CHAPTER 15

管理、ロギング、およびトラブルシューティング

この章では、次の内容について説明します。

SNMP の設定

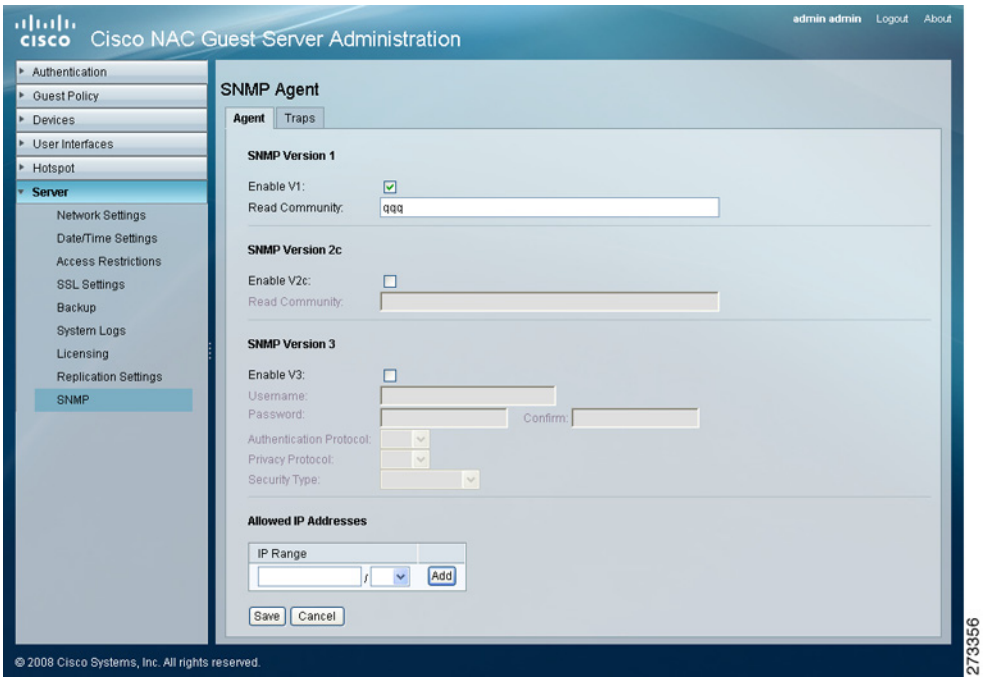
Cisco NAC ゲスト サーバでは、SNMP（簡易ネットワーク管理プロトコル）を介してシステムを監視する管理アプリケーションがサポートされます。SNMP バージョン 1、2c、および 3 がサポートされます。

アプライアンスでは、特定の設定が定義済みの値を超えたときに SNMP トラップを送信して通知することもできます。

SNMP Agent の設定

管理インターフェイスから、[Server] >[SNMP] を選択します（図 15-1 を参照）。

図 15-1　SNMP の設定



次のオプションを設定できます。

- SNMP バージョン 1 の設定
- SNMP バージョン 2c の設定
- SNMP バージョン 3 の設定
- SNMP 許可アドレスの設定

SNMP バージョン 1 の設定

ステップ 1　SNMP バージョン 1 をイネーブルにするには、[Enable V1] チェックボックスをオンにします。

ステップ 2　[Read Community] に読み取りアクセスに使用する SNMP 読み取りコミュニティ名を入力します。

ステップ 3　「SNMP 許可アドレスの設定」（P.15-3）の手順に従って、SNMP を使用したアプライアンスへのアクセスを許可する許可 IP アドレスを設定します。

ステップ 4　[Save] をクリックします。

SNMP バージョン 2c の設定

ステップ 1　SNMP バージョン 2c をイネーブルにするには、[Enable V2c] チェックボックスをオンにします。

ステップ 2　[Read Community] に読み取りアクセスに使用する SNMP 読み取りコミュニティ名を入力します。

ステップ 3　「SNMP 許可アドレスの設定」（P.15-3）の手順に従って、SNMP を使用したアプライアンスへのアクセスを許可する許可 IP アドレスを設定します。

