監査およびログ

設定アーカイブとソフトウェア管理の変更を監査する（ネットワーク監査）

[ネットワーク監査（Network Audit）] [変更監査ダッシュボード（Change Audit Dashboard）] ウィンドウに、設定アーカイブとソフトウェア管理機能を使用して行われたデバイスへの変更が表示されます。これらの変更を表示するには、**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク監査（Network Audit）]** を選択します。Cisco EPN Managerによって、最新のデバイスの変更が変更のタイプ（設定アーカイブ、ソフトウェアイメージ管理）とともに一覧表示されます。例については、次を参照してください。

- 設定アーカイブ操作に関するネットワーク監査の確認
- ソフトウェア イメージ操作に関するネットワーク監査の確認

また、デバイスの 360 度ビューの [最新の変更（Recent Changes）] タブで、デバイスの最新の変更を表示することもできます。基本デバイス情報を取得する：[デバイス 360（Device 360）] ビューを参照してください。

ユーザ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。

変更監査レポートの生成

変更監査レポートには、ユーザが Cisco EPN Manager の機能を使用して実行したアクションのリストが表示されます。次の表に、変更監査レポートの表示内容の例を示します。

機能	例
デバイス管理	デバイス「209.165.202.159」が追加された
ユーザ管理	ユーザ「mmjones」が追加された
管理（Administration）	209.165.202.129 からのユーザ jlsmith のログアウトが成功 認証に失敗した209.165.202.125 からのユーザ fjclark のログインに失敗
コンフィギュレーションの変更	CLI コマンド：ip access-list standard testremark test
モニタリングポリシー	モニタリング テンプレート「IF Outbound Errors (Threshold)」が作成された
構成テンプレート	構成テンプレート「Add-Host-Name-IOS-Test」が作成された
ジョブ	[設定の展開 - 展開ビュー（Config Deploy - Deploy View）] タイプの「Show-Users-On-Device-IOS_1」ジョブがスケジュールされた
インベントリ	論理ファイル「/bootflash/tracelogs/inst_cleanup_R0-0.log.19999.20150126210302」が削除された

変更監査レポートを定期的に実行するようにスケジュールできます。また、必要に応じてCisco EPN Managerから結果を電子メールで送信することもできます。さらに、この情報を変更監査通知で転送することもできます（変更監査通知の有効化および syslog レシーバの設定 （3 ページ）を参照）。

ステップ 1 **[レポート（Reports）]** > **[レポート起動パッド（Report Launch Pad）]** を選択し、**[コンプライアンス（Compliance）]** > **[監査の変更（Change Audit）]** を選択します。

ステップ 2 [新規（New）] をクリックして新しいレポートを生成します。

ステップ 3 [設定（Settings）] エリアに、レポート条件（期間、レポートの開始時点など）を入力します。

ステップ 4 後で実行するようにレポートをスケジュールするには、[スケジュール（Schedule）]エリアに設定を入力します。また、レポートの送信先となる電子メール アドレスを指定することもできます。

ステップ 5 レポートをすぐに実行するには、ウィンドウの下部にある [実行（Run）] をクリックします。

[レポートの実行結果（Report Run Result）] に、すべてのユーザおよび指定された期間内に行われた変更がリストされます。

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、ユーザ操作（ログイン、ログアウト、ユーザ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（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（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）] に次の情報が表示されます。

- ネットワーク監査ログ（Network audit logs）
- 監査データの変更元（Change audit data from）：
  - デバイス管理
  - ユーザ管理
  - 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）

[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、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。

Cisco EPN Manager は、[変更監査ダッシュボード（Change Audit Dashboard）] のすべての詳細を `/opt/CSCOlumos/logs/audit.log` に記録します。詳細については、監査ログ （20 ページ）を参照してください。

GUI から実行されたアクションを監査する（システムの監査）

（注） Cisco EPN Manager は、すべての監査変更通知を XML 形式でトピック **ChangeAudit.All** に送信します。通知を受信するためには、**ChangeAudit.All** に登録する必要があります。

[システムの監査（System Audit）] ウィンドウに、ユーザがアクセスしたすべての Cisco EPN Manager GUI ページが一覧表示されます。[システムの監査（System Audit）] を表示するには、

