スケジューリング

ここでは、タスクをスケジュールする方法について説明します。

タスクのスケジューリングについて

さまざまなタスクを、指定した回数（一度または繰り返し）実行するようにスケジュールを設定できます。

タスクはバックエンドにおいてUTCでスケジュールされるため、いつ現地で実行されるかは、日付と場所によって異なります。また、タスクはUTCでスケジュールされるため、サマータイムなど、所在地で実施される場合がある季節調整に合わせて調節されることもありません。このような影響を受ける場合、スケジュールされたタスクは、現地時間を基準とすると、夏期では冬期の場合よりも1時間「遅れて」実行されることになります。

一部のタスクは、初期設定プロセスによって自動的にスケジュールまたは実行されます。

- 最新のVDBをダウンロードしてインストールする1回限りのタスク。
- 最新の利用可能なソフトウェアの更新およびVDBをダウンロードするためにスケジュールされた週次タスク。
- ローカルに保存された構成のみのManagement Centerバックアップを実行するためにスケジュールされた週次タスク。

週次タスクを確認し、必要に応じて調整する必要があります。必要に応じて、VDBやソフトウェアを実際に更新し、構成を展開する新しい定期タスクをスケジュールしてください。

重要 スケジュールされたタスクが意図したとおりに確実に実行されることの確認を強くお勧めします。タスクによっては低帯域幅のネットワークに非常に負荷をかけることがあります（ソフトウェアの自動更新が含まれるタスクや、管理対象デバイスに更新をプッシュする必要があるタスクなど）。ネットワーク使用率が低い時間帯にこのようなタスクを実行するよう、スケジュールしてください。構成の展開など、他のタスクにより、トラフィックが中断される可能性があります。このようなタスクは、メンテナンス期間中にスケジュールする必要があります。

タスクスケジューリングの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- メンテナンス ユーザー

定期タスクの設定

定期タスクの頻度を設定する際には、すべてのタイプのタスクで同じ手順に従います。

Webインターフェイスのほとんどのページに表示される時間はローカル時刻であり、ローカル設定で指定したタイム ゾーンに従ってそれが決定されます。さらに、Management Centerは、該当する場合にはローカル時刻の表示を夏時間（DST）に合わせて自動的に調整します。ただし、DSTから標準時への移行日および元に戻る移行日をまたがる定期タスクは、移行を考慮して調整されません。つまり、標準時の午前2:00にタスク スケジュールを作成すると、DST期間中は午前3:00に実行されます。同様に、DSTの午前2:00にタスク スケジュールを作成すると、標準時には午前1:00に実行されます。

手順

ステップ1 システム（⚙）>**[ツール（Tools）]**>**[スケジューリング（Scheduling）]**を選択します。

ステップ2 [タスクの追加（Add Task）]をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] ドロップダウン リストから、スケジュールするタスクのタイプを選択します。

ステップ 4 [実行するタスクのスケジュール（Schedule task to run）] オプションの横にある [定期（Recurring）] をクリックします。

ステップ 5 [開始日付（Start On）] フィールドに、定期タスクを開始する日付を指定します。

ステップ 6 [繰り返し設定（Repeat Every）] フィールドに、タスクを繰り返す頻度を指定します。

数値を入力するか、[上へ（Up）]（▲）および[下へ（Down）]（▼）をクリックして、間隔を指定できます。たとえば、2 日おきにタスクを実行するには、2 を入力して [日（Days）] をクリックします。

