MICRO FOCUS

ZENworks 2017 Update 3
管理クイックスタート

2018 年 8 月

保証と著作権

保証と著作権、商標、免責事項、保証、輸出およびその他の使用制限、米国政府の規制による権利、特許ポリシー、および FIPS コンプライアンスの詳細については、https://www.novell.com/company/legal/ を参照してください。

目次

このガイドについて

この『*ZENworks 管理クイックスタート*』は、ZENworks Management システムを管理するための基本事項を短期間で習得するために役立ちます。ZENworks システムがインストールされている必要があります。まだインストールしていない場合は、『*ZENworks サーバインストールガイド*』を参照してください。

このガイドの情報は、次のように構成されます。

- (9 ページ) システム設定 : ZENworks 製品を使用する前に、ZENworks 管理ゾーンの設定について説明します。
- (55 ページ) 製品管理 : ZENworks 製品 (Asset Management、Configuration Management、Endpoint Security Management、Full Disk Encryption、および Patch Management) の使用方法について説明します。

対象読者

本ガイドは、ZENworks システムの設定、ZENworks システムの監視、あるいはデバイスまたはユーザの管理に関係する ZENworks のタスクを実行するすべてのユーザ向けに作成されています。

フィードバック

本マニュアルおよびこの製品に含まれているその他のマニュアルについて、皆様のご意見やご要望をお寄せください。オンラインヘルプの各ページの下部にある、*comment on this topic* リンクを使用してください。

その他のマニュアル

ZENworks には、製品について学習したり、製品を実装したりするために使用できるその他のマニュアル (PDF 形式および HTML 形式の両方) も用意されています。追加のマニュアルについては、ZENworks マニュアル Web サイト (http://www.novell.com/documentation/zenworks2017) を参照してください。

システム設定

次のセクションでは、ZENworks システムの設定について説明します。設定タスクは、使用している ZENworks 製品 (Configuration Management、Patch Management、Asset Management、および Endpoint Security Management) のいずれについても必要です。

1 クイックリスト

ZENworks サーバ (または複数のサーバ) をインストールしたら、ZENworks の時間の節約に役立つすべての機能を使用できるようになります。

ライセンス版または評価版の ZENworks 製品 (Configuration Management、Patch Management、Asset Management、Endpoint Security Management、および Full Disk Encryption) の使用を開始する前に、次のセクションの概念やタスクを確認する必要があります。これらのセクションでは、管理ゾーンの設定のために知っておくべき事項とその操作について簡単に説明します。

管理ツール

ZENworks には、ZENworks システムを管理するために Web ベースのコンソール (ZENworks コントロールセンター) とコマンドラインユーティリティ (zman) の両方が提供されています。少なくとも ZENworks コントロールセンターに習熟している必要があります。

タスク		詳細
	ZENworks コントロールセンターの起動	方法については、17 ページの 「ZENworks コントロールセンター」を参照してください。
	zman ユーティリティの実行方法の学習	zman ユーティリティは、ZENworks コントロールセンターと同様のタスクの多くを実行できるコマンドラインインタフェースです。 方法については、19 ページの 「zman コマンドラインユーティリティ」を参照してください。
	zac ユーティリティの実行方法の学習	zac ユーティリティは、ZENworks Agent のコマンドラインインタフェースです。 方法については、21 ページの 「zac コマンドラインユーティリティ」を参照してください。

ゾーン設定

管理ゾーンのインストール時にアクティブ化した ZENworks 製品が提供する管理機能をフル活用するには、管理ゾーンを確実に正しく設定するためにいくつかの設定タスクを実行する必要があります。

タスク		詳細
	デバイスの構成用フォルダおよびグループの作成	ZENworks 環境設定の適用および同様のデバイス上でのタスクの実行に関するオーバーヘッドを簡単にするためにデバイスをフォルダおよびグループに構成します。個々のデバイスで割り当てを行ったり、タスクを実行するのではなく、フォルダまたはグループにある各デバイスで割り当てやタスクを継承しながら、フォルダやグループを管理できます。 方法については、23 ページの 「デバイスの構成 : フォルダとグループ」を参照してください。
	登録キーまたはルールの作成	ZENworks Agent は管理するそれぞれのデバイスに展開する必要があります。ZENworks Agent をデバイスに展開するとき、デバイスは管理ゾーンに登録されます。 登録キーまたは登録ルールを使用して、自動的にデバイスを適切なフォルダおよびグループに割り当て、フォルダおよびグループに関連付けられている割り当てをデバイスに迅速に継承させることができます。 方法については、27 ページの 「登録キーおよび登録ルールの作成」を参照してください。
	ユーザソースの追加	ZENworks の信頼されたユーザソースを提供する 1 つまたは複数の LDAP ディレクトリに接続できます。 ユーザソースを追加すると、ZENworks 管理者アカウントと LDAP ユーザアカウントを関連付け、デバイスと、デバイスを主に使用するユーザを関連付けることができます。また、ユーザを追加すると、次の ZENworks 製品の機能を追加することができます。 ◆ **環境設定の管理 :** バンドルおよびポリシーをユーザやデバイスに割り当てることができます。ユーザベースのインベントリレポートを使用できます。 ◆ **Asset Management:** ソフトウェアライセンスをユーザ単位およびデバイス単位で示すことができます。 ◆ **Endpoint Security Management:** ポリシーをユーザやデバイスに割り当てることができます。 方法については、29 ページの 「ユーザソースへの接続」を参照してください。

タスク		詳細
	追加管理者アカウントの作成	インストール中に、デフォルトの ZENworks 管理者アカウント (Administrator) が作成されます。これはスーパー管理者アカウントです。管理ゾーン内での完全な管理権を持ちます。 追加管理者アカウントを作成し、スーパー管理者権限を付与することができます。または、制限された権限を持つ管理者アカウントを作成して、管理者のアクセス可能なタスク、デバイス、およびユーザの範囲を制限することができます。 方法については、30 ページの 「管理者アカウントの作成」を参照してください。
	管理者グループアカウントの作成	管理者グループを作成することを選択できます。管理者グループに権利と役割を割り当てる場合は、割り当てられた権利と役割はグループ内のすべてのメンバーに適用できます。 方法については、31 ページの 「管理者グループアカウントの作成」を参照してください。
	ゾーン環境設定の変更	管理ゾーンは最も一般的な設定に事前設定されています。現時点で設定を変更する必要はありませんが、大まかな設定を確認しておきたいこともあります。 方法については、32 ページの 「環境設定の変更」を参照してください。
	ZENworks ソフトウェアの更新	システム更新機能を使用すると、タイムリーに ZENworks ソフトウェアのアップデートを入手できるだけでなく、アップデートのダウンロードをスケジュールすることもできます。 方法については、33 ページの 「ZENworks ソフトウェアの更新」を参照してください。
	場所の作成	セキュリティポリシーはグローバルに適用することも、固有の場所に適用することもできます。グローバルポリシーはすべての場所に適用されます。場所ベースのポリシーは、デバイスのネットワーク環境がその場所に定義された環境に一致すると ZENworks Agent が判断する場合にのみ適用されます。 方法については、34 ページの 「場所の作成」を参照してください。

エージェントの展開

ZENworks Agent は、ZENworks サーバと通信して、デバイスで管理タスクを実行します。管理するすべてのデバイスに ZENworks Agent を展開する必要があります。ZENworks Agent を展開することにより、エージェントファイルをインストールし、デバイスを管理ゾーンに登録します。

タスク		詳細
	ZENworks Agent 機能の有効化	ZENworks Agent には、各 ZENworks 製品 (Asset Management、Configuration Management、Endpoint Security Management、Full Disk Encryption、および Patch Management) に固有の機能が含まれています。デフォルトでは、アクティブ化した製品 (ライセンス版および評価版) の機能は管理ゾーンのインストール時に有効になります。ただし、ZENWorks コントロールセンターの環境設定を確認する必要があります。 方法については、37 ページの 「ZENworks Agent 機能の設定」を参照してください。
	ZENworks Agent の保護	ZENworks Agent のアンインストールおよびセルフディフェンスの設定を行うことができます。 方法については、39 ページの 「ZENworks Agent のセキュリティの設定」を参照してください。
	ZENworks Agent のインストール	ZENworks Agent をデバイスにインストールするにはさまざまな方法があります。 • ZENworks コントロールセンターを使用してエージェントを ZENworks サーバからデバイスに展開します。 • デバイス側では、Web ブラウザを使用して ZENworks サーバからエージェントをダウンロードし、インストールします。 • エージェントをイメージに含め、イメージをデバイスに適用します。 方法については、40 ページの 「ZENworks Agent のインストール」を参照してください。
	ZENworks Agent へのログインと使用	デバイスでユーザ割り当て済みバンドルおよびポリシーを受け取るには、管理ゾーンにログインする必要があります。 方法については、44 ページの 「ZENworks Agent の使用」を参照してください。

システムメッセージ

ゾーン内で管理タスクを実行すると、情報が記録されてゾーンの状態とそこで行われているアクティビティを参照できるようになります。

タスク		詳細
	システムメッセージの表示	ZENworks システムは、情報、警告およびエラーメッセージを生成して、ソフトウェアの配布やポリシーの適用などのアクティビティを監視する手助けとなります。 方法については、47 ページの 「システムメッセージの参照」を参照してください。

タスク		詳細
	ウォッチリストの作成	アクティビティを詳しく監視したいデバイス、バンドル、およびポリシーがある場合、それらをウォッチリストに追加できます。 方法については、49 ページの 「ウォッチリストの作成」を参照してください。

2 管理ツール

ZENworks では、ZENworks システムを管理するために、Web ベースのコンソール (ZENworks コントロールセンター) とコマンドラインユーティリティ (zman) の両方が提供されています。次のセクションでは、管理ツールのアクセス方法および使用法について説明します。

ZENworks コントロールセンター

ZENworks コントロールセンターは、管理ゾーンのすべての ZENworks サーバにインストールされます。どの ZENworks サーバでも、すべての管理タスクを実行できます。ZENworks コントロールセンターは、Web ベースの管理コンソールなので、任意のサポートされているワークステーションからアクセスできます。

Novell iManager を使用してネットワーク環境でその他の Micro Focus 製品を管理する場合、ZENworks コントロールセンターを有効にして iManager から起動できます。詳細については、「Novell iManager を使用したコントロールセンターへのアクセス」(『*ZENworks コントロールセンターリファレンス*』) を参照してください。

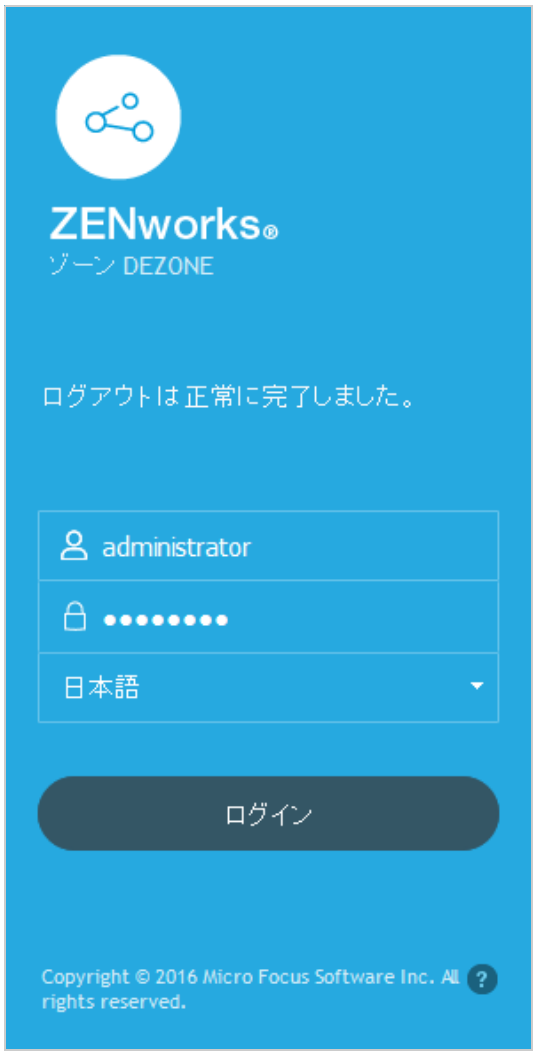
ZENworks コントロールセンターへのアクセス

1 Web ブラウザで、次の URL を入力します。

`https://`*`ZENworks_Server_Address:port`*

ZENworks_Server_Address は、ZENworks サーバの IP アドレスまたは DNS 名に置き換えてください。デフォルトポート (80 または 443) を使用していない場合は、*port* の指定が必要です。ZENworks コントロールセンターには HTTPS 接続が必要です。HTTP 要求は、HTTPS にリダイレクトされます。

［ログイン］ダイアログボックスが表示されます。



2 ［ユーザ名］フィールドに「Administrator」と入力します。

3 ［パスワード］フィールドには、インストール時に作成した管理者パスワードを入力します。

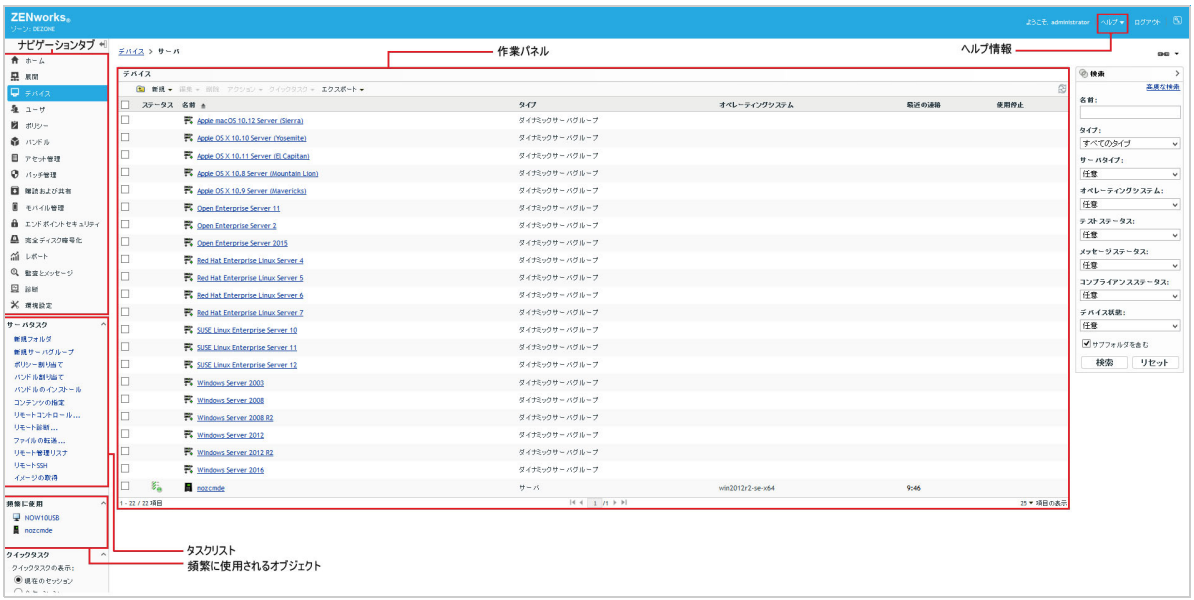
認可されていないユーザが ZENworks コントロールセンターにアクセスできないようにするために、ログインの試行で 3 回失敗した場合、管理者アカウントが無効化されます。また、ログインを再度試行するまでに、60 秒のタイムアウトが実施されます。これらのデフォルト値を変更する場合は、「デフォルトのログインを無効にする値の変更」(『*ZENworks コントロールセンターリファレンス*』) を参照してください。

