Nagios® XI™

Nagios XI
管理者ガイド

Rev. 3.5

2017.02.06

ジュピターテクノロジー

目次

変更履歴

版	発行日	変更内容
第 1.0 版	2013/10/07	新規作成
第 2.0 版	2014/07/02	Nagios XI 2014 に対応
第 3.0 版	2016/02/04	構成変更, Nagios XI 5.2.3 に対応
第 3.1 版	2016/02/29	Nagios XI 5.2.5 に対応
第 3.2 版	2016/03/07	一部の技術文書リンク更新
第 3.3 版	2016/03/23	一部の技術文書リンク更新
第 3.4 版	2016/11/25	Nagios XI 5.3.3 に対応
第 3.5 版	2017/02/06	Nagios XI 5.4 に対応

1　はじめに

Nagios XIをお選びいただきましてありがとうございます。Nagios XIはあなたの重要なITインフラストラクチャコンポーネントを監視する強力なアプリケーションです。

1.1　Nagios XIとは

Nagios XI は企業規模のソリューションであり、問題が重要なビジネスプロセスに影響を与える前に組織にITインフラストラクチャーについての洞察を与えます。

Nagios XI はシステム、アプリケーション、サービス、ビジネスプロセスが適切に機能するよう全体のITインフラストラクチャーを監視します。障害があった際には、Nagiosはその問題について関係者にアラートを出すことができます。これにより障害がビジネスプロセス、エンドユーザー、顧客に影響を与える前に改善策を取ることができます。Nagios があれば、目に見えないインフラストラクチャーの障害がなぜ組織に影響を与えてしまったかを説明する必要がなくなります。

Nagios XI は組み込み済みの機能およびサードパーティ拡張やアドオンを通して、数百のアプリケーションサービス、プロトコル、コンピューターハードウェアを監視できます。

Nagios XIおよびその機能に関する説明については、以下をご参照ください:

弊社 Nagios XI 紹介ページ:
http://www.jtc-i.co.jp/product/nagios/nagiosxi.html

Nagios Enterprises 社 Nagios XI 紹介ページ(英語):
http://www.nagios.com/products/nagiosxi/

1.2　このガイドについて

このガイドは、Nagios XIの管理者ガイドです。Nagios XIシステムの管理、運用方法について説明します。管理者権限レベルの方が日本語ユーザーインターフェースで Nagios XI を使用することを想定しています。

Nagios XIのユーザー権限レベルの使用方法(Nagios XIの基本機能、監視結果の閲覧、レポート閲覧など)については、別ガイド「Nagios XI ユーザーガイド」をお読みください。

このガイドは別文書へのリンクを含んでいます。リンク名が英語のものは Nagios Enterprises 社が作成したオリジナルの技術文書(英語)へのリンクです。リンク先のドキュメントについて不明な点がございましたら、弊社までお問い合わせください。

2　インストレーション

2.1　システム要件(Linuxソースインストレーションの場合)

Nagios XI をインストールするサーバが以下の要件を満たしていることをご確認ください。

ハードウェア要件はさまざまな要件に依存します。
以下は一般的な利用環境における参考データです:

	最小要件	推奨要件
CPU	1 GHz	2+ GHz 以上
メモリ	1 GB	4 GB
ハードディスク	8 GB	40 GB
その他		RAID 5
OS	RHEL 5.x/6.x (32 および 64bit) / 7.x または CentOS 5.x/6.x (32 および 64bit) / 7.x	

メモ: ハードウェア要件に関する詳しい情報については、「Nagios XI ハードウェア要件」をご参照ください。

2.2　インストレーションオプション

Nagios XI には、以下の2つのインストールオプションがあります。

- **Nagios XI 仮想マシンを使用する**:

  Nagios XI を素早く構築し開始できます。仮想マシンは VMware ESX、vSphere、その他の VMware サーバ製品がデプロイされているエンタープライズ環境で使用できます。

- **Nagios XI を Linux サーバ(RHEL/CentOS)に手動インストールする**:

  このオプションは、Nagios XI を(例えば性能の理由から)物理サーバまたはサポートされた Linux ディストリビューションが稼働する仮想サーバ上にインストールしたい場合に選択します。

ニーズに合うオプションを選択して下さい。どちらを選べばよいかわからない場合は、すぐに使用できる Nagios XI 仮想マシンを使用することをお勧めします。

各種インストーラーは、弊社 ソフトウェアダウンロードページからダウンロードしていただけます。

2.3　インストレーションと初期セットアップ

Nagios XIのインストレーションおよび初期セットアップ手順については、以下の資料をお読みください。

Nagios XI セットアップガイド

3　システム設定

Nagios XI のシステム設定は、**管理**ページで行います。

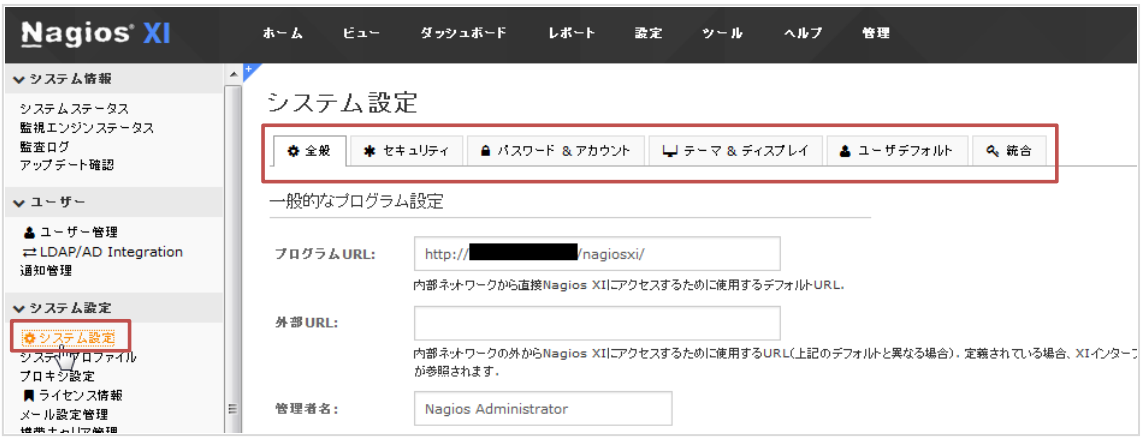
メモ:

- **管理**メニューは管理者権限を持つユーザーにのみ表示されます。
- 画面幅が狭い場合、下図のように画面上部のメニューは折りたたまれた状態で表示されます。**「ナビゲーション」**メニューにマウスをかざすと、プライマリメニュー項目が表示されます。

3.1　システム設定

システム設定(**「管理 -> システム設定」**)ページでは、Nagios XI Web インターフェースの URL、管理者名、管理者メールアドレス、タイムゾーン、インターフェースのテーマ設定、ユーザーのデフォルト表示言語設定などを設定します。

システム設定ページは、6つのタブページに分かれています。



3.1.1　「全般」タブページ

「全般」タブページでは、システム全般の設定を行います。このページの内容は初期セットアップの最終セットアップ作業時に設定されます。

一般的なプログラム設定:

項目	説明
プログラム URL	内部ネットワークから直接 Nagios XI にアクセスするために使用するデフォルト URL
外部 URL	内部ネットワークの外から Nagios XI にアクセスするために使用する URL(上記と異なる場合)。定義されている場合、XI インターフェースへ素早くアクセスできるようにメールアラートでこの URL が参照されます。
管理者名	Nagios XI 管理者名
管理者メールアドレス	Nagios XI 管理者のメールアドレス
更新を自動的に確認する	チェックありの場合、Nagios XI の更新チェックを自動実行します。更新チェックを行うにはインターネットの接続環境が必要です(デフォルト:チェックあり)
ホスト/サービスのステータスの HTML タグを許可する	ホストおよびサービス(プラグイン)アウトプットに HTML タグを許可するかどうか。チェックありの場合、HTML タグを許可

タイムゾーン設定:

システムのタイムゾーンをドロップダウンリストから選択します。

CCM 統合設定:

Core コンフィグマネージャへのアクセス時に、ログイン認証画面を表示する場合は、**「CCM ログインを分離」**にチェックをつけます(デフォルト:チェックなし)

その他の設定:

項目	説明
監査ログをファイルに書込む	チェックすると、すべての監査ログイベントが `/usr/local/nagiosxi/var/components/auditlog.log` ファイルに書き込まれます(デフォルト:チェックなし)。
認知済みデフォルト	障害の認知時にデフォルトで有効にしたいオプションにチェックをつけます。(**スティッキー認知**(デフォルトチェックあり)、**通知を送信**(デフォルトチェックあり)、 **永続コメント**(デフォルトチェックなし))
機密フィールドのオートコンプリート	チェックすると、機密フィールドのオートコンプリートが有効になります(デフォルト: チェックあり)。

3.1.2 「セキュリティ」タブページ

「セキュリティ」タブページでは、デフォルトのフレーム制限（frame または iframe 使用不可）を無効にすることができます（デフォルト： 制限あり）。

グラフやチャートなどをカスタム UI や Web ページで表示するようカスタマイズする場合に制限の使用有無を選択することができます。

クリックジャッキングについては以下をご参照ください：

https://www.hacksplaining.com/prevention/click-jacking
https://www.w3.org/TR/CSP2/
https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet

3.1.3 「パスワード＆アカウント」タブページ

「パスワード＆アカウント」タブページでは、アカウントロックの有無とローカルパスワード要件を設定することができます。

メモ： デフォルトでは、アカウントロックおよびパスワード要件の強制は無効に設定されています。

アカウントロック：

項目	説明
アカウントロックを有効にする	チェックを付けると、ログイン試行回数を超えてログインに失敗すると、アカウントがロックされます（デフォルト= 無効）。
ログイン試行回数	指定回数を超えてログインに失敗すると、アカウントがロックされます（デフォルト= 3）。
ロックアウト期間	アカウントはロックアウト後、指定された期間（秒）のあいだ、Nagios XI にログインすることができません（デフォルト= 300）。ロック解除を管理者が行う場合は、「0」を指定してください。

ローカルのパスワード要件:

項目	説明
要件を強制する	「パスワードの複雑さ」で指定した要件が順守されることを強制します(デフォルト= 無効)。
パスワード有効期間	指定した有効期間(日)が超過すると、パスワードの変更が要求されます(デフォルト= 90)。パスワード有効期限を無期限にしたい場合は、「0」を指定してください。
パスワードの最小文字数	指定した文字数より長いパスワードを設定するよう強制されます(デフォルト= 8)。

パスワードの複雑さ(ローカルのパスワード要件の強制を有効にした場合のみ表示されます):

項目	説明
複雑さの要件を強制する	パスワードを構成する文字(大文字、小文字、数字、特殊文字)の最小出現回数を強制します(デフォルト=無効)。
大文字の最小文字数	指定した回数以上、大文字が含まれる必要があります。
小文字の最小文字数	指定した回数以上、小文字が含まれる必要があります。
数字の最小文字数	指定した回数以上、数字が含まれる必要があります。
特殊文字の最小文字数	指定した回数以上、特殊文字が含まれる必要があります。

3.1.4 「テーマ & ディスプレイ」タブページ

「テーマ & ディスプレイ」タブページでは、システムデフォルトのユーザーインターフェースやグラフのテーマ、グラフスケールなどを指定します。

テーマ設定:

XI ユーザーインターフェースのテーマを以下から選択します。

項目	説明
XI 5 – モダン	Nagios XI 5 の新しいユーザーインターフェース
XI 2014	Nagios XI 2014 のユーザーインターフェース
クラッシック XI	Nagios XI 2012 以前のユーザーインターフェース

ディスプレイ設定:

項目	説明
Highcharts カラーテーマ	**「デフォルト(白)」**、**「クラッシック(グレー)」**のいずれかを選択できます。
パフォーマンスグラフページおよびホスト/サービス詳細ページに Highcharts を使用します	パフォーマンスグラフを Highcharts で表示する場合はチェックをつけます(デフォルト:チェックあり)

Highcharts グラフのスケール	**「リニア」、「対数」**のいずれかを選択できます。 （デフォルト：「リニア」）
Highcharts グラフのデフォルトタイプ	**「エリア（スタック）」、「エリア」、「ライン」、「スプライン」**のいずれかを選択できます（デフォルト：「ライン」）

データ設定（Highcharts）：

項目	説明
凡例を表示する	**「最新値（Last）」、「平均（Avg）」、「最大（Max）」**の表示非表示を指定できます（デフォルト=すべて有効）。
計算	平均/最大/最新値を計算するときに null 値を無視する場合は選択します（デフォルト=無効）

警告/クリティカル線の表示設定（Highcharts）：

項目	説明
表示ボタン	警告およびクリティカル線を表示するボタンの表示/非表示を指定します（デフォルト=オン　表示あり）。
自動表示	グラフの読込および描画時に警告およびクリティカル線を表示するかどうかを指定します（デフォルト=　オフ　表示なし）。

3.1.5　「ユーザデフォルト」タブページ

「ユーザデフォルト」タブページでは、システムデフォルトの表示言語、日付フォーマット、数値フォーマットを指定します。

デフォルトのユーザー設定：

項目	説明
言語	**「英語」、「チェコ語」、「ドイツ語」、「スペイン語」、「フランス語」、「イタリア語」、「日本語」、「韓国語」、「ポーランド語」、「ポルトガル語」、「ロシア語」、「中国語（簡体字）」、「中国語（繁体字）」**のいずれかを選択します。（デフォルト：**「英語」**）
日付フォーマット	**「YYYY-MM-DD　HH:MM:SS」、「MM/DD/YYY　HH:MM:SS」、「DD/MM/YYYY HH:MM:SS」**のいずれかを選択します。
数値フォーマット	**「1000.00」、「1,000.00」、「1.000,00」、「1 000,00」、「1'000,00」**のいずれかを選択します。

3.1.6　「統合」タブページ

Nagios Fusion でこの Nagios XI を監視するために必要な**「Fuse キー」**を取得できます。

3.2 プロキシ設定

Nagios XI にはアップデートの自動確認、RSS のダウンロード、コンポーネントや設定ウィザードの更新確認など、インターネットへアクセスする機能があります。インターネットアクセスにプロキシサーバーを経由する必要がある場合は、**プロキシ設定**(**「管理 -> システム設定 -> プロキシ設定」**)を行ってください。

インターネットアクセスにプロキシサーバーを介する環境の場合は、
「更新チェックのためにプロキシを有効にする」チェックボックスにチェックをつけます。

プロキシ設定:

項目	説明
プロキシアドレス	プロキシサーバーのアドレス
プロキシポート	プロキシに使用するポート
プロキシ認証	プロキシの認証情報
HTTP トンネルを使用	HTTP トンネルを使用する場合はチェックをつけます

編集が完了したら、**「設定の更新」**をクリックしてください。

3.3 ライセンス設定

ライセンス情報(**「管理 -> システム設定 -> ライセンス情報」**)ページでは、ライセンスキーの設定やライセンス統計の確認を行えます。

Nagios XI はインストールすると、60 日間無料トライアルモードで起動します。正規ライセンスをお持ちの場合は、「Nagios XI – ライセンス適用とアクティベーション」ガイドに従って、ライセンスの適用およびアクティベーションを行ってください。

Nagios XI はフリー版としても使用することができます。フリー版は無償で永続的にご利用いただけますが、監視対象ホスト数は7台に制限されます（監視対象サービス数に上限はありません）。フリー版としてご利用になりたい場合は、「フリーライセンス適用マニュアル」に従って、フリーライセンスの適用を行ってください。

ライセンスに関するお問い合わせ、更新のお申し込み等については、弊社にご依頼ください。

メモ:

- Nagios XI には Standard と Enterprise の2つのエディションがあります。Enterprise エディションは Standard エディションのすべての機能を含み、さらに追加・強化された機能を利用できます。Standard と Enterprise の機能比較については、「機能一覧」をご覧ください。
- Standard エディションは永久ライセンスです。
- Enterprise エディションは1年ごとのサポート更新が必要です。
  次年度以降 Enterprise エディションライセンスのサポート更新を行わなかった場合、Enterprise エディションの機能のみ使用できなくなります（Standard エディションの機能は使用できます）。

3.4 メール設定

メール設定管理(「**管理 -> システム設定 -> メール設定管理**」)ページでは、Nagios XI がメール送信に使用するメールサーバの設定を行います。アラート通知メールやレポートメールの送信に使用されます。

メモ: このページの設定は初期セットアップ作業時に設定済みのはずです。

注記: XI サーバに有効な DNS 名が設定されていない場合、メール送信に失敗する場合があります。

一般的なメール設定:

項目	説明
メールの送信元	メールの送信元情報
メール方法	「Sendmail」、「SMTP」のいずれかを選択します。
デバッグログ	有効にするとメールのデバッグログが保存されます(デフォルト=無効)。

SMTP 設定:

「**一般的なメール設定 -> メール方法**」で「**SMTP**」を選択した場合は以下を設定します。

項目	説明
ホスト	SMTP サーバの IP アドレスまたはホスト名
ポート	SMTP で使用するポート番号（例：25）
ユーザー名	（認証を使用する場合）ユーザー名
パスワード	（認証を使用する場合）パスワード
セキュリティ	「**なし**」、「**TLS**」、「**SSL**」のいずれかを選択します。

編集が完了したら、「**設定を更新**」をクリックしてください。

3.4.1 テストメールの送信

「**テストメールを送信**」をクリックすると、「**メール設定のテスト**」ページが開きます。このページでメール設定が正しいことをテストできます。

「**テストメールを送信**」をクリックすると、表示されたメールアドレスにメールが送信されます。

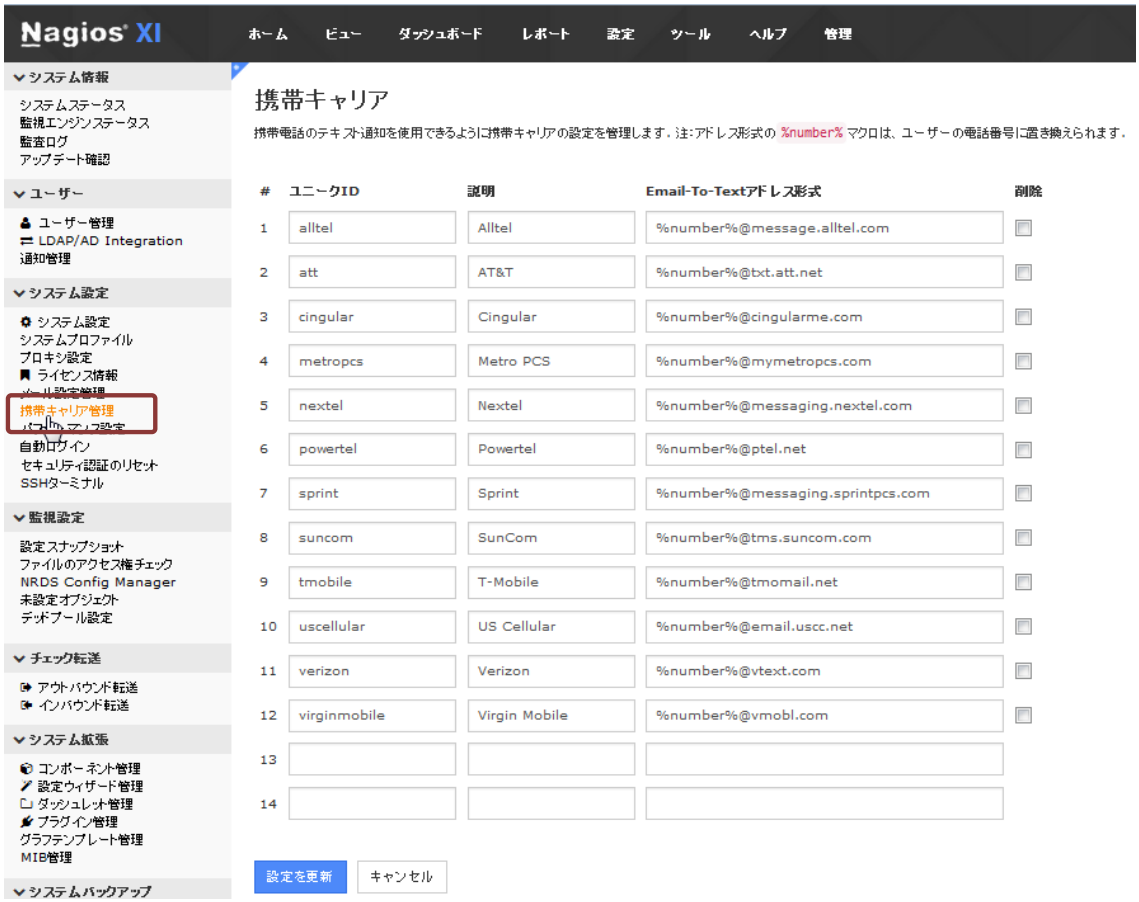
メモ： 送信先のメールアドレスを変更したい場合は、「**メールアドレスを変更する**」リンクをクリックし、アカウント情報ページでメールアドレスを変更してください。

3.5 携帯キャリア管理（SMSメール設定）

Nagios XI では、アラート通知を携帯のショートメールで受信することができます。携帯のショートメールでアラート通知を受信するには、事前に**携帯キャリア管理**（「**管理 -> システム設定 -> 携**

帯キャリア管理」）ページで携帯キャリアの登録を行う必要があります。

メモ：ユーザーが携帯のショートメールでアラート通知を受信するには、個人のアカウントの通知オプションで**「携帯テキストメッセージ」**の通知オプションを有効にしておく必要があります。「Nagios XI ユーザーガイド」または「SMS アラートの設定」をお読みください。



3.5.1 携帯キャリアの追加

携帯キャリアを追加するには、以下の情報を入力し、**「設定を更新」**をクリックします。

項目	説明
ユニーク ID	この携帯キャリアを識別するための ID
説明	この携帯キャリアの説明
Email-To-Text アドレス形式	アドレス形式（%number%は、ユーザーの電話番号に置換されます。

3.5.2 携帯キャリアの削除

不要な携帯キャリア設定を削除するには、削除したい携帯キャリアの**「削除」**チェックボックスにチェックをつけて**「設定を更新」**をクリックします。

3.5.3 デフォルト設定に戻す

携帯キャリア設定をデフォルト設定に戻したい場合は、画面下部にある**「デフォルトにもどす」**リンクをクリックして**「設定を更新」**をクリックします。

3.6 パフォーマンス設定

パフォーマンス設定(**「管理 -> システム設定 -> パフォーマンス設定」**)ページでは、Nagios XI のパフォーマンスに影響を与えるいくつかのインターフェース設定を変更できます。

パフォーマンス設定ページは、6つのタブページに分かれています。

メモ: Nagios XI システムのパフォーマンスを向上させる方法については「性能向上」もお読みください。

3.6.1 「ページ」タブページ

「ページ」タブページでは、統合画面(Ajax リクエスト)の使用有無を設定できます。Nagios XI はページの再読み込みなしでブラウザウィンドウに最新情報を表示するため、Ajax リクエスト経由でバックエンドから XML データを取り込みます。デフォルトでは Ajax ページ(統合されていない画面)が使用されていますが、Ajax コール関連の負荷を減らすため、非 Ajax ページ(統合された画面)を使用することもできます。

ページ設定:

項目	説明
統合されたタクティカル概要を使用する	チェックをつけると、**「ホーム -> タクティカル概要」**、**「ビュー -> タクティカル概要」**でNagios Core の**「Tactical Monitoring Overview」**ページが表示されます(英語)。 (デフォルト:チェックなし)
統合されたホストグループ画面を使用する	チェックをつけると、**「ホーム -> 詳細 -> ホストグループサマリ」**、**「ホーム -> 詳細 -> ホストグループ概要」**、**「ホーム -> 詳細 -> ホストグループグリッド」**で Nagios Core の**「Current Network Status」**ページが表示されます(英語)。 (デフォルト:チェックなし)
統合されたサービスグループ画面を使用する	チェックをつけると、**「ホーム -> 詳細 -> サービスグループサマリ」**、**「ホーム -> 詳細 -> サービスグループ概要」**、**「ホーム -> 詳細 -> サービスグループグリッド」**で Nagios Core の**「Current Network Status」**ページが表示されます(英語)。(デフォルト:チェックなし)

注記:

- チェックをつけると該当ページが Nagios Core の画面となります(英語表記)。
- 統合されたページのコンポーネントはダッシュレットとしてダッシュボードに追加することはできません。

3.6.2 「ダッシュレット」タブページ

「ダッシュレット」タブページでは、ダッシュレットのリフレッシュレートを変更できます。ダッシュレットは**「ダッシュレットリフレッシュマルチプライアー」**(ミリ秒)とダッシュレットの**「リフレッシュレート」**(秒)を乗算した間隔で自動更新されます。

例えばデフォルト設定の場合、**「管理タスク」**ダッシュレットの内容は 1分(1000 ミリ秒 × 60)間隔でリフレッシュされます。

リフレッシュ間隔を変更したいダッシュレットのリフレッシュレートを変更し、**「設定を更新」**をクリックしてください。

3.6.3 「データベース」タブページ

「データベース」タブページでは、各データベースにおけるデータの保持期間を指定できます。Nagios XI はユーザーに監視対象要素に関する即時性のある情報を提供したりレポートしたりするために現在および過去の情報をさまざまなデータベースに保管しています。Nagios XI データベーステーブルは時間が経過するにつれ、サイズが大きくなりすぎる可能性があります。データベースサイズが大きくなりすぎると、性能の低下、ディスクスペースやディスク I/O 使用量の増加をもたらします。データベース設定については「Nagios XI Database Optimization」をお読みください。