ステップ 4　[Save] をクリックします。

SNMP バージョン 3 の設定

ステップ 1　SNMP バージョン 3 をイネーブルにするには、[Enable V3] チェックボックスをオンにします。

ステップ 2　[Username] に、読み取りアクセスに使用するユーザ名を入力します。

ステップ 3　[Password] に、パスワードを入力し正しく入力したことを確認するためにもう一度入力します。

ステップ 4　ドロップダウン メニューから認証プロトコル [MD5]（HMAC-MD5-96）または [SHA]（HMAC-SHA-96）を選択します。

ステップ 5　ドロップダウン メニューからプライバシー プロトコル（DES または AES）を選択します。

ステップ 6　ドロップダウン メニューからセキュリティ タイプ（[Authentication] または [Encryption]）を選択します。

ステップ 7　「SNMP 許可アドレスの設定」（P.15-3）の手順に従って、SNMP を使用したアプライアンスへのアクセスを許可する許可 IP アドレスを設定します。

ステップ 8　[Save] をクリックします。

SNMP 許可アドレスの設定

ステップ 1　IP アドレスとプレフィックス長からなる IP アドレス範囲を入力します。例：

- SNMP によるアプライアンスへのアクセスをすべてのアドレスに許可する場合は、「0.0.0.0/0」と入力します。
- アプライアンスへのアクセスを 192.168.1.0 ～ 255 の範囲の任意のアドレスに許可する場合は、「192.168.1.0/24」と入力します。
- アプライアンスへのアクセスを 172.16.45.2 のホストだけを許可する場合は、「172.16.45.2/32」と入力します。

ステップ 2　[Add] ボタンをクリックします。

ステップ 3　任意の数のアドレスについて、ステップ 1 およびステップ 2 を繰り返すことができます。

ステップ 4　[Save] をクリックします。

SNMP トラップ サポート

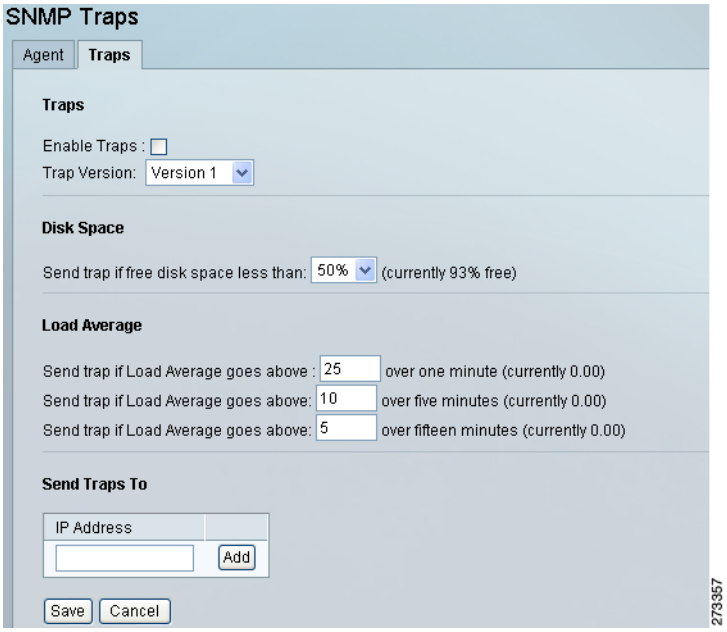
NAC ゲスト サーバは、特定のシステム イベントに基づいて SNMP マネージャーに SNMP トラップを送信するように設定できます。

SNMP トラップの設定

（注）　SNMP トラップは、「トラップ」に設定されているコミュニティ ストリング付きで送信されます。Cisco NAC ゲスト サーバは、認証/ウォームスタート トラップをサポートしていません。

ステップ 1　管理インターフェイスから、[Server] > [SNMP] > [Traps] を選択します（図 15-2 を参照）。

図 15-2　SNMP トラップの設定



ステップ 2　トラップをイネーブルにする場合は、[Enable Traps] チェックボックスをオンにします。

ステップ 3　ドロップダウンからトラップ バージョン（[Version 1]、[Version 2c]、または [Informs]）を選択します。

ステップ 4　ディスク スペースが指定された値を下回ると、NAC ゲスト サーバによってトラップが送信されます。[Disk Space] ドロップダウン フィールドに、トラップ送信の値を入力します。