4 ［ログイン］をクリックして ZENworks コントロールセンターを表示します。

別の管理者としてログインする方法の詳細については、「コントロールセンターへのアクセス」(『*ZENworks コントロールセンターリファレンス*』) を参照してください。

ZENworks コントロールセンターの操作

次の［サーバ］ページは、ZENworks コントロールセンターの標準的な画面を示しています。



ナビゲーションタブ : 左側のウィンドウのタブを使用すると、ZENworks の機能領域を移動できます。たとえば、このサーバページでは、サーバに関連付けられたタスクを管理できます。

タスクリスト : 左側のウィンドウのタスクリストからは、現在のページで最も頻繁に実行するタスクにすばやくアクセスできます。タスクリストはページごとに異なります。たとえば、［デバイス］ページのタスクリストにはデバイス関連のタスクが、［環境設定］ページのタスクリストには環境設定関連のタスクがそれぞれ表示されます。

頻繁に使用されるオブジェクト : 左側のウィンドウの［頻繁に使用］リストには、最も使用頻度の高い順から低い順に、アクセスした上位 10 のオブジェクトが表示されます。オブジェクトをクリックすると、直接そのオブジェクトの詳細ページに移動します。

作業パネル : 作業パネルでは、ZENworks システムの管理および監視を行います。パネルは、現在のページによって異なります。上の例では、［デバイス］と［検索］という 2 つの作業パネルがあります。［デバイス］パネルには、サーバ、フォルダ、サーバグループ、作成されたダイナミックサーバグループのリストが表示されます。このパネルはサーバの管理に使用します。［検索］パネルでは、サーバ名、オペレーティングシステム、ステータスなどの条件に従って［デバイス］パネルをフィルタリングできます。

ヘルプ情報 : ［ヘルプ］ボタンは、現在のページに関する情報が提供されているヘルプトピックにリンクされています。［ヘルプ］ボタンのリンクは、現在のページによって異なります。

zman コマンドラインユーティリティ

zman ユーティリティは、ZENworks コントロールセンターで多くのタスクを実行するためのコマンドライン管理インタフェースを提供します。たとえば、コンテンツをバンドルに追加したり、ポリシーをデバイスに割り当てたり、デバイスを登録したりできます。コマンドラインユーティリ

ティを使用する主な利点は、繰り返し操作または一括操作を処理するためのスクリプトを作成できることです。ZCC と同様に、zman ユーティリティはすべてのプライマリサーバにインストールされますが、実行できるのはサーバ上のコマンドラインからのみです。

zman ユーティリティの主要な目的は、スクリプトによって操作を実行できるようにすることです。ただし、コマンドラインから手動で操作を実行することもできます。

- 20 ページの 「ディレクトリ」
- 20 ページの 「構文」
- 20 ページの 「コマンドのヘルプ」

ディレクトリ

このユーティリティは、次の場所のすべての ZENworks サーバにインストールされます。

%ZENWORKS_HOME%\bin

%ZENWORKS_HOME% は、ZENworks のインストールパスを示します。Windows では、デフォルトパスは C:\Program Files (x86)\Novell\Zenworks\bin です。Linux では、デフォルトパスは /opt/novell/zenworks/bin です。

構文

zman ユーティリティの基本的な構文は次のとおりです。

zman *category-action* [*options*]

たとえば、ソフトウェアバンドルをデバイスに割り当てる場合、次のコマンドを使用します。

zman bundle-assign workstation bundle1 wks1

ここで、bundle-assign が category-action となり、オプションは workstation bundle1 wks1 です。この例では、option はデバイスタイプ (workstation)、バンドル名 (bundle1)、およびターゲットデバイス (wks1) です。

たとえば、デバイスのインベントリスキャンを開始するには、次のコマンドを使用します。

zman inventory-scan-now device/servers/server1

ここで、inventory-scan-now は category-action となり、device/servers/server1 はスキャン対象のデバイスのフォルダパスを指定するオプションです。

コマンドのヘルプ

コマンドを理解するには、オンラインヘルプを使用するか、『*ZENworks コマンドラインユーティリティリファレンス*』の「zman(1)」を参照することが早道です。

オンラインヘルプを使用するには、次の操作を行います。

1. ZENworks サーバのコマンドプロンプトで「zman --help」と入力します。

このコマンドでは、基本的な使用法 (構文) および使用可能なコマンドカテゴリのリストが表示されます。または次のように入力してヘルプを使用することもできます。

コマンド	説明
zman --help | more	カテゴリ別にすべてのコマンドが一覧表示されます。
zman *category* --help | more	カテゴリ内のすべてのコマンドが一覧表示されます。
zman *command* --help | more	コマンドのヘルプが表示されます。

zac コマンドラインユーティリティ

zac ユーティリティには、ZENworks Agent で使用できるタスクを実行できるコマンドライン管理インタフェースが提供されています。

- 21 ページの 「ディレクトリ」
- 21 ページの 「構文」
- 22 ページの 「コマンドのヘルプ」

ディレクトリ

このユーティリティは、次の場所のすべての Windows 管理対象デバイスにインストールされます。

%ZENWORKS_HOME%\bin

%ZENWORKS_HOME% は、ZENworks のインストールパスを示します。デフォルトパスは、32 ビット Windows デバイスでは c:\program files\novell\zenworks\bin、64 ビット Windows デバイスでは c:\program files (x86)\novell\zenworks\bin です。

構文

zac ユーティリティでは、次の基本的な構文を使用しています。

zac *コマンド/オプション*

たとえば、バンドルをデバイスで起動するには、次のコマンドを使用します。

zac bundle-launch "bundle 1"

ここで、bundle-launch がコマンドとなり、コマンドオプションは bundle 1 です。この例では、オプションは起動されるバンドルの表示名です。バンドルの表示名にスペースが含まれている場合は、引用符で囲む必要があります。

たとえば、インベントリスキャンをデバイスで開始するには、次のコマンドを使用します。

zac inv scannow

ここで、inv がコマンドとなり、コマンドオプションは scannow です。

コマンドのヘルプ

コマンドを理解するには、オンラインヘルプを使用するか、『*ZENworks コマンドラインユーティリティリファレンス*』の「zac for Windows(1)」を参照することが早道です。

オンラインヘルプを使用するには、次の操作を行います。

1 管理対象デバイスのコマンドプロンプトで、次のコマンドのいずれかを入力します。

コマンド	説明
zac --help	すべてのコマンドを一覧表示します。
zac *command* --help	コマンドの詳細なヘルプが表示されます。

3 管理ゾーンの環境設定

ZENworks では、最小の努力で多数のデバイスおよびユーザを効率的に管理できます。この管理作業の最初のステップは、ZENworks の機能のすべての利点を利用できるように管理ゾーンを確実に設定することです。

次のセクションでは、実行する継続的な管理タスクを最大限にサポートする管理ゾーンをセットアップするために理解しておく必要がある基本概念について説明します。それぞれの項目は管理概念を説明し、概念に関連するタスクを実行するための一般的なステップを提供します。

デバイスの構成：フォルダとグループ

ZENworks コントロールセンターを使用して、個々のデバイスオブジェクトで直接タスクを実行してデバイスを管理できます。ただし、この方法は管理するデバイスが少ない場合にのみ効率的です。多数のデバイスの管理を最適化するため、ZENworks ではデバイスをフォルダおよびグループに分類し、フォルダまたはグループごとにタスクを実行してデバイスを管理できます。

フォルダおよびグループは、いつでも作成できます。ただし、最もよい方法はフォルダおよびグループを作成し、デバイスをゾーンに登録することです。これによって、登録キーおよびルールを使用して、デバイスの登録時に自動的にデバイスを適切なフォルダおよびグループに追加することができます (27 ページの 「登録キーおよび登録ルールの作成」を参照)。

フォルダ

フォルダは、デバイスを整理してデバイスの管理を簡素化するための優れたツールです。すべてのフォルダ上で、環境設定の適用、コンテンツの割り当て、およびタスクの実行を行えます。この場合、フォルダのデバイスはその設定、割り当て、タスクを継承します。

最適の結果を得るには、類似の環境設定要件のデバイスを同じフォルダに配置することです。フォルダ内のすべてのデバイスで同じコンテンツまたはタスクが必要な場合、フォルダにコンテンツを割り当てることもできます。ただし、フォルダ内のすべてのデバイスが同じコンテンツ、タスクの要件を持っているとは限りません。したがって、デバイスをグループに分類し、適切なコンテンツとタスクを各グループに割り当てることができます (次の 25 ページの 「グループ」を参照)。

たとえば、3 つの異なるサイトにワークステーションがあるとします。3 つのサイトのワークステーションに対して異なる環境設定を適用するとします。その場合は、次の 3 つのフォルダ (/Workstations/Site1、/Workstations/Site2、および /Workstations/Site3) を作成し、各フォルダに該当するワークステーションを配置します。すべてのワークステーションに対してほとんど同じ構成の設定を適用するため、これらの設定は管理ゾーンで行います。ただし、サイト 1 とサイト 2 ではソフトウェアインベントリおよびハードウェアインベントリの収集を毎週実行し、サイト 3 では月に 1 回だけ収集を実行します。管理ゾーンでインベントリの収集を毎週に設定し、サイト 3 のフォルダを上書きして毎月を適用します。サイト 1 とサイト 2 ではインベントリを週次で収集し、サイト 3 ではインベントリを月次で収集します。

フォルダの作成

1 ZENworks コントロールセンターで、［デバイス］タブをクリックします。

2 ［ワークステーション］フォルダ 、［サーバ］フォルダ、または［モバイルデバイス］フォルダをクリックします。

3 ［新規］>［フォルダ］の順にクリックし、［新規フォルダ］ダイアログボックスを表示します。

4 ［名前］フィールドに新しいフォルダの名前を入力します。

ZENworks コントロールセンターの中でオブジェクト (フォルダ、グループ、バンドル、ポリシーなど) に名前を付ける場合は、名前が以下の規則に従うようにしてください :

- 名前はフォルダ内で一意である必要があります。
- ZENworks データベースに使用されているデータベースソフトウェアによっては、同じ名前に対して大文字および小文字が区別されない場合があります。ZENworks に含まれる組み込みデータベースは大文字と小文字を区別しないため、「Folder 1」と「FOLDER 1」は同じ名前と見なされ、同じフォルダ内で使用することはできません。大文字と小文字を区別する外部データベースを使用している場合、Folder 1 と FOLDER 1 は別個となります。
- 空白を使用する場合、コマンドラインに名前を入力するには、引用符で囲む必要があります。たとえば、zman ユーティリティで「Folder 1」と入力するには、引用符で囲む必要があります (“Folder 1”)。
- 次の文字は無効なので使用できません。/ \ * ? : " ' < > | ` % ~

5 ［OK］をクリックしてフォルダを作成します。

また、zman ユーティリティで workstation-folder-create および server-folder-create コマンドを使用してデバイスフォルダを作成することもできます。詳細については、『*ZENworks コマンドラインユーティリティリファレンス*』の「ワークステーションコマンド」および「サーバコマンド」を参照してください。

グループ

フォルダと同様、デバイスグループにコンテンツを割り当て、タスクを実行することもできます。この場合、グループのデバイスはその割り当てとタスクを継承します。フォルダとは異なり、環境設定をグループに適用することはできません。

グループにより、コンテンツ割り当てとタスクに層が追加され、柔軟性が増します。一部のケースで、フォルダにあるすべてのデバイスでデバイスに同じコンテンツを割り当てて同じタスクを実行したくない場合があります。また、別のフォルダ内の 1 つ以上のデバイスでデバイスに同じコンテンツを割り当ててタスクを実行したい場合があります。これを行うには、デバイスをグループに追加して (どのフォルダにデバイスが含まれているかにかかわりなく)、コンテンツをグループに割り当ててタスクを実行します。

たとえば、また 3 つのサイトのワークステーションの例で見てみましょう (24 ページの 「フォルダ」を参照)。各サイトのいくつかのワークステーションで同じ会計ソフトウェアが必要であるとします。グループに対してソフトウェアを割り当てることが可能であるため、Accounting グループを作成し、対象となるワークステーションをそのグループに追加し、適切な会計ソフトウェアをそのグループに割り当てます。同様に、グループを使用して、Windows 環境設定ポリシーおよびセキュリティポリシーを割り当てることができます。

グループに対して割り当てを行う利点は、そのグループに含まれるすべてのデバイスが割り当てを受け取りますが、割り当ては 1 回実行するだけですみます。さらに、1 つのデバイスが複数の一意のグループに属することができ、複数のグループからの割り当てを受け取ることができます。たとえば、あるデバイスをグループ A とグループ B に割り当てるとすると、デバイスは両方のグループに割り当てられたソフトウェアを継承します。

ZENworks ではグループと動的グループの両方が提供されています。コンテンツ割り当て、またはタスクの実行の観点から見ると、グループおよびダイナミックグループ機能はまったく同じです。2 つのタイプのグループの唯一の違いは、グループにデバイスを追加する方法です。グループの場合は、手動でデバイスを追加する必要があります。ダイナミックグループでは、グループのメンバーに合致するデバイスの条件を定義しておき、デバイスがその条件に一致すると自動的に追加されます。

ZENworks には、いくつかの事前定義されたダイナミックサーバグループ (Windows 2012 Server、Windows 2003 Server、SUSE Linux Enterprise Server など) が含まれています。

ZENworks には、ダイナミックワークステーショングループ (Windows XP Workstation、Windows 8 Workstation、Windows Vista Workstation、SUSE Linux Enterprise Desktop など) も含まれています。これらのオペレーティングシステムを持つデバイスは、該当するダイナミックグループに自動的に追加されます。