ステップ 7 [実行時刻（Run At）] フィールドで、定期タスクを開始する時刻を指定します。

ステップ 8 週または月単位で実行するタスクの場合は、[繰り返す（オン）（Repeat On）] フィールドでタスクを実行する日付を選択します。

ステップ 9 ジョブに名前を付けます。

ステップ 10 作成するタスクのタイプについて残りのオプションを選択します。

- [バックアップ（Backup）]：Management Center のバックアップのスケジュール （4 ページ）の説明に従って、バックアップジョブをスケジュールします。
- [CRL のダウンロード（Download CRL）]：証明書失効リストのダウンロードの設定 （6 ページ）の説明に従って、証明書失効リストのダウンロードをスケジュールします。
- [ポリシーの展開（Deploy Policies）]：ポリシー展開の自動化 （7 ページ）の説明に従って、ポリシーの展開をスケジュールします。
- [Nmap スキャン（Nmap Scan）]：Nmap スキャンのスケジュール （9 ページ）の説明に従って、Nmap スキャンをスケジュールします。
- [レポート（Report）]：レポートの生成の自動化 （10 ページ）の説明に従って、レポート生成をスケジュールします。
- [Cisco推奨ルール（CiscoFirepower Recommended Rules）]：Cisco 推奨の自動化 （12 ページ）の説明に従って、自動更新をスケジュールします。
- [最新の更新のダウンロード（Download Latest Update）]：ソフトウェア ダウンロードの自動化 （14 ページ）またはVDB 更新のダウンロードの自動化 （17 ページ）の説明に従って、ソフトウェアまたは VDB の更新のダウンロードをスケジュールします。
- [最新の更新のインストール（Install Latest Update）]：ソフトウェア インストールの自動化 （15 ページ）またはVDB 更新のインストールの自動化 （18 ページ）の説明に従って、Management Center または管理対象デバイスでのソフトウェアまたは VDB の更新のインストールをスケジュールします。
- [最新の更新のプッシュ（Push Latest Update）]：ソフトウェア プッシュの自動化 （15 ページ）の説明に従って、管理対象デバイスへのソフトウェア更新のプッシュをスケジュールします。

- [URLフィルタリングデータベースの更新（Update URL Filtering Database）]：スケジュール設定されたタスクを使用したURL フィルタリング更新の自動化 （19 ページ）の説明に従って、URL フィルタリングデータの自動更新をスケジュールします。

ステップ 11 [保存（Save）] をクリックします。

スケジュール バックアップ

Secure Firewall Management Centerでスケジューラを使用して、それ自体のバックアップを自動化することができます。Management Centerからデバイスのリモートバックアップをスケジュールすることもできます。バックアップの詳細については、バックアップ/復元を参照してください。

すべてのデバイスがリモートバックアップをサポートしているわけではないことに注意してください。

Management Center のバックアップのスケジュール

Management Center でスケジューラを使用して、Management Center とデバイスのバックアップを自動化することができます。すべてのデバイスがリモートバックアップをサポートしているわけではないことに注意してください。詳細については、バックアップ/復元 を参照してください。

（注） 初期構成の一環として、システムは（ローカルに保存された）設定のみの週次 Management Center バックアップをスケジュールします。このタスクを確認し、必要に応じ、 このトピック。

始める前に

バックアップ設定を指定するバックアッププロファイルを作成します。バックアッププロファイルの作成を参照してください。

このタスクを実行するには、グローバルドメインに属している必要があります。

手順

ステップ 1 システム（⚙） > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 [ジョブ タイプ（Job Type）] リストから、[バックアップ（Backup）] を選択します。

ステップ 3 [1回（Once）] または [定期（Recurring）] のどちらでバックアップするかを指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの場合、定期タスクの設定 （2 ページ）を参照してください。

ステップ 4 [ジョブ名（Job Name）] を入力します。

ステップ 5 [バックアップタイプ（Backup Type）] で、[Management Center] をクリックします。

ステップ 6 [バックアッププロファイル（Backup Profile）] を選択します。

ステップ 7 （オプション）[コメント（Comment）] を入力します。

コメントは手短にします。それらはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。

ステップ 8 （オプション）[ステータスの送信先（Email Status To:）] フィールドに、メール アドレスまたはメール アドレスのコンマ区切りのリストを入力します。

タスクのステータス メッセージを送信するように電子メール リレー サーバーを設定する方法については、メール リレー ホストおよび通知アドレスの設定を参照してください。

ステップ 9 [保存（Save）] をクリックします。

リモート デバイス バックアップのスケジュール

Management Center でスケジューラを使用して、Management Center とデバイスの両方のバックアップを自動化することができます。すべてのデバイスがリモートバックアップをサポートしているわけではないことに注意してください。詳細については、バックアップ/復元を参照してください。

このタスクを実行するには、グローバルドメインに属している必要があります。

手順

ステップ 1 **システム（⚙）** > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 [ジョブ タイプ（Job Type）] リストから、[バックアップ（Backup）] を選択します。

ステップ 3 [1回（Once）] または [定期（Recurring）] のどちらでバックアップするかを指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの場合、定期タスクの設定 （2 ページ）を参照してください。

ステップ 4 [ジョブ名（Job Name）] を入力します。

ステップ 5 [バックアップのタイプ（Backup Type）] で、[デバイス（Device）] をクリックします。

ステップ 6 1 つ以上のデバイスを選択します。

お使いのデバイスがリストにない場合、リモートバックアップはサポートされていません。

ステップ 7 バックアップ用のリモートストレージを設定しなかった場合は、[管理センターで取得する（Retrieve to Management Center）] を有効または無効にできます。