3.6.4 「サブシステム」タブページ

「サブシステム」タブページでは、サブシステムプロセスの有効/無効を切り替えることができます。使用しないサブシステムプロセスを無効にすることで、わずかですが CPU の使用率やディスクアクティビティを低下させることできます。

サブシステムオプション:

項目	説明
アウトバウンドデータ転送を有効にする	チェックするとアウトバウンドデータ転送が有効になります。(デフォルト: チェックなし)
未設定オブジェクトのリスナーを有効にする	チェックすると未設定オブジェクトのリッスンが有効になります。(デフォルト:チェックあり)
サブシステムのロギングを有効にする	チェックするとサブシステムのロギングが有効になります。(デフォルト:チェックあり)

3.6.5 「自動実行」タブ

「自動実行」タブページでは、**「レポート」**および**「メトリックス」**(**「ホーム -> 詳細 -> メトリック」**)で自動実行を行うかどうかを指定できます。自動実行が有効(チェックなし)の場合、各種レポートおよびメトリックページを開くと自動的にレポートおよびメトリックが表示されます。

自動実行ページパフォーマンスオプション:

項目	説明
ページロード時のレポート自動実行を無効にする	チェックするとレポートページ表示時に、レポートが実行されなくなります。(デフォルト: チェックなし)
ページロード時のメトリックスロードを無効にする	チェックするとメトリックページ表示時に、メトリック表示が実行されなくなります。(デフォルト: チェックなし)

3.6.6 「バックエンドキャッシュ」タブ

「バックエンド」タブページでは、データベースコールの一部をキャッシュするバックエンドキャッシュ機能を有効化することができます。デフォルトは無効です。

注記:

- この機能を有効にすると、リアルタイムデータではなくなります。データをリアルタイムに表示したい場合は、この機能を使用しないでください。
- 大量のホストおよび/またはサービスチェックを実行しているシステムのパフォーマンスを大幅に向上できます。
- チェック数が少ない(<1,000)システムでこの機能を有効にするとパフォーマンスに有害となるため、推奨しません。

- ホスト/サービスを頻繁に追加、削除するシステム上でこの機能を有効にすることは、推奨しません。

バックエンドキャッシュ設定:

項目	説明
バックエンドキャッシュを有効にする	バックエンドキャッシュ機能を使用する場合はチェックを付けます(デフォルト=チェックなし)。
バックエンドキャッシュの場所	バックエンドキャッシュの保存先を指定します(デフォルト=/usr/local/nagiosxi/tmp/backendcache)。apache ユーザが書込み権限を有すること。
バックエンドキャッシュの有効期間	キャッシュされる期間(秒)を指定します(デフォルト= 300)。

3.7 自動ログイン設定

自動ログイン(**「管理 -> システム設定 -> 自動ログイン」**)ページでは、自動ログイン機能の有効/無効を切り替えることができます。自動ログイン機能を有効にすると、指定したユーザーで Nagios XI Web インターフェースに自動でログインできます(ログイン画面でのユーザー、パスワードの入力が省略されます)。この機能はデフォルトでは無効となっています。

自動ログインを有効にするには、**「自動ログインを有効にする」**チェックボックスにチェックをつけてログインに使用したいアカウントをドロップダウンリストから選択します。

設定が完了したら、**「設定を更新」**をクリックします。

3.8 セキュリティ認証設定

セキュリティ認証情報(**「管理 -> システム設定 -> セキュリティ認証のリセット」**)ページでは、Nagios XI システムが使用する内部セキュリティ認証情報をリセットできます。セキュリティの観点から、Nagios XI の使用を開始する前にデフォルトのパスワードを変更してください。

メモ: このページの設定は初期セットアップ作業時に設定済みのはずです。

注記:

- **「コンポーネントの認証情報」**はシステムのさまざまな場所で使用されます。このパスワードは忘れないようにしてください。
- **「サブシステムの認証情報」**はシステムが内部的に使用します。これは記憶する必要はありません。

新しい認証情報を入力したら、**「認証情報を更新」**をクリックしてください。

3.9 チェック転送設定

Nagios XI はホストおよびサービスのチェック結果をリモートの Nagios サーバへ送信(アウトバウンド転送)したり、外部アプリケーションやリモートの Nagios サーバが実施したホストおよびサービスチェック結果を受信(インバウンド転送)したりすることができます。

3.9.1 アウトバウンド転送

アウトバウンドチェック転送設定(**「管理 -> チェック転送 -> アウトバウンド転送」**)ページでは、ホストとサービスチェックの結果をリモートの Nagios サーバに送信するための設定を行えます。

こちらをお読みください。

メモ:

- アウトバウンド転送には、NRDP や NSCA を使用できます。
- アウトバウンドチェック転送は、分散監視環境において利用されます。

3.9.2 インバウンド転送

インバウンドチェック転送設定(**「管理 -> チェック転送 -> インバウンド転送」**)ページでは、外部アプリケーション、サービス、リモートの Nagios サーバからのホストおよびサービスチェック結果を受け入れるための設定を行えます。

こちらをお読みください。

メモ:

- インバウンド転送には、NRDP や NSCA を使用できます。
- インバウンドチェック転送は、分散監視環境や外部アプリケーションおよびサービスから Nagios にデータを送信したい環境において利用されます。

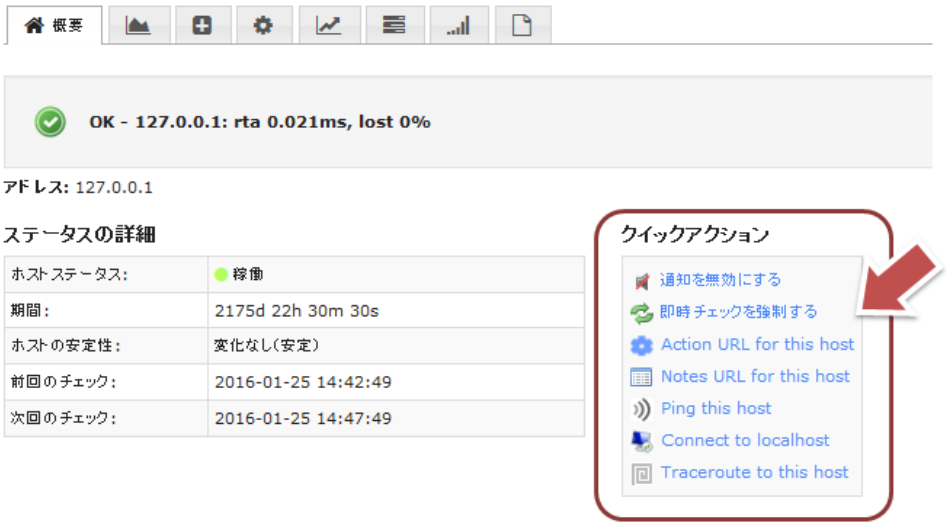
3.10 コンポーネント設定

Nagios XI には多数のコンポーネントが含まれています。コンポーネントの中には設定を変更することができるものがあります。

コンポーネントのデフォルト設定は、**コンポーネント管理**(**「管理 -> システム拡張 -> コンポーネント管理」**)ページから変更できます。設定変更が可能なコンポーネントには**設定**欄に**設定の編集**アイコンが表示されています。

3.10.1 カスタムアクションの設定

アクションコンポーネント(**「管理 -> システム拡張 -> コンポーネント管理 -> アクション」**)をカスタマイズすることで、**「ホストステータス詳細」**または**「サービスステータス詳細」**の**「概要」**タブページにある**「クイックアクション」**セクションにカスタムアクションを追加できます。



「ホストステータス詳細」または**「サービスステータス詳細」**ページに特定のタスクにアクセスするためのカスタムリンクを追加したい場合に使用してください。詳しくは、「Actions Component」をお読みください。

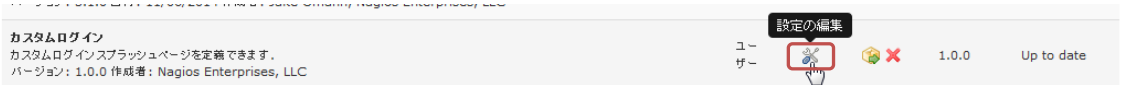
3.10.2 カスタムログインページの設定(カスタムログイン)

カスタムログインコンポーネント(**「管理 -> システム拡張 -> コンポーネント管理 -> カスタムログイン」**)をカスタマイズすることで、ログイン時のスプラッシュページ(下図の赤枠部分)をカスタマイズすることができます。

変更手順は以下のとおりです:

Step 1. **「管理 -> システム拡張 -> コンポーネント管理」**を選択して、**「コンポーネントの管理」**ページを開きます。

Step 2. **カスタムログイン**コンポーネントの**「設定を編集」**アイコンをクリックします。



Step 3. **「カスタムログインスプラッシュを有効にする」**チェックボックスにチェックをつけます。

Step 4. **「インクルードファイル」**フィールドにログインページで使用するインクルードファイルへのパスを入力します。

Step 5. **「設定を適用」**をクリックします。

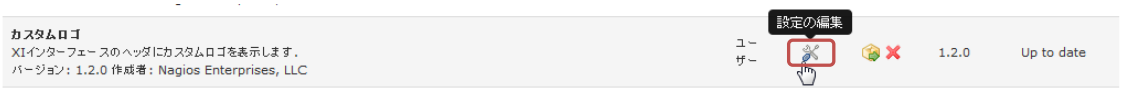
3.10.3 カスタムロゴ設定

カスタムロゴコンポーネント(**「管理 -> システム拡張 -> コンポーネント管理 -> カスタムロゴ」**)をカスタマイズすることで、Nagios XI Web インターフェースの画面左上に表示されるロゴイメージ(デフォルトは Nagios XI ロゴ)を変更できます。

ロゴを変更する手順は以下のとおりです:

Step 1. **「管理 -> システム拡張 -> コンポーネント管理」**を選択して、**「コンポーネントの管理」**ページを開きます。

Step 2. **カスタムロゴ**コンポーネントの**「設定を編集」**アイコンをクリックします。



Step 3. **「カスタムロゴを有効にする」**チェックボックスにチェックをつけます。

Step 4. **「ロゴ画像」**フィールドに使用したいロゴ画像ファイル名を入力します。

メモ: ロゴファイルは、`/usr/local/nagiosxi/html/images/`に保存してください。ファイルサイズは `100px X 42px` としてください。

Step 5. **「ロゴテキスト」**フィールドにマウスオーバー時に表示させたいテキストを入力します。

Step 6. **「ロゴターゲット」**フィールドにロゴクリック時のターゲット(新しいタブを開く場合は `_blank`、同一フレームに開く場合は `_top`)を入力します。

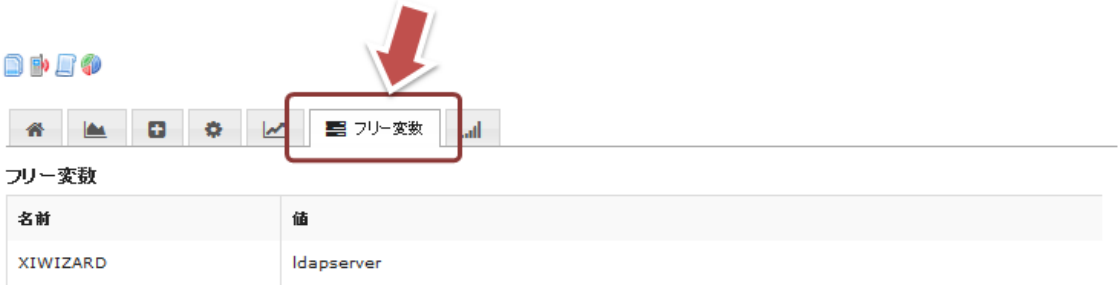
Step 7. **「ターゲット URL」**フィールドにロゴクリック時に開く Web ページの URL を入力します。

Step 8. **「設定を適用」**をクリックします。

メモ: 変更を確認するには、ブラウザ全体を一度リフレッシュさせてください。

3.10.4 フリー変数タブの追加

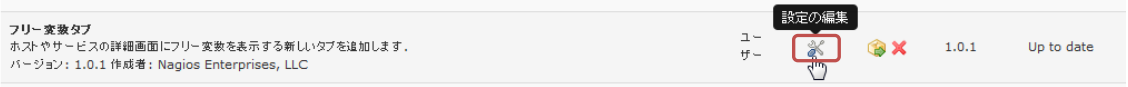
フリー変数タブコンポーネント(**「管理 -> システム拡張 -> コンポーネント管理 -> フリー変数タブ」**)をカスタマイズすることで、**「ホストステータス詳細」**および**「サービスステータス詳細」**ページに**「フリー変数」**タブを追加することができます。



フリー変数タブを追加する手順は以下のとおりです:

Step 1. **「管理 -> システム拡張 -> コンポーネント管理」**を選択して、**「コンポーネントの管理」**ページを開きます。

Step 2. **フリー変数タブ**コンポーネントの**「設定を編集」**アイコンをクリックします。



Step 3. **「設定を適用」**をクリックします。

メモ: 現在のバージョン(1.0.1)には、フリー変数タブを除去する機能がありません。

3.10.5 グローバルイベントハンドラの設定

グローバルイベントハンドラコンポーネント(**「管理 -> システム拡張 -> コンポーネント管理 -> グローバルイベントハンドラ」**)をカスタマイズすることで、ホストやサービスのステータス変化や通知が発生したときに、Nagios XI サーバ上で指定したコマンドをローカル実行させることができます。

グローバルイベントハンドラを使用すれば、カスタム開発したスクリプトを実行することができます。詳しくは、「グローバルイベントハンドラの設定」をお読みください。

メモ: イベントハンドラについては、「イベントハンドラの紹介」をお読みください。

3.10.6 ホームページのカスタマイズ

ホームページ変更コンポーネント(**「管理 -> システム拡張 -> コンポーネント管理 -> ホームページ変更」**)をカスタマイズすることで、ログイン直後に表示される**ホーム**ページを変更できます。

Nagios XI Web インターフェースにログインした直後に表示されるホームページ(ランディングページ)をカスタマイズしたい場合は、「ランディングページのカスタマイズ」をお読みください。

3.10.7 MultiTech iSMSの統合利用

Multi-Tech iSMS 統合コンポーネント(**「管理 -> システム拡張 -> コンポーネント管理 -> Multi-Tech iSMS 統合」**)から、Multi-Tech iSMS との統合設定を行えます。

詳しくは「MultiTech iSMS Integration With Nagios XI」をお読みください。

3.10.8 Nagios Incident Managerの統合利用

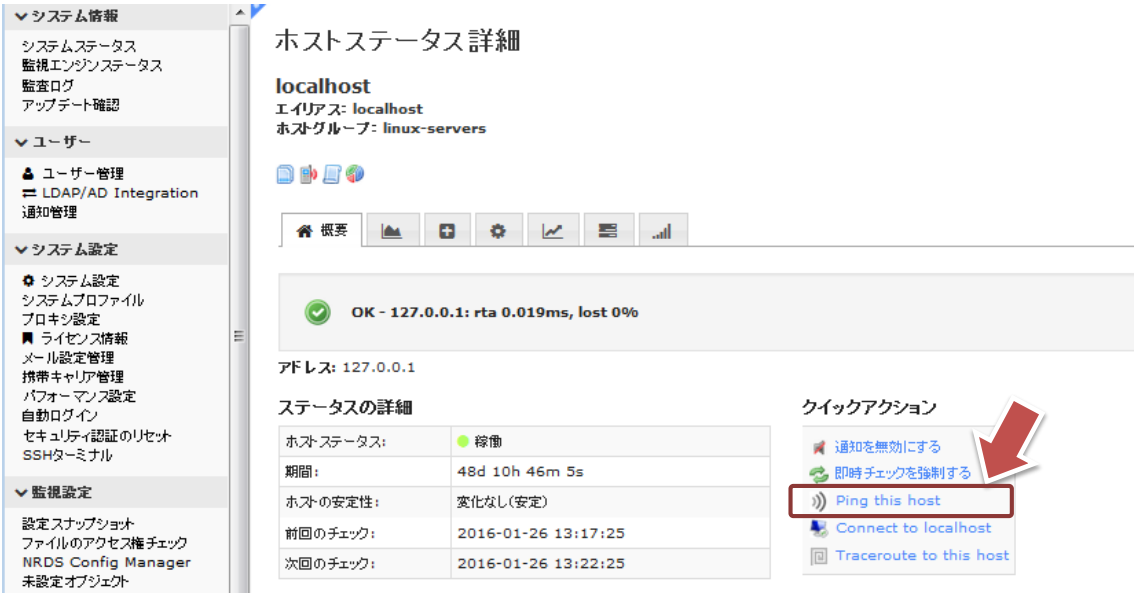
Nagios IM 統合コンポーネント(**「管理 -> システム拡張 -> コンポーネント管理 -> Nagios IM 統合」**)から、Nagios Incident Manager との統合設定を行えます。

詳しくは「How To Integrate Incident Manager With Nagios XI」をお読みください。

3.10.9 Pingアクション設定(Ping Action)

Ping Action コンポーネント(**「管理 -> システム拡張 -> コンポーネント管理 -> Ping Action」**)から、**「ホストステータス詳細 -> 概要」**タブページにある**「クイックアクション」**セクションの Ping アクションへのリンクの表示/非表示を切り替えることができます。

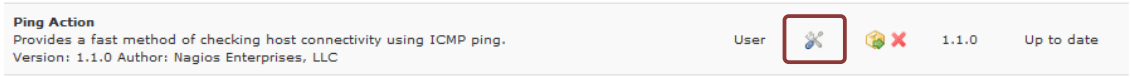
メモ:デフォルトは有効です(Ping アクションリンクが表示されます)。



Ping アクションの表示非表示を切り替える手順は以下のとおりです:

Step 1. **「管理 -> システム拡張 -> コンポーネント管理」**を選択して、**「コンポーネントの管理」**ページを開きます。

Step 2. **Pinig Action** コンポーネントの**「設定を編集」**アイコンをクリックします。



Step 3. Ping アクションを表示したい場合はチェックボックスにチェックをつけます。
Ping アクションを非表示にしたい場合はチェックを外します。

Step 4. **「設定を適用」**をクリックします。

3.10.10 RDP/VNC接続設定

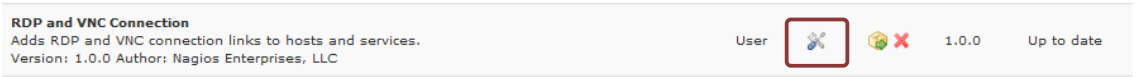
RDP および VNC 接続コンポーネント(**「管理 -> システム拡張 -> コンポーネント管理 -> RDP および VNC 接続」**)から、**「ホストステータス詳細 -> 概要」**タブページにある**「クイックアクション」**セクションの接続(**Connect to**)アクションへのリンクの表示/非表示を切り替えることができます。

メモ:デフォルトは有効です(**Connect to** アクションリンクが表示されます)。

Connect to アクションの表示非表示を切り替える手順は以下のとおりです:

Step 1. **「管理 -> システム拡張 -> コンポーネント管理」**を選択して、**「コンポーネントの管理」**ページを開きます。

Step 2. **RDP および VNC 接続**コンポーネントの**「設定を編集」**アイコンをクリックします。



Step 3. **Connect to** アクションを表示したい場合はチェックボックスにチェックをつけます。
Connect to アクションを非表示にしたい場合はチェックを外します。

Step 4. **「設定を適用」**をクリックします。

3.10.11 SNMPTrap送信設定(SNMP Trap Sender)

SNMP Trap Sender コンポーネント(**「管理 -> システム拡張 -> コンポーネント管理 -> SNMP Trap Sender」**)では、ホストまたはサービスの状態が変化(アラートが発生)したときに、Nagios XI から他の管理ホストまたはネットワーク管理システムに SNMP Trap を送信するように設定できます。

詳しくは、「SNMP トラップ送信」をお読みください

3.10.12 Traceroute**アクション設定**

Traceroute アクションコンポーネント(**「管理 -> システム拡張 -> コンポーネント管理 -> Traceroute アクション」**)から、**「ホストステータス詳細 -> 概要」**タブページにある**「クイックアクション」**セクションの Traceroute アクションへのリンクの表示/非表示を切り替えることができます。

メモ:デフォルトは有効です(**Traceroute** アクションリンクが表示されます)。

Traceroute アクションの表示非表示を切り替える手順は以下のとおりです:

Step 1. **「管理 -> システム拡張 -> コンポーネント管理」**を選択して、**「コンポーネントの管理」**ページを開きます。

Step 2. **Traceroute アクション**コンポーネントの**「設定を編集」**アイコンをクリックします。

Step 3. Traceroute アクションを表示したい場合はチェックボックスにチェックをつけます。
Traceroute アクションを非表示にしたい場合はチェックを外します。

Step 4. **「設定を適用」**をクリックします。

3.10.13 カスタムインクルード

カスタムインクルードコンポーネント(**「管理 -> システム拡張 -> コンポーネント管理 -> カスタムインクルード」**)では、Nagios XI システムにファイルをアップロードすることができます。

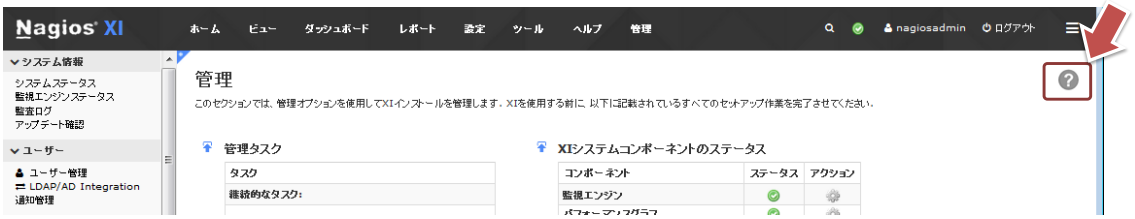
アップロード可能なファイル種類は以下のとおりです:

```
.css, .js, .png, .jpg, .jpeg, .gif, and .bmp
```

詳しくは、ナレッジベース「Using The Custom Includes Component」をお読みください。

3.10.14 ヘルプシステム設定

デフォルト設定の場合、Nagios XI Web インターフェースの各ページには**ヘルプ**アイコンが表示されています。この**ヘルプ**アイコンをクリックすると、現在開いているページに関するヘルプ情報(ビデオ、技術文書)へのリンクが表示されます(リンク先情報は英語です)。



ヘルプシステムコンポーネント(**「管理 -> システム拡張 -> コンポーネント管理 -> ヘルプシステム」**)では、**ヘルプ**アイコンの表示/非表示を切り替えることができます。

メモ: デフォルトは有効です(**ヘルプ**アイコンが表示されます)。

ヘルプアイコンの表示非表示を切り替える手順は以下のとおりです:

Step 1. **「管理 -> システム拡張 -> コンポーネント管理」**を選択して、**「コンポーネントの管理」**ページを開きます。

Step 2. **ヘルプシステム**コンポーネントの**「設定を編集」**アイコンをクリックします。

Step 3. ヘルプアイコンを表示したい場合は、**「ヘルプシステムを有効にする」**チェックボックスにチェックをつけます。ヘルプアイコンを非表示にしたい場合は、チェックを外します。(デフォルト: チェックなし)

Step 4. ユーザーにヘルプアイコンの表示非表示の変更を許可する場合は、**「ユーザーによるヘルプ設定の上書きを許可する」**チェックボックスにチェックをつけます。許可しない場合は、チェックを外します。(デフォルト:チェックあり)

メモ: チェックされている場合、ユーザーは**「マイアカウント -> ヘルプシステム」**メニューからヘルプシステムの表示設定を変更できます。

Step 5. **「設定を適用」**をクリックします。

3.10.15 LDAP/Active Directoryの統合利用(LDAP / Active Directory Integration)

Nagios XI ではログイン時のユーザー認証に Windows Active Directory 認証を使用することもできます。

LDAP / Active Directory Integration コンポーネント(**「管理 -> システム拡張 -> コンポーネント管理 -> LDAP / Active Directory Integration」**)では、認証に使用するサーバおよび証明書の管理を行えます。

メモ: このページへは**「管理 -> ユーザー -> LDAP/AD Integration」**からもアクセスできます。

詳しくは、「Authenticating with Active Directory in Nagios XI」をお読みください。

3.10.16 Nagios BPI

Nagios BPI コンポーネント(**「管理 -> システム拡張 -> コンポーネント管理 -> Nagios BPI」**)では、BPI(Nagios Business Process Intelligence)に関する設定を行えます。

メモ: このページへは**「ホーム -> BPI -> BPI 設定の編集」**からもアクセスできます。

詳しくは、「Using Nagios BPI」をお読みください。

3.10.17 Nagios Network Analyzerの統合利用

Nagios Network Analyzer Integration コンポーネント(**「管理 -> システム拡張 -> コンポーネント管理 -> Nagios Network Analyzer Integration」**)では、お使いの Nagios Network Analyzer との統合設定を行えます。

メモ: ご利用いただくには、Nagios Network Analyzer が必要です。

詳しくは、「Nagios Network Analyzer - Nagios XI / Nagios Core との統合」をお読みください。

3.10.18 Userマクロ

User マクロコンポーネント(**「管理 -> システム拡張 -> コンポーネント管理 -> User マクロ」**)では、System および User マクロの検出、作成、表示を制御することができます。