グループの作成

1 ZENworks コントロールセンターで、［デバイス］タブをクリックします。

2 サーバ用のグループを作成する場合は、［サーバ］フォルダをクリックします。

または

ワークステーション用のグループを作成する場合は、［ワークステーション］フォルダをクリックします。

または

モバイルデバイス用のグループを作成する場合は、［モバイルデバイス］フォルダをクリックします。

3 ［新規］>［サーバグループ］(ワークステーションの場合は［新規］>［ワークステーショングループ］、モバイルデバイスの場合は［新規］>［モバイルデバイスグループ］) の順にクリックして、新しいグループの作成ウィザードを起動します。

4 ［基本情報］ページで、［グループ名］フィールドに新規グループの名前を入力し、［次へ］をクリックします。

グループ名は命名規則に準拠している必要があります。

5 ［サマリ］ページで［完了］をクリックし、メンバーを追加しないでグループを作成します。

または

グループにメンバーを追加する場合は［次へ］をクリックしてからステップ 6 に進みます。

6 ［グループメンバの追加］ページで、［追加］をクリックしてグループにデバイスを追加し、デバイスの追加が完了したら［次へ］をクリックします。

7 ［サマリ］ページで［完了］をクリックしてグループを作成します。

また、zman ユーティリティで workstation-group-create および server-group-create コマンドを使用してデバイスグループを作成することもできます。詳細については、『*ZENworks コマンドラインユーティリティリファレンス*』の「ワークステーションコマンド」および「サーバコマンド」を参照してください。

ダイナミックグループの作成

1 ZENworks コントロールセンターで、［デバイス］タブをクリックします。

2 サーバ用のグループを作成する場合は、［サーバ］フォルダをクリックします。

または

ワークステーション用のグループを作成する場合は、［ワークステーション］フォルダをクリックします。

または

モバイルデバイス用のグループを作成する場合は、［モバイルデバイス］フォルダをクリックします。

3 ［新規］>［ダイナミックサーバグループ］(ワークステーションの場合は［新規］>［ダイナミックワークステーショングループ］、モバイルデバイスの場合は［新規］>［ダイナミックモバイルデバイスグループ］) の順にクリックして、新しいグループの作成ウィザードを起動します。

4 ［基本情報］ページで、［グループ名］フィールドに新規グループの名前を入力し、［次へ］をクリックします。

グループ名は命名規則に準拠している必要があります。

5 ［グループメンバー用のフィルタの定義］ページで、デバイスがグループのメンバーになるために満たす必要がある条件を定義して、［次へ］をクリックします。

［ヘルプ］ボタンをクリックすると、条件の作成の詳細が表示されます。

6 ［サマリ］ページで、［完了］をクリックしてグループを作成します。

フォルダおよびグループの割り当ての継承

フォルダにコンテンツを割り当てる場合、フォルダ内にあるグループを除くすべてのオブジェクト (ユーザ、デバイス、サブフォルダ) が割り当てを継承します。たとえば、BundleA と PolicyB を DeviceFolder1 に割り当てると、フォルダ内のすべてのデバイス (サブフォルダ内のすべてのデバイスも含む) がその 2 つの割り当てを継承します。ただし、DeviceFolder1 にあるデバイスグループは、割り当てを継承しません。原則的に、フォルダの割り当ては、そのフォルダ内にあるグループには適用されません。

登録キーおよび登録ルールの作成

ZENworks Agent をデバイスに展開するとき、デバイスは管理ゾーンに登録され、管理対象デバイスとなります。登録の一貫として、デバイスの ZENworks 名およびデバイスを追加するフォルダまたはグループを指定できます。

デフォルトでは、デバイスの ZENworks 名としてデバイスのホスト名が使用され、/Servers または /Workstations フォルダに追加され、他のグループのメンバーにはなりません。手動でデバイスを別のフォルダに移動してグループに追加できますが、デバイスの数が多い場合や新規デバイスを連続して登録する場合には、面倒な仕事である場合もあります。大量のデバイスを管理する最もよい方法は、登録時にデバイスを自動で正しいフォルダおよびグループに追加することです。

登録時にデバイスをフォルダおよびグループに追加するには、登録キーまたは登録ルール、あるいはその両方を使用できます。登録キーまたは登録ルールの両方とも、フォルダおよびグループメンバーをデバイスに割り当てることができます。ただし、登録にどちらか 1 つまたは両方を使用するかどうかを選択する前に、キーとルールには違いがあることに留意してください。

この機能はモバイルデバイスには該当しません。

- 27 ページの 「登録キー」
- 28 ページの 「登録ルール」
- 28 ページの 「デバイス命名テンプレート」
- 29 ページの 「その他の情報の参照場所」

登録キー

登録キーは、手動で定義またはランダムに生成された英数字の文字列です。デバイスに ZENworks Agent を展開中に、登録キーが提供されなければなりません。最初にデバイスを ZENworks サーバに接続するときに、デバイスはキー内に定義されているフォルダまたはグループに追加されます。

1 つまたは複数の登録キーを作成して、デバイスが希望のフォルダおよびグループ内にあるようにすることができます。たとえば、すべての販売部のワークステーションが /Workstations/Sales フォルダに追加されているが、チーム割り当てによって、これが 3 つのグループ (SalesTeam1、SalesTeam2、SalesTeam3) に分かれるようにすることができます。3 つの登録キーを作成して、各キーを設定し、販売部のワークステーションを /Workstations/Sales フォルダと適切なチームグループに追加することもできます。各ワークステーションが正しい登録キーを使用している限りは、これは適切なフォルダおよびグループに追加されます。

登録キーを作成するには、次の手順に従います。

1. ZENworks コントロールセンターで、［設定］タブをクリックし、次に［登録］タブをクリックします。
2. ［登録キー］パネルで、［新規作成］>［登録キー］の順にクリックして、新規登録キーの作成ウィザードを起動します。
3. プロンプトに従って、キーを作成します。

   ウィザードの各ステップで何を指定するかの詳細については、［ヘルプ］ボタンをクリックしてください。

zman ユーティリティで registration-create-key コマンドを使用して登録キーを作成することもできます。詳細については、『*Zenworks コマンドラインユーティリティリファレンス*』の「登録コマンド」を参照してください。

登録ルール

展開中に登録キーを入力しない場合、またはデバイスを自動的に前もって定義された条件 (オペレーティングシステムタイプ、CPU、または IP アドレスなど) に基づいて別のフォルダおよびグループに追加しない場合は、登録ルールを使用できます。

ZENworks には、サーバとワークステーションについてそれぞれ別のデフォルト登録ルールがあります。キーを使わずにデバイスを登録し、登録ルールが作成されていない場合、デフォルトの登録ルールが適用されて、フォルダの割り当てが決まります。2 つのデフォルトルールによって、すべてのサーバは /Servers フォルダに追加され、すべてのワークステーションは /Workstations フォルダに追加されます。

2 つのデフォルトルールは、サーバまたはワークステーションの登録が失敗しないように指定されています。したがって、これら 2 つのデフォルトルールを削除したり変更したりすることはできません。ただし、デバイスの登録時にデバイスをフィルタして異なるフォルダやグループに追加できるようにする追加のルールを定義できます。23 ページの 「デバイスの構成 : フォルダとグループ」で推奨されているように、類似した環境設定を持つデバイス用のフォルダ、および類似した割り当てを持つデバイス用のグループがすでに作成されている場合、新しく登録されたデバイスは自動的に該当する環境設定および割り当てを継承します。

登録ルールを作成するには、次の手順に従います。

1. ZENworks コントロールセンターで、［設定］タブをクリックし、次に［登録］タブをクリックします。
2. ［登録ルール］パネルで、［新規作成］をクリックして新規登録ルールの作成ウィザードを起動します。
3. プロンプトに従って、ルールを作成します。

   ウィザードの各ステップで何を指定するかの詳細については、［ヘルプ］ボタンをクリックしてください。

zman ユーティリティで ruleset-create コマンドを使用して登録ルールを作成することもできます。詳細については、『*ZENworks コマンドラインユーティリティリファレンス*』の「ルールセットコマンド」を参照してください。

デバイス命名テンプレート

デバイス命名テンプレートに従って、登録時にデバイスの名前が付けられます。デフォルトでは、デバイスのホスト名が使用されます。マシン変数 ${HostName}、${GUID}, ${OS}、${CPU}、${DNS}、${IPAddress}、および ${MACAddress} を組み合わせて、自由に名前を変更できます。

1. ZENworks コントロールセンターで、［設定］タブをクリックします。
2. ［管理ゾーンの設定］パネルで、［デバイス管理］をクリックします。
3. ［登録］をクリックして［登録］ページを表示します。
4. ［デバイス命名テンプレート］パネルで、  をクリックして、リストから目的のマシン変数を選択します。

   1 つまたは複数の変数を組み合わせて使用できます。次に例を示します。

   ${HostName}${GUID}
5. ［OK］をクリックし、変更を保存します。

その他の情報の参照場所

デバイスの登録の詳細については、『*ZENworks 検出、展開、およびリタイアリファレンス*』を参照してください。

ユーザソースへの接続

ZENworks の信頼されたユーザソースを提供する 1 つまたは複数の LDAP ディレクトリに接続できます。

ユーザソースを追加すると、ZENworks 管理者アカウントと LDAP ユーザアカウントを関連付け、デバイスと、デバイスを主に使用するユーザを関連付けることができます。また、ユーザを追加すると、次の ZENworks 製品の機能を追加することができます。

- **環境設定の管理 :** バンドルおよびポリシーをユーザやデバイスに割り当てることができます。ユーザベースのインベントリレポートを使用できます。
- **Asset Management:** ソフトウェアライセンスをユーザ単位およびデバイス単位で示すことができます。
- **Endpoint Security Management:** ポリシーをユーザやデバイスに割り当てることができます。

LDAP ディレクトリをユーザソースとして定義する場合、ディレクトリに影響はありません。ZENworks で必要なのは LDAP ディレクトリへの読み込みアクセスのみで、すべての割り当て情報は ZENworks データベースに保存されます。ユーザソースへの接続時に必要な特定の読み込み権限の詳細については、『*ZENworks ユーザソースおよび認証リファレンス*』の「ユーザソース接続の作成」を参照してください。

ユーザソースとして Novell eDirectory および Microsoft Active Directory に接続できます。最小要件は、Windows 2000 SP4 にインストールされた Novell eDirectory 8.7.3 および Microsoft Active Directory です。LDAP の最小要件はバージョン 3 です。

LDAP ディレクトリに接続した後、ユーザ名を表示するディレクトリ内にコンテナを定義します。たとえば、MyCompany という名前の Microsoft Active Directory ドメインツリーを使用しているとします。すべてのユーザは、MyCompany ツリーの MyCompany/Users および MyCompany/Temp/Users という 2 つのコンテナに属しています。MyCompany ツリーをソースとして、MyCompany/Users および MyCompany/Temp/Users を別々のユーザコンテナとして参照できます。こうすることで、ディレクトリ内部でのアクセスをユーザを含むコンテナにのみ制限できます。

追加したコンテナに属するユーザに加えて、ZENworks コントロールセンターではコンテナ内に含まれるユーザグループも表示されます。これで、個々のユーザとユーザグループの両方の管理を行えるようになります。

ユーザソースに接続するには、次の手順に従います。

1. ZENworks コントロールセンターで、［設定］タブをクリックします。
2. ［ユーザソース］パネルで、［新規作成］をクリックして新規ユーザソースの作成ウィザードを起動します。
3. プロンプトに従ってユーザソースを作成します。

   ウィザードの各ステップで何を指定するかの詳細については、［ヘルプ］ボタンをクリックしてください。

zman ユーティリティで user-source-create コマンドを使用してユーザソースへの接続を作成することもできます。詳細については、『*ZENworks コマンドラインユーティリティリファレンス*』の「ユーザコマンド」を参照してください。

モバイルデバイスの登録のためにユーザソースを有効化する方法の詳細については、「Configuring User Sources」(『ZENworks 2017 Mobile Management Reference』) を参照してください。

ZENworks 管理者アカウントの作成

インストール中に、デフォルトの ZENworks 管理者アカウント (Administrator) が作成されます。このアカウントはスーパー管理者アカウントと呼ばれ、管理ゾーンに対するフル管理権を提供します。

通常、管理タスクを実行する各ユーザに対して管理者アカウントを作成します。これらのアカウントは、スーパー管理者アカウントとして定義したり、制限された権限を持つ管理者アカウントとして定義できます。たとえば、管理ゾーン内のデバイスの検出と登録のみを許可する管理者アカウントをユーザに付与できます。または、デバイスへのバンドルの割り当てのみを許可するアカウントを作成することもできます。または、契約、ライセンス、文書管理などのアセット管理タスクの実行にアカウントを制限することができます。

場合によっては、複数の管理者アカウントに同じ管理権が必要になることがあります。各アカウントに個別に権限を割り当てるのではなく、管理者の役割を作成して、役割に管理権を割り当て、アカウントを役割に追加できます。たとえば、数人の管理者が必要とする管理権を提供するヘルプデスク役割を作成します。

管理者グループを作成することを選択できます。管理者グループに権利と役割を割り当てる場合は、割り当てられた権利と役割はグループ内のすべてのメンバーに適用できます。

管理者アカウントの作成

1 ZENworks コントロールセンターで、［管理者］タブをクリックします。

2 ［管理者］パネルで、［新規］>［管理者］の順にクリックして［新しい管理者の追加］ダイアログボックスを表示します。

3 次のフィールドに情報を入力します。

［新しい管理者の追加］ダイアログボックスでは、名前またはパスワードを提供して新しい管理者アカウントを作成できます。またはユーザソースの既存のユーザに基づいて新しい管理者を作成できます。オプションで、ログインしている管理者と同じ権限を新しい管理者に付与できます。

名前とパスワードを提供して新しい管理者を作成する：このオプションは、手動で名前およびパスワードを指定して新しい管理者アカウントを作成する場合にのみ選択してください。

ユーザソース内のユーザを基準にする：このオプションは、ユーザソースからのユーザ情報に基づいて新しい管理者アカウントを作成する場合に選択してください。これを行うには、［追加］をクリックして、目的のユーザを参照して選択します。

自分の持っているのと同じ権限をこの管理者に付与します：このオプションは、新しい管理者に、現在ログインしている管理者と同じ権利を割り当てます。スーパー管理者権限がある場合は、新しい管理者がスーパー管理者として作成されます。

4 ［OK］をクリックして、［管理者］パネルに新しい管理者を追加します。

5 新しい管理者の権限または役割を変更する必要がある場合は、管理者アカウントをクリックしてから［権限］タブをクリックし、アカウントの詳細を表示します。

6 ［スーパー管理者］オプションが選択されている場合は、オプションの選択を解除します。

スーパー管理者権限を変更することはできません。

7 ［割り当てられた権限］パネルを使用して割り当てられている権限を変更します。

8 ［割り当て済みの役割］パネルを使用して、割り当てられている役割を変更します。

9 ［適用］をクリックして変更内容を保存します。

ZENworks の管理者アカウント、管理者の権限、または管理者の役割を作成する方法の詳細については、『ZENworks Administrator Accounts and Rights Reference』を参照してください。

zman ユーティリティで admin-create コマンドを使用して ZENworks 管理者アカウントを作成することもできます。詳細については、『*ZENworks コマンドラインユーティリティリファレンス*』の「管理者コマンド」を参照してください。