- 有効（デフォルト）：バックアップが Management Center の `/var/sf/remote-backup/` に保存されます。

- 無効：バックアップがデバイスの /var/sf/backup に保存されます。

リモート バックアップ ストレージを設定している場合、バックアップ ファイルはリモートに保存され、このオプションは無効になります。詳細については、「バックアップとリモートストレージの管理」を参照してください。

ステップ 8 （オプション）[コメント（Comment）] を入力します。

コメントは手短にします。それらはスケジュール予定表ページの[タスクの詳細（Task Details）] セクションに表示されます。

ステップ 9 （オプション）[ステータスの送信先（Email Status To:）] フィールドに、メール アドレスまたはメール アドレスのコンマ区切りのリストを入力します。

タスクのステータス メッセージを送信するように電子メール リレー サーバーを設定する方法については、メール リレー ホストおよび通知アドレスの設定を参照してください。

ステップ 10 [保存（Save）] をクリックします。

証明書失効リストのダウンロードの設定

Management Centerのローカル Web インターフェイスを使用して、この手順を実行する必要があります。

アプライアンスのユーザ証明書または監査ログ証明書を有効にするアプライアンスのローカル設定で証明書失効リスト（CRL）のダウンロードを有効にすると、CRL のダウンロード タスクが自動的に作成されます。スケジューラを使用してタスクを編集し、更新の頻度を設定できます。

始める前に

- ユーザ証明書または監査ログ証明書を有効にして設定し、1 つ以上の CRL のダウンロード URL を設定します。詳細については、有効な HTTPS クライアント証明書の強制と有効な監査ログ サーバー証明書の要求を参照してください。

手順

ステップ 1 システム（⚙） > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブタイプ（Job Type）] から、[CRL のダウンロード（Download CRL）] を選択します。

ステップ 4 CRL ダウンロードをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定 （2 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 タスクについてコメントするには、[コメント（Comment）] フィールドにコメントを入力します。

[コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 7 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、Management Centerで有効な電子メール中継サーバが設定されている必要があります。

ステップ 8 [保存（Save）] をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定

ポリシー展開の自動化

Management Center の設定を変更した後は、影響を受けるデバイスへ変更を展開する必要があります。

⚠

注意 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断する Snort プロセスが再開します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。Snort の再起動によるトラフィックの動作および展開またはアクティブ化された際に Snort プロセスを再起動する設定を参照してください。

手順

ステップ 1 **システム**（⚙） > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブタイプ（Job Type）] から、[ポリシーの展開（Deploy Policies）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定 （2 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [デバイス（Device）] フィールドで、ポリシーを展開するデバイスを選択します。

ステップ 7 [最新のデバイスへの展開をスキップする（Skip deployment for up-to-date devices）] チェックボックスを、必要に応じてオンまたはオフにします。

デフォルトでは、ポリシーの展開プロセス中のパフォーマンスを向上させるため、[最新のデバイスへの展開をスキップする（Skip deployment for up-to-date devices）] オプションが有効になっています。

（注） システムは、Management Center の Web インターフェイスから開始されたポリシーの展開が進行中の場合、スケジュール設定されたポリシーの展開タスクを実行しません。同様に、システムは、スケジュール設定されたポリシーの展開タスクが進行中の場合、Web インターフェイスからポリシーの展開を開始することを許可しません。

ステップ 8 タスクについてコメントを付加するには、[コメント（Comment）] フィールドにコメントを入力します。

[コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 9 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 10 [保存（Save）] をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定
展開が必要な設定変更

Nmap スキャンの自動化

ネットワーク上のターゲットに対する定期的な Nmap スキャンをスケジュールできます。スキャンを自動化すると、Nmap スキャンによって以前に提供された情報を更新できます。システムは Nmap から提供されるデータを更新できないため、このデータを最新に保つには定期的に再スキャンする必要があります。また、ネットワーク上のホストに識別不能なアプリケーションやサーバがあるかどうか自動的に検査するよう、スキャンをスケジュールすることもできます。

さらに、Discovery Administrator が修正用に Nmap スキャンを使用する場合があることにも注意してください。たとえば、ホストでオペレーティング システム競合が発生したために、Nmap スキャンがトリガーされることがあります。スキャンが実行されると、そのホストでのオペレーティング システムの更新済み情報が取得され、こうして競合が解決されます。