詳しくは、「User マクロコンポーネントについて」をお読みください。

4　ユーザー管理

Nagios XI のユーザー管理は**「管理 -> ユーザー」**下のメニューから行います。

4.1　ユーザーの作成と編集/ユーザー権限の理解

新規ユーザーの作成および既存ユーザーの編集方法、ユーザー権限の管理については、以下の資料をお読みください。

Nagios XI ユーザーの作成・編集/ユーザー権限

4.2　ユーザーと連絡先

Nagios XI の「ユーザー」と Nagios Core の「連絡先」の関係や「ユーザー」の追加方法についてより深く理解したい場合は、以下の資料をお読みください。

Nagios XI ユーザーと Nagios Core 連絡先

メモ: Nagios Core の管理経験がある、または Nagios Core を Nagios XI に移行したい Nagios 管理者向けの資料です。

4.3　連絡先グループ

連絡先グループを作成すれば、Nagios Core の連絡先を論理的なグループ（例: 部署別、チーム別）に分けて管理することができます。連絡先グループの作成手順については、以下の資料の**「連絡先グループの定義」**をお読みください。

Nagios XI におけるマルチテナント

4.4　マルチテナント

マルチテナント（単一の Nagios XI インスタンスで複数のユーザーやグループまたはクライアントのインフラを監視したい）環境で使用する場合は、以下の資料をお読みください。

Nagios XI におけるマルチテナント

4.5 LDAP/AD統合

LDAP/Active Directory サーバから Nagios XI にログインするユーザーをインポートすることができます。以下の資料をお読みください。

Authenticating with Active Directory in Nagios XI

4.6 通知管理

Enterprise エディションの場合は、**通知管理**(「**管理** -> **ユーザー** -> **通知管理**」)ページで、ユーザーの通知設定を行うことができます。「一括通知管理」をお読みください。

5 監視設定

Nagios XI では Web ユーザーインターフェース上で監視設定を行うことができます。監視登録は、設定ウィザードの利用、Core コンフィグマネージャでの手動設定、設定ファイルのインポート(Nagios Core からの移行)により行うことができます。

5.1 設定ウィザード

Nagios XI には監視登録作業をガイドする設定ウィザードが多数登録されています(**「設定 -> 設定ウィザード」**)。設定ウィザードを使用すれば、新しいデバイス、サービス、アプリケーションの監視を簡単に開始できます。

組込済みのウィザードは以下のとおりです(XI 5.4.x):

ウィザード	内容
自動検出	自動検出ジョブで検出したサーバ、デバイス、サービスを監視します
BPI ウィザード	Nagios BPI グループのサービスチェックを作成します
ホストのクローンとインポート	既存のホストのクローンを素早く簡単に作成します。登録済みの監視設定と同等の監視設定を複数ホストに対して一括登録したい場合に便利です。
DHCP	DHCP サーバを監視します。
DNS Query	DNS lookup/query を介してホストまたはドメイン名を監視します。
ドメインの有効期限	ドメインの有効期限を監視します
メール配信	メールサーバの受信とシミュレートされたユーザーのメールメッセージを検査します。SMTP サーバにメールを送信し、IMAP フォルダのメールを受信してチェックします。
Esensors Websensor	Esensors Websensor で温度、湿度、照度を監視します

Exchange Server	Microsoft® Exchange サーバを監視します。 サービスステータス、プロトコル可用性、パフォーマンスメトリクスを監視します。(この監視には Windows エージェントインストールが必要です。)
フォルダウォッチ	数、サイズ、経過をクエリできる Perl 駆動の正規表現でディレクトリやファイルを監視します(対象サーバ:Linux/Unix サーバ。 監視には SSH を使用します。)
FTP Server	FTP サーバにログインしファイル転送機能を監視します
一般的なネットワーク機器	一般的な IP ネットワーク機器を監視します(ICMP ping を使用してデバイスを監視します)。
LDAP サーバ	LDAP サーバを監視します。
Linux サーバ	リモートの Linux サーバを監視します。(この監視には Linux エージェントインストールが必要です。)
Linux SNMP	SNMP を使用して Linux サーバやワークステーションを監視します
Mac OS X	Mac OS X マシンを監視します
メールサーバ	メールサーバを監視します SMTP, IMAP, POP の可用性, RBL ブラックリストチェックを行います。
MongoDB データベース	MongoDB データベースの監視
MongoDB サーバ	MongoDBL サーバを監視します
マウントポイント	NFS、CIFS、DAVFS マウントポイントを監視します (サポート対象:nfs, nfs4, davfs, cifs, fuse, simfs, glusterfs, ocfs2, lustre)
MSSQL データベース	MSSQL データベースを監視します
MSSQL クエリ	MSSQL データベースクエリを監視します
MSSQL サーバ	MSSQL サーバを監視します
MySQL Query	MySQL データベースクエリを監視します
MySQL サーバ	MySQL サーバを監視します
Nagios Log Server	Nagios Log Server で収集されたログをクエリを実行して監視します
Nagiostats ウィザード	XI サーバの内部パフォーマンスを監視します
Nagios XI サーバ	リモート Nagios XI サーバを監視します
NCPA	NCPA エージェントの監視
Nagios Network Analyzer	Nagios Network Analyzer サーバ上のソース、ビュー、ソースグループを監視します
NRPE	NRPE を使用してリモートの Linux/Unix サーバを監視します.
Oracle Query	Oracle クエリを監視します。(Oracle プラグインのインストールが必要です)
Oracle Serverspace	Oracle サーバを監視します。(Oracle プラグインのインストールが必要です)
Oracle 表領域	Oracle の表領域を監視します。(Oracle プラグインのインストールが必要です)

パッシブチェック	パッシブサービスチェックとセキュリティ警告などのイベントを監視します
Postgres データベース	Postgres データベースを監視します。 接続ステータス、データベースサイズ、テーブルサイズ、リレーションサイズを監視します。
Postgres クエリ	Postgres データベースクエリを監視します
Postgres サーバ	Postgres サーバを監視します
プリンター	HP JetDirect® 互換のネットワークプリンターを監視します
RADIUS サーバ	RADIUS サーバを監視します
SLA	サービス品質保証（SLA）が満たされていることを確認するために、SLA を監視します
SNMP	SNMP を使用して、デバイス、サービス、アプリケーションを監視します
SNMP トラップ	SNMP トラップを監視します
SNMP ウォーク	監視するために SNMP 有効デバイスをスキャンします
Solaris	Solaris サーバを監視します。（この監視には Solaris エージェントのインストールが必要です）
SSH プロキシ	SSH を使用してリモートの Linux、UNIX、または Mac OS/X マシンを監視します
ネットワークスイッチ/ルータ	ネットワークスイッチまたはルータを監視します。 スイッチまたはルータのポートステータスおよび帯域使用量を監視できます。サービス追加についてはこちらをお読みください。
TCP/UDP ポート	標準のネットワークポートおよびカスタムの TCP/UDP ポートを監視します。
TFTP	TFTP サーバの接続または特定のファイルを監視します
VMware	VMware ホストまたはゲスト VM を監視します
WatchGuard	WatchGuard デバイスを監視します
Web サイト	Web サイトの監視
Web サイト改ざん	改ざん検出のため Web サイトを監視します
Web サイト URL	特定の Web URL を監視します
Web トランザクション	synthentic Web トランザクションを監視します
Windows デスクトップ	Microsoft® Windows XP, Windows Vista, Windows 7,8,10 のデスクトップを監視します。（この監視には Windows エージェントのインストールが必要です）
~~Windows イベントログ~~	~~Windows のイベントログを監視します。~~ （Windows イベントログの監視には Nagios Log Server のご利用を推奨いたします。）
Windows サーバ	Microsoft® Windows 2000, 2003, 2008, 2012 サーバを監視します。（この監視には Windows エージェントのインストールが必要です）
Windows SNMP	SNMP を使用して、Microsoft® Windows ワークステーションまたはサーバを監視します。

Windows WMI	WMI を使用して、Microsoft® Windows ワークステーションまたはサーバを監視します

さらに、Nagios Exchange Web サイトから追加のウィザードを入手し、Nagios XI に追加することもできます。追加ウィザードのインストールに関する情報については、「Nagios XI 設定ウィザードのインストール」を参照してください。

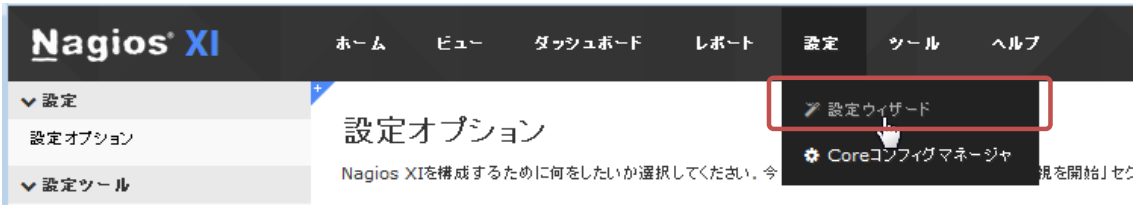
メモ: 使用したい設定ウィザードが存在しない場合や設定ウィザードに監視したい項目が存在しない場合は、Core コンフィグマネージャを使用して監視登録を行うことができます。Core コンフィグマネージャについては、「Core コンフィグマネージャ」をご参照ください。

5.1.1 設定ウィザードを使用して新しい監視を登録する

ここでは、設定ウィザードの一般的な使用方法を説明します。

メモ: 例として **「Web サイト監視」**ウィザードの使用手順を紹介します。

Step 1. **「設定 -> 設定ウィザード」** を選択します。



> **メモ**: プライマリメニューが折りたたまれている場合は**「設定」> 「今すぐ監視を開始」**をクリックしてください。

Step 2. ウィザードを選択画面で使用したい設定ウィザードをクリックします。

メモ:

- **「表示」**セクションの**「検索」**ボックスで設定ウィザード名の一部を入力すると、該当する設定ウィザードのみが画面に表示されます。

- アイコンをクリックすることで、関連する設定ウィザードのみを表示させることもできます。

Step 3. ウィザードの指示に従って情報を入力します。

メモ: ウィザードで問われる項目は使用する設定ウィザードによって異なります。例えば**「Web サイト」**ウィザードは監視対象サイトの URL をたずねます。

Step 4. **次へ**をクリックします。

Step 5. 監視するサービスを指定します。

メモ: ウィザードで指定できる項目は使用する設定ウィザードによって異なります。

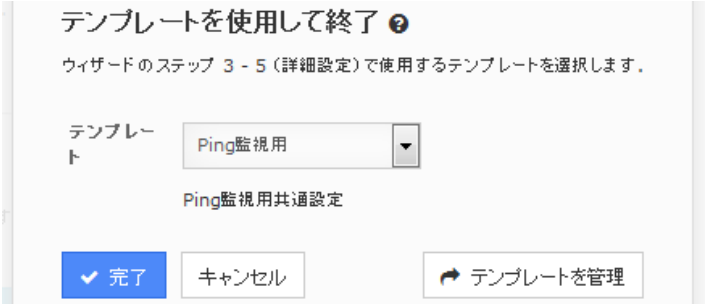
メモ: 既に監視登録済みのホストに対してサービスを追加したい場合は、登録済みのホスト名と同じ名前を**「ホスト名」**に指定してください。IP アドレスが既存であっても、ホスト名が異なる場合、別ホストとして登録されます。

監視したい項目のチェックボックスにチェックをつけます。
監視が不要な項目のチェックボックスのチェックを外します。

メモ: 使用する設定ウィザードにより、表示項目が異なります。

Step 6. **次へ**または**テンプレートで終了**をクリックします。

メモ: **テンプレートで終了**を選択した場合は、**「テンプレートを指定して終了」**画面で使用したいテンプレートを選択して、**完了**をクリックします。



（以降は、**「次へ」**を選択した場合の手順です。）

Step 7. ホストおよびサービスの監視間隔を指定します。

メモ： デフォルトの監視間隔は5分です。障害が検知された場合は、1分おきに5回確認します。

Step 8. **次へ**をクリックします。

Step 9. 障害発生時の通知方法および通知先を指定します。

障害が検出された場合の通知方法について以下から選択します。

- **「通知を送信しない」**: 通知は送信されません
- **「通知をすぐに送信する」**:
  アラート通知が指定した通知先にすぐに送信されます（デフォルト）。
- **「通知を送信する前に X 分待機する」**:
  アラート通知が指定した通知先に X 分経過後に送信されます。

障害が解決しない場合の通知間隔を指定します（デフォルトは 60 分間隔）。

アラート通知の送信先を指定します。この設定ウィザードを実行したユーザーはデフォルトでアラート通知の送信先に指定されます。特定の連絡先や連絡先グループを指定したい場合は、チェックボックスにチェックをつけます。

連絡先に指定されたユーザーや連絡先グループに所属するユーザーは、この設定ウィザードで登録されたホスト、サービスを閲覧できるようになります。

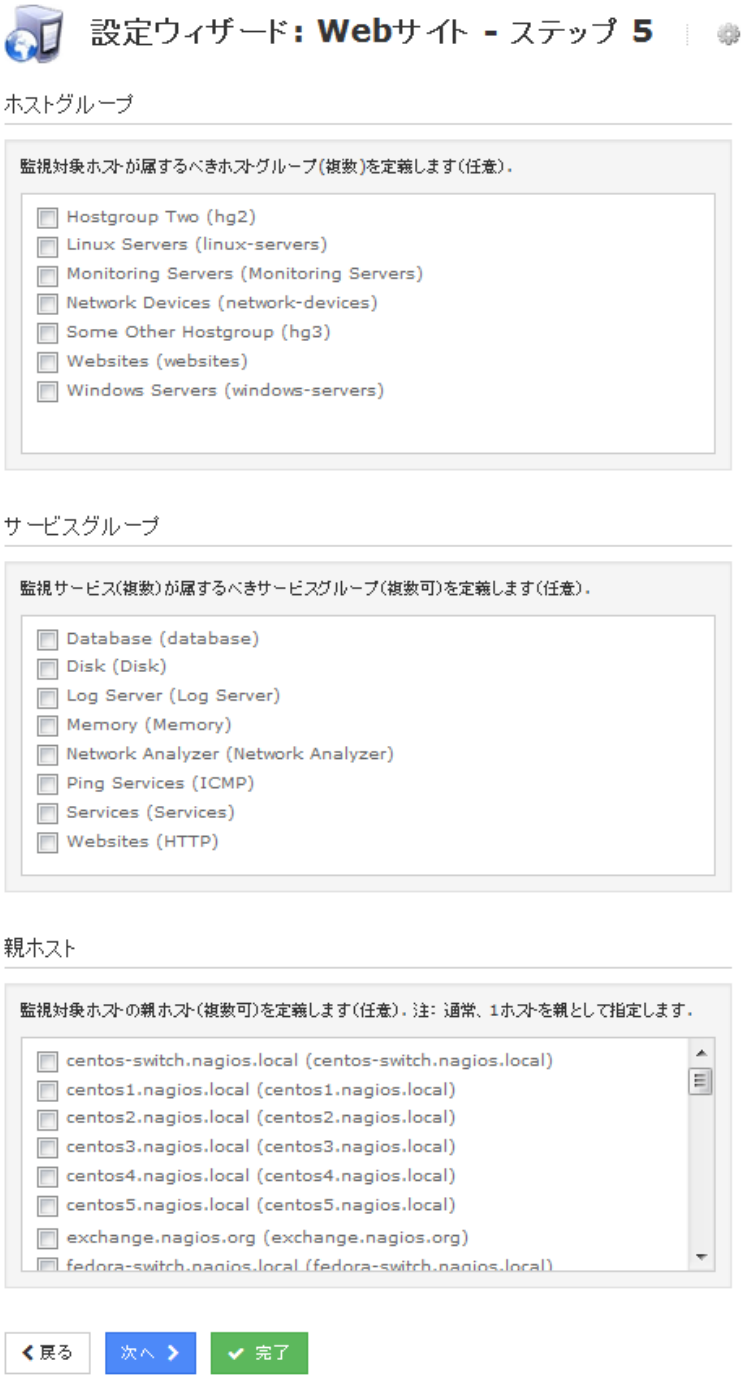
メモ:

- **「その他の個別連絡先」**欄には、Nagios Core の連絡先が表示されます。Nagios Core の連絡先は**「管理 -> ユーザー -> ユーザー管理 -> 新規ユーザーの追加」**で**「監視の連絡先を作成する」**にチェックをつけて Nagios XI ユーザーを作成すると自動的に作成されます。連絡先については、「ユーザーと連絡先」をご参照ください。

- **「特定の連絡先グループ」**欄には、既存の連絡先グループが表示されます。事前に連絡先グループを作成しておく必要があります。連絡先グループについては、「連絡先グループ」をご参照ください。

Step 10. **次へ**をクリックします。

Step 11. 所属させるホストグループ、サービスグループ、親ホストを指定します。



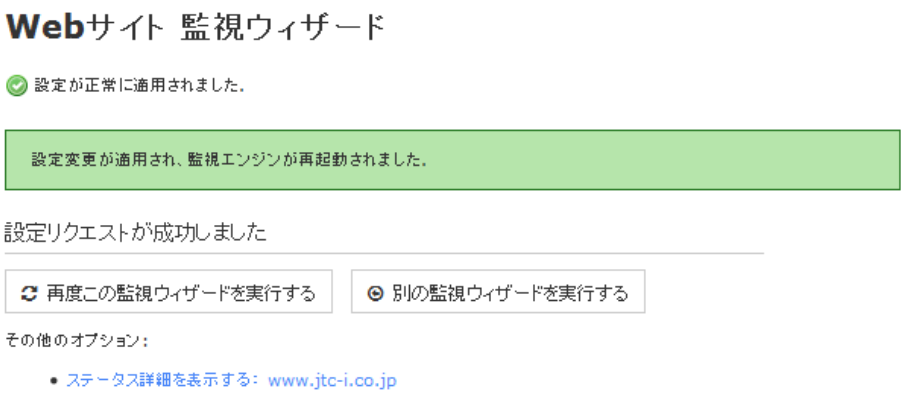
メモ:

- **「ホストグループ」**欄には既存のホストグループが表示されます。ホストグループについては、「ホスト管理」をご参照ください。
- **「サービスグループ」**欄には既存のサービスグループが表示されます。サービスグループについては、「サービス管理」をご参照ください。

Step 12. **次へ**をクリックします。

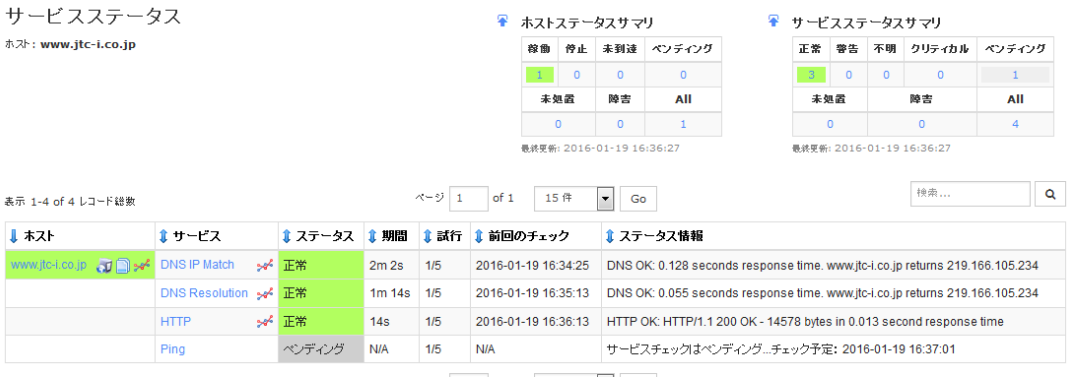
Step 13. **適用**ボタンをクリックします。

Step 14. 設定が正常に適用されたことを確認します。



メモ:

- 適用すると、自動的に設定スナップショットが作成されます。設定内容に問題があるなど処理が正常に完了しなかった場合は、設定の適用がキャンセルされます（前回の設定スナップショットの状態のままとなります）。適用に失敗した場合はエラーメッセージを確認し、修正したうえで再度設定をやり直してください。
- 設定ウィザードの設定 で**「設定を適用しない」**が選択されていた場合は、監視エンジンは再起動されません（監視設定自体はデータベースに登録されましたが、実際の監視は開始しません）。
- **「ステータス詳細を表示する」**リンクをクリックすると、サービスステータスページに登録した監視項目が表示されます。



5.1.2 設定テンプレートを使用する

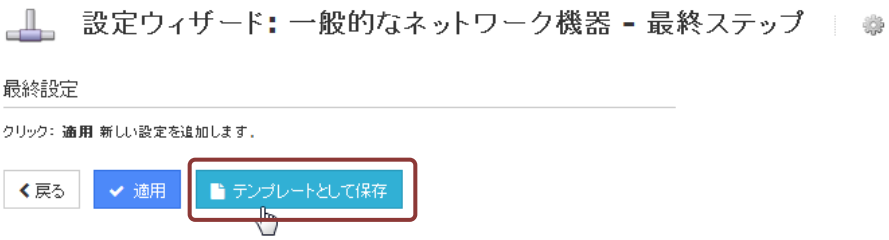
設定テンプレートを作成することで、監視設定、通知設定、グループ設定、親ホスト設定をテンプレート化することができます。「ステップ3」以降の設定内容が共通する場合に便利です

5.1.2.1 設定テンプレートを作成する

設定テンプレートの作成手順は以下のとおりです:

Step 1. 「設定ウィザードを使用して新しい監視を登録する」の「Step 12」までの作業を行います。

Step 2. 最終ステップで**テンプレートとして保存**をクリックします。



Step 3. **テンプレートとして保存**画面で識別のための**タイトル**と**説明**を入力します。

Step 4. **保存**をクリックします。

5.1.2.2 設定テンプレートを編集する

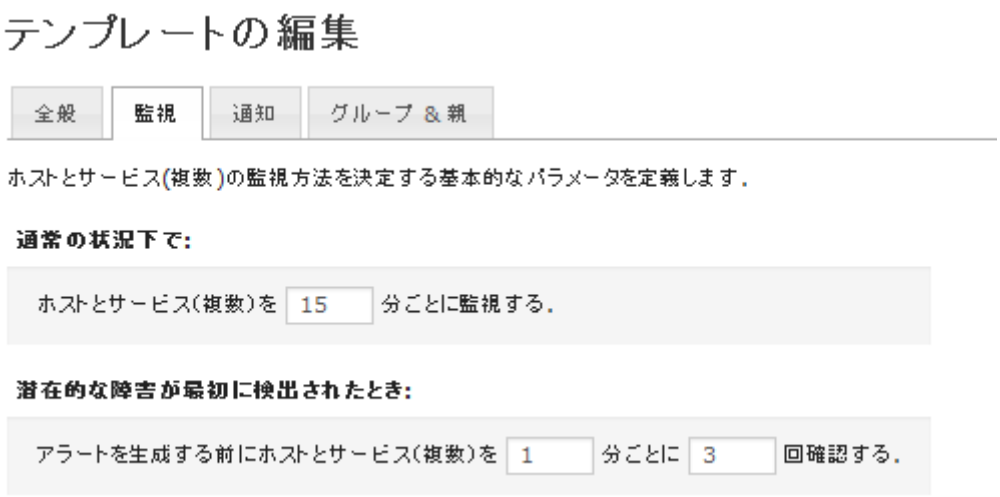
既存の設定テンプレートを編集する手順は以下のとおりです:

Step 1. **設定** > **設定ツール** > **テンプレートを管理**を選択します。

Step 2. 編集したいテンプレートの**編集** アイコンをクリックします。

Step 3. テンプレートを編集します。

メモ: タブごとに設定項目が分かれて表示されます。



Step 4. **変更を保存**をクリックします。

5.1.2.3 設定テンプレートを削除する

既存の設定テンプレートを削除する手順は以下のとおりです:

Step 1. **設定** > **設定ツール** > **テンプレートを管理**を選択します。

Step 2. 削除したいテンプレートの**削除** アイコンをクリックします。

または、チェックボックスにチェックをつけて画面下部のリストから**「削除」**を選択します

Step 3. 確認画面で **OK** をクリックします。

5.1.3 Linux

設定ウィザード － ウィザードを選択(**「設定 -> 設定ウィザード」**)ページで、**Linux**  アイコンをクリックすると、Linux 監視に関連するウィザードのみが表示されます。

以下の設定ウィザードへのリンクが表示されます:

フォルダウォッチ	Linux サーバ	Linux SNMP	マウントポイント
NCPA	NRPE	SSH プロキシ監視	

注記: ご利用のバージョンによって項目が異なる可能性があります。

5.1.3.1 フォルダウォッチ

フォルダウォッチウィザードでは、SSH でリモートホストに接続し、指定した正規表現クエリに合致するディレクトリのファイル数、ファイル経過時間、ファイルサイズを監視できます。

注記: リモートホストにパスワードなしで SSH ログインできない場合、このウィザードは正しく機能しません。

5.1.3.2 Linux サーバ

Linux サーバウィザードでは、NRPE エージェントがインストールされた Linux サーバに対して以下のメトリックを簡単に監視登録することができます。

監視項目	説明
Ping	ICMP ping を使用してサーバを監視します。 ネットワークの遅延と稼働時間を見るために便利です。
yum update ステータス	RPM パッケージが最新かどうかを監視します。
ロード	サーバの負荷(1, 5, 15 分の値)を監視します。