[管理（Administration）] > **[設定（Settings）]** > **[システムの監査（System Audit）]** を選択します。

次の表に、クイック フィルタを使用して [システムの監査（System Audit）] ページで見つかる情報の一部を示します。クイック フィルタを有効にするには、[表示（Show）] ドロップダウン リストから [クイック フィルタ（Quick Filter）] を選択します。

実行されたアクションの検索対象：	次の手順を実行します。
特定のユーザ	[ユーザ名（Username）] クイック フィルタ フィールドにユーザ名を入力します。
ユーザ グループ内のすべてのユーザ	[ユーザ グループ（User Group）] クイック フィルタ フィールドにグループ名を入力します
特定の仮想ドメイン内のデバイス	[アクティブ仮想ドメイン（Active Virtual Domain）] クイック フィルタ フィールドに仮想ドメイン名を入力します。
Web GUI ルート ユーザ	[表示（Show）] ドロップダウン リストから、[ルート ユーザ ログ（Root User Logs）] を選択します。
特定のデバイス	[IP アドレス（IP Address）] クイック フィルタ フィールドに IP アドレスを入力します。
特定の日付	[監査時間（Audit Time）] クイック フィルタ フィールドに日付を入力します（*yyyy–mmm–dd* の形式）。

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 （6 ページ）
SNMP	管理対象デバイスとの対話を取得します。	SNMP トレースの有効化および SNMP ログ設定（レベル、サイズ）の調整 （19 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 （19 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（Job）] 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 インスタンスを選択します。

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（Logs）] フィールドを見つけ出して、[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。
メール ログ ファイル（Cisco Technical Center 宛てなど）	電子メール ID のカンマ区切りリストを入力し、**[Send]** をクリックします。

トラブルシューティングのためのログ ファイルのダウンロードとメール送信

（注） この手順では、ログ メッセージ レベルを [トレース（Trace）] に設定します。システム パフォーマンスに影響しないように、ログ メッセージ レベルを必ず元の設定に戻してください。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [ロギング（Logging）]** を選択し、[ログファイル設定（Log File Settings）] を選択します。

ステップ 2 後でリセットする必要があるため、[メッセージ レベル（Message Level）] ドロップダウンリストの設定をメモします。

ステップ 3 [ログモジュールの有効化（Enable Log Modules）] 領域で、目的の [ログモジュール（Log Modules）] を選択します。

ログモジュール	説明
AAA	このログモジュールは、ncs-0-0.log ファイル、nms_sys_error.log ファイル、usermgmt.log ファイル、およびXmpUserMgmtRbac.log ファイルを有効にします。ユーザがログインするとログが印刷されます。ローカル、TACACS、RADIUS、および SSO モードの変更など、 AAA モードの変更が実行されます。
アクセスワークフロー	このログモジュールは、ifm_access_workflow.log ファイルを有効にします。
アクションフレームワーク	このログモジュールは、nms-actions.log ファイルを有効にします。
Alertcache	このログモジュールは、alertcache.log ファイルと alertcache_error.log ファイルを有効にします。
APIC	このログモジュールは、PNP プロファイルが APIC と同期したときに発生するログをキャプチャする ifm_apic.log ファイルを有効にします。
APICPIIntegration	このログモジュールは、プロファイルがサイトとして APICEM で同期されたときにログをキャプチャする apic_pi_integration.log ファイルを有効にします。
AppNav	このログモジュールは、テンプレートに ACL 設定を保存し、テンプレートから ACL を削除し、WAAS インターフェイスを作成および更新するとき、およびサービスノードグループとコントローラグループを作成、更新、削除するときに、ログをキャプチャするために appNav.log ファイルを有効にします。
アシュアランス AppClassifier（Assurance AppClassifier）	このログモジュールは、着信 AVC/ワイヤレス NetFlow データでの NBAR 分類に関連する情報をキャプチャする assurance_appclassifier.log ファイルを有効にします。これは、Cisco EPN Manager での NetFlow 処理の一環として、フローレコードのアプリケーションの分類または識別を行うためのものです。
アシュアランス NetFlow（Assurance Netflow）	このログモジュールは、さまざまな NetFlow デバイスから Cisco EPN Manager へ送信する着信 NetFlow データの処理に関する情報をキャプチャする assurance_netflow.log ファイルを有効にします。UDP ポート 9991 で受信したフローエクスポートで実行された NetFlow 処理に関連する情報をログに記録します。