ステップ 5　トラップ送信の値となる負荷平均値を指定します。負荷平均が 1 分間、5 分間、または 15 分間にわたって値を超えると、トラップが送信されます。負荷平均は標準の Linux 式を使用して計算されます。**uptime** コマンドを使用すると、コマンド ラインから負荷平均を確認できます。

ステップ 6　SNMP トラップを送信する各 IP アドレスを入力し、[Add] ボタンをクリックします。

ステップ 7　[Save] ボタンをクリックして変更を保存します。

SNMP MIB ファイル

NAC ゲスト サーバがサポートする MIB は、/usr/share/snmp/mibs にあります。MIB ファイルを取得するには、ゲスト サーバへの SFTP 接続を使用する必要があります。Windows プラットフォームの場合、http://winscp.net から無償の SFTP クライアントを入手できます。

ステップ 1　Cisco NAC ゲスト サーバへの SFTP 接続を開きます。認証のクレデンシャルはコマンドラインと同じです。root ユーザ名と初期セットアップでこのアカウントに割り当てたパスワードを使用してログインします。

ステップ 2　**/usr/share/snmp/mibs** ディレクトリに移動し、ファイルをダウンロードします。

システム ロギング

Cisco NAC ゲスト サーバ内のすべての処理は、データベースにロギングされます。これにより、次の操作が可能になります。

- アプリケーションの正常な操作プロセスの一部として発生したすべての処理を確認する
- 管理者およびスポンサーの処理をログに記録する
- システム ログを作成する

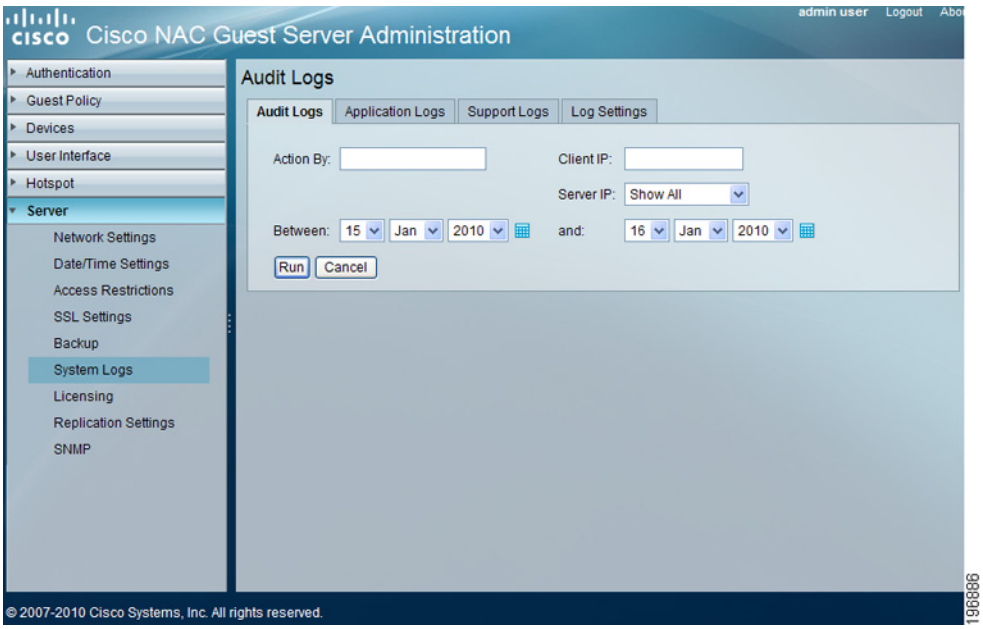
（注）　ロギング レベルを作成して常に保守することが重要です。詳細については、「ログ設定」（P.15-9）を参照してください。

監査ログ

監査ログには管理者およびスポンサーの処理が記録されます。監査ログは次の 4 つの方法で作成できます。

ステップ 1　管理インターフェイスから監査ログ機能にアクセスするには、[Server] > [System Logs] を選択し（図 15-3 を参照）、[Audit Logs] タブをクリックします。