CPU 統計	サーバ CPU 統計情報を監視します（% user, system, iowait, and idle）
メモリ使用	サーバのメモリ使用量を監視します。
スワップ使用	サーバのスワップ使用量を監視します。
オープンファイル	サーバで開いているファイル数を監視します。
ユーザー	サーバに現在ログインしているユーザー数を監視します。
プロセス数	サーバで実行中のプロセス総数を監視します。
ディスク使用	サーバのディスク使用量を監視します。 パスには、マウントポイントまたはパーティション名を指定します。
サービス	稼動状態を確認するために監視するサービスを指定します。 通常 init プロセスによって開始されます。
プロセス	稼動を確認するために監視すべきプロセスを指定します。

NRPE エージェントのインストール手順については、「Linux エージェントのインストール」をお読みください。

5.1.3.3 Linux SNMP

Linux SNMP ウィザードでは、SNMP を使用して Linux サーバのメトリックを監視登録することができます。

監視項目	説明
Ping	ICMP ping でマシンを監視します。 ネットワークの遅延と稼働時間を見るために便利です。
CPU	マシンの CPU(CPU 使用率)を監視します。
物理メモリ使用	マシンの物理（実）メモリ使用を監視します。メモリバッファありにするにはチェックボックスのチェックをはずしてください。
スワップ使用	マシンのスワップ使用状況を監視します。
ディスク使用	マシンのディスク使用量を監視します。
プロセス	稼働確認のために監視が必要なプロセスを指定します。プロセス名は大文字と小文字が区別されます。

詳しくは、「SNMP での Linux 監視」をお読みください。

5.1.3.4 マウントポイント

マウントポイントウィザードでは、指定したマウントポイントが存在するか、正しく実装されているかを監視できます。次のマウントポイントタイプがサポートされます: `nfs, nfs4, davfs, cifs, fuse, simfs, glusterfs, ocfs2, lustre`

5.1.3.5 NCPA

NCPA ウィザードでは、NCPA エージェントがインストールされたサーバに対して以下のメトリックを簡単に監視登録することができます。

監視項目	説明
CPU 使用	システムの CPU 使用を監視します。
メインメモリ使用	システムのメインメモリを監視します。
スワップ使用	システムで使用された割当てスワップの割合を監視します。
ディスク使用	ディスク容量の警告およびクリティカルの割合を指定します。
ネットワークインターフェース	ネットワークインターフェースの帯域使用量を監視します。(単位: MB)
サービス	稼動状態を確認するために監視するサービスを指定します。
プロセス	稼働確認のために監視が必要なプロセスを指定します。プロセス名は大文字と小文字が区別されます。

詳しくは、「How To Monitor Devices Using The NCPA Agent and Wizard」をお読みください。

5.1.3.6 NRPE

NRPE ウィザードでは、NRPE エージェントがインストールされたサーバを簡単に監視登録することができます。

監視項目	説明
Ping	ICMP ping でマシンを監視します。 ネットワークの遅延と稼働時間を見るために便利です。
Current Users	check_users リモートコマンドでサーバに現在ログインしているユーザー数を監視します。
Current Load	check_load リモートコマンドでサーバの負荷を監視します。
Total Processes	check_total_procs リモートコマンドで実行中のプロセス総数を監視します。

上記に加えて実行したいリモートコマンドを独自に追加することができます。詳しくは「NRPE でのホスト監視」をお読みください。

5.1.3.7 SSH プロキシ監視

SSHプロキシウィザードでは、SSH を使用してリモートのサーバを監視する設定を簡単に登録することができます。

監視項目	説明
Ping	ICMP ping でマシンを監視します。 ネットワークの遅延と稼働時間を見るために便利です。
Root Disk Space	check_disk リモートコマンドで root ディスク容量を監視します。
Current Users	check_users リモートコマンドでサーバに現在ログインしているユーザー数を監視します。(デフォルト引数: -w 5 –c 10)。
Total Processes	check_procs リモートコマンドで実行中のプロセス総数を監視します。(デフォルト引数: -w 150 -c 170)。

上記に加えて実行したいリモートコマンドを独自に追加することができます。詳しくは「SSH でのホスト監視」をお読みください。

5.1.4 Windows

設定ウィザード － ウィザードを選択（**「設定 -> 設定ウィザード」**）ページで、**Windows** アイコンをクリックすると、Windows 監視に関連するウィザードのみが表示されます。

以下の設定ウィザードへのリンクが表示されます：

Exchange Server	MSSQL データベース	MSSQL クエリ	MSSQL サーバ
NCPA	NRPE	Windows デスクトップ	Windows サーバ
Windows SNMP	Windows WMI		

注記：ご利用のバージョンによって項目が異なる可能性があります。

5.1.4.1 Exchange Server

Exchange Server ウィザードでは、Windows エージェントがインストールされた Windows Exchange サーバに対して以下のメトリックを簡単に監視登録することができます。

基本サービス：

監視項目	説明
Ping	ICMP ping を使用してサーバを監視します。 ネットワークの遅延と稼働時間を見るために便利です。
SMTP	SMTP サービスが利用可能であることを監視します。
IMAP	IMAP サービスが利用可能であることを監視します。
POP	POP サービスが利用可能であることを監視します。
RBL ブラックリストチェック	メールサーバが公開 RBL（リアルタイムブラックリスト）にリストされているかどうかをチェックします。

OWA HTTP	HTTP 経由で Outlook Web Access の可用性を監視します。
OWA HTTPS	HTTPS（SSL で保護）経由で Outlook Web Access の可用性を監視します。

Exchange サービス：

監視項目	説明
Core サービス	Exchange に不可欠な core サービス（以下で指定）が稼動していることをチェックします。 MSExchangeADTopology,MSExchangeAntispamUpdate,MSExchangeEdgeSync,MSExchangeFDS,MSExchangeImap4,MSExchangeIS,MSExchangeMailboxAssistants,MSExchangeMailSubmission,MSExchangeMonangePop3,MSExchangeRepl,MSExchangeSA,MSExchangeSearch,MSExchangeServiceHost,MSExchangeTransport,MSExchangeTransportLogSearch,msftesql-Exchange
Web サービス	Exchange に不可欠な Web サービス（以下で指定）が稼動していることをチェックします。 W3SVC

メモ： 上記項目の監視には Windows エージェントのインストールが必要です。

Exchange のメトリック：

監視項目	説明
Messages Pending Routing	ルーティングがペンディング状態の SMTP メッセージ数を監視します。（デフォルト引数： w 25 c 100）
Remote Queue Length	リモート配信用の SMTP キュー内のメッセージの総数を監視します。（デフォルト引数： w 25 c 50）

メモ： 上記項目の監視には Windows エージェントのインストールが必要です。

Windows エージェントのインストール手順については、「Windows エージェント（NSClient++）のインストール」をお読みください。

5.1.4.2 MSSQL データベース

MSSQL データベースウィザードでは、MSSQL データベースに対して以下のメトリックを簡単に監視登録することができます。

監視項目	説明
接続時間	データベース接続にかかる時間を監視します。
データベースサイズ	データベースサイズを監視します。

ログファイル使用	使用中のログファイルを監視します。
オープン接続	現在オープンしている接続数を監視します。
1 秒当たりのトランザクション	1 秒当たりのトランザクション数を監視します。
ログキャッシュヒット率	ログキャッシュヒット率を監視します。
Log Wait	小さいログバッファに起因するログ待機を監視します。
Log Growth	不適切なパーティションサイズに起因するログの拡張を監視します。
Log Shrink	不適切なパーティションサイズに起因するログ圧縮を監視します。
Log Truncation	不正な形式のテーブルに起因するログ切り捨てを監視します。
Log Flush Wait Time	ログがフラッシュされるまでの合計待ち時間を監視します。

5.1.4.3 MSSQL クエリ

MSSQL クエリウィザードでは、指定した MSSQL クエリに対して予想される結果が戻されるかを簡単に監視登録することができます。結果が数値の場合は、閾値を指定できます。

5.1.4.4 MSSQL サーバ

MSSQL サーバウィザードでは、MSSQL サーバに対して以下のメトリックを簡単に監視登録することができます。

監視項目	説明
接続時間	サーバへの接続に要する時間を監視します。
バッファヒット率	バッファヒット率を監視します。
ページ検索	1 秒あたりのページルック数を検索します。
空き容量(Free Pages)	空き容量(Free Pages)を監視します。
Target Pages	ターゲットページ(Target Pages)数を監視します。
Database Pages	データベースのページ数を監視します。
Stolen Pages	Stolen Pages 数を監視します。
Lazy Writes	レイジーライターにより書き込まれたバッファーの 1 秒あたりの数を監視します。
先行読取り	使用を見越して読み取られた 1 秒あたりのページ数を監視します。
Page Reads	物理的なデータベースページ読み取りが実行される 1 秒あたりの回数を監視します。
チェックページ	ディスクにフラッシュされた 1 秒あたりのページ数を監視します。
Page Writes	データベースページ書き込みが実行される 1 秒あたりの回数を監視します。
Lock Requests	1 秒あたりに要求された新しいロック数を監視します。
Lock Timeouts	1 秒あたりにタイムアウトしたロック要求の数を監視します。
Deadlocks	デッドロックが発生した 1 秒あたりのロック要求の数を監視します。

Lock Waits	1 秒あたりのロック要求の数を監視します。
Page Splits	1 秒あたりのページ分割の数を監視します。
Lock Wait Time	ロックの総待機時間を監視します。
Average Wait Time	実行の平均待ち時間を監視します。

5.1.4.5 NCPA

NCPA エージェントウィザードでは、NCPA エージェントがインストールされた Windows サーバに対して以下のメトリックを簡単に監視登録することができます。

監視項目	説明
CPU 使用	システムの CPU 使用を監視します。
メインメモリ使用	システムのメインメモリを監視します。
スワップ使用	システムで使用された割当てスワップの割合を監視します。
ディスク使用	ディスク容量の警告およびクリティカルの割合を指定します。
ネットワークインターフェース	ネットワークインターフェースの帯域使用量を監視します。(単位: MB)
サービス	稼動状態を確認するために監視するサービスを指定します。
プロセス	稼働確認のために監視が必要なプロセスを指定します。プロセス名は大文字と小文字が区別されます。

詳しくは、「How To Monitor Devices Using The NCPA Agent and Wizard」をお読みください。

5.1.4.6 NRPE

NRPE ウィザードでは、NRPE エージェントがインストールされた Windows サーバを簡単に監視登録することができます。

監視項目	説明
Ping	ICMP ping でマシンを監視します。 ネットワークの遅延と稼働時間を見るために便利です。
Current Users	check_users リモートコマンドでサーバに現在ログインしているユーザー数を監視します。
Current Load	check_load リモートコマンドでサーバの負荷を監視します。
Total Processes	check_total_procs リモートコマンドで実行中のプロセス総数を監視します。

上記に加えて実行したいリモートコマンドを独自に追加することができます。詳しくは「NRPE でのホスト監視」をお読みください。

5.1.4.7 Windows デスクトップ

Windows デスクトップウィザードでは、Windows エージェントがインストールされた Windows デスクトップマシンに対して以下のメトリックを簡単に監視登録することができます。

監視項目	説明
Ping	ICMP ping でマシンを監視します。 ネットワークの遅延と稼働時間を見るために便利です。
CPU	マシンの CPU 使用率を監視します。
メモリ使用	マシンのメモリ使用量を監視します。
Uptime	マシンの稼働時間を監視します。
ディスク使用	マシンのディスク使用量を監視します。

Windows エージェントのインストール手順については、「Windows エージェント(NSClient++)のインストール」をお読みください。

5.1.4.8 Windows サーバ

Windows サーバウィザードでは、Windows エージェントがインストールされた Windows サーバに対して以下のメトリックを簡単に監視登録することができます。

監視項目	説明
Ping	ICMP ping を使用してサーバを監視します。 ネットワークの遅延や稼働時間を見るために便利です。
CPU	サーバの CPU 使用率を監視します。
メモリ使用	サーバのメモリ使用量を監視します。
Uptime	サーバの稼働時間を監視します。
ディスク使用	サーバのディスク使用量を監視します。
サービス	指定されたサービスの稼働を監視します。
プロセス	指定されたプロセスの稼動を監視します。
パフォーマンスカウンタ	指定されたパフォーマンスカウンタを監視します。

Windows エージェントのインストール手順については、「Windows エージェント(NSClient++)のインストール」をお読みください。

5.1.4.9 Windows SNMP

Windows SNMP ウィザードでは、SNMP を使用して Windows マシンのメトリックを監視登録することができます。

監視項目	説明
Ping	ICMP ping でマシンを監視します。 ネットワークの遅延や稼働時間を見るために便利です。
CPU	マシンの CPU 使用率を監視します。
物理メモリ使用	マシンの物理(実)メモリの使用状況を監視します。
仮想メモリ使用	マシン上の仮想メモリの使用状況を監視します。
ディスク使用	マシンのディスク使用量を監視します。

サービス	指定されたサービスの稼働を監視します。
プロセス	指定されたプロセスの稼動を監視します。

5.1.4.10 Windows WMI

Windows WMI ウィザードでは、WMI（Windows Management Instrumentation）を使用して Windows マシンのメトリックを監視登録することができます。

監視項目	説明
Ping	ICMP ping でマシンを監視します。 ネットワークの遅延や稼働時間を見るために便利です。
CPU	マシンの CPU 使用率を監視します。
メモリ使用	マシンのメモリ使用量を監視します。
ページファイル使用	マシンのページファイルの使用状況を監視します。
ディスク使用	マシンのディスク使用量を監視します。
サービス	指定されたサービスの稼働を監視します。
プロセス	指定されたプロセスの稼動を監視します。
イベントログ	指定されたベントログの発生回数を監視します。

詳しくは、「Monitoring Windows With WMI」をお読みください。

5.1.5 その他のOS

設定ウィザード － ウィザードを選択（**「設定 -> 設定ウィザード」**）ページで、**その他の OS** アイコンをクリックすると、Linux/Windows 以外の OS 監視に関連するウィザードが表示されます。

以下の設定ウィザードへのリンクが表示されます：

フォルダウォッチ	Mac OSX 監視	マウントポイント	NCPA
NRPE	Solaris	SSH プロキシ	

注記：ご利用のバージョンによって項目が異なる可能性があります。

5.1.5.1 フォルダウォッチ

こちらをお読みください。

5.1.5.2 Mac OSX 監視

Mac OSX ウィザードでは、NRPE エージェントがインストールされた Mac OSX サーバに対して以下のメトリックを簡単に監視登録することができます。

監視項目	説明
Ping	ICMP ping でマシンを監視します。 ネットワークの遅延や通常の稼働時間を監視するために役立ちます。
ロード	サーバの負荷(1/5/15 分の値)を監視します。
CPU 統計	サーバの CPU 統計 (% user, system, idle)を監視します。
メモリ使用	サーバのメモリ使用量を監視します。
ユーザー	サーバに現在ログインしているユーザー数を監視します。
プロセス数	サーバで実行中のプロセス総数を監視します。
ディスク使用	サーバのディスク使用量を監視します。 パスには、マウントポイントまたはパーティション名を指定します。
プロセス	指定されたプロセスの稼動を監視します。

NRPE エージェントのインストール手順については、「Installing the XI Mac OSX Agent」をお読みください。

5.1.5.3 マウントポイント

こちらをお読みください。

5.1.5.4 NCPA

こちらをお読みください。

5.1.5.5 NRPE

こちらをお読みください。

5.1.5.6 Solaris

Solaris ウィザードでは、NRPE エージェントがインストールされた Solaris 10 サーバに対して以下のメトリックを簡単に監視登録することができます。

監視項目	説明
Ping	ICMP ping でサーバを監視します。 ネットワークの遅延や通常の稼働時間を監視するために役立ちます。
ロード	サーバの負荷(1, 5, 15 分の値)を監視します。
CPU 統計	サーバの CPU 統計 (user, system, iowait %s)を監視します。
メモリ使用	サーバの空きメモリを監視します。
スワップ使用	サーバのスワップ使用量を監視します。
オープンファイル	サーバで開いているファイル数を監視します。
ユーザー	サーバに現在ログインしているユーザー数を監視します。
プロセス数	サーバで実行中のプロセス総数を監視します。
ディスク使用	サーバのディスク使用量を監視します。 パスには、マウントポイントまたはパーティション名を指定します。
サービス	指定されたサービスの稼働を監視します。
プロセス	指定されたプロセスの稼動を監視します。

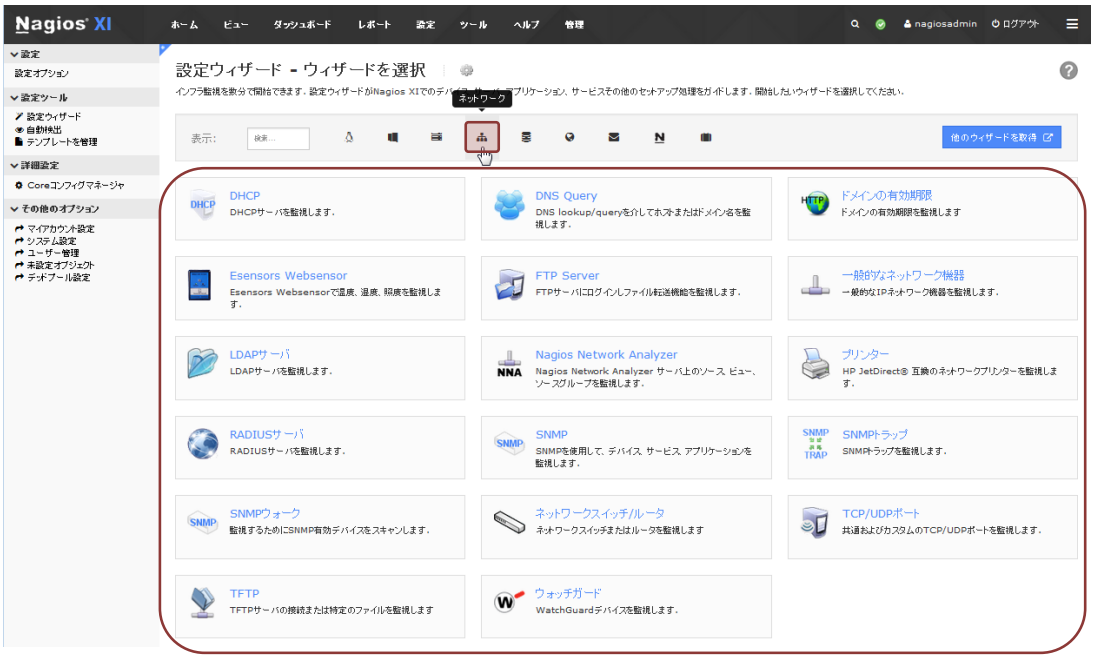
NRPE エージェントのインストール手順については、「Installing The XI Solaris Agent」をお読みください。

5.1.5.7 SSH プロキシ

こちらをお読みください。

5.1.6 ネットワーク

設定ウィザード - ウィザードを選択(**「設定 -> 設定ウィザード」**)ページで、**ネットワーク** アイコンをクリックすると、ネットワーク監視に関連するウィザードが表示されます。



以下の設定ウィザードへのリンクが表示されます：

DHCP	DNS Query	ドメイン有効期限
Esensors Websensor	FTP Server	一般的なネットワーク機器
LDAP サーバ	Nagios Network Analyzer	プリンター
RADIUS サーバ	SNMP	SNMP トラップ
SNMP ウォーク	ネットワークスイッチ/ルータ	TCP/UDP ポート
TFTP	WatchGuard	

5.1.6.1 DHCP

DHCP ウィザードでは、ネットワーク上で DHCP サーバが利用可能かどうか（DHCP リクエストを送信し、応答が正しいかどうか）を簡単に監視登録することができます。

5.1.6.2 DNS Query

DHCP Query ウィザードでは、DNS ルックアップでドメイン名から IP アドレスを解決できるか、解決された IP アドレスが期待通りの結果であるかを簡単に監視登録することができます。

5.1.6.3 ドメイン有効期限

ドメイン有効期限ウィザードでは、指定した日数が残っているかを簡単に監視登録することができます。

5.1.6.4 Esensors Websensor

Esensors Websensor ウィザードでは、温度、湿度、光源レベルなどの環境条件を簡単に監視登録することができます。詳しくは、「Monitoring A Websensor EM08」をお読みください。

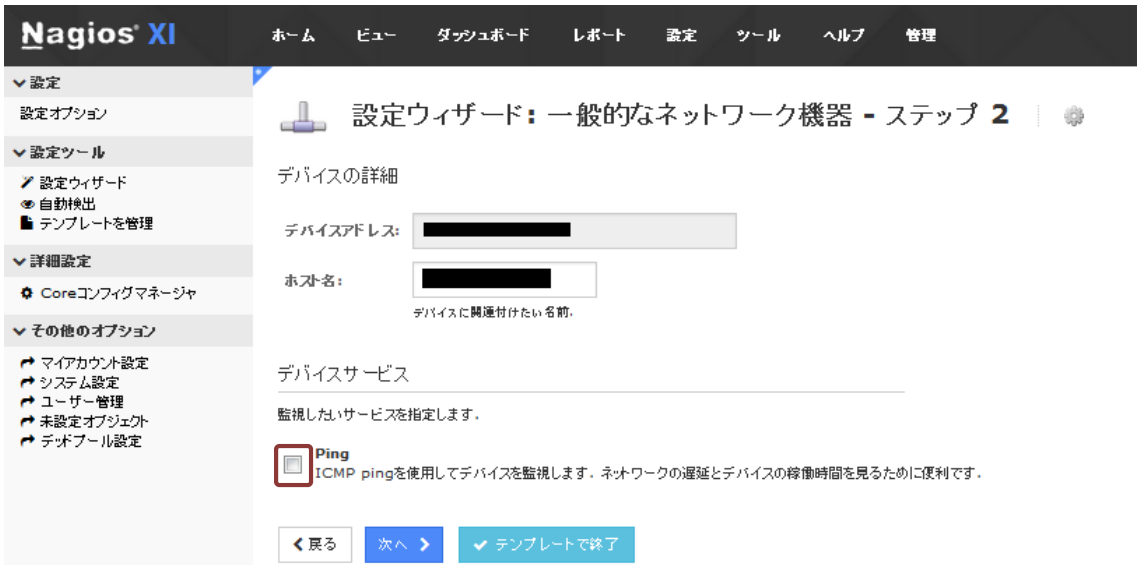
5.1.6.5 FTP Server

FTP Server ウィザードでは、FTP サーバにログインし、ファイル転送が可能かを簡単に監視登録することができます。

5.1.6.6 一般的なネットワーク機器

一般的なネットワーク機器ウィザードでは、ネットワーク機器の死活監視(ping 監視)を簡単に登録することができます。

メモ: デフォルトでは **Ping** チェックボックスにチェックがついていますが、このホスト監視にすでに Ping 監視を実施している(またはこのウィザードで新規にホストの監視登録を行う)場合、この IP アドレスに対して Ping 監視が2つ登録されてしまいます(ホスト監視と Ping サービス監視で2つ)。新規ホストの登録の場合やすでに Ping 監視で既存ホストを監視している場合は、重複を避けるため、**Ping** チェックボックスのチェックを外してください。



5.1.6.7 LDAP サーバ

LDAP サーバウィザードでは、LDAP サーバが利用可能かどうか(LDAP サーバにバインドできるか)を簡単に監視登録することができます。

メモ: Active Directory を LDAP で監視する方法については、「Monitor Active Directory with LDAP」をお読みください。

5.1.6.8 Nagios Network Analyzer

Nagios Network Analyzer ウィザードでは、統合設定済みの Nagios Network Analyzer サーバ上のソース、ビュー、ソースグループを簡単に監視登録することができます。Nagios Network Analyzer の統合設定手順については、「Nagios Network Analyzer – Nagios XI / Nagios Core との統合」をお読みください。

5.1.6.9 プリンター

プリンターウィザードでは、HP JetDirect®互換のネットワークプリンターが利用可能かどうかを簡単に監視登録することができます。

5.1.6.10 RADIUS サーバ

RADIUS サーバウィザードでは、RADIUS サーバが利用可能かどうか（RADIUS サーバ認証に成功するか）を簡単に監視登録することができます。

5.1.6.11 SNMP

SNMP ウィザードでは、OID を指定して監視登録することができます。

5.1.6.12 SNMP トラップ

SNMP トラップウィザードでは、SNMP トラップ受信監視を登録することができます。SNMP トラップ受信による監視を行いたい場合は、「Nagios XI での SNMP トラップ統合」をお読みください。

5.1.6.13 SNMP ウォーク

SNMP ウォークウィザードでは、SNMP ウォークを実施して監視を登録することができます。

5.1.6.14 ネットワークスイッチ/ルータ

ネットワークスイッチ/ルータウィザードでは、死活（Ping）、インターフェースステータス、MRTG によるインターフェース帯域使用量の監視を登録することができます。

すでに登録済みのスイッチまたはルータにインターフェースの帯域監視を追加する場合は、「既存スイッチまたはルータへのサービス追加」をお読みください。

メモ: デフォルトでは「ステップ 2」ページの **Ping** チェックボックスにチェックがついていますが、このホスト監視にすでに Ping 監視を実施している（またはこのウィザードで新規にホストの監視登録を行う）場合、この IP アドレスに対して Ping 監視が2つ登録されてしまいます（ホスト監視と Ping サービス監視で2つ）。新規ホストの登録の場合やすでに Ping 監視で既存ホストを監視している場合は、重複を避けるため、**Ping** チェックボックスのチェックを外してください。

