管理

この章では、管理者にとって役立つ一般的な情報を提供します。説明する項目は次のとおりです。

ログイン名とパスワード（デフォルト）

デフォルトのログイン名とパスワードを次の表に示します。

ユーザ（User）	ログイン/パスワード
OpAdmin およびシェルユーザ	最初の Threat Grid/TGSH ダイアログでランダムに生成されたパスワードを使用し、次に OpAdmin 設定ワークフローの最初の手順で入力した新しいパスワードを使用します。 パスワードを紛失した場合は、「管理者パスワードのリセット」の手順に従ってください。
Threat Grid Web ポータル UI 管理者	Login: **admin** パスワード：最初の OpAdmin パスワードを使用して初期化します。初期化の後、独立した状態になります。
CIMC	Login: **admin** Password: **password**

管理者パスワードのリセット

デフォルトの管理者パスワードは、アプライアンスの初期設定と設定の際にTGSHダイアログのみで表示されます。初期設定が完了すると、管理者パスワードは、読み取り可能なテキストで表示されなくなります。

（注） LDAP認証は、複数の管理者がいる場合に、TGSHダイアログとOpAdminログインに使用できます。アプライアンスにLDAP認証のみが設定されている場合、リカバリ モードでパスワードをリセットすると、認証モードが再設定され、システムパスワードでもログインできるようになります。

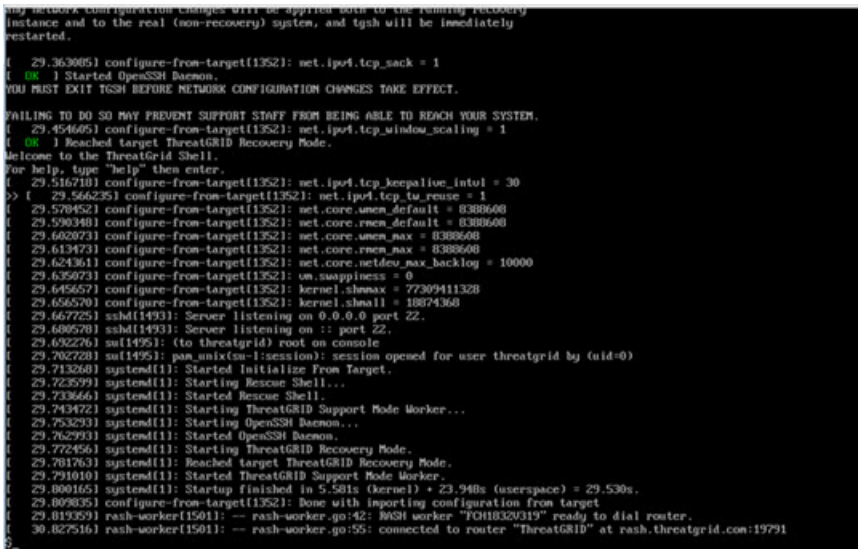
管理者パスワードを紛失してOpAdminにログインできない場合は、次の手順を実行してパスワードをリセットします。

ステップ1 Threat Gridアプライアンスを再起動して、すぐに[Recovery Options]から[**Recovery Mode**]を選択します。

図*1*:ブートメニュー：*[Recovery Mode]*

Threat Gridシェルが開きます。

図 *2* : リカバリモードの *Threat Grid* シェル



ステップ 2 `passwd` を実行して、パスワードを変更します。

図 *3 : Enter New Password*

（注） このモードではコマンドプロンプトが常に表示されるとは限りません。また、ロギング出力がいずれかの時点で入力と重なるように表示されることがあります。この表示は入力には影響しません。ブラインド入力を続けることができます。2 行のロギング出力は無視します。

ステップ 3 パスワードを（ブラインドで）入力し、**Enter** キーを押します。

ステップ 4 パスワードをもう一度入力して、**Enter** キーを押します。

（注） パスワードは表示されません。

ステップ 5 「**Reboot**」と入力し、**Enter** キーを押して、アプライアンスを通常モードで起動します。

（注） v2.10 以降、パスワードのリセットを有効にするために再起動前に exit コマンドを実行する必要はなくなりました。

更新プログラムのインストール

Threat Grid アプライアンスを新しいバージョンに更新する前に、『*Cisco Threat Grid Appliance Setup and Configuration Guide*』で説明されている手順に従って、初期セットアップと設定を完了しておく必要があります。