図 15-3　システム ログ



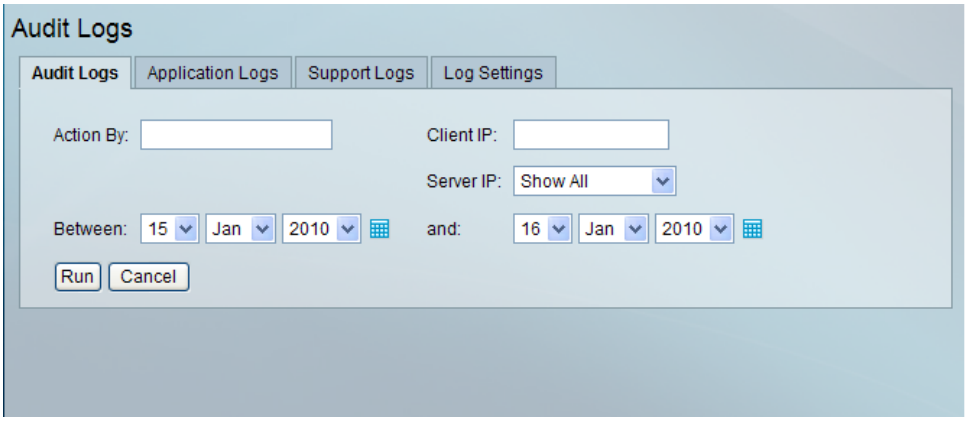
ステップ 2　監査ログ レポートは、4 つのカテゴリを使用して実行できます（図 15-4 を参照）。

- [Action by]：管理者およびスポンサーのユーザ名を検索条件として使用してログを表示します。
- [Client IP]：クライアント IP アドレスを検索条件として使用してログを表示します。
- [Server IP]：サーバ IP を検索条件として使用してログを表示します。