注記:

- このウィザードで帯域幅監視登録を行うと自動で MRTG のコンフィグファイルが生成されますが、このコンフィグファイルには管理ダウン以外のすべてのインターフェースが記載されてしまい、5分ごとに全ポートに対する情報取得が実行されてしまいます。MRTG での情報収集が不要なインターフェースについては、お手数ですが `/etc/mrtg/conf.d/<IP アドレス>.cfg` から定義を削除してください。または、`/usr/bin/cfgmaker` コマンドを適切なフィルタ条件つきで手動実行してください。(詳しくは、cfgmaker マニュアルをご参照ください。) 上記の動作については開発元へ改善依頼中です(対応時期は不明です)。
- Nagios XI Web インターフェース上で帯域使用監視サービス(xxx Bandwidth サービス)を削除しても上記 MRTG のコンフィグファイルは自動削除されない仕様となっており、手動でコンフィグファイルを削除しない限りいつまでもMRTGによる情報収集が継続することとなってしまっています。帯域使用量の監視が不要となったインターフェースについては Nagios XI Web インターフェース上で該当サービスを削除していただいたあと、`/etc/mrtg/conf.d/<IP アドレス>.cfg` を手動で削除してください。上記の動作については開発元へ改善依頼中です(対応時期は不明です)。
- Nagios XI 2014 以前のバージョンをお使いの場合、既に帯域使用監視のためのサービスが登録済み(MRTG のコンフィグファイルが存在する)の機器について別のインターフェースの帯域使用監視を追加登録したい場合は、事前に MRTG のコンフィグファイル(`/etc/mrtg/conf.d/<IP アドレス>.cfg`)を手動削除してからこのウィザードを実行してください。詳しくは「既存スイッチまたはルータへのサービス追加」をお読みください。

5.1.6.15 TCP/UDP ポート

TCP/UDP ポートウィザードでは、指定ポートが利用可能であるかを簡単に監視登録することができます。

5.1.6.16 TFTP

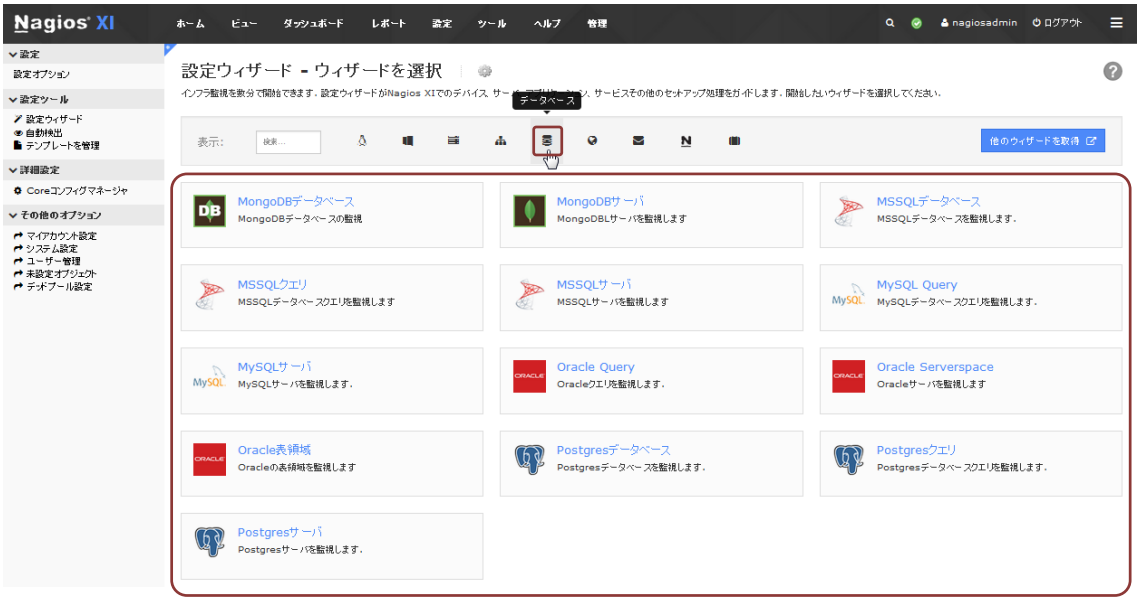
TFTP ウィザードでは、TFTP サーバへ接続可能か、指定したファイルが存在するかを簡単に監視登録することができます

5.1.6.17 WatchGuard

WatchGuard ウィザードでは、WatchGuard を簡単に監視登録することができます。詳しくは「WatchGuard Wizard Usage」をお読みください。

5.1.7 データベース

設定ウィザード - ウィザードを選択(**「設定 -> 設定ウィザード」**)ページで、**データベース** アイコンをクリックすると、ネットワーク監視に関連するウィザードが表示されます。



以下の設定ウィザードへのリンクが表示されます:

MongoDB データベース	MongoDB サーバ	MSSQL データベース
MSSQL クエリ	MSSQL	MySQL Query
MySQL サーバ	Oracle Query	Oracle Serverspace
Oracle 表領域	Postgres データベース	Postgres クエリ
Postgres サーバ		

5.1.7.1 MongoDB データベース

MongoDB データベースウィザードでは、MongoDB データベースに対して以下のメトリックを簡単に監視登録することができます。詳しくは、「Monitoring a MongoDB Database」をお読みください。

監視項目	説明
コレクション数	データベース内のコレクション数を監視します。
オブジェクト数	データベース内のオブジェクト(ドキュメント)数を監視します。
データベースサイズ	データベースサイズ(バイト)を監視します。

5.1.7.2 MongoDB サーバ

MongoDB サーバウィザードでは、MongoDB データベースに対して以下のメトリックを簡単に監視登録することができます。詳しくは、「Monitoring a MongoDB Server」をお読みください。

監視項目	説明
接続確認	ホストへの接続を監視します。
空き接続	利用可能な空き接続の割合を監視します。
メモリ使用	MongoDB サーバのメモリ使用量を監視します。
Mapped メモリ使用	MongoDB サーバの mapped メモリの使用状況を監視します。
ロック時間パーセント	MongoDB サーバがロックされた時間の割合を監視します。
平均フラッシュタイム	フラッシュ実行にかかる平均時間を監視します。
前回フラッシュ時間	前回のフラッシュからの経過時間を監視します。
インデックスミス率	インデックスヒットのミス率を監視します。
データベース数	データベースの数を監視します。
コレクション数	コレクションの数を監視します。
1 秒あたりのクエリ数	1 秒あたりのクエリ数を監視します。
レプリケーションステータス	レプリケーションのステータスを監視します。 このチェックは、警告/クリティカルの引数を必要としません。
レプリケーション遅延	サーバのレプリケーション遅延を監視します。 遅延していない場合でも、このチェックは 10 秒以下の遅延を示す可能性があります。
レプリケーション遅延(%)	サーバのレプリケーション遅延(%)を監視します。

5.1.7.3 MSSQL データベース

こちらをお読みください。

5.1.7.4 MSSQL クエリ

こちらをお読みください。

5.1.7.5 MSSQL サーバ

こちらをお読みください。

5.1.7.6 MySQL Query

MySQL Query ウィザードでは、指定した MySQL クエリ結果が閾値内かどうかを簡単に監視登録することができます。

5.1.7.7 MySQL サーバ

MySQL サーバウィザードでは、MySQL サーバに対して以下のメトリックを簡単に監視登録することができます。

監視項目	説明
接続時間	サーバへの接続に要する時間を監視します。
Uptime	MySQL サーバが稼動している時間を監視します。
オープン接続	現在オープンしている接続数を監視します。
Thread Cache Hitrate	スレッドキャッシュのヒット率を監視します。
Query Cache Hitrate	クエリキャッシュのヒット率を監視します。
MyISAM Key Cache Hitrate	MyISAM Key キャッシュのヒット率を監視します。
InnoDB Buffer Pool Hitrate	InnoDB Buffer Pool のヒット率を監視します。
Log Wait	小さいログバッファに起因する InnoDB ログ待機を監視します。
Table Cache Hitrate	テーブルキャッシュのヒット率を監視します。
Index Usage	インデックスの使用を監視します。
Slow Queries	遅いクエリの数を監視します。
Long Running Processes	長い稼働プロセスの数を監視します。
Slave I/O	MySQL slave I/O が稼働していることをチェックします。
Slave SQL	MySQL slave SQL が稼動していることをチェックします。
Slave Lag	slave が master 遅延時間を監視します。

5.1.7.8 Oracle Query

注記: Oracle の監視を開始する前に Nagios XI サーバに Oracle プラグインをインストール、設定してください。手順については「Oracle Plugin Installation Instructions」をお読みください。

Oracle Query ウィザードでは、指定した Oracle クエリ結果が閾値内かどうかを簡単に監視登録することができます。

5.1.7.9 Oracle Serverspace

注記: Oracle の監視を開始する前に Nagios XI サーバに Oracle プラグインをインストール、設定してください。手順については「Oracle Plugin Installation Instructions」をお読みください。

Oracle Servrspace ウィザードでは、Oracle サーバに対して以下のメトリックを簡単に監視登録することができます。

監視項目	説明
接続時間	Oracle サーバとの接続にかかる時間を監視します。
接続ユーザー	接続しているユーザーの数を監視します。
SGA データバッファヒット率	SGA データバッファを監視します。
SGA ライブラリキャッシュヒット率	ライブラリキャッシュを監視します。

SGA ディクショナリキャッシュヒット率	SGA ディクショナリを監視します。
SGA 共有プールリロード率	SGA 共有プールを監視します。
SGA 共有プールフリー	SGA 共有プールを監視します。
PGA In Memory Sort 率	PGA メモリを監視します。
Soft Parse 率	Soft Parse 数を監視します。
リトライ率	Redo バッファリトライを監視します。
Redo I/O トラフィック	Redo からの I/O トラフィック量を監視します。
ロールヘッダー競合	ロールヘッダーの書き込み競合を監視します。
ロールブロック競合	ロールブロックの競合を監視します。
ロールヒット率	ロールヒットを監視します。
ロールラップ	ロールラップを監視します。
ロール拡張	ロール拡張を監視します。
フラッシュリカバリ領域の使用	フラッシュリカバリ領域を監視します。
SGA Latches Hit 率	SGA ラッチを監視します。

5.1.7.10 Oracle 表領域

注記: Oracle の監視を開始する前に Nagios XI サーバに Oracle プラグインをインストール、設定してください。手順については「Oracle Plugin Installation Instructions」をお読みください。

Oracle 表領域ウィザードでは、Oracle サーバに対して以下のメトリックを簡単に監視登録することができます。

監視項目	説明
表領域使用	表領域の使用量を監視します。
表領域のフリースペース	表領域の空き容量を監視します。
表領域がフルになるまでの残り時間	表領域がいっぱいになるまでにどのくらいかかるかを監視します。
表領域の断片化	表領域がどのくらい断片化されたかを監視します。
表領域の IO バランス	IO バランスの指標を監視します。
次のエクステント割当が可能	次のエクステントの割当が可能か表領域のセグメントを監視します。

5.1.7.11 Postgres データベース

Postgres データベースウィザードでは、Postgres データベースに対して以下のメトリックを簡単に監視登録することができます。

監視項目	説明
接続状態	データベースに接続できることを監視します。
データベースサイズ	データベースサイズを監視します。
テーブルサイズ	データベースのテーブルサイズを監視します。

リレーションサイズ	データベースのリレーションサイズを監視します。
シーケンス	データベースの残シーケンスの割合を監視します。

5.1.7.12 Postgres クエリ

Postgres クエリウィザードでは、指定した Postgres クエリ結果が閾値内かどうかを簡単に監視登録することができます。

5.1.7.13 Postgres サーバ

Postgres サーバウィザードでは、Postgres サーバに対して以下のメトリックを簡単に監視登録することができます。

監視項目	説明
接続状態	サーバに接続できることを監視します。
バックエンド接続	サーバへの同時接続数を監視します。
WAL ファイル	pg_xlog ディレクトリにある WAL ファイルの数を監視します。

5.1.8 Webサイト

設定ウィザード － ウィザードを選択(**「設定 -> 設定ウィザード」**)ページで、**Web サイト** アイコンをクリックすると、Web サイト監視に関連するウィザードが表示されます。

以下の設定ウィザードへのリンクが表示されます:

DNS Query	ドメインの有効期限	Web サイト
Web サイト改ざん	Web サイト URL	Web トランザクション

5.1.8.1 DNS Query

こちらをお読みください。

5.1.8.2 ドメインの有効期限

こちらをお読みください。

5.1.8.3 Web サイト

Web サイトウィザードでは、Web サイトに対して以下を簡単に監視登録することができます。詳しくは「Web サイトの監視」をお読みください。

監視項目	説明
HTTP	Web サーバが有効な HTTP 応答を返すか監視します。
Ping	Web サイトのサーバを ICMP ping で監視します。 ネットワークの遅延と Web サーバの一般的な稼働時間を見るために便利です。
DNS 解決	有効な IP アドレスに解決されるかを確認するために Web サイトの DNS 名を監視します。
DNS IP マッチ	Web サイトの DNS 名が現在既知の IP アドレスに解決されるかを確認するために、Web サイトの DNS 名を監視します。 DNS が予期せず変更されないこと(セキュリティ違反が発生したことを意味する)を確認するために役立ちます。
Web ページのコンテンツ	指定した文字列が Web ページのコンテンツ内に見つかることを確認します。コンテンツの不一致は、Web サイトがセキュリティ侵害されたか、正常に動作していないことを示している場合があります。
Web ページの正規表現マッチ	指定した正規表現が Web ページのコンテンツ内に見つかることを確認します。 コンテンツの不一致は、Web サイトがセキュリティ侵害されたか、正常に動作していないことを示している場合があります。

5.1.8.4 Web サイト改ざん

Web サイト改ざんウィザードでは、Web サイトの改変を簡単に監視登録することができます。詳しくは「Web サイトの改ざん監視」をお読みください。

5.1.8.5 Web サイト URL

Web サイト URL ウィザードでは、Web URL に対して以下を簡単に監視登録することができます。詳しくは「Web サイトの監視」をお読みください。

監視項目	説明
URL ステータス	Web サーバが有効な HTTP 応答を返すか確認します。
URL コンテンツ	指定した文字列が Web ページのコンテンツ内に見つかるかを確認します。 コンテンツの不一致は、Web サイトがセキュリティ侵害されたか、正しく機能していないことを示している場合があります。

URL コンテンツの正規表現マッチ	指定した正規表現が Web ページのコンテンツ内に見つかるかを確認します。 コンテンツの不一致は、Web サイトがセキュリティ侵害されたか、正しく機能していないことを示す場合があります。

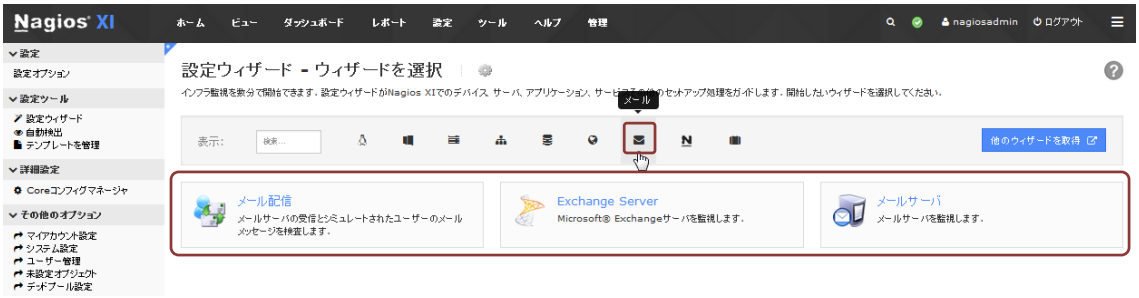
5.1.8.6 Web トランザクション

Web トランザクションウィザードでは、Web トランザクションを監視登録することができます。詳しくは「Web サイトの改ざん監視」をお読みください。

トランザクション監視を行うには、WebInject フォーマットのトランザクションテストケースが必要です。サンプルのテストケースはこちらです。

5.1.9 メール

設定ウィザード － ウィザードを選択(**「設定 -> 設定ウィザード」**)ページで、**メール** アイコンをクリックすると、メール監視に関連するウィザードが表示されます。



以下の設定ウィザードへのリンクが表示されます:

メール配信	Exchange Server	メールサーバ

5.1.9.1 メール配信

メール配信ウィザードでは、指定した SMTP サーバで送信されたテストメールを指定した IMAP サーバで受信できるかを簡単に監視登録することができます。

5.1.9.2 Exchange Server

こちらをお読みください。

5.1.9.3 メールサーバ

メールサーバーウィザードでは、メールサーバに対して以下を簡単に監視登録することができます。

監視項目	説明
Ping	ICMP ping を使用してサーバを監視します。 ネットワークの遅延と稼働時間を見るために便利です。
SMTP	SMTP サービスが利用可能であることを監視します。
IMAP	IMAP サービスが利用可能であることを監視します。
POP	POP サービスが利用可能であることを監視します。
RBL ブラックリストチェック	メールサーバが公開 RBL(リアルタイムブラックリスト)にリストされているかどうかをチェックします。

5.1.10 Nagios製品

設定ウィザード - ウィザードを選択(「**設定 -> 設定ウィザード**」)ページで、**Nagios 製品** アイコンをクリックすると、Nagios 製品の監視に関連するウィザードが表示されます。

以下の設定ウィザードへのリンクが表示されます:

自動検出	BPI ウィザード	ホストのクローンとインポート
Nagios Log Server	Nagiostats ウィザード	Nagios XI サーバ
NCPA	Nagios Network Analyzer	SLA

5.1.10.1 自動検出

自動検出ウィザードでは、自動検出されたノードを簡単に監視登録することができます。

メモ: このウィザードを実行する前に自動検出ジョブを実行する必要があります。自動検出ジョブの使用方法については、「自動検出」を参照してください。

5.1.10.2 BPI ウィザード

BPI ウィザードでは、Nagios BPI グループのステータス監視を簡単に登録することができます。BPI については「Using The BPI Addon」をお読みください。

5.1.10.3 ホストのクローンとインポート

ホストのクローンとインポートウィザードでは、複数のホストを既存ホストと同一条件で簡単に監視登録することができます。詳しくは、「ホストのクローンとインポート設定ウィザードの使用」をお読みください。

5.1.10.4 Nagios Log Server

Nagios Log Server ウィザードでは、Nagios Log Server で収集されたログを簡単に監視登録することができます。

メモ: 使用するには Nagios Log Server が必要です。

5.1.10.5 Nagiostats ウィザード

Nagiostats ウィザードでは、ローカルの Nagios サーバを簡単に監視登録することができます。

5.1.10.6 Nagios XI サーバ

Nagios XI サーバウィザードでは、リモートの Nagios XI サーバに対して以下を簡単に監視登録することができます。こちらをお読みください。

監視項目	説明
Ping	ICMP ping を使用してサーバをチェックします。 Nagios サーバのネットワーク可用性を監視するのに便利です。
Nagios XI Web インターフェース	リモートの Nagios XI サーバの Web インターフェースの可用性を監視します。
デーモン監視	監視エンジンとサポートデーモンが起動しているかを監視します。
ジョブ監視	core ジョブが実行しているかを監視します。
ロード	サーバ(1/5/15 分)の負荷を監視します。
I/O Wait	サーバ iowait の CPU 統計情報(ディスクの読み取り/書き込み待ち時間)を監視します。

5.1.10.7 NCPA

こちらをお読みください。

5.1.10.8 Nagios Network Analyzer

こちらをお読みください。

5.1.10.9 SLA

SLA ウィザードでは、指定したホスト、サービス、ホストグループ、サービスグループがサービス品

質保証(SLA)を満たしているかを簡単に監視登録することができます。

5.1.11 未分類

設定ウィザード － ウィザードを選択(**「設定 -> 設定ウィザード」**)ページで、**未分類** アイコンをクリックすると、未分類のウィザードが表示されます。

以下の設定ウィザードへのリンクが表示されます:

パッシブチェック	VMware

5.1.11.1 パッシブチェック

パッシブチェックウィザードでは、VMware ホストまたはゲストを簡単に監視登録することができます。「パッシブ監視」をお読みください。

5.1.11.2 VMware

注記: VMware の監視を開始する前に Nagios XI サーバに VMware SDK または ESX プラグインをインストール、設定してください。手順については「VMware 監視」をお読みください。

VMware ウィザードでは、VMware ESX, ESXi, vSphere, vCenter Server サーバに対して以下のメトリックを簡単に監視登録することができます。詳しくは「VMware 監視」をお読みください。

ホスト:

監視項目	説明
CPU Usage	CPU 使用率を監視します。
Memory	メモリ使用量を監視します。
Networking	ネットワークステータス、送受信を監視します。
Input / Output	Input/Output を監視します。
Datastore usage	データストアの使用量を監視します。
VM Status	VM のステータスを監視します。
Services	サービスを監視します。

ゲスト:

監視項目	説明
CPU Usage	CPU 使用率を監視します。
Memory	メモリ使用量を監視します。
Networking	ネットワークステータス、送受信を監視します。
Input / Output	Input/Output を監視します。
VM Status	VM のステータスを監視します。
CPU Usage	サービスを監視します。

注記: このウィザードでは閾値の指定を行えません。閾値を指定したい場合は、Core コンフィグマネージャのホストまたはサービス管理画面の**「一般設定」**タブページで引数を指定してください。

5.2 手動設定(設定ウィザード以外)

組込の設定ウィザードを使用しなくても監視登録を行うことができます。以下は Nagios ライブラリで公開されている監視登録手順例です。監視登録には Core コンフィグマネージャを使用します。

5.2.1 Windowsディスク使用量監視

以下の資料では Windows マシンのディスク使用量監視を登録する手順例を説明しています。

Adding Windows Disk Usage Checks In XI

5.2.2 Windowsアップデート監視

以下の資料では、新しい Windows アップデートの有無を監視する方法を説明しています。

Checking For Windows Updates

5.2.3 Apache Cassandra分散データベース監視

以下の資料では、Apache Cassandra 分散データベースを監視する方法を説明しています。データ、ハードウェアハウジングが適切に稼動していることを確認します。

How to Monitor Apache Cassandra

5.2.4 Swatchでのログ監視

以下の資料では、Simple Log Watcher(Swatch)を Nagios と併用して特定のイベントがシステムログに記録されたら通知するように設定する方法を説明しています。

Log Monitoring with Swatch

5.2.5 Apache Tomcat監視

以下の資料では、カスタム Apache ActiveMQ プラグインを追加し、Nagios XI サーバで“namely check_activemq”チェックを行う方法を説明しています。

Integrating Apache Tomcat Checks

5.2.6 JMX監視

以下の資料では、JMX アプリケーション監視を登録する方法を説明しています。

How To Monitor JMX With Nagios XI

5.2.7 WebLogic監視

以下の資料では、WebLogic を監視する方法について説明しています。WebLogic アプリケーションサーバーの健全性をよりわかりやすく表示したり障害が発生した場合に関係者へ通知したりすることができます。WebLogic は Java ベースのアプリケーションサーバーで、アプリケーションと Java 環境間のミドルウェアとして動作します。現在の接続数、ヒープ使用、スタックスレッドなどさまざまな側面を監視できます。

Monitoring WebLogic With Nagios XI

5.2.8 Apache ActiveMQ監視

以下の資料では、カスタム Apache ActiveMQ プラグインの使用方法と Apache ActiveMQ サーバを監視する方法について説明しています。Apache ActiveMQ サーバーキューにいくつのオブジェクトがあるかについて最新の情報を取得します。

How To Monitor Apache ActiveMQ

5.3 エージェント

5.3.1 クロスプラットフォームエージェント

以下の資料では、Nagios XI が NCPA エージェント（Nagios Cross Platform Agent）を介してアクティブにマシンを監視する方法について説明しています。NCPA は Windows および Linux マシン上にインストールできる、上級のクロスプラットフォームエージェントです。

How To Monitor Devices Using The NCPA Agent and Wizard

5.3.2 Windowsエージェント

5.3.2.1 NSClient++エージェントのインストール

Windows デスクトップまたはサーバを Nagios でエージェント監視するには、最初に監視対象マシンにエージェントをインストールする必要があります。以下の資料では、Nagios XI または Nagios Core でマシンを監視するために Windows エージェント（NSClient++）をインストール、設定する手順を説明しています。

Windows エージェント(NSClient++)のインストール

5.3.2.2 NSClient++で NRPE の有効化

以下の資料では、Windows クライアントシステム上で Nagios XI 用 NSClient++の NRPE リスナーを設定する方法について説明しています。

Enabling the NRPE Listener in NSClient++ (version 0.3.x)
NRPE リスナー（NSClient++ 0.4.x）の有効化 (version 0.4.x)

5.3.2.3 NSClient++の大規模デプロイ

以下の資料では、NSClient++エージェントを大規模な環境にデプロイする方法について説明しています。この目的を達成するために、Microsoft SCCM 2007 で NSClient++やその設定ファイルを多くのワークステーションにサイレントプッシュできることを示します。

Mass Deploy NSClient++

5.3.2.4 FTP サーバの構成

以下の資料では、Nagios XI サーバ上に FTP サーバを構成する方法を説明しています。Windows 環境の監視に Nagios XI を使用する場合に、NSClient++をデプロイするためのコンポーネントとして FTP を使用することができます。