管理者グループアカウントの作成

1 ZENworks コントロールセンターで、［管理者］タブをクリックします。

2 ［管理者］パネルで、［新規］>［管理者グループ］の順にクリックして、［新しい管理者グループの追加］ダイアログボックスを表示します。

3 次のフィールドに情報を入力します。

［新しい管理者グループの追加］ダイアログボックスでは、グループ名を提供し、メンバーをグループに追加して、新しい管理者グループアカウントを作成できます。またはユーザソースの既存のユーザグループに基づいて新しい管理者グループを作成できます。各管理者グループ名は固有にする必要があります。

名前を提供しメンバーを追加して新しい管理者グループを作成する：このオプションは、手動で名前を指定し、メンバーを追加して新しい管理者グループアカウントを作成する場合に選択してください。メンバーを追加するには、［追加］をクリックしてから、目的の管理者を参照して選択します。管理者はいくつでもグループに追加できます。別の管理者グループをグループに追加することはできません。

ユーザソース内のユーザグループを基準にする：このオプションは、ユーザソースからのユーザグループ情報に基づいて新しい管理者グループアカウントを作成する場合に選択してください。これを行うには、［追加］をクリックして、目的のユーザグループを参照して選択します。

各ユーザグループのユーザメンバーを管理者としてすぐにインポートします。このオプションを選択すると、選択したユーザグループのユーザメンバーを管理者としてすぐに追加できるようになります。

4 ［OK］をクリックして、［管理者］パネルに新しい管理者グループを追加します。

5 新規の管理者グループの権限または役割を変更する必要がある場合は、管理者グループアカウントをクリックしてから、［権限］タブをクリックし、アカウントの詳細を表示します。

6 ［割り当てられた権限］パネルを使用して割り当てられている権限を変更します。

7 ［割り当て済みの役割］パネルを使用して、割り当てられている役割を変更します。

8 ［適用］をクリックして変更内容を保存します。

ZENworks の管理者グループアカウント、管理者の権限、または管理者の役割を作成する方法の詳細については、『*ZENworks Administrator Accounts and Rights Reference*』を参照してください。

zman ユーティリティで admin-create コマンドを使用して ZENworks 管理者アカウントを作成することもできます。詳細については、『*ZENworks コマンドラインユーティリティリファレンス*』の「管理者コマンド」を参照してください。

環境設定の変更

管理ゾーン環境設定では、ゾーンに対する広範囲な機能動作を制御することができます。デバイス管理設定では、デバイスが更新された情報を確認するために ZENworks サーバにアクセスする頻度、動的グループの更新頻度、およびどのレベルのメッセージ (情報、警告、またはエラー) を ZENworks Agent で記録するかを制御することができます。イベントおよびメッセージの設定、検出および展開の設定、その他さまざまな設定があります。

デバイスに適用する管理ゾーンの設定は、ゾーン内のすべてのデバイスに継承されます。23 ページの 「デバイスの構成 : フォルダとグループ」で説明したように、ゾーン設定をデバイスフォルダまたは個別のデバイス上で設定することによって上書きすることができます。これにより、必要に応じて最多のデバイスに適用するゾーン設定を確立して、フォルダおよびデバイス上の設定を上書きすることができます。

デフォルトでは、ゾーンの設定は一般的な機能を提供する値を使用して事前に設定されています。ただし、ご使用の環境の必要性に応じて、最も適した値に設定を変更できます。

ゾーンでの環境設定の変更

1 ZENworks コントロールセンターで、［環境設定］タブをクリックします。

2 ［管理ゾーンの設定］パネルで、変更する設定の設定カテゴリ (［デバイス管理］、［検出と展開］、［イベントとメッセージング］など) をクリックします。

3 設定をクリックして、詳細ページを表示します。

4 必要に応じて設定を変更します。

設定の詳細については、『*ZENworks Management Zone Settings Reference*』を参照してください。

5 ［OK］または［適用］をクリックします。

環境設定がデバイスに適用されると、設定がフォルダレベルまたはデバイスレベルで上書きされない限り、設定はゾーン内のすべてのデバイスに継承されます。

フォルダの環境設定の変更

1 ZENworks コントロールセンターで、［デバイス］タブをクリックします。

2 ［デバイス］パネル (［管理対象］タブ) で、設定を変更するフォルダを参照します。

3 フォルダ名の横にある［詳細］をクリックして、フォルダの詳細を表示します。

4 ［設定］タブをクリックします。

5 ［設定］パネルで、設定を変更するカテゴリ (［デバイス管理］、［インフラストラクチャ管理］など) をクリックします。

6 設定をクリックして、詳細ページを表示します。

7 必要に応じて設定を変更します。

設定の詳細については、『*ZENworks Management Zone Settings Reference*』を参照してください。

8 ［OK］または［適用］をクリックします。

環境設定は、設定がサブフォルダまたは個別のデバイス上で上書きされない限り、サブフォルダに含まれるすべてのデバイスを含めフォルダ内のすべてのデバイスによって継承されます。

デバイスでの環境設定の変更

1 ZENworks コントロールセンターで、［デバイス］タブをクリックします。

2 ［デバイス］パネル (［管理対象］タブ) で、設定を変更するデバイスを参照します。

3 デバイスを見つけたら、デバイス名をクリックして詳細を表示します。

4 ［設定］タブをクリックします。

5 ［設定］パネルで、設定を変更するカテゴリ (［デバイス管理］、［インフラストラクチャ管理］など) をクリックします。

6 設定をクリックして、詳細ページを表示します。

7 必要に応じて、設定を変更します。

設定の詳細については、ZENworks コントロールセンターで［ヘルプ］ボタンをクリックしてください。

8 設定の変更が完了したら、［OK］(または［適用］) をクリックして変更内容を保存します。

ゾーン共有とサブスクリプション

ZENworks の加入機能と共有機能を使用すると、コンテンツオブジェクト (バンドルやポリシーなど) を共有して、それらを複数の ZENworks ゾーンにわたって割り当てることができます。

- **共有ゾーン :** コンテンツを共有します。
- **加入者ゾーン :** 共有ゾーンに加入して、共有されたコンテンツを独自のゾーンに複製します。

ZENworks コントロールセンターでは、［インフラストラクチャ管理］パネルの［ゾーン共有］設定リンクを使用して、ゾーンの共有アクティビティを管理することができます。

共有ゾーンでは、プライマリサーバが共有サーバとして識別されます。このサーバを介して、すべてのコンテンツ共有アクティビティが実行されます。加入者ゾーンの登録は、共有ゾーンから加入者キーを指定することによって行われます。加入者キーは、加入者に対して、いかなるコンテンツに関する権限も与えません。加入者キーは、加入者登録専用です。

この場合、必要なコンテンツは共有ゾーンから共有され、加入者ゾーンに複製されます。レプリケーションに関する問題が生じた場合は、通知されるので、是正措置を取ることができます。

詳細については、『*ZENworks Subscribe and Share Reference*』を参照してください。

ZENworks ソフトウェアの更新

ZENworks ソフトウェアは、インストール先である管理ゾーン内のすべてのデバイスで更新することができます。アップデートのダウンロードは、スケジュール化することができます。ソフトウェアの更新は、サポートパックリリースレベルで提供されるので、そのコンテンツを確認してからそ

れぞれの更新を適用するかどうかを選択できます (サポートパックリリースは累積的なものです)。最新の製品認識の更新 (PRU) をダウンロードして、ZENworks Inventory が新しいソフトウェアを認識できるように、ナレッジベースを更新することもできます。

詳細については、『*ZENworks System Updates Reference*』を参照してください。

場所の作成

デバイスのセキュリティ要件は、場所ごとに異なります。たとえば、空港内にあるデバイスと、企業ファイアウォール内のオフィスにあるデバイスでは、個々のファイアウォール制限が異なります。

デバイスのセキュリティ要件をその場所に合ったものにするため、ZENworks はグローバルポリシーと場所ベースのポリシーの両方をサポートしています。グローバルポリシーは、デバイスの場所とは無関係に適用されます。場所ベースのポリシーは、デバイスの現在の場所が、ポリシーに関連付けられた場所の条件を満たす場合にのみ適用されます。たとえば、会社オフィスの場所ベースポリシーを作成し、これをラップトップに割り当てた場合、このポリシーは、ラップトップの場所が会社オフィスであるときにのみ適用されます。

場所ベースのポリシーを使用する場合は、最初に、自分の会社や組織に合った場所を定義する必要があります。場所とは、特定のセキュリティ要件が設定されているプレースやプレースタイプを意味します。たとえば、オフィス、自宅、または空港でデバイスを使用する場合のセキュリティ要件は異なります。

場所はネットワーク環境に応じて定義されます。ニューヨークと東京にオフィスがあると仮定してください。両方のオフィスには同じセキュリティ要件が設定されています。したがって、「オフィス」場所を作成し、ニューヨークオフィスと東京オフィスの 2 つのネットワーク環境に関連付けます。これらの環境はそれぞれ、ゲートウェイ、DNS サーバ、およびワイヤレスアクセスポイントの一連のサービスによって明示的に定義されます。ZENworks Agent は、その現在の環境がニューヨークオフィスのネットワーク、または東京オフィスのネットワークに合致していると判断した場合は常に、その場所を「オフィス」に設定し、「オフィス」場所に関連付けられているセキュリティポリシーを適用します。

次のセクションでは、場所の作成方法を説明します。

- 34 ページの 「ネットワーク環境の定義」
- 35 ページの 「場所の作成」
- 36 ページの 「管理対象デバイスでの場所とネットワーク環境の選択」

ネットワーク環境の定義

ネットワーク環境定義は場所の基本要素です。ネットワーク環境は、場所を作成するときに定義できます。ただし、最初にネットワーク環境を定義してから、場所を作成するときにそのネットワーク環境を追加することをお勧めします。

ネットワーク環境を作成する :

1. ZENworks コントロールセンターで、［環境設定］ > ［場所］の順にクリックします。
2. ［ネットワーク環境］パネルで、［新規］をクリックして新しいネットワーク環境の作成ウィザードを起動します。
3. ［詳細の定義］ページで、ネットワーク環境名を指定して［次へ］をクリックします。
4. ［ネットワーク環境の詳細］ページで、次を指定します。

アダプタタイプに限定：デフォルトでは、このページで定義するネットワークサービスは、デバイスの有線、ワイヤレス、およびダイアルアップのネットワークアダプタに照合して評価されます。特定のアダプタタイプに評価を限定する場合は、［有線］、［ワイヤレス］、または［ダイヤルアップ］を選択します。

最小一致：このネットワーク環境を選択するために一致する必要がある定義済みネットワークサービスの最小数を指定します。

このネットワーク環境を選択するために一致する必要がある定義済みネットワークサービスの最小数を指定します。

たとえば、1 つのゲートウェイアドレス、3 つの DNS サーバ、および 1 つの DHCP サーバを定義した場合、合計 5 つのサービスが存在します。このネットワーク環境を選択するには、これらのサービスのうち最低 3 つが一致する必要があると指定できます。

最小一致数を指定した場合は、次のことを確認します。

- ［一致が必要］というマークの付いたサービスの数より小さい数にできません。
- 定義済みサービスの合計数より大きな数にしないでください。この数を超えると、最小一致に到達しなくなり、ネットワーク環境を選択できなくなります。

ネットワークサービス：現在のネットワーク環境がこのネットワーク環境に一致するかどうかを調べるために、ZENworks Agent が評価するネットワークサービスを定義できます。定義するネットワークサービスのタブを選択します。［追加］をクリックして、必要な情報を指定します。

5 ［次へ］をクリックして［概要］ページを表示し、［完了］をクリックします。

場所の作成

場所を作成する際、場所名を入力して、該当するネットワーク環境を場所と関連付けます。

1 ZENworks コントロールセンターで、［環境設定］>［場所］の順にクリックします。

2 ［場所］パネルで、［新規］をクリックして新しい場所の作成ウィザードを起動します。

3 ［詳細の定義］ページで、場所名を指定して［次へ］をクリックします。

4 ［ネットワーク環境の割り当て］ページで、次の操作を行います。

4a ［既存のネットワーク環境を場所に割り当てます］を選択します。

4b ［追加］をクリックし、場所を定義するネットワーク環境を選択し、［OK］をクリックして、選択したネットワーク環境をリストに追加します。

4c ネットワーク環境の追加を完了したら、［次へ］をクリックします。

5 ［概要］ページで［完了］をクリックして場所を作成し、［場所］リストに追加します。

ZENworks Agent によって識別されたネットワーク環境が複数の場所に含まれている場合は、リストの順序に従って使用する場所が決定されます。デフォルトでは、先頭にリストされている場所が選択されます。リストの順序を変更するには、［Move Up (上に移動)］および［Move Down (下に移動)］オプションを使用します。

zman ユーティリティで network-environment-create コマンドおよび location-create コマンドを使用して、ネットワーク環境を作成したり、作成されたネットワーク環境を使用する関連した場所を作成することもできます。詳細については、『*Zenworks コマンドラインユーティリティリファレンス*』の「登録コマンド」を参照してください。

管理対象デバイスでの場所とネットワーク環境の選択

ZENworks コントロールセンターに複数の場所とネットワーク環境が定義されている場合、管理対象デバイス上の ZENworks Agent は定義済みのすべてのネットワーク環境をスキャンして一致する環境を識別します。ZENworks Agent は、識別された複数の環境から、一致するネットワークサービス (クライアント IP アドレスや DNS サーバなど) の数が最も多いネットワーク環境を選択します。次に ZENworks Agent は、順番にリストされている場所をスキャンし、選択されたネットワーク環境のいずれかを含む最初の場所を識別子して、その場所とこの場所内に含まれる最初に一致したネットワーク環境を選択します。

次に例を示します。

- ZENworks コントロールセンターに定義されている場所は、L1 および L2 の順でリストされています。
- L1 内のネットワーク環境は、NE1、NE2、および NE4 の順序でリストされています。
- L2 内のネットワーク環境は、NE2、NE3、および NE4 の順序でリストされています。
- 管理対象デバイス上の ZENworks Agent は、NE2、NE3、および NE4 が管理対象デバイスですべて一致していることを検出します。

NE2 と NE4 にはそれぞれ一致する 2 つのネットワークサービスがあり、NE3 は一致するネットワークサービスが 1 つしかない場合、NE2 と NE4 が最もネットワークサービスに一致するため ZENworks Agent はこれらを選択します。NE2 は L1 で最初にリストされているネットワーク環境であり、L1 と NE2 は場所およびネットワーク環境として選択されているからです。