ログモジュール	説明
アシュアランス PfR（Assurance PfR）	このログモジュールは、PfRMonitoringプロセスに関連する情報をキャプチャする assurance_pfr.log ファイルを有効にします。
アシュアランス WirelessUser（Assurance WirelessUser）	このログモジュールは、WirelessUser ジョブを実行してユーザデータを読み取り、そのデータを WIRELESS_ASSURANCE トリガーによって追加されたメモリキャッシュに挿入したときの情報をキャプチャする assurance_wirelessuser.log ファイルを有効にします。
アシュアランス WSA（Assurance WSA）	このログモジュールは、WLC がデバイスから Cisco EPN Manager へのデータを処理している間に情報をキャプチャする wsa_collector.log、access_log、assurance_wsa.log、および error_log の各ファイルを有効にします。ログは、ワイヤレスコントローラのデータ収集の一環として生成されます。
AVC ユーティリティ（AVC Utilities）	このログモジュールは、aems_avc_utils.log ファイルを有効にします。AVC設定機能に固有のユーティリティフローのログは、このコンポーネントの一部として生成されます。
CIDS デバイスのログ（CIDS Device Logs）	このログモジュールは、XDEに移行されないデバイスのデバイスパック操作に関連する情報をキャプチャします。
回線/VCトレース	このログモジュールは、nms-multilayer.log ファイルを有効にします。
cluster_core	このログモジュールは、cluster.core.log ファイルを有効にします。
収集	このログモジュールは、デバイスの準備状況を確認するために起動されるダッシュレットの情報をキャプチャします。
共通ヘルパー（Common Helper）	このログモジュールは、XMP共通の関連情報をキャプチャします。
コンプライアンス	このログモジュールは、ifm_compliance.log ファイルを有効にします。
設定（Configuration）	このログモジュールは、CLI、複合、MBC などのテンプレートがデバイスに展開されている場合に、ifm_config.log ファイルを有効にします。サービスビ

ログモジュール	説明
	ジネスロジックの実行デバッグログがキャプチャされます。
設定アーカイブ（Configuration Archive）	このログモジュールは、ifm_config_archive.log ファイルと ifm_config_archive_core.log ファイルを有効にします。ログはGUIで選択されたログレベルに基づいてキャプチャされ、設定アーカイブの収集、設定アーカイブの上書き、設定アーカイブのロールバック、設定アーカイブの展開など、設定アーカイブモジュールがサポートするすべての動作に対してログが記録されます。
設定アーカイブコア（Configuration Archive Core）	このログモジュールは、設定アーカイブの収集、設定アーカイブの上書き、設定アーカイブのロールバック、設定アーカイブの展開のような操作の実行中にサービスレイヤとデバイスパック間でのやり取りでの情報をキャプチャする ifm_config_archive_core.log ファイルを有効にします。
設定テンプレート	このログモジュールは、ifm_config.log ファイルと ifm_template.log ファイルを有効にします。これらのファイルは、システムテンプレート、複合テンプレート、または機能テンプレートがデバイスに展開され、展開ジョブが作成されたときにログに記録されます。GUI で選択したログレベル（INFO、ERROR、TRACE）に基づいてログがキャプチャされ、デバイスに展開された設定テンプレートに対してログが記録されます。
コンテナ管理（Container Management）	このログモジュールは、ifm_container.log ファイルのログを有効にします。このファイルは、コンテナ管理が仮想アプライアンスのライフサイクル操作（インストール、アクティブ化、アンインストール、および非アクティブ化）を実行するときにログに記録されます。
クレデンシャル管理	このログモジュールは、NMS_SysOut.log ファイルからのログを有効にします。
クレデンシャルプロファイル（Credential Profile）	このログモジュールは、プロファイルの作成、削除、およびプロファイル更新の情報をキャプチャする ifm_credential_profile.log ファイルを有効にします。