Configure FTP for Nagios

5.3.3 Linuxエージェント

5.3.3.1 Linux エージェントのインストール

Nagios XI で Linux/Unix デスクトップまたはサーバをエージェント監視するには、最初に監視対象サーバにエージェントをインストールする必要があります。以下の資料では、Nagios XI でマシンを監視するために Linux エージェントをインストール、設定する手順について説明しています。

Linux エージェントのインストール

Linux エージェントは以下の URL からダウンロードできます。

http://assets.nagios.com/downloads/nagiosxi/agents/linux-nrpe-agent.tar.gz

経験豊富な管理者の方へ: 現在、Nagios XI Linux エージェントは RHEL, Fedora, CentOS のみをサポートしていますが、あなたは他のディストリビューションまたは NIX ボックスで動作できるように変更できるかもしれません。XI Linux エージェントは NRPE、公式 Nagios プラグイン、追加プラグイン、いくつかの特定の NRPE 設定ファイルオプションとの組み合わせです。単独の Nagios XI Linux エージェントは Ubuntu や Debian で利用できます(ライブラリ内に資料があります)。

5.3.3.2 Ubuntu/Debian Linux エージェントのインストール

以下の資料では、監視対象の Ubuntu および Debian サーバに Linux 監視エージェントをインストールする方法について説明します(Kubuntu や Edubuntu のような Ubuntu のバリエーションも含みます)。Ubuntu/Debian ファミリーのバージョンはあなたのディストリビューションパッケージ管理システムを使用してエージェントを簡単にインストールする方法を提供します。これらの手順は CrunchBang, easypeasy, gNewSense, Xandros, MEPIS, Mint, Knoppix, Baltix, Guadalinux, eBox, Untangle, Vyatta のような関連ディストリビューションでもほとんど修正なしで機能するでしょう。

Installing The Nagios Ubuntu and Debian Linux Agent

5.3.3.3 Static Linux エージェントのインストール

以下の資料では、Linux マシン上でスタティックなバイナリ Linux 監視エージェントをインストールする方法について説明しています。スタティックなバイナリエージェントにより、1つ以上の Linux マシンにコンパイル済みのスタティックなバイナリのリンク済みセットを簡単にインストールできます。

Installing The Nagios XI Static Linux Agent

5.3.3.4 ソースベース NRPE インストレーション

以下の資料では、ソースから Nagios XI 用の NRPE をインストールし設定する方法について説明しています。この資料は NRPE または Nagios XI を初めて使用する、または NRPE をソースベースでインストールしなければならない管理者を対象としています(サポート対象外の Linux ディストリビューションであるまたは企業のビルド環境にセキュリティ上の制約があるなどの場合)。

Source Based NRPE Installation and XI

5.3.3.5 NRPE のトラブルシューティング

以下の資料では、NRPE エージェントの問題をトラブルシュートする方法について説明しています。この資料は一般的な問題やエラーの解決策やトラブルシューティングのヒントについてもカバーしています。また、NRPE で問題を体系的にドリルダウンするための単純なフレームワークを提供します。

NRPE Troubleshooting and Common Solutions

5.3.4 MacOSXエージェント

以下の資料では、OS/X エージェントのインストール方法について説明しています。

Installing the XI MacOSX Agent

5.3.5 Solarisエージェント

以下の資料では、Solaris エージェントのインストール方法について説明しています。

Solaris Monitoring Agent Installation

5.3.6 AIXエージェント

以下の資料では、AIX エージェントのインストール方法について説明しています。

AIX Monitoring Agent Installation

5.4 自動検出

自動検出機能を使用すると、Nagios XI が指定したネットワーク上に存在するデバイスを自動的に検出します。

5.4.1 新しい自動検出ジョブを登録する

Step 1. **設定** > **自動検出**を選択します。

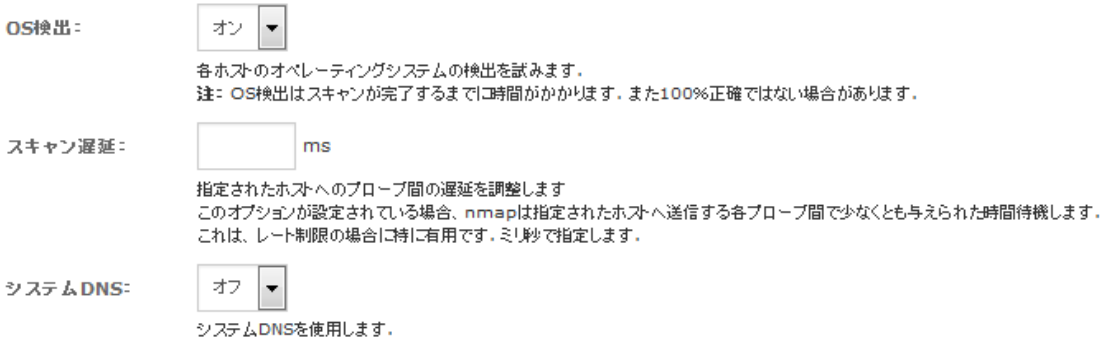
Step 2. **新しい自動検出ジョブ**をクリックします。

Step 3. スキャン対象のネットワークアドレス/ネットマスクを指定します。

必要に応じて「**除外する IP アドレス**」を指定します。

メモ:

- Standard エディションの場合は、スケジュール頻度で**「1回のみ」**を指定できます。Enterprise エディションの場合は、**「毎日」**、**「毎週」**、**「毎月」**を選択できます。
- **「詳細オプションを表示」**リンクをクリックすると、OS 検出の有無、スキャン遅延、システム DNS の使用有無を指定できます。



Step 4. **「実行」**をクリックします。

メモ: 指定するネットワーク範囲が広い場合、完了までに時間がかかります。

Step 5. **「ジョブリストを更新」**をクリックします。

Step 6. 検出デバイスを確認します。アクション欄の**「ジョブ結果を表示」**アイコンをクリックします。

Step 7.　スキャン結果を確認します。

「検出したホストの総数」欄の**「すべて表示」**リンクをクリックすると、「検出されたアイテム」セクションに登録済みのホストを含むすべてのホストが一覧表示されます。

「データのエクスポート」欄の**「CSV」**リンクをクリックすると、検出したホストの情報を CSV ファイルでダウンロードできます。

「基本的な監視設定」欄の**「新しいホスト」**リンクをクリックすると、**「設定ウィザード: Auto-Discovery」**ページに遷移します。

「検出されたアイテム」セクションの**「Show discovered services」**リンクをクリックすると、検出されたサービスを確認できます。


検出されたアイテム

ホスト およびサービス 自動検出スキャン中に以下が見つかりました。

Hide services

アドレス	ホスト名	タイプ	デバイス/オペレーティングシステム[格底]	MACベンダ	ステータス	Service Name	Port	Protocol
192.168.91.242	192.168.91.242	Linuxサーバ	Linux 2.6.32 - 3.10 [100%]	VMware	New			
						ssh	22	tcp
						http	80	tcp
						https	443	tcp
						mysql	3306	tcp
192.168.91.243	192.168.91.243	Linuxサーバ	Linux 2.6.32 - 3.10 [100%]	VMware	New			
						ssh	22	tcp
						http	80	tcp
						shell	514	tcp
						nrpe	5666	tcp

Step 8. 画面上部の「**自動検出ジョブに戻る**」リンクをクリックして前のページに戻ります。

5.4.2 既存の自動検出ジョブを今すぐ実行する

Step 1. **設定** > **自動検出**を選択します。

Step 2. 実行したいスキャン対象の**再実行** アイコンをクリックします。

Step 3. ジョブが完了するまでしばらく待ちます。

5.4.3 既存の自動検出ジョブを編集する

Step 1. **設定** > **自動検出**を選択します。

Step 2. 編集したいスキャン対象の**編集**アイコンをクリックします。

Step 3. ジョブを編集します。

Step 4. **実行**をクリックします。

5.4.4 既存の自動検出ジョブを削除する

Step 1. **設定** > **自動検出**を選択します。

Step 2. 削除したいスキャン対象の**削除**アイコンをクリックします。

注記: 確認メッセージは表示されません。ご注意ください。

5.5 パッシブ監視

パッシブ監視とは、外部のアプリケーションやサーバなど監視対象側から監視結果を Nagios XI サーバに送信してくる監視方法です。パッシブ監視を設定する方法については、「パッシブサービスの設定」をお読みください。

メモ: これに対し Nagios XI から監視対象へ問合せを行う監視は**「アクティブ監視」**と呼ばれます。

5.5.1 NRDP

NRDP（Nagios Remote Data Processor）は、柔軟なデータ転送プロセッサです。Nagios XI でのパッシブチェックに使用できます。NRDP の概要については「NRDP の概要」をお読みください。

メモ: Nagios XI には NRDP アドオンがインストール済みです。すぐに利用できます。

5.5.2 NSCA

NSCA (Nagios Service Check Adapter)を使用してパッシブチェックを行うこともできます。NSCA アドオンの使用法については「How to Use the NSCA Addon」をお読みください。

メモ: Nagios XI には NSCA アドオンがインストール済みです。

5.5.3 NRDS

「NRDS Config Manager」ページ（**「管理 -> 監視設定 -> NRDS Config Manager」**）では、Nagios Remote Data Sender(NRDS)で、さまざまなオペレーティングシステムのパッシブエージェントに設定やプラグインを配備することができます。

パッシブエージェントは現在の設定と必要なプラグインを Nagios XI サーバからダウンロードし、チェックを実行して結果を Nagios XI サーバにポストします。詳しくは、「NRDS でのパッシブ監視」をお読みください。

5.5.4 Windowsのパッシブチェック

5.5.4.1 NSClient++でのパッシブ監視

NSClient++を使用してパッシブチェックを行う方法については、「Using NSClient++ For Passive Checks」をお読みください。

5.5.4.2 NRDS_Win でのパッシブ監視

NRDS_Win を使用して Windows ホストをパッシブ監視する場合は、「Passive Monitoring with NRDS_Win」をお読みください。

NRDS_Win は Nagios プラグインを処理しチェック結果を戻す軽量なクライアントです。このパッシブエージェントは結果を 80 ポート(HTTP)または 443 ポート(HTTPS)で Nagios に戻します。ファイアウォールルールのため、Nagios が監視したいホストに到達できないがホストは Nagios に通信できる状況において有効です。パッシブ監視はすべてのチェック処理がクライアントで実行され、結果のみが戻されるので、非常に拡張性が高いです。

また、NRDS_Win には設定やプラグインを自動更新する機能があります。すべての設定は NRDS 設定マネージャで中央管理されます。

5.5.5 未設定オブジェクトの監視

NSCA や NRDP API により外部エージェントやアプリケーションから Nagios XI へ送信されたホストやサービスのパッシブチェック結果は、Nagios XI で監視登録されるまで監視エンジンで処理されません。これらのホストおよびサービスは、**「未設定オブジェクト」**ページ(**「管理 -> 監視設定 -> 未設定オブジェクト」**)に未設定オブジェクトとして表示されます。**「未設定オブジェクト」**ページから未設定オブジェクトを簡単に監視登録することができます。

未設定オブジェクトを Nagios XI に登録する手順については、「Monitoring Unconfigured Objects With Nagios XI」をお読みください。

5.6 その他

5.6.1 設定スナップショット

Nagios XI では、**「設定を適用」**すると自動的に監視設定のスナップショットが作成、保存されます。保存済みのスナップショットを復元（リストア）することで、過去のある時点の監視設定に簡単に戻すことができます。設定スナップショットについては、こちらをお読みください。

5.6.2 デッドプール設定

注記：この機能は Enterprise エディションでのみ利用できます。

指定した期間より長い期間障害ステータスが継続しているホストおよびサービスを自動的に削除することができます。デッドプール設定については、こちらをお読みください。

5.6.3 クリティカルや警告ステータスをOKと判定させるNegateプラグインの使用

以下の資料では、Negate プラグインの理解と使用方法について説明しています。この資料はホストまたはサービスが致命的または警告状態であるが OK であると逆に表示させたい管理者を対象としています。

Negate プラグインの使用

5.6.4 ホスト死活監視方法の変更

ホストの死活監視（ステータスチェック）方法を変更したい場合は、以下の資料をお読みください。

ホスト死活監視方法の変更

5.6.5 機密情報をマスクするUserマクロの使用

以下の資料では、User マクロを実装、使用する方法について説明しています。ユーザー名やパスワードなどの機密情報をマスクしたい場合に以下の資料をお読みください。User マクロはプラグインやイベントハンドラへのパスの指定にも役立ちます。また、！ や ＄ のような不正な文字も User マクロを使用すれば Core コンフィグマネージャで使うことができます。

User マクロの理解

5.7 Smokeping統合

以下の資料では、Smokeping と Nagios XI でネットワーク遅延を監視する方法について説明しています。この資料は内部ネットワーク内または Web サーバのような外部ホストのいずれかでネットワーク遅延の問題があるときに通知を受けたい Nagios XI 管理者を対象としています。

Integrating Smokeping With Nagios XI

5.7.1 手動での設定ファイル管理

監視設定ファイルを手動で管理したい（設定ウィザードや Core コンフィグマネージャを使用せずにファイルベースで監視登録を行う）場合は、以下の資料をお読みください。

手動での設定管理

6 Coreコンフィグマネージャ

Core コンフィグマネージャは Nagios XI 監視エンジンを管理するための上級インターフェースを提供します。ホストグループ、サービスグループ、連絡先グループ、テンプレート、コマンドの作成、編集、削除などさまざまな作業を行うことができます。設定ウィザードを使用せずにホストやサービスの監視設定を追加したり、設定ウィザードを使用して登録したホストやサービス設定を変更したり削除したりすることができます。

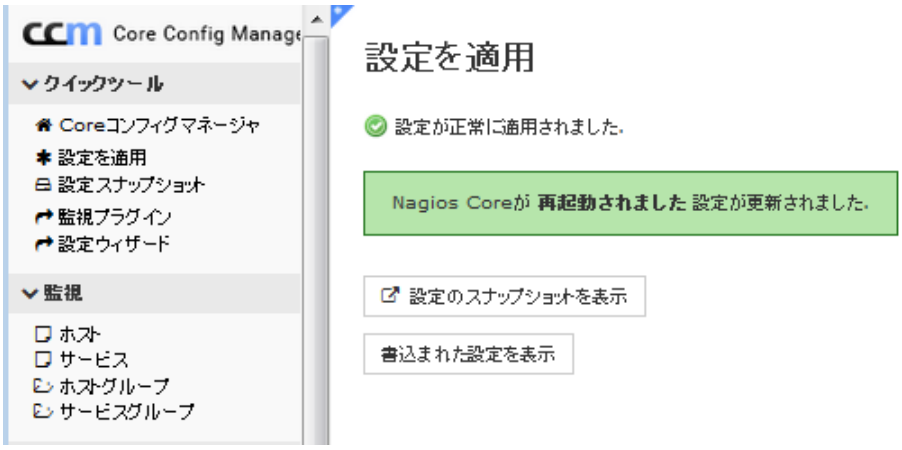
6.1 クイックツール

「**クイックツール**」メニューからは、設定の適用やスナップショットのダウンロード、確認、復元、アーカイブを行えます。

6.1.1 設定を適用

Core コンフィグマネージャ上で設定を変更し終わったら、システムに変更を反映するために設定を適用してください。

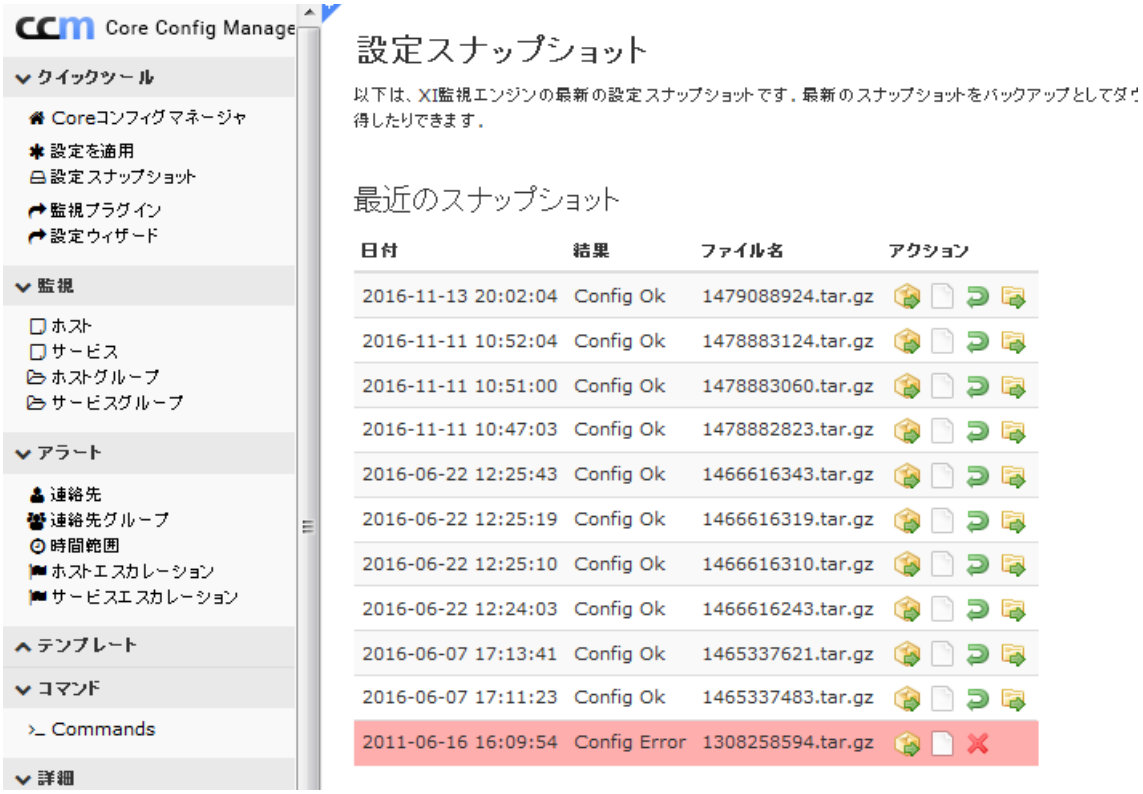
設定の適用に成功すると、Nagios Core が再起動され、自動的に設定のスナップショットが保存されます。



設定の適用に失敗した場合は、エラーメッセージを確認してエラーの原因を修正してください。

6.1.2 設定スナップショット

「設定スナップショット」ページ（**「設定 -> Core コンフィグマネージャ -> クイックツール -> 設定スナップショット」**）では、過去に自動作成されたスナップショットの一覧およびアーカイブ済みのスナップショットを確認できます。また、スナップショットはローカルにダウンロードしたり復元（リストア）したりすることができます。



スナップショットは、Core コンフィグマネージャ上で**「設定を適用」**したり設定ウィザードを最終ステップで適用したりすると自動的に作成、保存されます。

「最近のスナップショット」には直近12件のスナップショットが作成日時の新しい順（降順）に一覧表示されます。スナップショットのファイル名はスナップショットが作成された Unix 時間となります。

スナップショットをローカルにダウンロードするには、**ダウンロード**アイコンをクリックします。
設定適用時の検証結果を確認する場合は、**表示**アイコンをクリックします。
任意のスナップショットを復元したい場合は、リストアをクリックします。

スナップショットをアーカイブしておくことで、ある特定の時点のスナップショットを分かりやすい名前を付けて保存することができます。以前の設定に戻したいときに便利です。

6.2 監視

「監視」メニューには、監視対象のホスト、サービス、ホストグループ、サービスグループを管理するためのリンクがあります。

6.2.1 ホスト管理

Core コンフィグマネージャ上でのサービス管理は、**「設定 -> Core コンフィグマネージャ -> 監視 -> ホスト」**で行えます。

以下の資料では、Nagios XI Core コンフィグマネージャを使用してホストおよびホストグループを管理する方法について説明しています。ホストの追加、編集、削除、コピー、情報表示、ホストグループの管理、ホストテンプレートの使用方法について説明しています。

ホスト管理

ホストの死活監視方法を変更したい場合は「ホスト死活監視方法の変更」をお読みください。

メモ: 設定ウィザードを使用して登録されたホストのほとんどは、ホストの死活監視に ICMP Ping が使用されます。

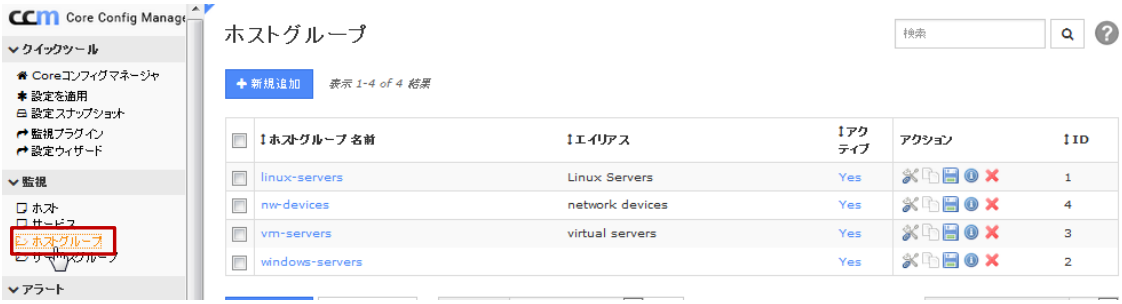
6.2.2 サービス管理

Core コンフィグマネージャ上でのサービス管理は、**「設定 -> Core コンフィグマネージャ -> 監視 -> サービス」**で行えます。画面構成および使用方法は「ホスト管理」とほぼ同じです。

6.2.3 ホストグループ管理

Core コンフィグマネージャ上でのホストグループ管理は、**「設定 -> Core コンフィグマネージャ -> 監視 -> ホストグループ」**で行います。「ホスト管理」をお読みください。

メモ: 「設定ウィザードのステップ 5」で希望のホストグループを表示させるには、ウィザード実行前にホストグループを作成しておく必要があります。



6.2.4 サービスグループ管理

Core コンフィグマネージャ上でのサービスグループ管理は、**「設定 -> Core コンフィグマネージャ -> 監視 -> サービスグループ」**で行います。

メモ: 「設定ウィザードのステップ 5」で希望のサービスグループを表示させるには、ウィザード実行前にサービスグループを作成しておく必要があります。サービスグループの作成手順はホストグループの作成手順とほぼ同じです。

6.3 テンプレート管理

ホスト、サービス、連絡先は指定されたテンプレートから初期値を継承します。テンプレートは、ホスト、サービス、連絡先の共通設定を行うのに役立ちます。

テンプレート管理は、**「設定 -> Core コンフィグマネージャ -> テンプレート」** 下で行います。
使用方法については「ホスト管理」をお読みください

6.4 コマンド管理

コマンド管理は、**「設定 -> Core コンフィグマネージャ -> コマンド -> Command」**で行います。

カスタムプラグインを追加した場合の新しいコマンド定義の作成や既存のコマンド定義の編集や削除を行えます。カスタムプラグインを追加したい場合は「プラグインの管理」をお読みください。

6.5 詳細

ホスト依存関係、サービス依存関係の登録、編集、削除や Nagios Core 設定（nagios.cfg）、Nagios Core CGI 設定（cgi.cfg）の閲覧、編集を行えます。

6.6 ツール

「ツール」メニューには、エスカレーションウィザード、ホストおよびサービス名や監視属性の一括変更を行うためののリンクがあります。設定ファイルのインポートや書込みツールは、主に Nagios Core からの移行時に使用します。

6.6.1 静的な設定エディタ

「静的な設定エディタ」を使用すると、Core コンフィグマネージャデータベースに保管されていない設定ファイルを編集することができます。監視設定を Core コンフィグマネージャデータベースに取り込まずに運用する場合は、「手動での設定管理」をお読みください。

6.6.2 Userマクロ

「**User マクロ**」を使用すると、Nagios XI システムの User マクロを編集したり選択オプションに表示する System マクロを追加、削除したりすることができます。

詳しくは、「User マクロコンポーネントについて」をお読みください。

6.6.3 エスカレーションウィザード

「**エスカレーションウィザード**」を使用すれば、複数のホストやサービスのエスカレーションチェーンを一度に定義することができます。アラート通知のエスカレーションについては「Understanding Nagios XI Notification Escalations」をお読みください。

6.6.4 一括変更ツール

注記：この機能は Enterprise エディションでのみ利用できます。

「**一括変更ツール**」を使用すると、指定したホストおよびサービスの設定を変更することができます。このツールはテンプレートで定義された設定や関係に依存せず、指定された設定で任意のテンプレート設定を上書きします。