注 : 管理対象デバイスで一致すると見なされたネットワーク環境の場合、ネットワーク環境で設定されているすべての制限を満たす必要があります。これには、ネットワーク環境に対して指定される［**最小一致数**］属性が含まれ、ネットワーク環境内のネットワークサービスに対して指定される［**一致が必要**］属性も含まれます。

ダッシュボード

ダッシュボード機能により、キーインジケータの包括的なスナップショットが提供されるため、ゾーン内のデバイスのヘルスとコンプライアンス全体に素早くアクセスできます。ダッシュボードを使用して、興味のある詳細分野にドリルダウンすることができます。

ZENworks ダッシュボードでは、ゾーン内のデバイスやパッチのステータスに関する情報を表示したり、必要なアクションを実行したりすることができます。

詳細については、『ZENworks Dashboard Reference』を参照してください。

4 ZENworks Agent の展開

ZENworks Agent は、管理するデバイスに展開する必要があります。次のセクションでは、エージェントの展開プロセスを理解するのに役立つ手順について説明します。

- 37 ページの 「ZENworks Agent 機能の設定」
- 39 ページの 「ZENworks Agent のセキュリティの設定」
- 40 ページの 「ZENworks Agent のインストール」
- 44 ページの 「ZENworks Agent の使用」

注 : デバイスが ZENworks Agent のインストール要件を満たさない場合は (『*ZENworks 2017 Update 3 System Requirements*』の Managed Device Requirements を参照)、デバイスにインベントリのみのモジュールをインストールして、デバイスのインベントリ作成をサポートすることができる可能性があります。詳細については、『*ZENworks 検出、展開、およびリタイアリファレンス*』を参照してください。

ZENworks Agent 機能の設定

ZENworks Agent は、さまざまなモジュールを使用して、デバイス上で機能を実行します。これらのモジュールは ZENworks Agent 機能と呼ばれます。各 ZENworks 製品には、次の表に示すように、その製品に関連付けられている固有の機能があります。左側の列は ZENworks 製品のリストで、他の列は ZENworks Agent 機能を示しています。

	アセット管理	バンドル管理	エンドポイントセキュリティ	完全ディスク暗号化	イメージ管理	パッチ管理	ポリシー管理	リモート管理	ユーザ管理
ZENworks Asset Management	✓								✓
ZENworks Configuration Management		✓			✓		✓	✓	✓
ZENworks Endpoint Security Management			✓						✓
ZENworks Full Disk Encryption				✓					

	アセット管理	バンドル管理	エンドポイントセキュリティ	完全ディスク暗号化	イメージング管理	パッチ管理	ポリシー管理	リモート管理	ユーザ管理
ZENworks Patch Management									

デフォルトでは、ZENworks 製品をアクティブ化すると、その ZENworks Agent 機能のすべてがインストールされて有効になります。ただし、ZENworks Asset Management だけは、ユーザ管理機能が自動的に有効になりません。

ユーザ管理機能は、すべての ZENworks 製品について、Windows 管理デバイス上でのみサポートされます。

デバイス上で機能をインストールまたは有効化しない場合は、管理ゾーン、デバイスフォルダ、または個々のデバイスで、アンインストールするか、無効にすることができます。

たとえば、ZENworks Configuration Management を使用し、リモート管理をデバイスと併用しない場合は、管理ゾーンで無効にすることができます。または、ZENworks Configuration Management および ZENworks Asset Management をインストールしているが、すべてのデバイス上で Asset Management を使用しない場合は、管理ゾーンで Asset Management 機能を有効にしてから、デバイスフォルダまたは個々のデバイス上で無効化 (またはアンインストール) することができます。

ZENworks Agent 機能をカスタマイズするには、エージェントを展開する前後に、次のセクションを参照してください。

- 38 ページの 「ZENworks Agent 機能のカスタマイズ」
- 39 ページの 「ZENworks Desktop Management Agent との共存」

ZENworks Agent 機能のカスタマイズ

最初の展開時に、ZENworks Agent は、管理ゾーンレベルで選択された機能をインストールし、有効にします。エージェントの登録後は、デバイスフォルダまたはデバイスレベルで定義された設定を使用します (ゾーン設定とは異なる場合)。

注 : ZENworks Agent 機能のカスタマイズは、Macintosh デバイスに対しては適用されません。

次の手順は、管理ゾーンレベルでの設定のカスタマイズ方法を示したものです。デバイスフォルダまたは個々のデバイスで設定をカスタマイズする方法の詳細については、『*ZENworks 検出、展開、およびリタイアリファレンス*』の「エージェント機能のカスタマイズ」を参照してください。

1 ZENworks コントロールセンターで、［設定］タブをクリックします。

2 ［管理ゾーンの設定］パネルで、［デバイス管理］> ［ZENworks Agent］の順にクリックします。

3 エージェント機能パネル :

- インストールしたくない機能がある場合は、その機能の横の［インストール済み］の選択を解除します。選択した機能は、デバイスにインストールされません。すべての機能の選択解除を選択した場合は、コアエージェントだけがインストールされます。
- インストールするが機能を無効にしたい場合は、その機能の横の［インストール済み］および［使用不可］を選択します。機能はデバイスにインストールされますが、機能しません。

バンドル管理、リモート管理、またはユーザ管理機能をインストールするには、デバイスの再起動が必要です。イメージ管理機能をインストールする際、Windows 2008 および Windows Vista の場合にのみ再起動が必要です。選択した再起動オプションに基づいてデバイスの再起動が要求されます。

4 変更を保存するには、［OK］をクリックします。

ZENworks Desktop Management Agent との共存

ZENworks Agent は、ZENworks Desktop Agent をインストールしているデバイスに展開できます。

ZENworks Agent と ZENworks Desktop Agent は、同一デバイス上に共存できます。これは、ZENworks Asset Management と ZENworks Desktop Management の併用をサポートすることが目的です。この場合、ZENworks Desktop Agent がインストールされているデバイスに ZENworks Agent を展開するときは、ZENworks Configuration Management に関連付けられてない ZENworks Agent 機能のみを使用し、バンドル管理、イメージ管理、ポリシー管理、リモート管理、またはユーザ管理機能は使用しないでください。これらの機能のいずれかを選択する場合、ZENworks Desktop Agent がアンインストールされてから、ZENworks Agent がインストールされます。

ZENworks Agent と ZENworks Desktop Agent の共存の詳細については、「ZENworks Agent の展開」(『*ZENworks 検出、展開、およびリタイアリファレンス*』) を参照してください。

ZENworks Agent のセキュリティの設定

デバイス上の ZENworks Agent のセキュリティを高めるには、エージェントのアンインストールおよびセルフディフェンスの設定を行います。

1 ZENworks コントロールセンターで、［環境設定］タブをクリックします。

2 ［管理ゾーンの設定］パネルで、［デバイス管理］をクリックし、次に［ZENworks エージェント］をクリックします。

3 ［エージェントセキュリティ］パネルで、次の設定を行います。

- **ユーザに ZENworks Agent のアンインストールを許可 :** ZENworks Agent をアンインストールするには、このオプションを選択します。
- **ZENworks Agent のアンインストールパスワードが必要 :** ZENworks Agent をアンインストールするために必要なパスワードを指定するには、このオプションを選択します。［変更］をクリックして、パスワードを設定します。

  アンインストールパスワードのユーザへの配布を防止するには、パスワードキージェネレータユーティリティを使用してパスワードキーを生成することをお勧めします。このキー (アンインストールパスワードを基に作成されます) は、アンインストールパスワードと同様に機能しますが、このキーの使用を制限するために単一のデバイスまたはユーザに関連付けることができます。

パスワードキージェネレータユーティリティには、左側のナビゲーションペインにある［設定タスク］リストからアクセスできます。

- **ZENworks Agent の上書きパスワードを有効にする :** ZENworks Agent で使用できる上書きパスワードを指定するには、このオプションを選択します。
  - デバイスの現在の場所と、その場所の割り当て方法についての情報にアクセスする。
  - エンドポイントセキュリティエージェントの管理オプションにアクセスする。このオプションを使用すると、現在適用されているセキュリティポリシーを無効にしたり (データ暗号化ポリシーを除く)、ポリシーの詳細情報を表示したり、エージェントステータス情報を表示したりできます。
  - Full Disk Encryption Agent の管理オプションにアクセスする。このオプションを使用すると、ポリシー情報の詳細やエージェントステータス情報を表示したり、次のような機能を実行したりできます。ユーザキャプチャの有効化およびボリュームの復号化。
  - ZENworks Agent をアンインストールする。
- **ZENworks Agent のセルフディフェンスを有効にする :** セルフディフェンスを有効にするには、このオプションを選択します。現時点では、セルフディフェンス機能の保護対象は ZENworks エンドポイントセキュリティエージェントのみです。その他の ZENworks Agent モジュールは保護されません。

  セルフディフェンスは、エンドポイントセキュリティエージェントがシャットダウンされたり、無効にされたり、変更されたりすることがないように保護します。ユーザが次のアクティビティのいずれかを実行する場合、デバイスは自動的に再起動されて、正しいシステム設定を復元します。
  - Windows タスクマネージャを使用した、エンドポイントセキュリティエージェントプロセスの終了。
  - エンドポイントセキュリティエージェントサービスの停止または一時停止。
  - 重要なファイルおよびレジストリエントリの削除。エンドポイントセキュリティエージェントに関連付けられた何らかのレジストリキーまたは値に変更が行われた場合、レジストリキーまたは値は直ちにリセットされます。
  - アダプタにバインドした NDIS フィルタドライバの無効化。

4 変更を保存するには、［OK］をクリックします。

ZENworks Agent のインストール

次のセクションでは、デバイス上に ZENworks Agent を手動でインストールする手順について説明します。

- 41 ページの 「Windows での手動インストール」
- 42 ページの 「Linux での手動インストール」
- 43 ページの 「Macintosh での手動インストール」

注 : ZENworks Agent の手動によるインストールに加え、ネットワークデバイスの検出および展開を使用してインストールを自動化することもできます。検出および展開プロセスは、この『クイックスタート』で説明する範囲を超えています。このプロセスの使用方法については、『*ZENworks 検出、展開、およびリタイアリファレンス*』を参照してください。

Windows での手動インストール

1 デバイスが必要な要件を満たしていることを確認します (『*ZENworks 2017 Update 3 システム要件*』の「管理対象デバイスの要件」を参照)。

2 ターゲットのデバイス上で、Web ブラウザを開き次のアドレスに移動します。

```
https://server:port/zenworks-setup
```

server を ZENworks サーバの DNS 名または IP アドレスに置き換え、ZENworks サーバがデフォルトポート (80 または 443) を使用していない場合のみ *port* を置き換えます。

Web ブラウザに ZENworks Agent の展開パッケージの一覧が表示されます。各アーキテクチャ (32 ビットおよび 64 ビット) 用に、次の種類のパッケージがあります。

- **ネットワーク (.NET が必要)** ネットワーク (.NET が必要) パッケージは、プレエージェントのみを目的のデバイスにインストールします。続いて、プレエージェントが ZENworks サーバから ZENworks Agent をダウンロードしてインストールします。ネットワーク (.NET が必要) パッケージでは、デバイスにエージェントを展開する前に、デバイス上に Microsoft .NET 4.0 以降がインストールされている必要があります。
- **スタンドアロン (.NET が必要)** スタンドアロン (.NET が必要) パッケージでは、デバイスにエージェントを展開する前に、デバイス上に Microsoft .NET 4.0 以降がインストールされている必要があります。このパッケージには Microsoft .NET インストーラを除く ZENworks Agent のインストールに必要なすべての実行可能ファイルが含まれています。
- **スタンドアロン :** スタンドアロンパッケージはプレエージェントをインストールし、目的のデバイス上に Microsoft .NET インストーラを含む、ZENworks Agent のインストールに必要なすべての実行可能ファイルを抽出します。続いてプレエージェントはローカルデバイスから ZENworks Agent をインストールします。スタンドアロンパッケージは、ZENworks Agent を現在ネットワークから接続解除されているデバイスにインストールする必要がある場合に便利です。パッケージをリムーバブルメディア (CD、USB フラッシュドライブなど) に保存し、スタンドアロンデバイスでメディアからパッケージを実行することができます。ZENworks Agent はデバイスにインストールされますが、デバイスがネットワークに接続されるまで登録および管理は行われません。
- **カスタム :** パッケージ名である、デフォルトエージェントは、事前定義された展開パッケージを参照します。［展開］>［展開パッケージの編集］を使用して作成されたカスタム展開パッケージは、パッケージの作成時に付けられた名前で表示されます。

3 使用する展開パッケージの名前をクリックし、パッケージをデバイスのローカルドライブに保存するか、ZENworks サーバから実行します。

4 パッケージをダウンロードしたら、デバイスでパッケージを起動します。

パッケージをコマンドラインから起動する際にパッケージで使用できるオプションの詳細については、『*ZENworks 検出、展開、およびリタイアリファレンス*』の「Windows、Linux、および Macintosh のパッケージオプション」を参照してください。

重要 : 完全なパッケージのインストールを選択する場合は、Windows Installer または .NET Framework のインストールによって、パッケージの起動後に再起動が要求されることがあります。再起動時に、さまざまなオプションを示すメッセージが表示されます。次のいずれかを行います。

- 何も実行しないで、5 分後に自動再起動する。
- ［キャンセル］をクリックする。後で再起動する必要があります。
- ［OK］をクリックして、すぐに再起動する

デバイスが再起動すると、インストールは自動的に再開します。

5 インストールの完了後に、Windows Installer または .NET Framework のインストール中にデバイスを再起動している場合はデバイスは自動的に再起動します。

デバイスは再起動するとき、管理ゾーンに登録され、ZENworks アイコンが通知領域 (システムトレイ) に配置されます。

ZENworks コントロールセンターで、デバイスは［デバイス］ページの \Servers フォルダまたは \Workstation フォルダに表示されます。

デバイスでの ZENworks Agent へのログインと使用の詳細については、44 ページの 「ZENworks Agent の使用」を参照してください。

Linux での手動インストール

ZENworks サーバを使用してデバイスに ZENworks Agent を配布するのではなく、手動でサーバから ZENworks Agent 展開パッケージをダウンロードしてエージェントをインストールすることができます。

重要 : ルートまたは管理者の権限を持っている場合は、Linux 上に ZENworks Agent をインストールできます。

1 デバイスが必要な要件を満たしていることを確認します (『*ZENworks 2017 Update 3 システム要件*』の「管理対象デバイスの要件」を参照)。

