh xde DEBUG 1.2.3.4,5.6.7.8
```

デバイス固有のロギングが有効になっているデバイスのリストの表示

デバイス固有のロギングが有効になっているデバイスのリストを表示するには、次のコマンドを実行します。

```
/opt/CSCOlumos/bin/listDeviceLevelDebug.sh logName
```

logName：必要に応じて xde または inventory と入力します。

例

```
/opt/CSCOlumos/bin/listDeviceLevelDebug.sh inventory
```

デバイス固有のロギングの無効化

指定したログのデバイス固有のロギングを無効にするには、ログレベルを INFO に設定します。これにより、すべてのデバイスのデバイス固有のロギングが無効になります。

```
/opt/CSCOlumos/bin/setDeviceLevelDebug.sh logName INFO
```

logName：必要に応じて xde または inventory と入力します。

（注） 特定のデバイスに対してロギングを無効にすることはできません。

例

```
/opt/CSCOlumos/bin/setDeviceLevelDebug.sh inventory INFO
```

インベントリ検出プロセスのログ

inventory-discovery-process のログは、 `/opt/CSCOlumos/logs/inventory-discovery-process` で確認できます。

inventory-discovery-process のログレベルを変更するには、管理者 CLI で次のコマンドを入力します（Cisco EPN Manager サーバーとの SSH セッションを確立するを参照）。

- ログレベルを INFO に変更するには、次のコマンドを実行します。

  ```
  /opt/CSCOlumos/bin/setLogLevel.sh logName INFO inventory-discovery-process
  ```

- ログレベルを DEBUG に変更するには、次のコマンドを実行します。

```
/opt/CSCOlumos/bin/setLogLevel.sh logName DEBUG inventory-discovery-process
```

logName：必要に応じて XDE または Inventory と入力します。

外部ロケーションへのシステム ログの同期

ncs（Cisco EPN Manger ログ）および os ログをローカルまたは NFS ベースのリポジトリに同期するように設定できます。

ログをリポジトリに同期するには、次の手順を実行します。

始める前に

ログを同期するローカルまたは NFS ベースのリポジトリを作成します。この方法の詳細については、リポジトリのセットアップと管理を参照してください。

ステップ 1 Cisco EPN Manager サーバーとの CLI セッションを開きます。「CLI 経由の接続」を参照してください。

ステップ 2 コンフィギュレーション モードで次のコマンドを入力してシステムログを同期します。

- ncs ログを同期する場合：

```
logging sync-logs ncs repository repository-name
```

- os ログを同期する場合：

```
logging sync-logs os repository repository-name
```

repository-name は自身で設定したリポジトリです。

（注） 同期を無効にするには、代わりに configure terminal モードで次のコマンドを入力します。

- ncs ログの同期を無効にする場合：

```
no logging sync-logs ncs repository repository-name
```

- os ログの同期を無効にする場合：

```
no logging sync-logs os repository repository-name
```

ステップ 3 コンフィギュレーション モードを終了します。

```
exit
```

例

例 1

```
(config)# logging sync-logs ncs repository myrepository
```

```
(config)# logging sync-logs os repository myrepository
config# exit
```

例 2

```
(config)# no logging sync-logs ncs repository myrepository
(config)# no logging sync-logs os repository myrepository
config# exit
```

セキュリティ ログ

Cisco EPN Manager では、過去のアクティブな Web GUI または CLI セッションで、ルート ユーザーと admin および super-user ユーザー グループのメンバーが実行したセキュリティ関連アクションのログが保持されます。

ログに記録される情報には、イベントの説明、ユーザーがタスクを実行したクライアントの IP アドレス、およびタスクが実行された時刻が含まれます。次のイベントがログに記録されます。

- ユーザーのログイン
- ユーザーのログアウト
- ユーザーの作成
- ユーザーの追加
- ユーザーの削除
- ユーザーのロック
- ユーザーのロック解除
- Linux シェルの入力
- ユーザーの変更（メール、パスワード）

このログの詳細を表示するには、次のコマンドを入力します。このコマンドを使用するには、管理 CLI ユーザーとしてログインする必要があります。詳細については、Cisco EPN Manager サーバーとの SSH セッションを確立するを参照してください。