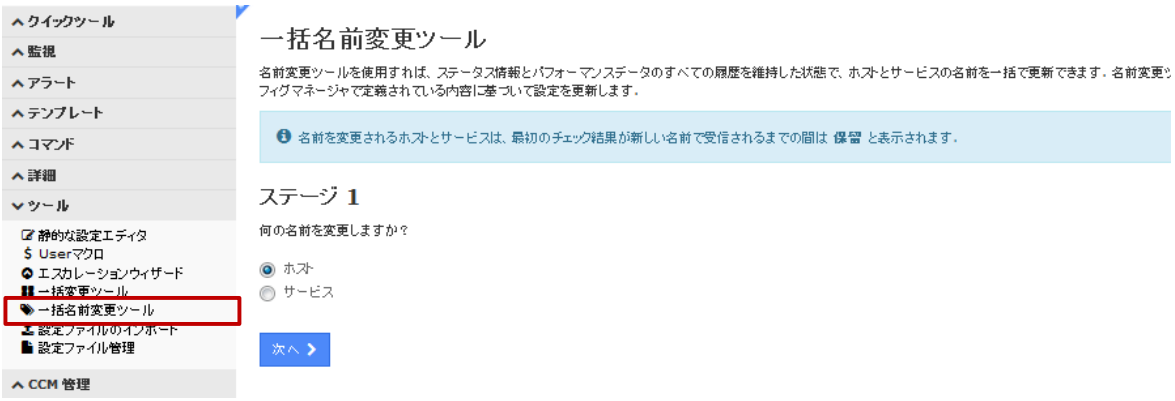
以下の変更ツールを利用できます：

変更ツール	説明
単一設定オプションを変更する	ホスト/サービスの設定オプション値を変更できます。
コマンドおよび引数を変更する	ホスト/サービスに指定したコマンドおよびコマンド引数の値を変更できます。
連絡先を追加する	ホスト/サービスの連絡先を追加できます。
連絡先を削除する	ホスト/サービスの連絡先を削除できます。
連絡先グループを追加する	ホスト/サービスの連絡先グループを追加できます。
連絡先グループを削除する	ホスト/サービスの連絡先グループを削除できます。
ホストグループを追加する	ホストにホストグループを追加できます。
ホストグループを削除する	ホストからホストグループを削除できます。
親ホストを追加する	ホストに親ホストを追加できます。
親ホストを削除する	ホストから親ホストを削除できます。
サービスを追加する	既存のサービスをもとにホストにサービスを追加できます。
テンプレートを変更する	ホストまたはサービスのテンプレート定義を上書きします。
設定名を変更する	サービスの設定名を変更できます。

6.6.5 名前変更ツール

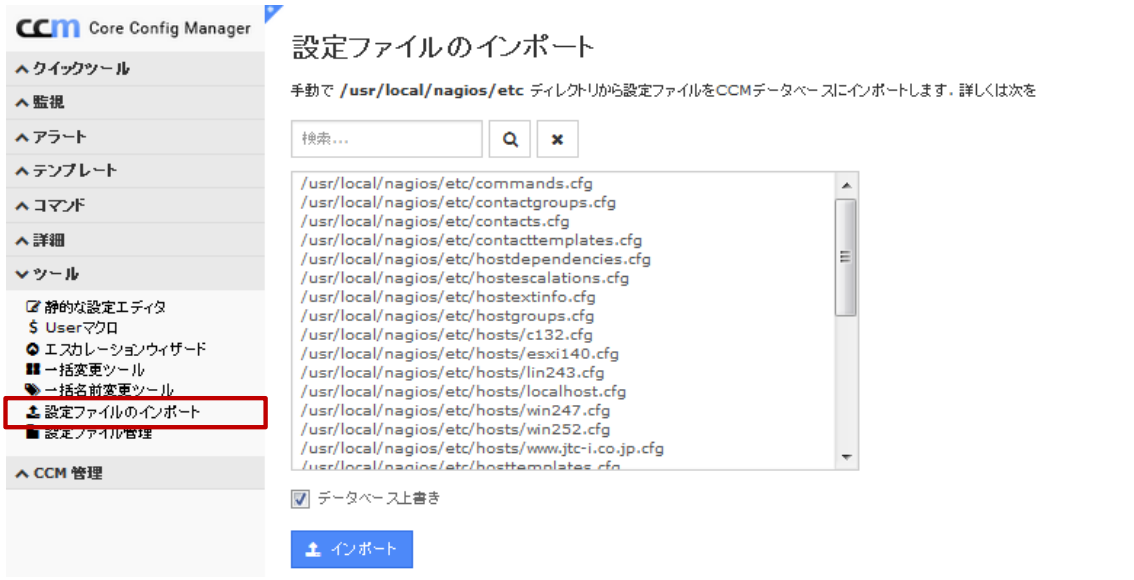
注記： この機能は Enterprise エディションでのみ利用できます。

「名前変更ツール」を使用すれば、ステータス情報とパフォーマンスデータのすべての履歴を維持した状態で、ホストとサービスの名前を一括で更新できます。名前変更ツールは、Core コンフィグマネージャで定義されている内容に基づいて設定を更新します。



6.6.6 設定ファイルのインポート

「設定ファイルのインポート」では手動で編集した設定ファイルを Core コンフィグマネージャデータベースに取り込むことができます。この機能は通常 Nagios Core からの移行作業で使用されます。Nagios Core の設定ファイルインポート手順については「設定ファイルのインポート」をお読みください。



6.6.7 設定ファイル管理

「設定ファイル管理」を使用すると、新しい設定ファイルの内容（ホスト、サービス、ホストグループ、サービスグループ、ホストテンプレート、サービステンプレート、タイムピリオド、連絡先、連絡先グループ、エスカレーション、依存関係）を Nagios XI サーバにエスポートできます。また、エクスポートされた設定の検証や設定の削除、Nagios の再起動を行えます。この機能は通常 Nagios Core からの移行作業や設定ファイルを手動編集した場合に使用します。使用方法については、「設定のファイル書き込み」をお読みください。

メモ： Nagios Core からの移行手順については「Nagios Core からの移行」をお読みください。

7　通知管理

Nagios XI は障害を検知すると、その問題について関係者にアラートを通知することができます。この章では、通知機能の設定について説明します。

7.1　通知設定

ユーザーは**「通知オプション」**メニューからアラート通知の受信有無、受信する場合はどのタイプのアラートをいつ受信するかを設定することができます。詳しくは、「メールとテキスト通知の設定」をお読みください。

7.2　通知変数

ユーザーは**「通知メッセージ」**ページで受信する通知メッセージの内容をカスタマイズすることができます。通知メッセージには変数（例：%Host%）を使用できます。使用可能な変数については、「通知変数」をお読みください。

注記：言語設定で**「日本語」**が選択されている場合でも、変数値は英語で表示されます。

7.3 通知エスカレーション設定

ホストやサービスのアラートが指定回数を超えて通知された後に、別のサポートレベルの人に問題を知らせる「エスカレーション」機能を利用できます。通知のエスカレーション設定については「XI Notification Escalations」をお読みください。

7.4 一括通知管理

注記: この機能は Enterprise エディションでのみ利用できます。

Enterprise エディションをご利用の場合、**「通知設定の管理」**ページ(**「管理 -> ユーザー -> 通知管理」**)で、通知メッセージ内容や通知オプションを保存し複数の Nagios XI ユーザーまたは連絡先グループに一括適用することができます。

注記: Nagios XI で作成された連絡先(「Nagios XI ユーザーと Nagios Core 連絡先」に従って作成された連絡先)の通知設定のみが対象となります。

7.4.1 通知管理の作成

通知設定を複数の Nagios XI ユーザーまたは連絡先に一括で適用したい場合は、以下の作業を行います。

Step 1. **「管理 -> ユーザー -> 通知管理」**を選択します。

Step 2. **「テンプレートタイトル」**にテンプレート名を入力します。

Step 3. このテンプレートをすべてのユーザーのデフォルトにしたい場合は、**「これらの通知メッセージをすべてのユーザーのデフォルトとして設定する」**にチェックをつけます。

Step 4. **「メールメッセージ」**タブで、ホストおよびサービスのアラートメール件名とメッセージを編集します。

Step 5. **「モバイルテキスト（SMS）メッセージ」**タブを選択し、ホストおよびサービスのアラートメール件名とメッセージを編集します。

Step 6. **「通知設定」**タブを選択し、以下を指定します。

通知設定を展開	通知設定を展開する場合はチェックをつけます。
通知を有効にする	選択したユーザーの通知を有効にする場合はチェックをつけます。
通知設定をロック	選択したユーザーに通知設定の変更を許可しない場合はチェックをつけます。 **注記**：ロックを有効にすると、ユーザーは自身のアカウントページから通知設定を変更できません。

Step 7. **「メール」**タブまたは**「モバイルテキスト（SMS）」**タブで通知メールを受信したいイベントのタイプをチェックします。

メモ：⚠のチェックボックスを選択した場合、**「優先度　高」**のメールが送信されます。

Step 8. （通知期間を設定したい場合は）**「通知期間」**タブを選択し、通知期間の展開セクションのチェックボックスにチェックをつけ、**「通知時刻」**を指定します。

Step 9. **「ユーザーに展開」**タブを選択し、このテンプレートを適用したい Nagios XI ユーザーまたは連絡先グループを選択します。

Step 10. **「テンプレートを保存」**を選択します。

Step 11. **「プリファレンスを展開」**を選択します。

7.4.2 既存の通知テンプレートの変更

既存の通知テンプレートを変更する場合は、**「利用可能な保存済みテンプレート」**ドロップダウンリストから変更したいテンプレートを選択して**「テンプレートをロード」**をクリックした後、テンプレート定義を編集し、**「テンプレートを保存」**をクリックします。

7.4.3 既存の通知テンプレートの削除

「利用可能な保存済みテンプレート」ドロップダウンリストから削除したいテンプレートを選択し、**「テンプレートを削除」**をクリックします。

7.5 Core連絡先にXIのphpmailer SMTP設定を使用させる

以下の資料では、Nagios XI ユーザーとのリンクを持たない Nagios Core 連絡先に（SMTP リレー設定を含む）XI のメール設定を使用させる手順を説明しています。

Configuring Core Contacts to Use Xi's PHP Mailer

8　基本機能

この章では、Nagios XI で監視しているホストやサービスの確認方法やダッシュボード、ビューの使用方法について紹介します。その他、ユーザー権限レベルのユーザーが利用できる機能については「Nagios XI ユーザーガイド」をお読みください。

8.1　ホスト・サービスの確認

Nagios XI インターフェースでホストやサービスの詳細情報を確認する手順については、「ホスト・サービスの詳細情報表示」をお読みください。

8.2　ダッシュボードの理解と使用

ダッシュボードは個別ユーザーが画面表示する情報をカスタマイズできるように設計された Nagios XI の強力な機能です。ダッシュボードは重要で最もよく使用する関連情報を表示するために使用されます。ダッシュボードは Nagios XI ユーザーごとに固有です。ユーザーは自分のニーズにあわせて独自のダッシュボードセットを作成し Nagios XI をカスタマイズすることができます。

ダッシュボードの使用と管理方法については、「ダッシュボードの理解と使用」をお読みください。

8.3　ビューの理解と使用

ビューは個別ユーザーが Nagios XI ページや有益な外部の Web サイトに素早くアクセスできるように設計されています。ビューは、一般的にネットワークオペレーションセンター（NOC）やパブリックな場所のウォールモニターに重要な情報を表示させたい管理者が使用します。

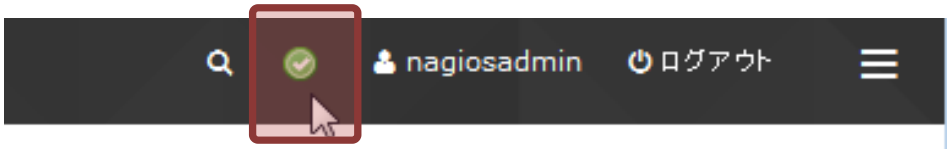
ビューの使用と管理方法については、「ビューの理解と使用」をお読みください。

9　システム管理

この章では、Nagios XI システムの情報取得や、運用・管理について説明します。

9.1　システムステータスの確認

Nagios XI システムのステータスはプライマリメニュー上のステータスアイコンで確認できます。



ステータスアイコンをクリックすると、ポップアップ画面に各サービスのステータスアイコンが表示されます。

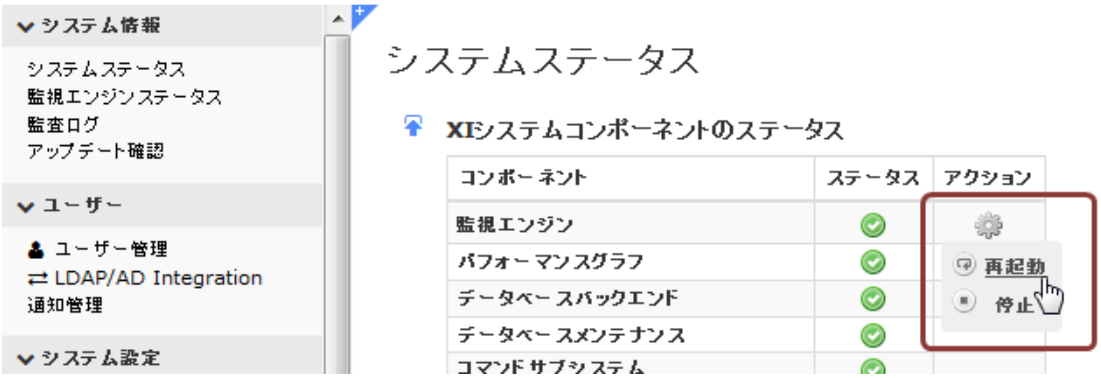
サービスが正常に稼働している場合、緑色のチェック  アイコンが表示されます。
ダウンしているサービスがある場合、赤いエクスクラメーションアイコンが表示されます。

システムステータスは、「**管理 -> システム情報 -> システムステータス**」からも確認できます。

9.1.1 コンポーネントのステータス

「**システムステータス**」ページ(「**管理 -> システム情報 -> システムステータス**」)では、システムコンポーネントのステータスおよびサーバ統計情報を確認できます。

アクション欄の  アイコンから、システムコンポーネントの再起動、停止、開始を行うことができます。



9.1.2 サーバ統計

「**サーバ統計**」では、Nagios XI サーバのロード、CPU 統計、メモリ、Swap を確認できます。

9.2　システムエンジンステータスの確認

「監視エンジンステータス」ページ(**「管理 -> システム情報 -> 監視エンジンステータス」**)から、監視エンジンのプロセスステータス、イベントキュー状況、チェック統計、パフォーマンス情報を確認できます。

9.2.1　監視エンジンプロセス

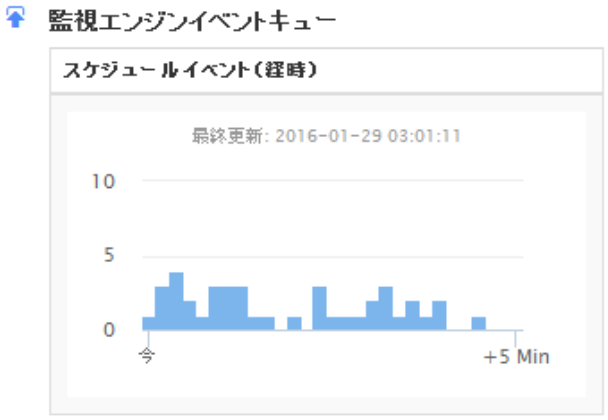
「監視エンジンプロセス」では、各プロセスの稼働状況を確認できます。有効なプロセスは**「値」**欄に  、無効のプロセスは  が表示されます。

監視エンジンが停止している場合は、**「プロセス状態」**の**「値」**に  が表示されます。監視エンジンが停止している場合は、  アイコンをクリックすることでプロセスを開始できます。

「アクション」欄の  アイコンをクリックすると該当のプロセスが無効化され、 アイコンをクリックするとプロセスが有効化されます。

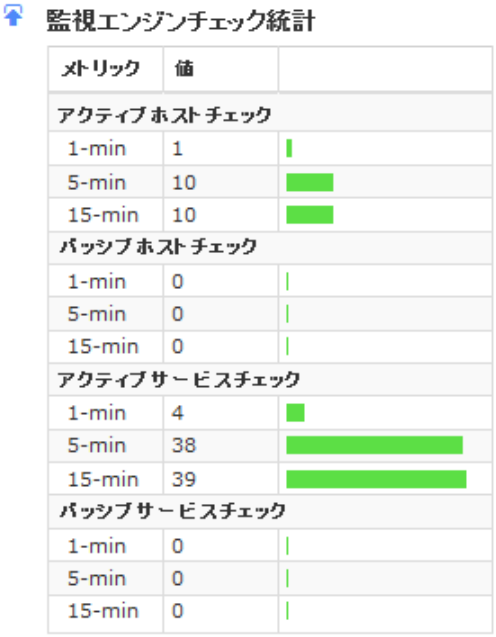
9.2.2 監視エンジンイベントキュー

「監視エンジンイベントキュー」では、現在から 5 分後までにイベントキューに配置されているイベント数を表示します。デフォルトでは 5 秒ごとにリフレッシュされます。



9.2.3 監視エンジンチェック統計

「監視エンジンチェック統計」では、1 分間、5分間、15分間ごとのアクティブホストチェック、パッシブホストチェック、アクティブサービスチェック、パッシブサービスチェックの件数を確認できます。



監視エンジンチェック統計

メトリック	値
アクティブホストチェック	
1-min	1
5-min	10
15-min	10
パッシブホストチェック	
1-min	0
5-min	0
15-min	0
アクティブサービスチェック	
1-min	4
5-min	38
15-min	39
パッシブサービスチェック	
1-min	0
5-min	0
15-min	0

9.2.4 監視エンジンパフォーマンス

「監視エンジンパフォーマンス」では、ホストチェック遅延、ホストチェック実行時間、サービスチェック遅延、サービスチェック実行時間の最小、最大、平均時間を確認できます。

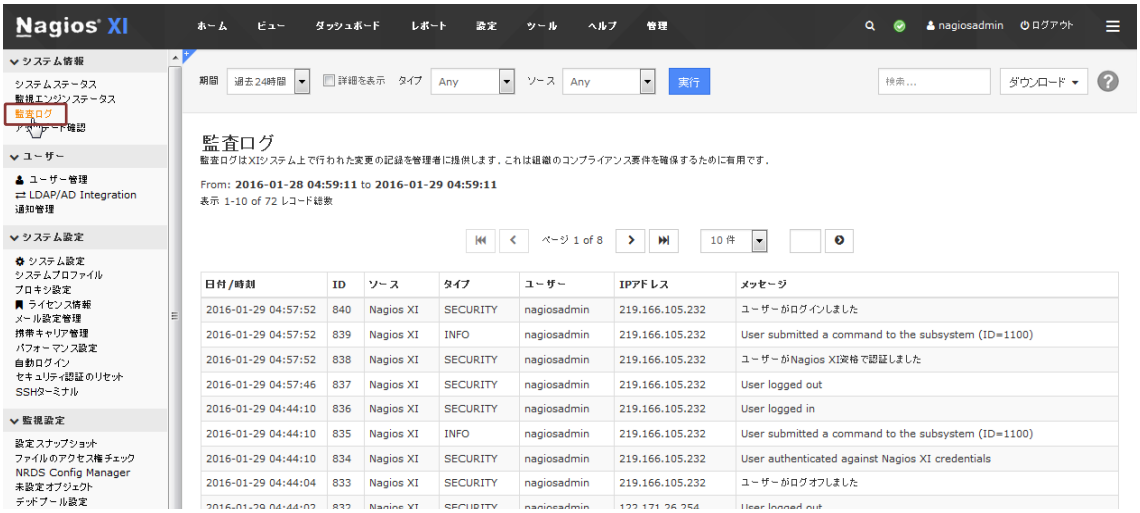
監視エンジンパフォーマンス

メトリック	値
ホストチェック遅延	
Min	0.00 sec
Max	1.00 sec
Avg	0.12 sec
ホストチェック実行時間	
Min	0.00 sec
Max	0.60 sec
Avg	0.14 sec
サービスチェック遅延	
Min	0.00 sec
Max	0.00 sec
Avg	0.00 sec
サービスチェック実行時間	
Min	0.00 sec
Max	4.37 sec
Avg	0.25 sec

9.3 監査ログの確認

注記： この機能は Enterprise エディションでのみ利用できます。

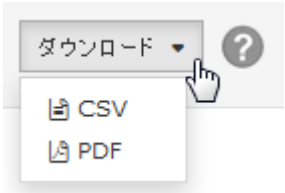
「監査ログ」ページ（**「管理 -> システム情報 -> 監査ログ」**）では、Nagios XI システム上で行われた変更の記録を閲覧できます。



画面上部のオプションから、表示するログを制限することができます。

オプション	説明
期間	対象期間を指定できます。（デフォルト：過去 24 時間）
詳細を表示	チェックすると**「詳細」**欄が追加され、詳細情報が表示されます。
タイプ	表示するログのタイプを選択できます。
ソース	表示するログソースを選択できます。
検索フィールド	キーワードを含むログを抽出することができます。

「ダウンロード」ドロップダウンボタンで、結果を CSV または PDF ファイルでダウンロードすることができます。



9.4 アップデート確認

「アップデート」ページ（**「管理 -> システム情報 -> アップデート確認」**）では、Nagios XI のアップ

デート有無を確認することができます。

注記: アップデートを確認するには、インターネット接続が必要です。

「アップデートをチェック」をクリックすると、Nagios XI のアップデートの確認を実行します。

アップデートが存在する場合、この画面からバージョンアップを実行することができます。
アップグレード手順については「Web UI からのアップグレード」をお読みください。

メモ: 手動でアップグレードを行う場合は、「手動アップグレード」をお読みください。

9.5 システムプロファイルの確認とダウンロード

「システムプロファイル」ページ（**「管理 -> システム設定 -> システムプロファイル」**）では、Nagios XI システムのプロファイルを表示したりダウンロードしたりすることができます。

サポートのご依頼をいただいた際に、調査のためにシステムプロファイルのご提供を依頼する場合があります。システムプロファイルを御提供いただけますと、サポート技術者はお客様のシステムをより簡単に理解することができます。

システムプロファイルをダウンロードするには、**「プロファイルをダウンロード」**ボタンをクリックしてください。

9.6 SSHターミナル

注記: この機能は Enterprise エディションでのみ利用できます。

「**SSH ターミナル**」ページ(「**管理 -> システム設定 -> SSH ターミナル**」)は、Nagios XI サーバ端末への Web ベースセッションを提供します。このインターフェースから、Nagios XI サーバにログインし、アップグレードや診断などを行うことができます。

注記:

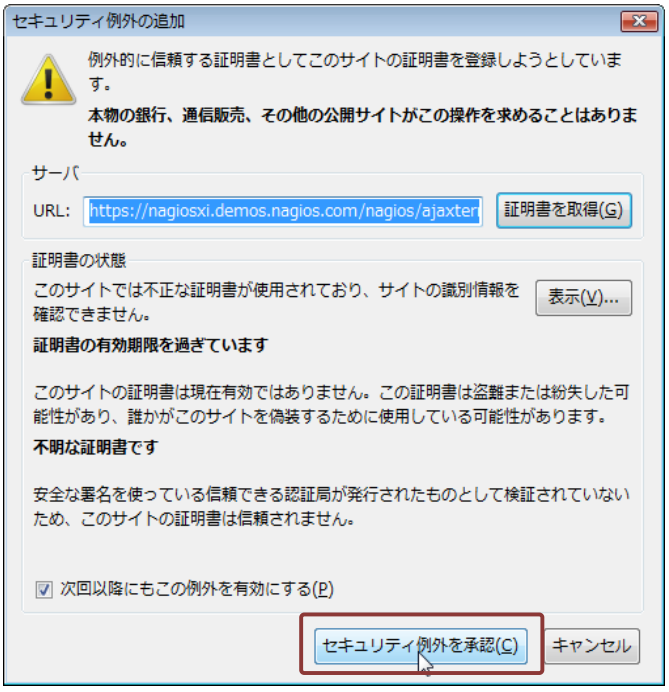
- Firefox または Chrome の使用を推奨します。Internet Explorer は、SSH ターミナルを使用するために互換モードを有効にする必要があります.
- SSH ターミナルにアクセスするには、ログイン認証情報を再入力する必要があります。
- 初めて SSH ターミナルにアクセスする場合は、新しいウィンドウでこのページを開いて、ブラウザでセキュリティ例外を許可する必要があります。

セキュリティの例外を追加する手順(Firefox の場合)は以下のとおりです:

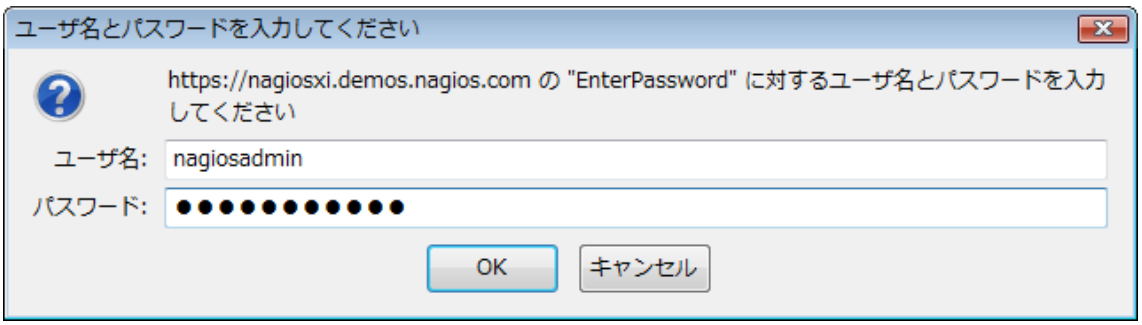
Step 1. 「**新しいウィンドウでターミナルを開く**」をクリックします。