以前に Nmap スキャン機能を使用したことがない場合は、スケジュール スキャンを定義する前に、Nmap スキャンを設定します。

関連トピック

Nmap スキャン

Nmap スキャンのスケジュール

システムで検出されたホストのオペレーティング システム、アプリケーション、またはサーバーが Nmap スキャンの結果で置き換えられると、システムは、Nmap によって置換されたホストに関する情報を更新しなくなります。Nmap によって提供されるサービスやオペレーティング システムのデータは、もう 1 度 Nmap スキャンを実行するまで静的な状態のままになります。Nmap を使用したホストのスキャンを計画している場合は、Nmap 提供のオペレーティング システム、アプリケーション、またはサーバを最新の状態に保つために、定期的なスキャン スケジュールをセットアップしてください。ネットワーク マップからホストが削除されて再び追加されると、Nmap スキャン結果はすべて破棄され、システムはホストに関するすべてのオペレーティング システムとサービスのデータのモニタリングを再開します。

手順

ステップ 1 **システム**（⚙） > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブタイプ（Job Type）] から、[Nmap スキャン（Nmap Scan）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定 （2 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [Nmap 修復（Nmap Remediation）] フィールドで、Nmap 修復を選択します。

ステップ 7 [Nmap ターゲット（Nmap Target）] フィールドで、スキャン ターゲットを選択します。

ステップ 8 [ドメイン（Domain）] フィールドで、増補するネットワーク マップを持つドメインを選択します。

ステップ 9 タスクにコメントを付ける場合は、[コメント（Comment）] フィールドにコメントを入力します。

ヒント [コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 10 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 11 [保存（Save）] をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定

レポートの生成の自動化

一定期間ごとにレポートを実行するよう自動化できます。

始める前に

- リスク レポート以外のレポートの場合：レポート テンプレートを作成します。詳細については、レポート テンプレートを参照してください。
- スケジューラを使用してメール レポートを配布するには、メール リレーのホストを設定し、レポートの受信者およびメッセージ情報を指定します。メール リレー ホストおよび通知アドレスの設定 と、（リスク レポート以外のレポートの場合）レポートの生成時の電子メール配布または（リスク レポートの場合）リスク レポートの生成、表示および印刷を参照してください。
- （オプション）スケジュール設定されたレポートのファイル名、出力フォーマット、時間枠、またはメール配布の設定を設定または変更します。スケジュールされたレポート生成設定の指定 （11 ページ）を参照してください。
- レポートの出力形式として PDF を選択する場合は、テンプレートの各セクションの結果数が PDF の制限を超えないことを、レポート テンプレートで確認してください。詳細については、レポート テンプレート フィールドを参照してください。

手順

ステップ 1 システム（⚙） > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブタイプ（Job Type）] リストから、ジョブを選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定 （2 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [レポートテンプレート（Report Template）] フィールドで、リスクレポート、またはレポートテンプレートを選択します。

ステップ 7 タスクについてコメントを付加するには、[コメント（Comment）]フィールドにコメントを入力します。

[コメント（Comment）]フィールドはスケジュール予定表ページの[タスクの詳細（Task Details）]セクションに表示されます。コメントは手短にします。

ステップ 8 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）]フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力

します。ステータスメッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

（注） このオプションを設定しても、レポートは配布されません。

ステップ 9 レポートのデータがない場合（たとえばレポート期間中に特定のタイプのイベントが発生しなかった場合）にレポート電子メール添付ファイルを受信しないようにするには、[空のレポートも添付（If report is empty, still attach to email）] チェックボックスを選択します。

ステップ 10 [保存（Save）] をクリックします。

スケジュールされたレポート生成設定の指定

このタスクを実行するには、管理者権限またはセキュリティアナリスト権限が必要です。

スケジュールされたレポートのファイル名、出力形式、時間枠、電子メール配布の設定を指定または変更するには、次の手順に従います。

手順

ステップ 1 [概要（Overview）] > [レポート（Reporting）] > [レポート テンプレート（Report Templates）] の順に選択します。

ステップ 2 変更するレポート テンプレートの [編集（Edit）] をクリックします。

ステップ 3 PDF 出力を選択する場合は、次のようにします。

a) レポートのいずれかのセクションで、結果数の横に黄色い三角形が示されているかどうかを調べます。

b) 黄色の三角形が示されている場合、三角形の上にマウスカーソルを重ねると、PDF 出力のそのセクションに対して許容される結果の最大数が表示されます。

c) 黄色い三角形が示されているセクションごとに、結果数を最大数未満の数に削減します。

d) 黄色い三角形が示されなくなったら、[保存（Save）] をクリックします。

ステップ 4 [生成（Generate）] をクリックします。

（注） 今すぐレポートを生成せずにレポート生成の設定を変更する場合は、テンプレート設定ページで [生成（Generate）] をクリックする必要があります。レポートを生成しない限り、テンプレート リスト ビューで [生成（Generate）] をクリックしても変更は保存されません。