ログ レポートは、1 つのカテゴリ、複数のカテゴリ、またはすべてのカテゴリについて同時に実行できます。

ステップ 3　画面上の日付選択カレンダーを使用して検索条件の期間を選択し、[Run] ボタンをクリックします。

図 15-4　監査ログ

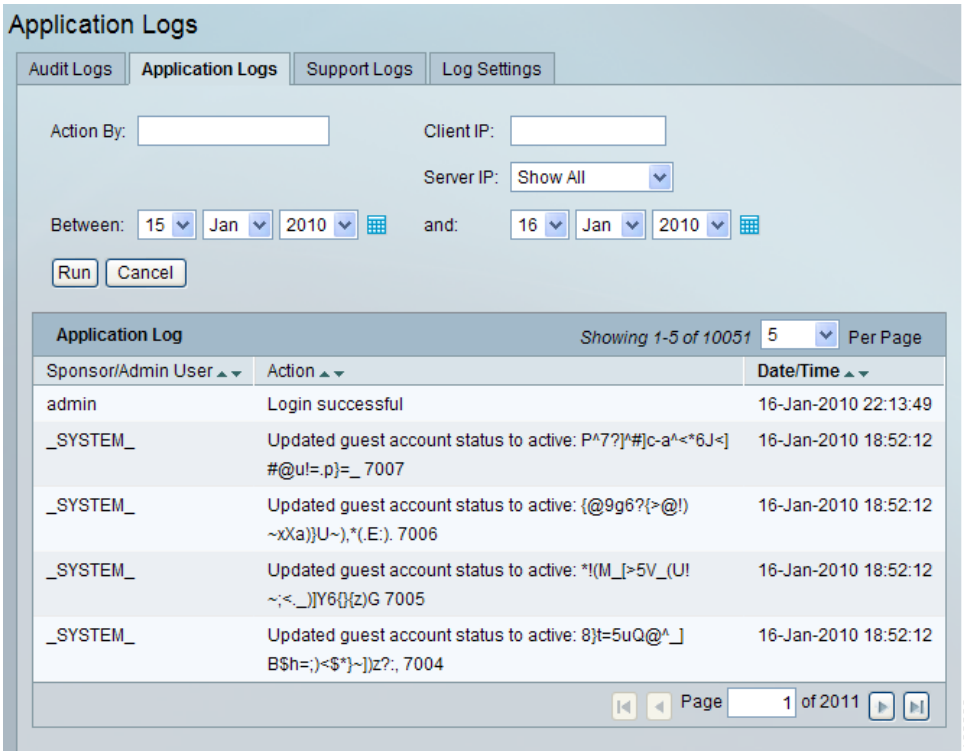


アプリケーション ログ

アプリケーション ログには、アプリケーション デバッグを含むアプリケーション ログが表示されます。

ステップ 1　管理インターフェイスからアプリケーション ログ機能にアクセスするには、[Server] > [System Logs] を選択し、[Application Logs] タブをクリックします（図 15-5 を参照）。

図 15-5　アプリケーション ログ



ステップ 2　アプリケーション ログ レポートは、次の 4 つのカテゴリを使用して実行できます。

- [Action by]：管理者およびスポンサーのユーザ名を検索条件として使用してログを表示します。
- [Client IP]：クライアント IP アドレスを検索条件として使用してログを表示します。
- [Server IP]：サーバ IP を検索条件として使用してログを表示します。

ログ レポートは、1 つのカテゴリ、複数のカテゴリ、またはすべてのカテゴリについて同時に実行できます。

ステップ 3　画面上の日付選択カレンダーを使用して検索条件の期間を選択し、[Run] ボタンをクリックします。

（注）　他の NAC ゲスト サーバ機能への影響を防ぐために、使用後すぐにデバッグをディセーブルにすることを推奨します。

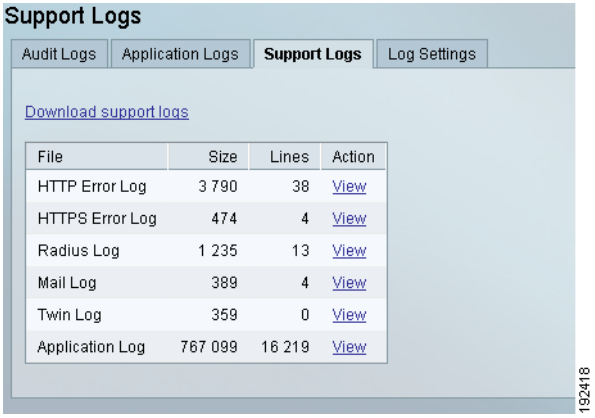
サポート ログ

サポート ログには、次の項目を格納する領域があります。

- HTTP エラー ログ
- RADIUS ログ
- メール ログ
- ツイン（NAC ゲスト サーバ間でレプリケーションを実行している場合はレプリケーション ログだけが該当）
- デバッグ ログ
- 監査ログ
- アプリケーション ログ
- XML ファイル

ステップ 1　管理インターフェイスからサポート ログ機能にアクセスするには、[Server] > [System Logs] を選択し、[Support Logs] タブをクリックします（図 15-6 を参照）。