2 ターゲットのデバイス上で、Web ブラウザを開き次のアドレスに移動します。

`http://server:port/zenworks-setup`

server を ZENworks サーバの DNS 名または IP アドレスに置き換え、ZENworks サーバがデフォルトポート (80 または 443) を使用していない場合のみ *port* を置き換えます。

Web ブラウザに、展開パッケージの一覧が表示されます。各アーキテクチャ (32 ビットおよび 64 ビット) 用に、次の種類のパッケージがあります。

- **ネットワーク :** このパッケージは、プレエージェントのみを目的のデバイスにインストールします。続いて、プレエージェントが ZENworks サーバから ZENworks Agent をダウンロードしてインストールします。
- **スタンドアロン :** スタンドアロンパッケージはプレエージェントをインストールし、目的のデバイスに JRE インストーラを含む、ZENworks Agent のインストールに必要なすべての実行可能ファイルを抽出します。続いてプレエージェントはローカルデバイスから ZENworks Agent をインストールします。スタンドアロンパッケージは、ZENworks Agent を現在ネットワークから接続解除されているデバイスにインストールする必要がある場合に便利です。パッケージをリムーバブルメディア (CD、USB フラッシュドライブなど) に保存し、スタンドアロンデバイスでメディアからパッケージを実行することができます。ZENworks Agent はデバイスにインストールされますが、デバイスがネットワークに接続されるまで登録および管理は行われません。
- **カスタム :** パッケージ名である、デフォルトエージェントは、事前定義された展開パッケージを参照します。**［展開］** > **［展開パッケージの編集］** を使用して作成されたカスタム展開パッケージは、パッケージの作成時に付けられた名前で表示されます。

3 使用したい展開パッケージの名前をクリックし、パッケージをデバイスのローカルドライブに保存し、chmod 755 *filename* コマンドの実行により、ファイルに実行可能権限を設定します。

パッケージをコマンドラインから起動する際にパッケージで使用できるオプションの詳細については、『*ZENworks 検出、展開、およびリタイアリファレンス*』の「Windows、Linux、および Macintosh のパッケージオプション」を参照してください。

4 (オプション) RHEL デバイスで、次のコマンドを実行します。

chcon -u system_u -t rpm_exec_t *filename*

5 端末ウィンドウで、パッケージをダウンロードしたディレクトリに移動し、コマンド */filename* を実行してデバイスでパッケージを起動します。ここで、［**filename**］はステップ 3 でダウンロードしたパッケージの名前です。

6 (条件付き) Linux デバイスのエージェントインストール後に通知領域に ZENworks 通知アイコンを表示する場合は、デバイスをログアウトしてからログインします。

ZENworks コントロールセンターで、デバイスは［デバイス］ページの \Servers フォルダまたは \Workstation フォルダに表示されます。

Macintosh での手動インストール

ZENworks ダウンロードページから展開パッケージをダウンロードして、ZENworks Agent を Macintosh デバイスに展開することができます。

重要

- ルートまたは管理者の権限を持っている場合は、Macintosh デバイス上に ZENworks Agent をインストールできます。

---

1 ターゲットの Macintosh デバイス上で、Web ブラウザを開き次のアドレスを入力します。

http://<server>/zenworks-setup

<server> を DNS 名または ZENworks サーバの IP アドレスに置き換えます。

2 ダウンロードする適切な Macintosh パッケージをクリックします。

注 : パッケージは 2 種類あります。

- **ネットワーク :** このパッケージで、必要な PKG ファイルをダウンロードするには ZENworks Server へのネットワークアクセスが必要です。
- **スタンドアロン :** エージェントをインストールするのに ZENworks Server へのアクセスは必要ありません。

---

3 コマンドプロンプトで、chmod +x<file_name> コマンドを実行して、ダウンロードした .bin ファイルに実行可能権限を指定します。

パッケージで使用できるオプションの詳細については、「Windows、Linux、および Macintosh のパッケージオプション」(『*ZENworks 検出、展開、およびリタイアリファレンス*』) を参照してください。

4 コマンドプロンプトで、パッケージをダウンロードしたディレクトリに移動し、次のコマンドを実行してデバイスでパッケージを起動します。

sudo ./filename

ここで、filename は 43 ページのステップ 2 でダウンロードしたパッケージの名前です。

5 Macintosh デバイスのエージェントインストール後に通知領域に ZENworks 通知アイコンを表示する場合は、デバイスをログアウトしてからログインします。

ZENworks コントロールセンターで、デバイスは［デバイス］ページの \Servers フォルダまたは \Workstation フォルダに表示されます。

注 : Macintosh デバイスに ZENworks Agent をインストールした後、PATH 変数に /opt/novell/zenworks/bin が追加されないため、そのディレクトリ内のコマンドを直接使用できなくなります。/opt/novell/zenworks/bin からコマンドを実行するには、次のいずれかを Macintosh デバイスで実行してください。

- デバイスに再度ログインします。
- コマンドにアクセスするための完全なパスを指定します。

  例 : /opt/novell/zenworks/bin/zac.

ZENworks Agent の使用

次のセクションでは、ログインおよび ZENworks Agent の使用に役立つ情報を提供します。

- 44 ページの 「管理ゾーンへのログイン」
- 44 ページの 「ZENworks Agent ビューの移動」
- 46 ページの 「管理対象デバイスのサテライトへの昇格」

管理ゾーンへのログイン

Windows 管理対象デバイスでオペレーティングシステムを起動するときに、ZENworks Agent が起動されて、デバイスに割り当てられているすべてのバンドルおよびポリシーが使用可能になります。ユーザに割り当てられているバンドルおよびポリシーを使用可能にするためには、ユーザは管理ゾーンにログインする必要があります。

ZENworks Agent は、Windows ログインクライアントまたは Novell ログインクライアントと統合され、ユーザにシングルログインを提供します。ユーザが Windows または Novell クライアントで eDirectory または Active Directory のアカウント情報を入力した場合、ユーザのアカウント情報が ZENworks ユーザソースのものと一致すると、管理ゾーンにログインします。一致しない場合、別の ZENworks Agent ログイン画面が表示され、正しいアカウント情報を入力するよう求められます。

たとえば、あるユーザが 2 つのディレクトリツリー Tree1 と Tree2 でアカウントを持っているとします。Tree1 は、管理ゾーンのユーザソースとして定義されていますが、Tree2 は定義されていません。そのユーザが Tree1 にログインすると、自動的に管理ゾーンにログインします。一方、そのユーザが Tree2 にログインした場合は、ZENworks Agent のログイン画面が表示され、Tree1 の資格情報を入力するよう求められます。

ZENworks Agent ビューの移動

ZENworks Agent には、次のビューがあります。

- 45 ページの 「ZENworks アプリケーション」
- 45 ページの 「ZENworks Explorer」
- 45 ページの 「ZENworks Icon」

ZENworks アプリケーション

ZENworks アプリケーションは、バンドルへのアクセスを提供するスタンドアロンのウィンドウです。このウィンドウは［スタート］メニューから起動できます (［スタート］メニュー > ［プログラム］ > ［Novell ZENworks］ > ［ZENworks アプリケーション］)。

ZENworks アプリケーションの左ペインには、次の項目が表示されます。

- **［すべて］フォルダ :** バンドルが配置されているフォルダにかかわらず、配布されているバンドルすべてが表示されます。
- **［ZENworks］フォルダ :** 別のフォルダに割り当てられていないバンドルすべてが表示されます。バンドルのデフォルトフォルダは ZENworks フォルダです。ただし、管理者はバンドルを整理するために追加フォルダを作成したり、ZENworks フォルダを名前変更したりすることもできます。

左ペインでフォルダを選択すると、そのフォルダ内に含まれているバンドルが右ペインに表示されます。次の操作を行うことができます。

- バンドルをインストールするか、すでにインストール済みのアプリケーションを起動する。
- バンドルのプロパティを表示する。プロパティには、バンドルの説明、バンドルのヘルプ担当者についての情報、バンドルを使用できる時間、バンドルに設定されたシステム要件などが含まれます。
- インストールしたアプリケーションを修復する。
- アプリケーションをアンインストールする。これは管理者が制御する機能で、有効になっていない場合もあります。

ZENworks Explorer

ZENworks Explorer は、Windows エクスプローラ用の拡張機能で、Windows エクスプローラ、デスクトップ、［スタート］メニュー、［クイック起動］ツールバー、および通知領域 (システムトレイ) にバンドルを表示できるようになります。次の図は、Windows Explorer に表示されるバンドルを示しています。

次の図は、デスクトップに表示されるバンドルを示しています。

ZENworks Window 内のバンドル上で実行されるタスクは、ZENworks Explorer で実行することもできます。

ZENworks Icon

ZENworks Icon は、Windows の通知領域 (システムトレイ) にあります。アイコンをクリックすると、［ZENworks Agent］ウィンドウを表示できます。

エージェントのプロパティを表示するには、［ZENworks Icon］を右クリックして［技術者アプリケーション］を選択します。［ZENworks Agent プロパティ］ウィンドウが表示されます。

プロパティウィンドウの左側のナビゲーション画面には、ZENworks Agent のステータスおよび各機能のリンクが含まれています。

- **ステータス :** エージェントが前回 ZENworks サーバに接続した時間や、Agent 機能が実行中であるかどうかなどの情報が表示されます。

- **ポリシー**：デバイスおよびログインユーザに割り当てられたポリシーが表示され、ポリシーが有効かどうかについても表示されます。ZENworks Configuration Management または ZENworks Endpoint Security Management が有効な場合にのみ含まれます。
- **バンドル**：デバイスおよびログインユーザに割り当てられているバンドルが表示されます。また、各バンドルの現在のインストールステータス (使用可能、ダウンロード中、インストール中など) およびバンドルが有効 (デバイスが配布の要件を満たしている) かどうかも表示されます。ZENworks Configuration Management または ZENworks Patch Management が有効な場合にのみ含まれます。
- **インベントリ**：デバイスのインベントリ情報が表示されます。ハードドライブ、ディスクドライブ、ビデオカードの製造元やモデルなどのハードウェアの詳細を表示できます。また、インストール済み Windows ホットフィックスとパッチ、およびインストール済みソフトウェア製品のバージョン番号と場所などのソフトウェアの詳細も表示できます。ZENworks Configuration Management または ZENworks Asset Management が有効な場合にのみ含まれます。
- **エンドポイントセキュリティ**：適用されるセキュリティポリシーの判断に使用されるエンドポイントセキュリティエージェントと場所に関する情報を表示します。ZENworks Endpoint Security Management が有効な場合にのみ含まれます。
- **リモート管理**：現在接続しているリモートオペレータおよびデバイスで有効になっているリモート管理ポリシーの設定に関する情報が表示されます。また、管理セッションを開始したり、セッションのセキュリティ設定を制御したりすることもできます。ZENworks Configuration Management が有効な場合にのみ含まれます。
- **サテライト**：サテライトサーバとして使用するデバイスのサテライト役割情報を表示します。サテライトの役割には、コレクション、コンテンツ、認証、イメージング、およびプロキシの結合が含まれます。

  この機能は、ZENworks 管理者がデバイスをサテライトとして使用している場合にのみ表示されます。
- **ログ**：ログファイルの場所、エージェントのログファイルがアップロードされる ZENworks サーバ、および次回ログのアップロードが予定されているスケジュールなど、ZENworks Agent のログファイルに関する情報が表示されます。また、記録されたメッセージの重大度レベルを決めることもできます。
- **Windows プロキシ** デバイスが ZENworks プライマリサーバの Windows プロキシとして機能するときに、デバイスで実行したディスカバリアクティビティおよび展開アクティビティの結果を表示します。

管理対象デバイスのサテライトへの昇格

サテライトは、認証、情報収集、コンテンツ配布、イメージングなど、ZENworks プライマリサーバが通常実行する役割の一部を実行できる管理対象デバイスです。サテライトとして、任意の管理対象 Windows デバイス、管理対象 Linux デバイス、または管理対象 Macintosh デバイスを指定できますが、プライマリサーバを指定することはできません。サテライトを設定する際には、サテライトが実行する役割を指定します (認証、コレクション、コンテンツ、またはイメージング)。サテライトは、ZENworks フレームワークのスナップインとなるサードパーティ製品によって追加される役割を実行することもできます。

サテライトの詳細と管理対象デバイスをサテライトに昇格する方法については、『*ZENworks プライマリサーバおよびサテライトリファレンス*』の「サテライト」を参照してください。

5 システムメッセージ

ZENworks を使用すると、管理ゾーン内のアクティビティをシステムメッセージを介して監視できます。

システムメッセージの参照

ZENworks システムでは、ソフトウェアの配布およびポリシーのアプリケーションなどのアクティビティを監視のサポートをするため、通常のメッセージ (情報)、警告メッセージ、およびエラーメッセージが生成されます。

各 ZENworks サーバおよび ZENworks Agent は、関連付けられているアクティビティのログを作成します。メッセージは、ZENworks コントロールセンターのさまざまなエリアに表示されます。

- **システムメッセージログ** : システムメッセージログには、［ダッシュボード］>［システムメッセージ］を選択してアクセスすることができ、ゾーン内のすべての ZENworks Server および ZENworks Agent からのメッセージが表示されます。
- **デバイスメッセージログ** : サーバまたはワークステーションの［概要］ページのデバイスメッセージログには、ZENworks サーバあるいは ZENworks Agent で生成されたメッセージが表示されます。たとえば、ワークステーション 1 用のメッセージログには、ワークステーション 1 の ZENworks Agent で生成されたすべてのメッセージが含まれます。
- **コンテンツメッセージログ** : バンドルまたはポリシーの［概要］ページのコンテンツメッセージログには、バンドルまたはポリシーに関連付けられた ZENworks サーバあるいは ZENworks Agent で生成されたメッセージのみが表示されます。たとえば、バンドル 1 のメッセージログには、3 つの ZENworks サーバと 100 の別々の ZENworks Agent で生成されたメッセージが含まれています。

メッセージのサマリの参照

ゾーン内のサーバ、ワークステーション、バンドル、およびポリシーに対して生成されたメッセージ数を示す概要を表示できます。

1 ZENworks コントロールセンターで、［ホーム］タブをクリックします。

［メッセージ概要］パネルには、管理ゾーンのすべてのサーバ、ワークステーション、ポリシー、およびバンドルのステータスが表示されます。たとえば、2 つのサーバで未承認の重大なメッセージ (当事者または他方の管理者が未確認のメッセージ) がある場合、 カラムに数字の 2 が表示されます。または、警告メッセージ付きの 3 つのバンドルと通常のメッセージの 5 つのバンドルがある場合、 カラムに数字の「3」が表示され、 カラムに「5」と表示されます。概要では次のことを行えます。