ステップ 5 設定を変更します。

ステップ 6 レポートを生成せずに新しい設定を保存するには、[キャンセル（Cancel）]をクリックします。

新しい設定を保存してレポートを生成するには、[生成（Generate）] をクリックし、この手順の残りのステップをスキップします。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 保存を求めるプロンプトが出されたら、まだ変更していない場合でも [OK] をクリックします。

Cisco 推奨の自動化

カスタム侵入ポリシーで保存済みの最新の設定を使用し、ネットワークのディスカバリ データに基づいてルール状態の推奨を自動的に生成することができます。

（注） 変更が未保存のまま、侵入ポリシーに関するスケジュール済み推奨がシステムによって自動生成される場合、自動生成された推奨をポリシーに反映させるには、そのポリシー内の変更を破棄してポリシーをコミットする必要があります。

タスクを実行すると、推奨ルール状態が自動的に生成され、ポリシーの設定に基づいて侵入ルールの状態が変更されます。変更されたルール状態は、侵入ポリシーを次回に展開するときに有効になります。

始める前に

- Cisco Secure Firewall Management Center デバイス構成ガイドの説明に従い、侵入ポリシーで Cisco 推奨ルールを設定します。
- タスクのステータス メッセージをメールで送るには、有効なメール リレー サーバーを設定します。
- 推奨を生成するには、IPS スマートライセンスまたは保護クラシックライセンスが必要です。

手順

ステップ 1 システム（⚙）> **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブタイプ（Job Type）] から、[Cisco推奨ルール（Cisco Recommended Rules）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定 （2 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [ポリシー（Policies）] の横で、推奨を生成する 1 つ以上の侵入ポリシーを選択します。[すべてのポリシー（All Policies）] チェックボックスをオンにして、すべての侵入ポリシーを選択します。

ステップ 7 （任意）[コメント（Comments）] フィールドにコメントを入力します。

コメントは手短にします。コメントはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。

ステップ 8 （任意）タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。

ステップ 9 [保存（Save）] をクリックします。

関連トピック

競合と変更：ネットワーク分析ポリシーと侵入ポリシー
シスコ推奨ルールについて
メール リレー ホストおよび通知アドレスの設定

ソフトウェアアップグレードの自動化

パッチを自動的にダウンロードし、メンテナンスリリースとパッチを適用することができます。

Management Center をアップグレードするには、ダウンロードタスクとインストールタスクをスケジュールします。管理対象デバイスをアップグレードするには、ダウンロードタスク、プッシュタスク、およびインストールタスクをスケジュールします。タスク間に十分な時間を空けるようにしてください。たとえば、プッシュがまだ実行されているときに実行するようにスケジュールされたインストールは失敗します。

この機能は、メジャーリリースではサポートされていません。アップグレードパッケージをダウンロードするには、インターネットアクセスが必要です。デバイスグループへのアップグレードをスケジュールすると、アップグレードは、グループ化されたすべてのデバイスで同時に実行されます。

（注） 初期構成の一環として、システムは週ごとのダウンロードをスケジュールします。このタスクを確認し、必要に応じ、ソフトウェア ダウンロードの自動化（14 ページ）。このタスクは、更新のみをダウンロードします。ユーザは、このタスクがダウンロードした更新をインストールする必要があります。

関連トピック

管理インターフェイス
更新

ソフトウェア ダウンロードの自動化

この手順を使用して、選択したパッチのダウンロードとメンテナンスリリースのスケジュールを設定します。グローバルドメインにいる必要があります。

（注） バージョン 7.4.1 以降では、このタスクではメンテナンスリリースをダウンロードしなくなりました。直接メンテナンス（およびメジャー）リリースを Management Center に直接ダウンロードするには、**システム**（⚙）> **[Product Upgrades]** を使用します。

始める前に

Management Center でインターネットにアクセスできることを確認します。

手順

ステップ 1 **システム**（⚙）> **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] リストから、[最新の更新のダウンロード（Download Latest Update）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定 （2 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [アップデート項目（Update Items）] の横の [ソフトウェア（Software）] チェックボックスをオンにします。

ステップ 7 タスクについてコメントするには、[コメント（Comment）] フィールドにコメントを入力します。

[コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 8 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 9 [保存（Save）] をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定

ソフトウェア プッシュの自動化

管理対象デバイスでのソフトウェア更新のインストールを自動化するには、インストールの前に、更新をデバイスにプッシュする必要があります。

ソフトウェア更新を管理対象デバイスにプッシュするタスクを作成する際には、更新がデバイスに確実にコピーされるよう、プッシュ タスクとスケジュール済みインストール タスクの間に十分な時間を確保してください。