ログモジュール	説明
DA	このログモジュールは、ifm_da.log ファイルと da_daemon.log ファイルを有効にし、SNMP ポーリング、NAM ポーリング、パケットキャプチャのワークフローなどの情報をキャプチャします。
データベース	このログモジュールは、rman.log ファイルと db_migration.log ファイルを有効にします。
データセンター	このログモジュールは、datacenterevent.log ファイルと ifm_datacenter.log ファイルを有効にします。デバイス（検索ソース、UCS、Nexus）の追加、編集、および削除すると同時に、これらのファイルにはデバッグ情報が含まれています。また、インベントリ モジュールのログには、データセンターのデバイスに関するデバッグ情報も含まれています。
デバイス クレデンシャルの検証	このログモジュールは、XDE.log ファイルを有効にします。
検出	このログモジュールは、ディスカバリ設定またはディスカバリジョブの作成、編集、および削除とディスカバリジョブの実行中にログをキャプチャする ifm_discovery.log ファイルと existenceDiscovery.log ファイルを有効にします。
分散キャッシュ	このログモジュールは、distributed-cache.log ファイルを有効にします。
DSM	このログモジュールは、仮想インベントリ ディスカバリ ソース マネージャに関連する情報をキャプチャします。
ems_assurance	このログモジュールは、ems-assurance.log ファイルを有効にします。
epnm_lcm	このログモジュールは、Life Cycle Manager（LCM）コンポーネントで使用される epnm-lcm.log ファイルを有効にします。
epnm_mcn	このログモジュールは、Model Changes Notifier（MCN）コンポーネントで使用される epnm-mcn.log ファイルを有効にします。
epnm_remote	このログモジュールは、epnm-remote.log ファイルを有効にします。

ログモジュール	説明
イベント処理	このログモジュールは、assurance_fault_error.log ファイルと assurance_fault.log ファイルを有効にします。
Fault Management	このログモジュールは、ifm_fault.log、xmp_correlation.log、および xmp_syslog.log の各ファイルを有効にします。
障害（Fault）	このログモジュールは、ifm_fault.log、xmp_correlation.log、および xmp_syslog.log の各ファイルを有効にします。
ファイアウォールと AVC の設定（Firewall and AVC Configuration）	このログモジュールは、AVC、ZBFW、QoS、および NAT 設定の詳細をキャプチャする aems_config.log ファイルを有効にします。
ファイアウォールと AVC のインベントリ（Firewall and AVC Inventory）	このログモジュールは、AVC、ZBFW、QoS、および NAT の設定を読み取ったデバイスインベントリ時間をキャプチャする aems_zbfw_ice_post_processors.log ファイルを有効にします。
ファイアウォールと AVC の REST API（Firewall and AVC REST API）	このモジュールは、AVC、ZBFW、QoS、NAT、および PPM の機能の REST API コールの詳細をキャプチャする aems_config_access_layer.log ファイルを有効にします。
ファイアウォールと AVC のユーティリティ（Firewall and AVC Utilities）	このログモジュールは、AVC/ZBFW/QoS、NAT、および PPM の機能で共通のユーティリティコールをキャプチャする aems_utils.log ファイルを有効にします。
ファイアウォールのユーティリティ（Firewall Utilities）	このログモジュールは、ZBFW ユーティリティコールをキャプチャする aems_zbfw_utils.log ファイルを有効にします。
一般	このログモジュールは、ifm_common.log ファイルを有効にします。
Geo サーバ	このログモジュールは、nms-geoserver.log ファイルを有効にします。
グループ化	このログモジュールは、ifm_grouping.log ファイルと grouping-spring.log ファイルを有効にします。グループの追加、編集、削除、ならびにメンバーの追加および削除の間にデータをキャプチャします。また、CSV 形式でグループをインポートまたはエクスポー