Step 2. 「**危険性を理解したうえで接続するには**」 ->「**例外を追加**」をクリックします。

Step 3. **「セキュリティ例外を承認」**をクリックします。



Step 4.　Nagios XI のログイン認証情報を入力し、「OK」をクリックします。



Step 5.　Ajaxterm ウィンドウが表示されたことを確認します。

9.7　ファイルのアクセス権チェック

「ファイルのアクセス権チェック」ページ（**「管理 -> 監視設定 -> ファイルのアクセス権チェック」**）では、Nagios XI 設定スクリプトファイルおよび Nagios Core 設定ファイルにアクセス権の問題がないかを確認できます。

9.8　デッドプール設定

注記： この機能は Enterprise エディションでのみ利用できます。

「デッドプール設定」ページ（**「管理 -> 監視設定 -> デッドプール設定」**）では、指定した閾値より長い期間障害ステータスが継続しているホストおよびサービスを自動的に削除することができます。もはや存在しない、または無効となったホストおよびサービスの監視システムを自動的に掃除するのに便利です。

「**一般設定**」タブページで、以下を設定します：

設定	説明
デッドプールプロセッサを有効にする	デッドプールプロセッサを有効にする場合は、チェックボックスにチェックをつけます。
ホスト/サービス削除でパフォーマンスデータファイル(RRD)を削除する	削除時にパフォーマンスデータ(RRD)も同時に削除する場合は、チェックボックスにチェックをつけます。
メール受信者	デッドプールアクティビティのメール通知先を指定します。

「**ホスト設定**」/「**サービス設定**」タブページでは以下を設定します：

設定	説明
ステージ 1 時間	障害ステータスにあるホスト/サービスを自動的に無効化しデッドプールに追加されたことを通知するまでの時間
削除時間	障害ステータスにあるホスト/サービスを自動的にデッドプールから除去し、監視設定から削除するまでの時間
除外フィルタ	デッドプール処理から除外するホスト/サービスの名前を指定します。完全一致または正規表現を含めることができます。

9.9 バックアップとリストア

以下の資料では、Nagios XI インストレーションをバックアップする方法と XI インストレーションを過去のバックアップから復元(リストア)する方法について説明しています。

バックアップとリストア

9.9.1 スケジュールバックアップ

「**スケジュールバックアップ**」ページ(「**管理 -> システムバックアップ ->スケジュールバックアップ**」)では、Nagios XI サーバのスケジュールバックアップを設定することができます。

スケジュールバックアップの手段として、FTP、SSH、ローカルのいずれかまたはすべてを指定することができます。

メモ: デフォルトはスケジュールバックアップが設定されていません。Nagios XI システムのバックアップがあれば、Nagios XI サーバの移行や障害復旧に役立ちます。スケジュールバックアップを設定して運用されることをお勧めします。

9.9.2 ローカルバックアップアーカイブ

「ローカルバックアップアーカイブ」ページ(**「管理 -> システムバックアップ -> ローカルバックアップアーカイブ」**)では、Nagios XI システムのバックアップを作成することができます。

「**バックアップを作成する**」ボタンをクリックすると、`/store/backups/nagiosxi` ディレクトリにバックアップファイルが保存されます。

注記： バックアップの作成には時間がかかります。現バージョンではバックアップ作成完了後に画面が自動でリフレッシュされませんので、バックアップ作成後しばらくしたらページを再読み込みしてバックアップの作成を確認してください。

バックアップしたファイルは、**ダウンロード**アイコンをクリックすると、ローカルにダウンロードすることができます。

名前変更アイコンをクリックすると、バックアップファイル名にプレフィックスを追加できます。

削除アイコンをクリックするとバックアップが削除されます。

9.10 データベースの復元

以下の資料では、Nagios XI でデータベースを復元する手順について説明しています。

Repairing The Nagios XI Database

9.11 ディレクトリ構造

Nagios XI に何が含まれているか、ファイルシステムのどこに存在するのかを理解することは、XI インストレーションのカスタマイズに役立ちます。以下の資料では Nagios XI のディレクトリ構造について説明しています。

ディレクトリ構造

9.12 ログの場所

以下の資料では、Nagios XI サーバ上のログ（Nagios Core ログ、Nagios XI ログ、システムログ）について説明しています。Nagios XI のロギングアーキテクチャについて理解したい管理者向けの情報です。

Logs Locations and Descriptions

9.13 仮想マシンのディスクサイズ変更

以下の資料では、Nagios XI VMware 仮想マシンのディスクサイズを増やす手順について説明しています。仮想マシンのディスクサイズを増やしたい場合は、以下の資料で説明されている作業を行ってください。

VM ディスクサイズの変更

9.14 Microsoft Hyper-VへのNagios XIインポート

以下の資料では、Nagios XI 仮想マシンを Microsoft Hyper-V 環境にインポートする手順を説明しています。Nagios XI 仮想マシンを Microsoft Hyper-V ハイパーバイザー環境で使用したい場合は、以下の資料で説明されている作業を行ってください。

Importing Nagios XI into Microsoft Hyper-V

9.15 性能向上

9.15.1 RAMディスクの使用

以下の資料では、頻繁な Nagios ファイルへのアクセスで I/O タイムを軽減するように RAM ディスクをセットアップする方法について説明しています。

Utilizing A RAM Disk In NagiosXI

9.15.2 リモートサーバーへのMySQLのオフロード

以下の資料では、中央の Nagios XI サーバから外部のリモートサーバーに MySQL サービスをオフロードする手順について説明しています。

Offloading MySQL To A Remote Server

9.15.3 性能向上

以下の資料では、非分散型環境で単一の Nagios XI サーバのアクティブチェック性能を最大化する方法について説明しています。

Maximizing XI Performance

9.15.4 データベースの最適化

Nagios XI はレポートを容易にしたりユーザーに監視対象要素に関する即時性のある情報を提供したりするために現在および過去の情報をさまざまなデータベースに保管しています。Nagios XI データベーステーブルは時間が経過するにつれ、サイズが大きくなりすぎる可能性があります。これは性能の低下、多くのディスクスペース、ディスク I/O 使用をもたらします。以下の資料では適切なデータベース設定を設定する方法について説明しています。

Nagios XI Database Optimization

9.15.5 rrdcachedの使用

以下の資料では、大規模インストレーションにおいて性能を向上させディスク I/O を軽減させるために Nagios で rrdcached を有効化する方法について説明しています。rrdcached は既存の RRD ファイルへのアップデートを受信して蓄積するデーモンです。十分なアップデートを受信するか指定の時間が経過したら、そのアップデートを RRD ファイルに書き込みます。

Using rrdcached with Nagios XI

9.16 リモートNagios XIサーバの管理

Nagios XI サーバの管理は監視サーバが組織のニーズに合うよう設定されていることやアプリケーションアップデート（パッチやアップグレード）が適用されていることを保証するため重要です。
リモートネットワークに存在する Nagios XI サーバの管理機能にアクセスできるようにするには、通常、ファイアウォールやルータの設定が必要です。以下の資料では、リモートの Nagios XI サーバを管理するための要件と方法について説明しています。

Managing Remote Nagios XI Servers

9.17 Ajaxターミナルのインストール

以下の資料では、Ajaxterm を Nagios XI に統合するための手順について説明しています。

Installing Ajax Terminal

10 システム拡張

この章では、Nagios XI システムの機能拡張に関する情報を紹介します。

10.1 コンポーネント

Nagos XI の**「コンポーネント」**は管理者がエンドユーザーおよび管理者の両方のために拡張機能を提供するためにインストールできるオプショナル拡張です。コンポーネントの管理は、**「管理 -> システム拡張 -> コンポーネント管理」**ページで行います。

例えば、新しい通知方法や UI 強化、更新を行うことができます。Nagios XI にコンポーネントをアップロード、インストール、管理する方法については、「コンポーネントのインストール」をお読みください。

カスタムコンポーネントを作成したい場合は、「XI Component Development」をお読みください。

10.2 設定ウィザード

Nagios XI の**「設定ウィザード」**は新しいデバイス、サービス、アプリケーションの監視をユーザーフレンドリーに行う手段を提供します。設定ウィザードの管理は、**「管理 -> システム拡張 -> 設定ウィザード管理」**ページで行います。

新しい設定ウィザードを入手、インストールする手順については、「Nagios XI 設定ウィザードのインストール」をお読みください。

カスタム設定ウィザードを作成したい場合は、「Writing Custom Wizards」をお読みください。

10.3 ダッシュレット

Nagios XI の**「ダッシュレット」**は UI に固有の情報を表示するためのコンテナとして使用できるアドオンです。ダッシュレットは1つ以上のダッシュボードに追加でき、最も有効な情報のルックアンドフィールになるようカスタマイズできます。ダッシュレットの管理は、**「管理 -> システム拡張 -> ダッシュレット管理」**ページで行います。

Nagios XI に新しいダッシュレットをアップロードしインストールする方法については「ダッシュレットのインストール」をお読みください。

10.3.1 Google Map統合

Nagios XI 用の Google Map コンポーネントにより、ホストのステータスを Google Map 上に表示させることができます。以下の資料では、Nagios XI に Google Map インテグレーションコンポーネントをダウンロード、インストール、セットアップする方法について説明しています。

Google Map Integration For Nagios XI

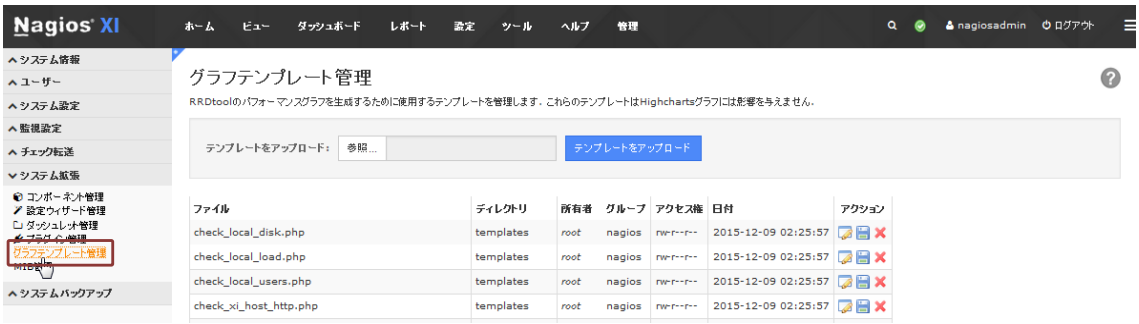
10.4 プラグイン

プラグインの管理は、カスタムまたはサードパーティ製のプラグインをアップロードして監視能力を拡張させたい管理者にとって重要なタスクです。

プラグインの管理方法については、「プラグインの管理」をお読みください。新しいプラグインの発見とインストール、コマンド定義、サービスでの使用についての内容も含みます。

10.5 グラフテンプレート

Nagios XI のパフォーマンスグラフで使用されるグラフテンプレートは、**「グラフテンプレート管理」**ページ(**「管理 -> システム拡張 -> グラフテンプレート管理」**)で行います。



注記: パフォーマンスグラフデータの表示にHighchartsグラフが使用される場合、このページで管理されているグラフテンプレートは使用されません。

10.6 MIB

「MIB」ページ(**「管理 -> システム拡張 -> MIB」**)では Nagios XI にインストール済みの MIB ファイルを管理できます。新しい MIB ファイルのアップロード、不要 MIB ファイルの削除を行えます。

SNMP トラップ受信による監視方法については、「SNMP トラップ統合方法」をお読みください。

10.7 その他のアドオン

利用したいアドオン、プラグイン、拡張が Nagios XI に組み込まれていない場合は、Nagios Exchange で探してみてください。このサイトでは Nagios コミュニティメンバーによって開発されたプラグイン、アドオン、拡張などが公開されています。

11 アップデート

この章では、Nagios XI システムのアップグレードに関する情報を紹介します。

11.1 アップデートの確認

Nagios XI インターフェースの画面下部にある**「更新を確認」**リンクをクリックすると、最新バージョンの有無を簡単に確認できます。

メモ: 新しいタブに Nagios Enterprises 社の「**Product Update Check**」ページが開きます。使用するには、インターネットの接続環境が必要です。

11.2 最新リリース情報の入手

最新の更新およびリリース情報をいち早く入手するには、Nagios Enterprises 社のメールニュースレターをご購読ください。

メモ: 重要な更新については、弊社からもメールニュースでお知らせいたします。

11.3 最新リリースの入手

Nagios XI の最新リリースは、Nagios XI Downloads にあります。このページは Nagios XI の最新開発スナップショットを含みます。

メモ: 弊社のソフトウェアダウンロードページからもダウンロードしていただけます。(ただし動作確認作業等のため、弊社ソフトウェアダウンロードページでの公開は Nagios Enterprises 社のリリースから数日～数週間後となります。また(影響が大きい不具合が見つかった場合など)公開を見送ることがございます。ご理解のほどよろしくお願いいたします。

11.4 アップグレード

既存の Nagios XI インストレーションを手動で最新リリースにアップグレードする方法については、「Nagios XI の手動アップグレード」をお読みください。

Web インターフェースからすばやく簡単にアップグレードしたい場合は、「Web UI でのアップグレード」をお読みください。

Nagios XI を最新バージョンへアップグレードすると、重要なパッチ、バグフィックス、セキュリティ、セキュリティの脆弱性から保護されます。

12 上級トピック

12.1 高可用性

Nagios XI の High Availability (HA) ソリューションは、Nagios XI が常に稼働していて IT インフラストラクチャーを監視していることを保証します。HA の目的は、プライマリの Nagios XI インターフェースが停止またはクラッシュした場合に他のインスタンスが自動的、シームレスに監視ジョブを引き継ぐことです。以下の資料では、Nagios XI で High Availability (HA)を達成するオプションについて説明します。

XI High Availability Options

12.1.1 Nagios XIサーバの監視

Nagios 管理者はたいていプライマリの監視サーバが適切に稼動しておりE メールその他の方法でアラート通知を送信するためインターネットに接続できることを保証する必要があります。以下の資料では、到達可能で適切に稼働していることを保証するために現場から離れた場所でプライマリの Nagios XI サーバを効果的に監視する方法について説明しています。

Monitoring A Nagios XI Server

12.2 Nagios Coreからの移行

以下の資料では、既存の Nagios Core インストレーションを Nagios XI に移行するための基本的な手順について説明しています。

Nagios Core からの移行

12.2.1 設定インポート準備ツール

Nagios XI には XI Web 設定フロントエンドを使用してネイティブの Nagios Core 設定ファイルをより簡単に管理できるフォーマットに事前処理する「設定ファイル準備」ツールがあります。この重要な準備ツールはネイティブの Nagios Core 設定ファイルを Nagios XI の Nagios Core コンフィグマネージャでインポートする前に使用すべきです。以下の資料では、Nagios XI 設定ファイルインポート準備ツールを使用する方法について説明しています。

Nagios XI 設定インポート準備ツールの使用

12.2.2 Nagios XIへの設定ファイルのインポート

Nagios XI には「設定インポート」ツールがあります。以下の資料では、Nagios Core 設定ファイルを XI Web インターフェースからインポートする方法について説明しています。

Nagios Core から Nagios XI へ設定ファイルのインポート

12.3 分散監視

12.3.1 分散監視ソリューション

以下の資料では、Nagios Core および Nagios XI で分散監視ソリューションを提供する方法について説明しています。

Distributed Monitoring Solutions For Nagios

12.3.2 MNTOSとの統合

以下の資料では、Nagios XI または Nagios Core に MNTOS（"Multi-Nagios Tactical Overview System"）監視集約ツールをインストールする方法について説明しています。MNTOS を使用すれば複数の Nagios 監視サーバの統合ビューをセットアップできるので、分散監視環境で役立ちます。

チュートリアルビデオ（英語）： Using MNTOS

Integrating MNTOS

12.3.3 Mod Gearmanとの統合

以下の資料では、Nagios XI システムに Mod Gearman をローカルインストールし、外部のワーカーシステムと一緒に使用する方法について説明しています。これにより Nagios XI マシン上のチェック遅延を減らし性能を向上させます。

Integrating Mod Gearman with Nagios XI

12.3.4 アウトバウンドチェック設定

以下の資料では、Nagios XI でアウトバウンドチェックを設定する方法について説明しています。アウトバウンドチェックは監視サーバがパッシブチェック結果を外部アプリケーションに送信する環境と同じように統合および分散監視環境で使用されます。

Configuring Outbound Checks With Nagios XI

12.3.5 インバウンドチェック設定

以下の資料では、Nagios XI でインバウンドチェックを設定する方法について説明しています。インバウンドチェックは監視サーバがパッシブチェック結果を外部アプリケーションに送信する環境と同じように統合および分散監視環境で使用されます。

Configuring Inbound Checks With Nagios XI

12.3.6 MSPの監視アーキテクチャーソリューション

以下の資料では、Managed Service Providers (MSPs)およびリモートロケーションの大規模組織のデプロイメントに適したさまざまな監視アーキテクチャについて説明しています。

Monitoring Architecture Solutions For MSPs

12.3.7 負荷分散(DNXの使用)

以下の資料では、DNX(Distributed Nagios eXecutor)ロードバランシングアドオンを Nagios Core および Nagios XI と統合する方法について説明しています。DNX は比較的規模の大きいインストレーションで Nagios XI 監視サーバの負荷を軽減させるために使用されます。

Using DNX With Nagios

12.4 Cactiのインストール

以下の資料では、Cacti を Nagios XI サーバにインストールして使用する方法について説明しています。この資料は既に Nagios XI を使用しており、インストール済みの Nagios XI に Cacti を追加することを想定しています。

Installing Cacti Alongside XI

12.5 Amazon EC2 クラウドでのNagios XIの使用

以下の資料では、新しいインストール済み Nagios XI サーバを Amazon EC2 クラウドに立ち上げる方法について説明しています。この資料は新しい Nagios XI インスタンスを Amazon Elastic Compute Cloud (EC2)に立ち上げたい、または既存の Nagios XI インストレーションを Amazon Elastic Compute Cloud (EC2)に移動させたい Nagios XI 管理者を対象としています。

Using Nagios XI In Amazon EC2 Cloud

12.6 Nagios XIでの自動ホスト管理

以下の資料では、コマンドラインからホストおよびサービスを Nagios XI に自動追加、削除する方法について説明しています。管理者の中にはクラウドコンピューティングまたは Puppet や Chef のようなソリューションがインストールされた大規模環境で、Nagios XI にホストやサービスを追加したり削除したりする処理を自動化しなければならない方もいるでしょう。管理者が監視環境の整合性を保持したまま Nagios XI で安全にホストやサービスを追加、削除する独自の自動化ソリューションを作成する手順のアウトラインを示します。

Automated Host Management

12.7 Nagios XIからLinux/Windowsサービスの再起動

管理者は Nagios XI からリモートの Windows ホスト・サービスを効果的に再起動できます。以下の資料では、致命的な状態に陥ったサービスを再起動するイベントハンドラをセットアップする方法を説明しています。

- Windows –

  http://assets.nagios.com/downloads/nagiosxi/docs/Restarting_Windows_Services_With_NRPE.pdf

- Linux –

  http://assets.nagios.com/downloads/nagiosxi/docs/Restarting_Linux_Services_With_NRPE.pdf

以下のリンク先にイベントハンドラを含む Nagios Exchange 投稿があります:

http://exchange.nagios.org/directory/Addons/Event-Handlers/Windows-Service-Restart-Event-Handler/details

12.8 Seleniumとの統合

以下の資料では、Selenium Web テストスクリプトを Nagios と統合する方法について説明しています。開始する前にこの資料をお読みください。

Integrating Selenium with XI

12.9 SSL設定

以下の資料では、SSL のセットアップ方法について説明しています。

SSL 設定

12.10 Nagios XI Active Directoryコンポーネントでの SSL使用

以下の資料では、Nagios XI 用 Active Directory コンポーネントで使用する証明書を Nagios XI サーバにインストールする方法について説明しています。この処理は LDAP サーバが自己署名証明書を持つ場合に必要です。

Using SSL with XI Active Directory

12.11 WAF(Mod_Security)の使用

以下の資料では、Apache Web サーバをもつ Mod_Security と Nagios XI を統合する方法について説明しています。セキュリティの観点から Nagios XI のフロントエンドに Mod_Security をおきたい Nagios XI 管理者向けの資料です。

Integrating Mod_Security With Nagios XI

12.12 イベントハンドラの紹介

以下の資料では、ホストまたはサービスのステータスが変化したときに事前定義アクションを実行するイベントハンドラを使用する方法について説明しています。上級の設定およびスクリプトに関するヒントを含んでいます。サービスの停止や再起動を超えたカスタムイベントハンドラスクリプトを実装したい Nagios XI 管理者向けの資料です。shell スクリプトや Nagios マクロについての基本的な知識が必要となります。

イベントハンドラ入門

13 開発者向け

13.1 イベントハンドラ

こちらをお読みください。

13.2 グローバルイベントハンドラ

こちらをお読みください。

13.3 バックエンドAPI

13.3.1 XI 2014 以前

注記: Nagios XI 5 で廃止されました。新しい REST API を使用してください。

Nagios XI ではバックエンド API を利用して現在のステータス情報などを XML フォーマットで取り出すことができ、Nagios の情報をサードパーティ製アプリケーションや外部の Web サイトと簡単に統合することができます。この資料ではバックエンド API とクエリ情報にアクセスする方法について説明しています。

Accessing The XI Backend API

Nagios XI のホスト/ステータス情報をパブリックなポータルまたはなんらかのディスプレイに統合したい場合、バックエンド API のアクセスコード例に興味があるかもしれません。以下の zip ファイルにはバックエンド API のサンプルコードがいくつか含まれています。必要に応じて編集してご利用ください。

Nagios XI Backend API Example Code

13.3.2 REST API(XI 5 以降)

Nagios XI 5 では、より多くの機能と Nagios XI システムの制御を含む REST API を利用できます。新しい API では、認証済みのコマンドで Nagios XI システムのデータを読取り、書込み、削除、更新できます。出力は JSON 形式です。使用方法については、**「ヘルプ -> Nagios XI API 文書」**をお読みください。

13.4 カスタム設定ウィザードの作成

以下の資料では、Nagios XI でカスタム設定ウィザードを作成する方法を説明しています。この資料はカスタムプラグインを使用して新しいウィザードを作成する、Nagios XI フレームワーク内でプログラミングツールを使用する方法についてもカバーしています。

Writing Custom Wizards

13.5 カスタムコンポーネントの作成

以下の資料では、Nagios XI コンポーネントを作成するためのフレームワークの利用方法について説明しています。

XI Component Development

13.6 autoIT統合

13.6.1 autoITスクリプトの使用

以下の資料では、リモートの Windows マシンで URL の読み込み時間をキャプチャし、NRPE を介して Nagios XI プラグインにプッシュして、nagios サービスにデータを戻す autoIT スクリプトを作成する方法について説明しています。

Using autoIT scripts with NRPE checks and Nagios XI

autoIT Timer プラグインの例はここにあります。

13.6.2 autoITチェックの使用

以下の資料では、autoIT スクリプト Windows シーケンス(.au3 ファイル)を Nagios での NRPE チェックを作成するバッチファイルと組み合わせる方法について説明しています。Windows システム上でオートメーションスクリプトを実行する NRPE チェックを作成したい管理者向けの資料です。

Using autoIT Checks with Nagios

13.6.3 autoITでのプログラム読み込み時間のチェック

以下の資料では、リモートの Windows マシンでプログラムの読み込み時間をキャプチャし、NRPE を介して Nagios XI プラグインにプッシュし、データを nagios サービスに戻す autoIT スクリプトの作成方法について説明しています。

Checking Program Loadtime With autoIT

autoIT Timer プラグインの例はここにあります。

13.7 アクションコンポーネントの作成

以下の資料では、アクションコンポーネントの作成方法について説明しています。

Actions Component

14 最後に

Nagios XI のユーザー権限レベルの使用方法（基本機能、監視結果の閲覧など）については、別ガイド「Nagios XI ユーザーガイド」をお読みください。

その他、Nagios XI に関する情報は以下にあります。

- ナレッジベース：
  Nagios Support Knowledgebase（英語）ページ。Nagios XI 関連ドキュメント、トラブルシューティング情報が掲載されています。

- Nagios XI トラブルシューティング：
  Common Problems Articles（英語）ページ。Nagios XI に関するトラブルとその解決策についての情報が掲載されています。

- サポートフォーラム：
  Nagios Support Forum（英語）ページが開きます。Nagios XI に関する投稿を閲覧したり自分の質問やノウハウを投稿しコミュニティで共有したりすることができます。

- Nagios ライブラリ：
  Nagios Library（英語）ページが開きます。Nagios 製品に関するチュートリアル、ビデオ、ヒント、ベストプラクティスなどのナレッジがまとめられています。一部の情報には Nagios 製品のライセンスを保有している方のみがアクセスできます。

お問い合わせ

弊社では、Nagios XI に関するご意見、フィードバックをお待ちしております。

ジュピターテクノロジー株式会社（Jupiter Technology Corp.）

住所：　〒183-0023 東京都府中市宮町 2-15-13 第 15 三ツ木ビル 8F
URL：　http://www.jtc-i.co.jp/
電話番号：　042-358-1250
FAX 番号：　042-360-6221
ご購入のお問い合わせ：
　お問い合わせフォーム　https://www.jtc-i.co.jp/contact/scontact.php
　メール　sales@jtc-i.co.jp
製品サポートのお問い合わせ：
　カスタマーポータル　https://www.jtc-i.co.jp/support/customerportal/

日本語マニュアル発行日 2017 年 02 月 06 日
本マニュアル原文 Nagios XI Administrator Guide
（構成および内容を変更しています）

ジュピターテクノロジー株式会社