このタスクを実行するには、グローバルドメインに属している必要があります。

手順

ステップ 1 システム（⚙） > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブタイプ（Job Type）] リストから、[最新の更新をプッシュ（Push Latest Update）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定 （2 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [デバイス（Device）] ドロップダウン リストから、更新するデバイスを選択します。

ステップ 7 タスクについてコメントするには、[コメント（Comment）] フィールドにコメントを入力します。

[コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 8 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 9 [保存（Save）] をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定

ソフトウェア インストールの自動化

管理対象デバイスへ更新をプッシュするタスクと、その更新をインストールするタスクの間に十分な時間を確保する必要があります。

このタスクを実行するには、グローバルドメインに属している必要があります。

注意 インストールする更新によっては、ソフトウェアのインストール後にアプライアンスがリブートする場合があります。

手順

ステップ 1 システム（⚙） > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] リストから、[最新の更新のインストール（Install Latest Update）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定 （2 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [デバイス（Device）] ドロップダウンリストから、更新をインストールするアプライアンス（Management Centerを含む）を選択します。

ステップ 7 [アップデート項目（Update Items）] の横の [ソフトウェア（Software）] チェックボックスをオンにします。

ステップ 8 タスクについてコメントするには、[コメント（Comment）] フィールドにコメントを入力します。

[コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 9 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 10 [保存（Save）] をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定

脆弱性データベースの更新の自動化

スケジュール機能を使用してシスコの脆弱性データベース（VDB）を更新できるため、常に最新の情報を使ってネットワーク上のホストを評価することができます。ダウンロード、インス

トール、およびその後の展開を個別のタスクとしてスケジュールし、タスク間に十分な時間を確保する必要があります。

（注） Management Center の初期設定では、1 回限りの操作でシスコから最新の VDB が自動的にダウンロードされてインストールされます。また、最新の VDB を含む最新の利用可能なソフトウェアアップデートをダウンロードする週次タスクもスケジュールされます。この週次タスクを確認し、必要に応じて調整することをお勧めします。必要に応じて、VDB を実際に更新し、構成を展開する新しい週次タスクをスケジュールしてください。

関連トピック

管理インターフェイス

VDB 更新のダウンロードの自動化

このタスクを実行するには、グローバルドメインに属している必要があります。

始める前に

Management Center にインターネット アクセスがあることを確認します。

手順

ステップ 1 システム（⚙） > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] リストから、[最新の更新のダウンロード（Download Latest Update）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定 （2 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [アップデート項目（Update Items）] の横の [脆弱性データベース（Vulnerability Database）] チェックボックスをオンにします。

ステップ 7 （任意）[コメント（Comments）] フィールドに簡単なコメントを入力します。

ステップ 8 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 9 [保存（Save）] をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定

VDB 更新のインストールの自動化

VDB 更新をダウンロードするタスクと、その更新をインストールするタスクの間に十分な時間を確保してください。

このタスクを実行するには、グローバルドメインに属している必要があります。

注意 ほとんどの場合、VDB 更新後の最初の展開では Snort プロセスが再起動され、トラフィックインスペクションが中断されます。これが発生すると、システムから警告が表示されます（更新されたアプリケーションディテクタとオペレーティングシステムのフィンガープリントについては再起動が必要ですが、脆弱性情報については不要です）。この中断中にインスペクションを続行せずにトラフィックがドロップされるかパスするどうかは、対象デバイスによるトラフィックの処理方法によって異なります。詳細については、「Snort の再起動によるトラフィックの動作」を参照してください。

手順

ステップ 1 **システム（⚙）** > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] リストから、[最新の更新のインストール（Install Latest Update）] を選択します。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。
- 定期タスクの詳細については、定期タスクの設定 （2 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 [デバイス（Device）] ドロップダウン リストから Management Center を選択します。

ステップ 7 [アップデート項目（Update Items）] の横の [脆弱性データベース（Vulnerability Database）] チェックボックスをオンにします。

ステップ 8 （任意）[コメント（Comments）] フィールドに簡単なコメントを入力します。

ステップ 9 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 10 [保存（Save）] をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定

スケジュール設定されたタスクを使用したURLフィルタリング更新の自動化

URL フィルタリングの脅威データが最新であることを確認するため、システムは、Cisco（Collective Security Intelligencecsi）クラウドからデータ更新を取得する必要があります。

デフォルトでは、URLフィルタリングを有効にすると、自動更新が有効になります。ただし、これらの更新が発生する時間を制御する必要がある場合には、デフォルトの更新メカニズムではなく、このトピックで説明されている手順を使用します。