ログモジュール	説明
	トしたり、ポートグループの作成、編集、およびポートグループの削除のときにもログをキャプチャします。
IFMCommon	このログモジュールは、ifm_common.log ファイルと ifm_common_helper.log ファイルを有効にします。
インベントリ	このログモジュールは、inventory.log、ifm_inventory.log、existenceInventory.log、および xde.log の各ファイルを有効にします。デバイスを追加、編集、および削除し、インベントリ収集を実行しているときに、データをキャプチャします。
キー証明書の管理	このログモジュールは、key_admin_web.log ファイルを有効にします。
MBC UI フレームワーク	このログモジュールは、mbcui_fw.log ファイルを有効にします。
Mobility	このログモジュールは、サーバに追加されたモビリティアンカーデバイスに関連する情報をキャプチャします。
モニタ（Monitor）	このログモジュールは、上位Nのメモリと上位NのCPUなどのモニタダッシュレットの起動中に表示される API に関連する情報をキャプチャします。
MSAP（MSAP）	このログモジュールは、ncs.logファイルを有効にします。これは、プロキシ設定やBBX設定などのMSEハイアベイラビリティのアクションに関連するデータをキャプチャします。
MSE	このログモジュールは、ncs.logファイルを有効にします。MSE の追加、編集、および削除と、SiteMap と MSE の同期などのモビリティサービスエンジンに関連するデータをキャプチャします。
NBIFW	このログモジュールでは、NBI API フレームワークのログレベルを変更できます。この情報は、xmpNbiFw.log ファイルに表示できます。
ncs_nbi	このログモジュールでは、統計情報NBIサービスのログレベルを変更できます。ncs_nbi.log ファイルで情報を閲覧することができます。

ログモジュール	説明
ネットワークテクノロジーオーバーレイ	このログモジュールは、technology-overlay.log ファイルと synce-technology-overlay.log ファイルを有効にします。
ネットワーク テクノロジー オーバーレイ プロバイダー	このログモジュールは、technology-overlay.log ファイルを有効にします。
ネットワーク トポロジ（Network Topology）	このログモジュールは、nms-topology.log ファイルおよび xmptopology.log ファイルを有効にします。このログモジュールは、[マップ（Maps）]>[ネットワークトポロジ（Network Topology）] ページに関連するログをキャプチャします。デバイス間のリンクの追加や削除などの情報がキャプチャされます。
NFVOS	このログモジュールは、esa dna 統合プロセスを追跡するために使用されます。
Nice	このログモジュールは、デバイスを追加した後に、トポロジ関連の情報をキャプチャします。
NMS アシュアランス永続性ロガー	このログモジュールは、nms-assurance-persistence.log ファイルを有効にします。
NMS 共通トレース	このログモジュールは、nms-common.log ファイルを有効にします。
nms_assurance	このログモジュールは、nms-assurance.log ファイルを有効にします。
通知	このログモジュールは、ncs-0-0.log、ncs_nb.log、および alarm_notification_policy.log の各ファイルからの情報をキャプチャします。
Optical	このログモジュールは、nms-optical.log、nms-optical-fault.log、 nms-optical-event.log、および nms-optical-cerberus.log ファイルを有効にします。
PA	このログモジュールは、ifm_sam.log ファイルと sam_daemon.log ファイルを有効にします。アプリケーションやサービスなどの情報、ダッシュボードやダッシュレットサービスの API コール、NAM 設定、NAM ポーリング、およびパケットキャプチャ機能のワークフローがキャプチャされます。
参加回線サービス	このログモジュールは、nms-paticipating-circuit.log ファイルを有効にします。

ログモジュール	説明
Ping	このログモジュールは、ネットワークデバイスのポーリング間隔ジョブに関連する情報をキャプチャします。ジョブが完了すると、システム内の各デバイスは ping を受信します。
PKI	このログモジュールは、pki.log ファイルを有効にします。
プラグ アンド プレイ	このモジュールを有効にすると、PNP プロファイルの作成およびプロビジョニング、ブートストラップの初期設定、APIC EM の同期のタイムフレームに関連する情報をキャプチャできます。これらのログは、ifm_pnp.log ファイルと ifm_apic.log ファイルにキャプチャされます。
pnpgateway	このログモジュールは、pnp_gateway_cns.log、pnp_gateway_image.log、および pnp_gateway.log ファイルを有効にします。
プロトコルパック管理（Protocol Pack Management）	このモジュールは、aems_ppm_service.log、ifm_container.log、jobManager.log、および ifm_jobscheduler.log の各ファイルを有効にします。これにより、プロトコルパックのインポート、プロトコルパックの配布、およびジョブの詳細に関連する情報がログに記録されます。
レポート	このモジュールを有効にすると、レポートに関連するクエリ、メモリ消費量、およびレポート生成のタイムフレームを表示できます。
REST サービス	このログモジュールは、nms-rest-service.log ファイルを有効にします。
RTTS	このログモジュールは、ifm_RTTS.log ファイルを有効にします。
サービス ディスカバリ	このログモジュールは、サービスで使用される nms-service-discovery.log ファイルと nms-service-discovery-distributed.log ファイルを有効にします。
サービス履歴	このログモジュールは、nms-service-history.log ファイルを有効にします。