- root フォルダを表示するオブジェクトタイプをクリックします。たとえば、［サーバ］をクリックして、サーバのルートフォルダを表示します (/ サーバ)。

- 任意のオブジェクトタイプで、いずれかのステータスカラム () の数字をクリックすると、現在そのステータスであるオブジェクトがすべて一覧表示されます。たとえば、通常ステータスのサーバのリストを確認するには、  カラムで数字をクリックします。
- オブジェクトタイプについては、［合計］列でメッセージ数をクリックして、重大、警告、または通常のメッセージのあるオブジェクトすべてを表示します。たとえば、［サーバ］の［合計］メッセージ数をクリックして、何らかのメッセージがあるサーバをすべてリスト表示します。

メッセージの承認

メッセージは、承認されるまではメッセージログにあります。メッセージは個別に、またはメッセージログ内のすべてのメッセージを一度に承認することができます。

1. ZENworks コントロールセンターで、［デバイス］タブをクリックします。
2. ZENworks サーバが見つかるまで Servers フォルダを移動します。
3. サーバをクリックして詳細を表示します。
4. ［サマリ］タブで、［メッセージログ］パネルを見つけます。

   ［メッセージログ］パネルは、ZENworks サーバによって生成されたすべてのメッセージ (情報、警告、およびエラー) を一覧表示します。次の表は、メッセージを承認および削除するためのさまざまな方法を説明しています。

タスク	ステップ	追加詳細
メッセージの承認	1. メッセージをクリックして、［メッセージ詳細情報］ダイアログボックスを表示します。 2. ［承認］をクリックします。	メッセージを承認しない場合は、［終了］をクリックしてダイアログボックスを閉じます。これによって、メッセージは［メッセージログ］リストにとどまります。
すべてのメッセージを承認する	1. 左のナビゲーションペインにある［タスク］リストで、［すべてのメッセージを承認］をクリックします。	
承認または未承認のメッセージすべてを表示する	1. ［詳細］ボタンをクリックして、［メッセージログの編集］ページを表示します。	承認および未承認のメッセージすべてを表示するのに加え、特定のステータスまたは日付のメッセージのみを表示したり、メッセージの詳細を表示したり、メッセージを承認したりすることもできます。 そのページにあるタスクの実行についての固有情報については、［メッセージログの編集］ページで［ヘルプ］ボタンをクリックします。
メッセージの削除	1. メッセージをクリックして、［メッセージ詳細ログ］ダイアログボックスを表示します。 2. ［削除］をクリックします。	メッセージを削除すると、ZENworks システムからメッセージが完全に削除されます。

また、zman ユーティリティで messages-acknowledge コマンドを使用して、デバイス、バンドル、およびポリシーに関連付けられたメッセージを承認することもできます。詳細については、『*ZENworks コマンドラインユーティリティリファレンス*』の「メッセージコマンド」を参照してください。

詳細の参照場所

システムメッセージの詳細については、『*ZENworks コントロールセンターリファレンス*』の「メッセージログの使用」を参照してください。

ウォッチリストの作成

ステータスを詳しく監視したいデバイス、バンドル、またはポリシーがある場合、それらをウォッチリストに追加できます。ウォッチリストは以下の情報を提供します。

- **エージェント**：サーバおよびワークステーションの場合、デバイスの ZENworks Agent が現在接続されているか ( )、または接続解除されているか ( ) かどうかが表示されます。
- : オブジェクトに重大なメッセージがあるかどうかを表示します。
- **タイプ**：オブジェクトのタイプを表すアイコンを表示します。たとえば、バンドルに、Windows バンドルであることを示す アイコンが表示されている場合があります。また、デバイスにサーバであることを示す が表示される場合があります。アイコンの上にマウスを合わせると説明が表示されます。

- **名前 :** オブジェクトの名前を表示します。名前をクリックしてオブジェクトのメッセージログに移動することができます。

デバイス、バンドル、またはポリシーをウォッチリストに追加する

1. ZENworks コントロールセンターで、［ホーム］タブをクリックします。
2. ［ウォッチリスト］パネルで、［追加］をクリックしてから、リストに追加したいオブジェクトタイプ (デバイス、バンドル、またはポリシー) を選択します。
3. 選択ダイアログボックスで、目的のオブジェクトを選択し、［OK］をクリックしてウォッチリストに追加します。

   たとえば、サーバを追加するには、サーバを参照して選択します。

オブジェクトは削除するまでウォッチリスト内に残ります。

6 監査管理

ZENworks では、監査管理機能を使用して、ZENworks システムで行われるアクティビティを正常に記録して表示することができます。監査管理機能を使用すると、ゾーン内で発生したさまざまなイベントをキャプチャすることができます。キャプチャされたイベントの詳細は、セキュリティおよびコンプライアンスの目的で使用することができ、環境内で重要なイベントが発生したときに、誰がどのシステムに対して何をしたかを特定することが可能になります。この機能を使用して、プライマリサーバ、サテライトサーバ、および管理対象デバイスに関連するアクティビティを集中監視することができます。

監査イベントのタイプ

ZENworks の監査イベントには、次の 2 つのタイプがあります。

- **変更イベント :** これらのイベントにより、ZENworks コントロールセンターや zman コマンドラインユーティリティを介してゾーンに加えられた設定の変更がキャプチャされます。バンドルの変更から ZENworks システムの変更に至るまで、さまざまな変更をキャプチャすることができます。たとえば、デバイスにバンドルを割り当てる管理者のアクティビティを記録する監査イベントを設定できます。
- **エージェントイベント** これらのイベントは、ZENworks の管理対象デバイスに発生したアクションをキャプチャします。デバイスイベントとも呼ばれています。

ゾーン内のすべてのデバイスまたは個別のデバイスに対して、変更イベントとエージェントイベントの両方を有効にすることができます。

イベントの有効化

イベントを監査するには、まず ZENworks コントロールセンターでイベントを有効化する必要があります。ゾーンまたはデバイスレベルでイベントを有効化することができます。ゾーンレベルで有効化されたイベントは、ゾーン内のすべてのデバイスに適用され、デバイスレベルで有効化されたイベントは、選択されたデバイスにのみ適用されます。

1. ZENworks コントロールセンターにログインします。
2. (ゾーン) ゾーンでイベントを有効化するには、［環境設定］>［管理ゾーンの設定］>［監査管理］をクリックします。

   または

   (デバイス) デバイスでイベントを有効化するには、［デバイス］>［管理対象デバイス］をクリックします。［サーバ］フォルダまたは［ワークステーション］フォルダでデバイスを探して、デバイスオブジェクトをクリックし、そのプロパティを表示してから、［設定］>［監査管理］をクリックします。

3 ［Events Configuration (イベント環境設定)］をクリックして、［Events Configuration (イベント環境設定)］ダイアログページを表示します。

4 ［変更イベント］または［エージェントイベント］タブで、［追加］をクリックし、［Add Change Events (変更イベントを追加)］または［Add Agent Events (エージェントイベントを追加)］ダイアログボックスを表示します。

変更イベントおよびエージェントイベントの各カテゴリの詳細については、『*ZENworks Audit Management Reference*』を参照してください。

5 ［変更イベント］または［エージェントイベント］ツリーを拡張し、必要なイベントを選択します。

6 ［Event Settings (イベント設定)］に対して、次の情報を指定します。

- **イベントの分類 :** イベントの重要性に基づき、［クリティカル］、［主要］、または［情報］のいずれかを選択します。
- **Days to keep (ファイルを保持する日数):** イベントが消去されるまでに保持される日数を指定します。
- **通知タイプ :** イベントの発生時に、電子メール、SNMP Trap、UDP を介して送信するか、またはローカルファイル宛てに送信するかを指定します。［Log message to a local file (ローカルファイルへのログメッセージ)］を選択した場合は、ローカルログファイルの設定を行う必要があります。

  すべての通知タイプを選択することもできます。詳細については、「メッセージログの使用」を参照してください。
- (エージェントイベント) 監査イベントを生成するためにデータが収集される［サンプル頻度］レートを指定します。このフィールドは、ZENworks Endpoint Security Management イベントまたは ZENworks Agent イベントが選択された場合にのみ表示されます。

7 イベントを追加するには［OK］をクリックします。

イベントを編集または削除するには、［Event Configuration (イベント環境設定)］ページでイベントを選択して、メニューバーから［編集］または［削除］をクリックします。一度に複数のイベントを選択するには、［Ctrl］を押したままクリックして選択します。

生成されたイベントの表示

有効化されたイベントが発生した場合は、監査イベントが生成されます。

監査イベントが生成されると、次の場所からイベントの詳細にアクセスできます。

- **ダッシュボード :** ZENworks コントロールセンターダッシュボードを介して監査データを表示できます。ダッシュボードには次のタブがあります。
  - **ダッシュボード :** このタブから、ゾーン内で発生した監査イベントの概要を表示できます。上位のイベントに関する重要なインジケータや影響を受けるオブジェクトを表示したり、イベントログビューでフィルタリングして詳細を確認することができます。デフォルトでは、このダッシュボードには、直近の 4 時間のイベント概要が示されます。さらに多くのデータを表示したい場合は、期間を変更できます。
  - **イベント (監査ログ):** このタブを使用すると、ゾーン内で発生したすべてのイベントを表示できます。この情報は、［Events Configuration (イベント環境設定)］ページと同様の形式で表示されます。イベントが生成されたカテゴリに対して、カウントが表示されます。たとえば、［Bundle Assignment Management (バンドル割り当て管理)］イベントが生成さ

れた場合は、ツリー構造の［Bundle Assignment Management (バンドル割り当て管理)］カテゴリに対して［1］が表示されます。イベントをクリックすると、右ペインにイベントの詳細が表示されます。

- **(変更イベント) オブジェクトフォルダ :** オブジェクトフォルダ (［デバイス］、［バンドル］、［ポリシー］および［Users (ユーザ)］) の［Audit (監査)］タブを使用すると、選択したフォルダ内のすべてのオブジェクトに対して生成された監査イベントを表示することができます。たとえば、バンドルフォルダ内のすべてのバンドルに対して生成されたイベントを表示できます。したがって、［バンドル］フォルダにすべてのバンドル関連のイベントを表示できます。この情報は、［Events Configuration (イベント環境設定)］ページと同様に分類されます。発生したイベントを参照することができ、さらに多くの情報が必要な場合は、イベントをクリックして、イベント詳細を表示できます。
- **(変更イベント) オブジェクト :** オブジェクトフォルダ内のオブジェクトに対する監査イベントを表示することもできます。たとえば、バンドルフォルダ内の特定のバンドルを選択すると、その特定のバンドルに対して生成されたイベントを表示できます。
- **(エージェントイベント) ［デバイス］フォルダ :** ［デバイス］フォルダの［Audit (監査)］タブを使用すると、特定のデバイス (サーバまたはワークステーション) に対して生成されたイベントを表示できます。

生成されたイベント詳細を表示するには、次の手順を実行します。

1 ZENworks コントロールセンターにログインします。

2 (ダッシュボード) ダッシュボードにイベントを表示するには、［ダッシュボード］> ［Events (イベント)］の順にクリックします。

または

(オブジェクトフォルダ) フォルダ (デバイスフォルダ、バンドルフォルダ、ポリシーフォルダなど) 内のすべてのオブジェクトに対するイベントを表示するには、そのフォルダの［詳細］リンクをクリックし、［Audit (監査)］タブをクリックします。

または

(オブジェクト) 特定のオブジェクト (デバイス、バンドル、ポリシーなど) に対するイベントを表示するには、そのオブジェクトをクリックし、［Audit (監査)］タブをクリックします。

(［デバイス］フォルダ) ［デバイス］フォルダ内のイベントを表示するには、左ペインで、［デバイス］をクリックします。ゾーン内のサーバ上でイベントが実行された場合には、そのサーバの［詳細］をクリックし、管理対象デバイス上でイベントが実行された場合には、ワークステーションの［詳細］をクリックします。次に［Audit (監査)］タブをクリックして、［Events (イベント)］画面を表示します。

3 ［変更イベント］または［エージェントイベント］タブをクリックします。

4 ツリー構造を拡張し、関連するカテゴリに移動します。

設定された監査イベントの数に応じて、カテゴリに対して関連するカウントが表示されます。

5 イベントをクリックします。

右側のペインに、生成されたイベントの詳細が表示されます。

注 : 新しいウィンドウでイベントの詳細を表示するには、  をクリックします。

製品管理

次のセクションでは、ZENworks 製品の使用に役立つ情報を提供します。セクションのいずれかを実行する前に 9 ページのパート I「システム設定」の設定タスクを完了している必要があります。

7 クイックリスト

管理ゾーンを設定したら (9 ページのパート I「システム設定」を参照)、ライセンス済みまたは評価中の ZENworks 製品について次のセクションの概念およびタスクをレビューする必要があります。

- 57 ページの 「Asset Management」
- 58 ページの 「環境設定の管理」
- 59 ページの 「Endpoint Security Management」
- 60 ページの 「Full Disk Encryption」
- 61 ページの 「パッチ管理」

Asset Management

ZENworks Asset Management では、ソフトウェアライセンスコンプライアンスの監視、ソフトウェア使用状況の追跡、およびデバイス、部署、サイト、またはコストセンターにライセンスを割り当てることによってソフトウェア所有権の追跡が可能です。

タスク	詳細
アセット管理の有効化	管理ゾーンのインストール時に、ライセンスキーを入力するか、評価をオンにして Asset Management を起動しなかった場合は、製品を使用する前にこれを行ってください。 方法については、63 ページの 「アセット管理の有効化」を参照してください。
アセット管理操作を実行するための ZENworks Agent の有効化	エージェントのアセット管理機能は、ZENworks Asset Management (フルライセンスまたは評価版) が有効になっている場合にはデフォルトで有効になっています。 エージェントのアセット管理機能がまだ有効になっていることを確認する必要があります。また、(デバイスに対してだけでなく) ユーザに対するソフトウェアライセンスを追跡したい場合、デフォルトで無効になっているユーザ管理機能を有効にする必要があります。方法については、63 ページの 「ZENworks Agent での Asset Management の有効化」を参照してください。
デバイスのスキャンによるソフトウェアおよびハードウェアインベントリの収集	デバイスをスキャンしてデバイスのソフトウェアおよびハードウェアインベントリを収集します。インベントリ情報はソフトウェア配布およびハードウェアアップグレードを決定する手助けとなります。 このタスクは、残りのタスクのいずれかを実行する前に行う必要があります。 方法については、64 ページの 「ソフトウェアインベントリおよびハードウェアインベントリの収集」を参照してください。

タスク	詳細
ソフトウェア使用の監視	使用しているソフトウェア製品の数量や頻度を分析するレポートを生成します。 方法については、65 ページの 「ソフトウェア使用状況の監視」を参照してください。
ソフトウェアのライセンスコンプライアンスの監視	インストールされたソフトウェア製品が正しくライセンスされているのか、アンダーライセンスなのか、オーバーライセンスなのかを確認します。 方法については、66 ページの 「ライセンスコンプライアンスの監視」を参照してください。
ライセンスの割り当て	組織内でライセンスを割り当てて、ライセンスの所有権と配布を追跡できます。ライセンスはデバイス単位または人口統計単位 (サイト、部署、コストセンター) に割り当てられます。 方法については、72 ページの 「ライセンスの割り当て」を参照してください。