通常、毎日の更新は小規模ですが、最終更新日から5日を超えると、帯域幅によっては新しいURL フィルタリング データのダウンロードに最長 20 分かかる場合があります。その後、更新自体を実行するのに最長で 30 分かかることがあります。

始める前に

- Management Center にインターネットアクセス権があることを確認してください（セキュリティ、インターネット アクセス、および通信ポート を参照）。
- URLフィルタリングが有効にされていることを確認します。詳細については、Cisco Secure Firewall Management Center デバイス構成ガイド の「*Enable URL Filtering Using Category and Reputation*」を参照してください。
- **[統合（Integration）] > [その他の統合（Other Integrations）]** メニューの **クラウド サービス（Cloud Services）** で [自動更新を有効にする（Enable Automatic Updates）] が選択されていないことを確認します。
- このタスクを実行するには、グローバルドメインに属している必要があります。URLフィルタリングライセンスも必要です。

手順

ステップ 1 システム（⚙） > **[ツール（Tools）] > [スケジューリング（Scheduling）]** を選択します。

ステップ 2 [タスクの追加（Add Task）] をクリックします。

ステップ 3 [ジョブ タイプ（Job Type）] リストから、[URL フィルタリング データベースの更新（Update URL Filtering Database）] を選択します。

ステップ 4 更新をスケジュールする頻度として、ワンタイム更新を示す [1 回（Once）] または定期更新を示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウンリストを使用して開始日時を指定します。

- 定期タスクの詳細については、定期タスクの設定 （2 ページ）を参照してください。

ステップ 5 [ジョブ名（Job Name）] フィールドに名前を入力します。

ステップ 6 タスクについてコメントするには、[コメント（Comment）] フィールドにコメントを入力します。

[コメント（Comment）] フィールドはスケジュール予定表ページの [タスクの詳細（Task Details）] セクションに表示されます。コメントは手短にします。

ステップ 7 タスクのステータス メッセージをメールで送信するには、[ステータスの送信先（Email Status To:）] フィールドにメールアドレス（またはコンマで区切った複数のメールアドレス）を入力します。ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。

ステップ 8 [保存（Save）] をクリックします。

関連トピック

メール リレー ホストおよび通知アドレスの設定

スケジュール済みタスクの確認

スケジュール済みタスクを追加した後、それらのタスクを表示したり、状態を評価したりできます。ページの [表示オプション（View Options）] セクションで、カレンダーやスケジュール済みタスク リストを使用してスケジュール済みタスクを表示できます。

カレンダー表示オプションを使用すると、どの日にどのスケジュール済みタスクが行われるかを表示できます。

タスク リストには、タスクとその状態のリストが表示されます。タスク リストは、カレンダーを開いたときにカレンダーの下に表示されます。また、カレンダーで 1 つの日付またはタスクを選択して表示することもできます。

以前に作成したスケジュール済みタスクを編集できます。この機能は、パラメータが正しいことを確認するために、スケジュール済みタスクを 1 度テストする場合に特に役立ちます。タスクが正常に完了したら、後で定期タスクに変更できます。

[スケジュール表示（Schedule View）] ページから 2 種類の削除操作を実行できます。まだ実行されていない特定のワンタイム タスク、または定期タスクのすべてのインスタンスを削除できます。定期タスクの 1 つのインスタンスを削除すると、そのタスクのすべてのインスタンスが削除されます。1 度だけ実行するようスケジュールされているタスクを削除すると、そのタスクだけが削除されます。

タスク一覧の詳細

表 *1:* タスク一覧のカラム

カラム	説明
名前	スケジュール済みタスクの名前と、関連付けられているコメントを表示します。
タイプ	スケジュール済みタスクのタイプを表示します。
開始時刻（Start Time）	スケジュールされている開始日時を表示します。
頻度（Frequency）	タスクの実行頻度を表示します。
前回の実行時間（Last Run Time）	実際の開始日時を表示します。 定期タスクの場合、これは最新の実行に適用されます。
最終実行ステータス（Last Run Status）	スケジュール済みタスクの現在の状態を次のように示します。 • **[チェックマーク（Check Mark）]**（）は、タスクが正常に実行されたことを示します。 • 疑問符アイコン（**[疑問符（Question Mark）]**（））は、タスクの状態が不明であることを示します。 • 感嘆符アイコン（）は、タスクが失敗したことを示します。 定期タスクの場合、これは最新の実行に適用されます。
次回の実行時間（Next Run Time）	定期タスクの次の実行時間を表示します。 ワンタイム タスクの場合に「該当なし（N/A）」と表示します。
作成者（Creator）	スケジュール済みタスクを作成したユーザの名前を表示します。
編集（Edit）	スケジュール済みタスクを編集します。
削除（Delete）	スケジュール済みタスクを削除します。