ログモジュール	説明
サービスへの影響の分析	このログモジュールは、障害が発生したサービス影響分析機能で使用される sia.log ファイルを有効にします。
サービスマルチレイヤ	このログモジュールは、nms-service-multilayer.log ファイルを有効にします。
サービスプロビジョニング UI	このログモジュールは、provisioning-ui.log ファイルを有効にします。
スマート ライセンス	このログモジュールは、ifm_smartagent.log ファイルと smart_call_home.log ファイルを有効にします。ifm_smartagent.log ファイルにはスマートライセンシングに関連するライセンスのログが含まれており、smart_call_home.log にはCSSM（Cisco Smart Software Manager）に送信された情報をキャプチャする Call Home のログが含まれています。これらのログは、定期的なイベントとユーザアクションベースのイベントでキャプチャされます。
SNMP	このログモジュールは、snmp.log ファイルと mibLibrary.log ファイルを有効にします。
特定の	このログモジュールは、ifm_app.log ファイルを有効にします。
SWIM	このモジュールを有効にすると、ifm_swim.log ファイルにソフトウェアイメージ管理モジュールのログを記録できます。これらのログは、GUI で選択されているログレベルに従ってキャプチャされます。ソフトウェアイメージの推奨事項、ソフトウェアイメージのアップグレード分析、ソフトウェアイメージのインポート、ソフトウェアイメージのアクティブ化、およびソフトウェアイメージのコミットのようなソフトウェアイメージの管理操作に関連する情報をログに記録します。
システム（System）	このログモジュールは、jobManager.log、lockManager.log、preference.log、grouping-spring.log、updates.log、poller.log、xmptopology.log、audit.log、connmanager.log、dpl_rest.log、datacenterevent.log、xmp-syslog.log、および webcontainer_filters.log ファイルを有効にします。
System Monitoring	このログモジュールは、ifm_sysmon.log ファイルを有効にします。これにより、ルールの開始時刻およ

ログモジュール	説明
	び終了時刻とともに、その間に実行された操作に関する情報がログに記録されます。
テクノロジーコレクション	このログモジュールは、technology_collection.log ファイルを有効にします。
ThreadManager	このログモジュールは、hybernate 関連情報をキャプチャする xmp _threadmanager.log ファイルを有効にします。
しきい値（Threshold）	このモジュールを有効にすると、しきい値モニタによって処理されるイベントの詳細を表示できます。
TrustSec	このモジュールを有効にすると、TrustSec 準備状況デバイス、適用可能なデバイス、デバイス分類、および対応デバイスの情報をキャプチャできます。このリストは、サービス TrustSec の準備状況で表示されます。ログは ifm_trustsec.log ファイルに表示できます。
WLAN AVC 設定（WLAN AVC Configuration）	このログモジュールは、aems_config_wlan.log ファイルを有効にして、WLAN設定のワークフロー関連情報を表示します。
XDE	このログモジュールは、xde.log ファイルを有効にします。
XMLMED	このモジュールを有効にすると、SOAP 要求と応答をキャプチャできます。これらのログは、ncs.log ファイルにも表示できます。

ステップ 4 [メッセージ レベル（Message Level）] ドロップダウンリストから [トレース（Trace）] を選択します。

ステップ 5 **[保存（Save）]** をクリックします。

ステップ 6 詳細情報をログに記録するため、システムで問題を再現します。

ステップ 7 [ログ ファイルのダウンロード（Download Log File）] エリアで、[ダウンロード（Download）] をクリックします。ダウンロード zip ファイルの名前は次のようになります。