図 15-6　サポート ログ



ステップ 2　下線の付いた [Action] リンクをクリックすると、リストに表示されているログを表示またはダウンロードできます。

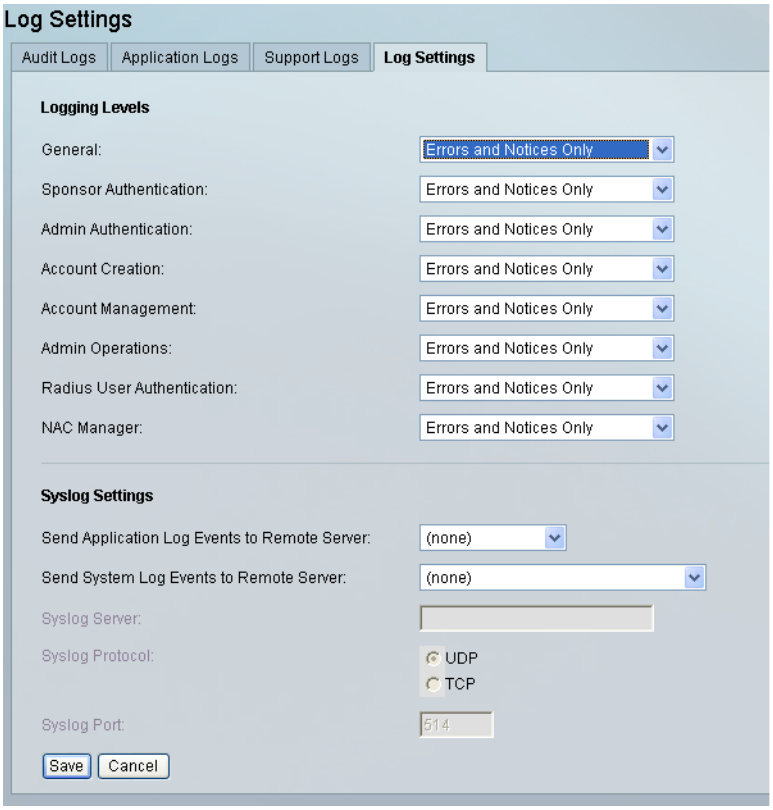
（注）　[Support Logs] ページには、最新の利用可能な各ログの詳細だけが表示されます。ただし、[View] または [Download] をクリックすると、そのカテゴリのすべてのログが取得され、表示されます。

ログ設定

[Log Settings] ページでは、管理者はロギング レベルの設定および syslog 設定の管理ができます。

ステップ 1　管理インターフェイスから [Log Settings] ページにアクセスするには、[Server] > [System Logs] を選択し、[Log Settings] タブをクリックします（図 15-7 を参照）。

図 15-7　[Log Settings] ページ



ステップ 2　[Logging Levels] では、管理者は複数の条件のロギング レベルを選択できます。

- [General] : [Errors and Notices only]、[Errors Notices and Info]、または [Errors Notices Info and Debugs] のロギングを設定できます。
- [Sponsor Authentication] : [Errors and Notices only]、[Errors Notices and Info]、または [Errors Notices Info and Debugs] のロギングを設定できます。
- [Admin Authentication] : [Errors and Notices only]、[Errors Notices and Info]、または [Errors Notices Info and Debugs] のロギングを設定できます。
- [Account Creation] : [Errors and Notices only]、[Errors Notices and Info]、または [Errors Notices Info and Debugs] のロギングを設定できます。
- [Account Management] : [Errors and Notices only]、[Errors Notices and Info]、または [Errors Notices Info and Debugs] のロギングを設定できます。
- [Admin Operation] : [Errors and Notices only]、[Errors Notices and Info]、または [Errors Notices Info and Debugs] のロギングを設定できます。

- [Radius User Authentication] : [Errors and Notices only]、[Errors Notices and Info]、または [Errors Notices Info and Debugs] のロギングを設定できます。
- [NAC Manger] : [Errors and Notices only]、[Errors Notices and Info]、または [Errors Notices Info and Debugs] のロギングを設定できます。

ステップ 3　[Syslog Settings] では、管理者は定義済みの syslog サーバに送信するログ イベントを指定できます。

- [Send Application Log Events to Remote Server] : ログに記録してサーバに送信するアプリケーション エラーのタイプを指定します。管理者は、[none]、[Audit]、[Errors]、または [Audit and Errors] を指定できます。
- [Send System Log Events to Remote Server] : ログに記録してサーバに送信するアプリケーション エラーのタイプを指定します。管理者は、[Emergency]、[Emergency and Alerts]、[Emergency Alerts and Critical]、または [Emergency Alerts Critical and Errors] を指定できます。
- [Syslog Server] : ログが送信される syslog サーバの DNS または IP アドレスを入力します。
- [Syslog Protocol] : UDP または TCP のいずれかのプロトコルを選択します。
- [Syslog Port] : syslog サーバのポートを定義します。

ステップ 4　[Save] ボタンをクリックして設定を保存します。

（注）　基本的な syslog 機能をテストするには、[Log Settings] ページに移動し、[Save] をクリックします。この操作を行うと、テスト メッセージがプライオリティ info (6) で syslog サーバに送信されます。