カレンダーのスケジュール済みタスクの表示

スケジュールされたタスクは、カレンダーに表示できます。

手順

ステップ 1 システム（⚙） > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 カレンダー ビューを使用して、次のタスクを実行できます。

- [二重左矢印（Double Left Arrow）]（«） をクリックすると、1 年前に戻ります。
- [左矢印（Single Left Arrow）]（‹） をクリックすると、1 か月前に戻ります。
- [右矢印（Single Right Arrow）]（›） をクリックすると、1 か月後に進みます。
- [二重右矢印（Double Right Arrow）]（») をクリックすると、1 年後に進みます。
- [今日（Today）] をクリックすると、現在の年月に戻ります。
- [タスクの追加（Add Task）] をクリックすると、新しいタスクをスケジュールできます。
- 1 つの日付をクリックすると、カレンダーの下にあるタスク リスト表に、特定の日付のスケジュール済みタスクがすべて表示されます。
- ある日付の特定のタスクをクリックすると、カレンダーの下にあるタスク リスト表にそのタスクが表示されます。

スケジュール済みタスクの編集

スケジュール済みタスクを編集できます。

手順

ステップ 1 システム（⚙） > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 カレンダーで、編集するタスク、またはタスクが表示されている日付をクリックします。

ステップ 3 [タスクの詳細（Task Details）] テーブルで、編集するタスクの横にある**[編集（Edit）]**（✎）をクリックします。

ステップ 4 タスクを編集します。

ステップ 5 [保存（Save）] をクリックします。

スケジュール済みタスクの削除

スケジュール済みタスクを削除できます。

手順

ステップ 1 システム（⚙） > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** を選択します。

ステップ 2 カレンダーで、削除するタスクをクリックします。繰り返しタスクの場合は、タスクのインスタンスをクリックします。

ステップ 3 [タスク詳細（Task Details）] テーブルで、[削除（Delete）]（🗑） をクリックし、選択内容を確認します。

スケジュール済みタスクの履歴

機能	最小 Management Center	最小 Threat Defense	詳細
スケジュール済みタスクでは、パッチおよび VDB 更新のみダウンロードされます。	7.4.1	任意（Any）	**アップグレードの影響。スケジュールされたダウンロードタスクは、メンテナンスリリースの取得を停止します。** [最新の更新のダウンロード（Download Latest Update）] スケジュール済みタスクでは、メンテナンスリリースはダウンロードされなくなり、適用可能な最新のパッチと VDB の更新のみがダウンロードされるようになりました。メンテナンス（およびメジャー）リリースを Management Center に直接ダウンロードするには、**システム**（⚙） > **[製品のアップグレード（Product Upgrades）]**を使用します。 その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。
自動 VDB ダウンロード。	7.3.0	いずれか	初期設定では、利用可能な最新のソフトウェアアップデート（最新の VDB を含む）をダウンロードするための週次タスクがスケジュールされます。この週次タスクを確認し、必要に応じて調整し、新しい週次タスクをスケジュールして実際に VDB を更新することを推奨します。アプリケーションディテクタとオペレーティングシステムフィンガープリントを有効にするためには、設定を展開する必要があります。 新規/変更された画面：システムで作成された [週次ソフトウェアダウンロード（Weekly Software Download）] のスケジュールされたタスクで、[脆弱性データベース（Vulnerability Database）] チェックボックスがデフォルトで有効になりました。
侵入ルールの自動更新。	6.6	任意（Any）	初期設定では、毎日の侵入ルールの更新が有効になります。このタスクを確認し、必要に応じて調整することを推奨します。更新されたルールを有効にするには、設定を展開する必要があります。

機能	最小 Management Center	最小 Threat Defense	詳細
ソフトウェアの自動ダウンロードと設定のバックアップ。	6.5	任意（Any）	初期設定では、次の週次タスクがスケジュールされます。 • FMC とその管理対象デバイスの利用可能な最新のソフトウェアアップデートをダウンロードする。 • ローカルに保存された設定のみのバックアップを実行する。 これらのタスクを確認し、必要に応じて調整することを推奨します。
多数の管理対象デバイスのリモートバックアップをスケジュールします。	6.4	任意（Any）	リモート デバイス バックアップ。 新規/変更された画面：定期バックアップを設定するときに、[バックアップタイプ（Backup Type）]（Management Center とデバイス）を選択できるようになりました。 プラットフォームの制限：デバイスはオンデマンドバックアップをサポートする必要があります。バックアップと復元の要件を参照してください。

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。