NCS-*hostname*-logs-*yy-mm-dd-hh-mm-ss*。

このファイルには、zip ファイルに含まれているすべてのファイルをリストした HTML ファイルがあります。

ifm_da.log ファイルと ifm_sam.log ファイルでキャプチャされた情報は、付属するクラスに分割されるようになりました。

- assurance_wirelessuser.log

- assurance_pfr.log
- assurance_netflow.log
- assurance_appclassifier.log

ifm_da.log ファイルには、Cisco EPN Manager に Netflow デバイスが追加された後、デバイスとそれぞれの pcap に関連する情報が記録されます。assurance_wirelessuser.log ファイルには、WirelessUser ジョブを実行し、ユーザ データを読み取って WIRELESS_ASSURANCE によって追加されたメモリ キャッシュに格納する際に取得した情報が記録されます。assurance_pfr.log ファイルには、PfR モニタリング関連の情報が格納されます。assurance_netflow.log ファイルには、さまざまな Netflow デバイスから Cisco EPN Manager に送信された着信 Netflow データの処理が記録されます。assurance_appclassifier.log ファイルには、着信 AVC/ワイヤレス NetFlow データでの NBAR 分類に関するログが格納されます。

ステップ 8 [電子メールでログ ファイルを送信（E-Mail Log File）] エリアで、電子メール ID をカンマで区切ったリストを入力します。

ステップ 9 [メッセージ レベル（Message Level）] ドロップダウンリストで元の設定に戻します。

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 ロギングオプション（Syslog Logging Options）]** 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、メッセージ送信先の宛先サーバの 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、8 つの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。

SNMP トレースの有効化および SNMP ログ設定（レベル、サイズ）の調整

SNMP トレースを有効にし、SNMP によって送受信されるパケットに関する詳細情報にアクセスします。これは、トラップのドロップ時など、トラブルシューティングの際に必要になることがあります。

次の変更を行うには、**[管理（Administration）]** > **[設定（Settings）]** > **[ロギング（Logging）]** を選択してから、**[SNMP ログ（SNMP Log）]** タブを選択します。

目的	次の手順を実行します。
特定のデバイスでの SNMP トレースの有効化	[SNMP ログ設定（SNMP Log Settings）] 領域で、次のようにします。 **1.** [SNMP トレースの有効化（Enable SNMP Trace）] チェックボックスと [値の表示（Display Values）] チェックボックスをオンにします。 **2.** トレースするデバイスの IP アドレスまたは DNS アドレス、あるいはその両方を入力し、[保存（Save）] をクリックします。
ログのサイズと保存されるログ番号の変更	[SNMP ログ ファイル設定（SNMP Log File Settings）] 領域で、次のようにします。 （注） これらの設定を変更するときは、（非常に多くのデータを保存するなどして）システム パフォーマンスに影響を与えないように注意してください。 **1.** ファイルの最大数とファイル サイズを調整します。 **2.** Cisco EPN Manager を再起動して、変更内容を有効にします。Cisco EPN Manager の停止と再起動 を参照してください。

監査ログ

Cisco EPN Manager は、`audit.log` の **[モニタ（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。

`audit.log` を表示するには、管理者 CLI で `/opt/CSCOlumos/logs/audit.log` に移動します（Cisco EPN Manager サーバとの SSH セッションの確立を参照）。

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 サーバとの SSH セッションの確立 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 サーバとの SSH セッションの確立を参照）。

- 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

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 ユーザと admin および super-user ユーザ 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。

- ユーザのログイン
- ユーザのログアウト
- ユーザの作成

- ユーザの追加
- ユーザの削除
- ユーザのロック
- ユーザのロック解除
- Linux シェルの入力
- ユーザの変更（メール、パスワード）

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。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 サーバとの SSH セッションの確立を参照してください。

```
show logging security
```

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 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	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に関する情報が含まれています。
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。 • raw • SSH2、Telnet • NETCONF • TL1	• 通知の種類（Notification type） • ターゲットデバイス • 接続ポート • [ユーザ名（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 サーバとの SSH セッションの確立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）。