（注） 新しい Threat Grid アプライアンスが古いバージョンのソフトウェアを搭載して出荷された場合、更新をインストールするには、まず初期設定を完了する必要があります。更新は、ライセンスがインストールされていない限りダウンロードされず、Threat Grid アプライアンス（データベースを含む）が完全に設定されていないと、正しく適用されない可能性があります。

更新をインストールする際、次の点を考慮する必要があります。

- Threat Grid アプライアンスの更新プログラムは OpAdmin Portal を使用して適用します。
- 更新サーバが更新を送信すると、クライアントは更新後のバージョンに完全に移行します。暫定リリースをスキップすることが常に可能というわけではありません。スキップできない場合、更新サーバは、次の更新をダウンロードする前に、アプライアンスにリリースをインストールするよう求めます。
- サーバが特定のバージョンのダウンロードを許可する場合、そのバージョンに直接移行することができます。つまり、単一のアップグレードに必要な再起動以外の再起動を途中で求められることはありません。
- 更新は不可逆です。つまり、新しいバージョンにアップグレードした後、前のバージョンに戻すことはできません。
- エアギャップ実装を使用しているユーザは、Threat Grid サポートに連絡して、ダウンロード可能な更新ブートイメージを入手することができます。

更新のインストール手順については、『*Cisco Threat Grid Appliance Setup And Configuration Guide*』の「Install Threat Grid Appliance Updates」のセクションを参照してください。

バージョン ルックアップ テーブル

正しいビルド番号と対応するリリースバージョンを確認するには、『*Cisco Threat Grid Appliance Version Lookup Table*』を参照してください。

更新に使用されるポート

Threat Grid アプライアンスは、ポート 22 を使用して SSH でリリース更新プログラムをダウンロードします。

- リリース更新は、Web ベースの管理インターフェイス（OpAdmin）からだけではなく、テキスト（curses）インターフェイスからも適用できます。
- DHCP を使用するシステムでは、明示的に DNS を指定する必要があります。DNS サーバが明示的に指定されていないシステムのアップグレードは失敗します。

更新のトラブルシューティング

「*database upgrade not successful*（データベースのアップグレードに失敗しました）」のメッセージは、新しいThreat Gridアプライアンスが古いバージョンのPostgreSQLを実行しており、データベースの自動移行プロセスに失敗したことを意味します。v2.0へのアップグレードの前に、この状態を修正することが必要です。

詳細については、『*Cisco Threat Grid Appliance Release Notes v2.0.1*』を参照してください。

データベーススキーマの更新

従来、スタンドアロンアプライアンスでは、システムがシングルユーザモードでオフラインになっている間に、更新に関連したデータベース移行が発生しました（最初にアップグレードされたノードがオンラインに戻った後に更新が発生したクラスタは除きます。こうしたクラスタが例外になるのは、バックグラウンドで実行される可能性のある非常に長い更新が発生するためです。このような更新はケースバイケースで処理されました）。

Threat Gridアプライアンス（v2.5.0以降）は、システムの再起動が完了した後にデータベーススキーマを更新します。そのため、起動プロセスの所要時間がやや長くなる場合があります。（非常に長い再起動は、引き続きケースバイケースで処理されます）。

以前のリリースでは、バックアップサポートが有効になっているクラスタ化されていないシステムは、NFSサーバがダウンした場合、正常な動作をベストエフォートで試行していました。この動作は、Elasticsearch機能の変更により、現在は保証できなくなっています。

v2.7.2以降、ES6ネイティブインデックスへのバックグラウンドElasticsearchインデックスの移行が有効になりました。この移行は、Elasticsearch 7.0以降が必要なバージョンのThreat Gridアプライアンスがインストールされる前に、正常に完了している必要があります。

（注） Elasticsearchインデックスの移行により、NFSバックアッププロセスに大幅な遅延が発生し、関連した警告が発生する可能性があります。インデックス移行がアクティブに進行中であることを示す場合、これらの警告は無視する必要があります。インデックス移行プロセスが長時間にわたって先に進まない場合は、サポート付きのチケットのみを生成する必要があります。