```
show logging security
```

Cisco EPN Manager は、セキュリティ関連アクションのログを常にローカルに保持します。

CLI からのイベント エントリにはプレフィックス「SYSTEM-CLI:」、Web インターフェイスからのエントリにはプレフィックス「SYSTEM-WEB:」が付いています。各イベント エントリの構造は JSON 形式に基づいており、JSON は有効です。

イベント CLI	• SYSTEM-CLI:SSH:LOGIN:FAILED:WRONG_PASSWORD • SYSTEM-CLI:SSH:LOGIN:FAILED:MAXIMUM_ATTEMPTS_REACHED

	• SYSTEM-CLI:SSH:LOGIN:SUCCESSFUL • SYSTEM-CLI:SSH:LOGOUT:SUCCESSFUL • SYSTEM-CLI:CONSOLE:LOGIN:WRONG_PASSWORD • SYSTEM-CLI:CONSOLE:LOGIN:SUCCESSFUL • SYSTEM-CLI:CONSOLE:LOGOUT:SUCCESSFUL • SYSTEM-CLI:USER:ADD • SYSTEM-CLI:USER:DELETE • SYSTEM-CLI:USER:GROUP • SYSTEM-CLI:USER:PASSWORD • SYSTEM-CLI:USER:PASSWORD:POLICY • SYSTEM-CLI:USER:ROLE • SYSTEM-CLI:USER:STATE:LOCK • SYSTEM-CLI:USER:STATE:UNLOCK • SYSTEM-CLI:USER:MAIL • SYSTEM-CLI:USER:OS:SHELL:ENTERED • SYSTEM-CLI:OS:SHELL:ENABLED • SYSTEM-CLI:OS:SHELL:DISABLED
イベント UI	• SYSTEM-WEB:UI:NCS:BODGE:LOGIN:SUCCESSFUL • SYSTEM-WEB:UI:LOGOUT • SYSTEM-WEB:UI:LOGIN:SUCCESSFUL • SYSTEM-WEB:UI:LOGIN:AUTHENTICATION_FAILED • SYSTEM-WEB:UI:USER:DELETE • SYSTEM-WEB:UI:USER:ADD • SYSTEM-WEB:UI:USER:STATE:UNLOCK • SYSTEM-WEB:UI:USER:STATE:LOCK • SYSTEM-WEB:UI:USER:UPDATE • SYSTEM-WEB:HM:LOGIN:AUTHENTICATION_FAILED

外部ロケーションへのセキュリティ ログの送信

リモートロギングがサポートされているため、セキュリティ関連のイベントをリモート syslog サーバーに転送するように設定できます。

ステップ 1 Cisco EPN Manager サーバーとの CLI セッションを開き、configure terminal モードを開始します。「CLI 経由の接続」を参照してください。

ステップ 2 次のコマンドを入力します。

```
logging security hostname[:port]
```

hostname はリモート ロギング ホスト サーバーの名前または IP アドレスです。

（注） このコマンドは、ポートが指定されていない場合、デフォルトで UDP ポート 514 にログを送信します。

ステップ 3 コンフィギュレーション モードを終了します。

```
exit
```

例

```
/admin(config)# logging security a.b.c.d
/admin(config)# exit
```

セキュリティイベントログ

Cisco EPN Manager は、次のイベントのログを security_events.log ファイルに保持します。

- 暗号プロトコルを介して作成または破棄されたセッション
- セキュリティ攻撃と考えられるもの

デフォルトでは、セキュリティ攻撃に関連するイベントはログに記録されます。暗号化セッションに関連する情報のロギングを有効にするには、ログレベルを **Info** に設定する必要があります。これを行うには、サーバーパスの /opt/CSCOlumos/bin の管理 CLI で次のコマンドを実行します。

```
./setLogLevel.sh SecurityEvents.crypto INFO
```

Event type	イベント	記録される情報
セキュリティ攻撃に関連するイベント	SQL インジェクションと LDAP インジェクション	入力検証エラー（データのソースには無関係）。ログに記録されるデータには、データが無効である理由が記載されています。
暗号化セッションに関連する情報	次のプロトコルを介して作成および破棄されたセッション。	• 通知の種類（Notification type） • ターゲットデバイス

Event type	イベント	記録される情報
	• raw • SSH2、Telnet • NETCONF • TL1	• 接続ポート • [ユーザー名（Username）] • 接続タイプ • セッションの詳細を

管理CLIで次のコマンドを入力して、ログの内容を表示できます。詳細については、Cisco EPN Manager サーバーとの SSH セッションを確立するを参照してください。

```
less /opt/CSCOlumos/logs/security_events.log
less /opt/CSCOlumos/logs/security_events.log.x
```

ここで、

- *x* は 1 以上の数になります（ローリング イベント ログファイルであるため）。

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。