環境設定の管理

ZENworks Configuration Management では、ソフトウェアのデバイスへの配布、Windows 環境設定ポリシーの適用、イメージングとイメージの適用を含む、デバイスの設定を管理できます。また、デバイスハードウェアおよびソフトウェアインベントリを収集して、アップグレードおよび購買決定について通知し、リモートの場所からデバイスにアクセスしてトラブルシューティングし、問題を解決することができます。

次のタスクは必要に応じて任意の順序で実行できます。

タスク	詳細
環境設定の管理の有効化	管理ゾーンのインストール時に、ライセンスキーを入力するか、評価をオンにして Configuration Management を起動しなかった場合は、製品を使用する前にこれを行ってください。 方法については、75 ページの 「環境設定の管理の有効化」を参照してください。
環境設定の管理操作を実行するための ZENworks Agent の有効化	ZENworks Agent がデバイス上で環境設定の管理を実行するには、適切なエージェント機能が有効になっている必要があります。これらの機能 (バンドル管理、イメージ管理、ポリシー管理、リモート管理、およびユーザ管理) は、ZENworks Configuration Management (フルライセンスまたは評価版) が有効化される場合、デフォルトで有効になっています。 機能が有効になっていることを確認する必要があります。または、特定の機能を使用したくない場合は、それらの機能を無効化できます。方法については、76 ページの 「ZENworks Agent での Configuration Management の有効化」を参照してください。

タスク	詳細
モバイルデバイスの登録	バンドルの展開やセキュリティポリシーの適用などモバイルデバイスの環境設定管理操作、およびさまざまなデバイス管理操作を実行できるようにするには、モバイルデバイスを ZENworks 管理ゾーンに登録する必要があります。手順については、『ZENworks 2017 Mobile Management Reference』を参照してください。
ソフトウェアの配布	バンドルを通じてソフトウェアを配布します。バンドルは、ソフトウェアのインストール、起動、およびアンインストール (必要な場合) に必要なソフトウェアファイルおよび指示を含んでいます。バンドルを作成して、Windows Installer アプリケーション (MSI および MSP の両方)、非 Windows Installer アプリケーション、Web リンク、シンクライアントアプリケーション、Linux アプリケーション、および Macintosh アプリケーションを配布できます。 方法については、76 ページの 「ソフトウェアの配布」を参照してください。
ポリシーの適用	デバイス動作をポリシーのアプリケーションを通じて制御します。ZENworks を使用すると、Windows Group ポリシー、ローミングプロファイルポリシー、ブラウザブックマークポリシー、プリンタポリシーなどを作成して適用できます。 方法については、78 ページの 「ポリシーの適用」を参照してください。
デバイスのイメージを取得およびイメージのデバイスへの適用	デバイスのイメージの作成、イメージのデバイスへの適用、およびイメージングスクリプトのデバイス上での実行を行うことができます。ZENworks Configuration Management は Preboot Services 機能を使用して、これらのイメージングタスクをスタートアップ時にデバイス上で実行します。 方法については、81 ページの 「イメージングデバイス」を参照してください。
デバイスのスキャンによるソフトウェアおよびハードウェアインベントリの収集	デバイスをスキャンしてデバイスのソフトウェアおよびハードウェアインベントリを収集します。インベントリ情報はソフトウェア配布およびハードウェアアップグレードを決定する手助けとなります。 方法については、98 ページの 「ソフトウェアインベントリおよびハードウェアインベントリの収集」を参照してください。

Endpoint Security Management

ZENworks Endpoint Security Management は、ポリシーを介してセキュリティ設定を適用することで、デバイスを保護することができます。リムーバブルストレージデバイス、無線ネットワーク、およびアプリケーションへのデバイスのアクセスを制御できます。また、暗号化によってデータを保護し、ファイアウォールの実施 (ポート、プロトコル、および制御リスト) を介してネットワーク通信を保護することができます。また、その場所に基づいてエンドポイントデバイスのセキュリティを変更できます。

次のタスクは表示される順序で行う必要があります。

タスク	詳細
エンドポイントセキュリティ管理の有効化	管理ゾーンのインストール時に、ライセンスキーを入力するか、評価をオンにして Endpoint Security Management を起動しなかった場合は、製品を使用する前にこれを行ってください。 方法については、109 ページの 「エンドポイントセキュリティ管理の有効化」を参照してください。
エンドポイントセキュリティエージェントの有効化	エンドポイントセキュリティエージェントは、デバイスにセキュリティポリシーを適用します。セキュリティポリシーを配布したい各デバイスにインストールし、有効にする必要があります。 方法については、110 ページの 「エンドポイントセキュリティエージェントの有効化」を参照してください。
場所の作成	セキュリティポリシーはグローバルに適用することも、固有の場所に適用することもできます。グローバルポリシーはすべての場所に適用されます。場所ベースのポリシーは、デバイスのネットワーク環境がその場所に定義された環境に一致すると Endpoint Security Agent が判断する場合にのみ適用されます。 場所ベースのポリシーを使用する場合は、場所を作成する必要があります。方法については、110 ページの 「場所の作成」を参照してください。
セキュリティポリシーの作成	デバイスセキュリティ設定は、セキュリティポリシーを介して設定されます。作成できるセキュリティポリシーは 11 種類あります。 方法については、110 ページの 「セキュリティポリシーの作成」を参照してください。
ユーザおよびデバイスへのポリシーの割り当て	セキュリティポリシーは、ユーザまたはデバイスに割り当てることができます。 方法については、113 ページの 「ユーザおよびデバイスへのポリシーの割り当て」を参照してください。
ゾーンへのポリシーの割り当て	デバイスが常に保護されるようにするために、ゾーンへポリシーを割り当てて、ポリシータイプごとにデフォルトのセキュリティポリシーを定義することができます。ゾーン割り当て済みポリシーは、デバイスがユーザ割り当て済みポリシーまたはデバイス割り当て済みポリシーでカバーされない場合に適用されます。 方法については、114 ページの 「ゾーンへのポリシーの割り当て」を参照してください。

Full Disk Encryption

ZENworks Full Disk Encryption は、デバイスの電源がオフのときや、デバイスがハイバネーションモードのときに、不正アクセスからデバイスのデータを保護します。データを保護するために、ディスクまたはパーティションの全体が暗号化されます。暗号化の対象には、一時ファイルやスワップファイル、オペレーティングシステムが含まれます。このデータには、認証済みユーザがログインするまでアクセスできなくなり、CD/DVD やフロッピーディスク、USB ドライブなどのメ

ディアからデバイスをブートしてもアクセスすることはできません。認証済みユーザの場合は、暗号化されていないディスク上のデータにアクセスするのと同じように、暗号化されたディスク上のデータにアクセスできます。

次のタスクは表示される順序で行う必要があります。

タスク	詳細
Full Disk Encryption の有効化	管理ゾーンのインストール時に、ライセンスキーを入力するか、評価をオンにして Full Disk Encryption を起動しなかった場合は、製品を使用する前にこれを行ってください。 方法については、115 ページの 「Full Disk Encryption のアクティブ化」を参照してください。
Full Disk Encryption Agent の有効化	Full Disk Encryption Agent はディスクの暗号化を実行します。ディスクを暗号化するデバイスごとにインストールし、有効化する必要があります。 方法については、116 ページの 「Full Disk Encryption Agent の有効化」を参照してください。
ディスク暗号化ポリシーの作成	デバイスディスクを暗号化するのに必要な情報は、ディスク暗号化ポリシーを介して Full Disk Encryption Agent に渡されます。少なくとも 1 つのポリシーを作成する必要があります。 方法については、116 ページの 「ディスク暗号化ポリシーの作成」を参照してください。
ポリシーのデバイスへの割り当て	ディスク暗号化ポリシーは、デバイス、デバイスグループ、またはデバイスフォルダにのみ割り当てることができます。 方法については、117 ページの 「ポリシーのデバイスへの割り当て」を参照してください。

パッチ管理

ZENworks Patch Management では、ソフトウェアの脆弱性の評価および脆弱性を除去するパッチの適用のプロセスを自動化することができます。

次のタスクは表示される順序で行う必要があります。

タスク	詳細
パッチ管理の有効化	ZENworks 管理ゾーンのインストール時に、サブスクリプションライセンスキーを入力するか、評価をオンにして Patch Management が有効化されなかった場合は、製品をアクティブ化する必要があります。 方法については、121 ページの 「パッチ管理の有効化」を参照してください。

タスク	詳細
パッチ管理操作を実行するための ZENworks Agent の有効化	ZENworks Agent がデバイスでパッチ管理操作を実行するには、エージェントのパッチ管理機能が有効になっている必要があります。パッチ管理機能は、ZENworks Patch Management (フルライセンスまたは評価版) が有効になっている場合にはデフォルトで有効になっています。 エージェントのパッチ管理機能が有効になっていることを確認する必要があります。方法については、122 ページの「ZENworks Agent での Patch Management の有効化」を参照してください。
サブスクリプションサービスの開始	ZENworks サーバでサブスクリプションサービスを開始する必要があります。このサーバはパッチをダウンロードし、他の ZENworks サーバに複製します (複数ある場合)。 方法については、122 ページの 「サブスクリプションサービスの開始」を参照してください。
パッチポリシーの作成	サブスクリプションサービスがパッチをダウンロードした後で、必要なパッチを適用します。 方法については、123 ページの 「パッチポリシーの作成」を参照してください。

8 アセット管理

次のセクションでは、ZENworks Asset Management を使用した、デバイスからのソフトウェアおよびハードウェアインベントリの収集、デバイスでのソフトウェア使用状況の監視、ソフトウェアライセンスコンプライアンスの監視について説明します。

アセット管理の有効化

管理ゾーンのインストール時に、ライセンスキーを入力するか、評価をオンにして Asset Management を起動しなかった場合は、次の手順を実行してください。

1 ZENworks コントロールセンターで、［環境設定］をクリックします。

2 ［ライセンス］パネルで、［ZENworks 2017 Asset Management］をクリックします。

3 ［製品の評価 / アクティブ化］を選択して、以下のフィールドに入力します。

使用評価 : このオプションを選択すると、60 日の評価期間が有効になります。60 日の評価期間終了後に製品を継続的に使用するには、製品ライセンスキーを申請しなければなりません。

製品ライセンスキー : Asset Management 用に購入したライセンスキーを指定します。製品ライセンスを購入するには、ZENworks Asset Management 製品サイト (http://www.novell.com/products/zenworks/assetmanagement) を参照してください。

4 ［OK］をクリックします。

ZENworks Agent での Asset Management の有効化

ZENworks Agent がデバイスでアセット管理操作を実行するには、エージェントのアセット管理機能が有効になっている必要があります。アセット管理機能は、ZENworks Asset Management (フルライセンスまたは評価版) が有効になっている場合にはデフォルトで有効になっています。

エージェントのアセット管理機能が有効になっていることを確認する必要があります。また、(デバイスに対してだけでなく) ユーザに対するソフトウェアライセンスを追跡したい場合、デフォルトで無効になっているユーザ管理機能を有効にする必要があります。方法については、37 ページの「ZENworks Agent 機能の設定」を参照してください。

注 : ZENworks Asset Management モジュールを有効にした後は、zac inv -f scannow コマンドを実行して、すべてのデバイスに対して強制的にフルスキャンを実行してください。このスキャンを実行しない限り、Asset Management のレポートは正確ではありません。

ソフトウェアインベントリおよびハードウェアインベントリの収集

デバイスのインベントリを行うとき、ZENworks Asset Management はデバイスからソフトウェアおよびハードウェアの情報を収集します。ZENworks コントロールセンターを使用すると、個別のデバイス向けのインベントリを表示したり、特定の基準に基づいて複数のデバイス向けのレポートを生成したりすることができます。

ソフトウェアインベントリは、特定のアプリケーションの使用状況を追跡したり、使用しているアプリケーションのすべてのコピーについて十分なライセンスがあることを確認するなど、いろいろな目的に使用できます。たとえば、会社でワープロソフトウェアのライセンスを 50 所有するとします。ソフトウェアインベントリを行い、60 個のデバイスにインストールされていることが判明しました。つまり、ライセンス契約に準拠していないことになります。ところが、過去 6 カ月間のソフトウェアに関する使用状況レポートを確認すると、実際には 45 個のデバイスしか使用していないことがわかりました。ソフトウェアを使用していない 15 個のデバイスからソフトウェアをアンインストールして、ライセンス契約に準拠するようにします。

ハードウェアインベントリは、特定のソフトウェアを実行するための要件をハードウェアが満たすことを確認するなど、いろいろな目的に使用できます。たとえば、経理部で会計ソフトウェアを新しいバージョンにするとします。新しいソフトウェアでは、プロセッサ、メモリ、ディスク容量などの要件が強化されています。デバイスから収集されるハードウェアインベントリを使用して、2 つのレポート、すなわち、要件を満たすすべてのデバイスのリストを表示するレポートと、要件を満たさないデバイスのリストを表示するレポートを作成できます。レポートに基づいて、ソフトウェアを準拠デバイスに配布し、非準拠デバイスにアップグレード計画を作成します。

デフォルトでは、デバイスは毎月 1 日の AM1:00 に自動的にスキャンされます。スケジュールおよびその他多くの［インベントリ］環境設定を ZENworks コントロールセンターの［環境設定］タブで変更することができます。

次のセクションでは、デバイススキャンの開始と収集したインベントリの使用について説明します。

- 64 ページの 「デバイススキャンの開始」
- 65 ページの 「デバイスインベントリの表示」
- 65 ページの 「インベントリレポートの生成」
- 65 ページの 「詳細の参照場所」

デバイススキャンの開始

デバイスのスキャンはいつでも開始できます。

1. ZENworks コントロールセンターで、［デバイス］タブをクリックします。
2. スキャンするデバイスが見つかるまで Servers または Workstations フォルダを移動します。
3. デバイスをクリックして詳細を表示します。

4 左ナビゲーションパネルにあるタスクリストで、［サーバインベントリスキャン］または［ワークステーションインベントリスキャン］をクリックしてスキャンを開始します。

［クイックタスクステータス］ダイアログボックスにはタスクの状態が表示されます。タスクが完了したら、［インベントリ］タブをクリックしてスキャンの結果を表示します。

同時に複数のデバイスをスキャンするには、デバイスがあるフォルダを開き、デバイスの横のチェックボックスをオンにして、［クイックタスク］>［インベントリスキャン］をクリックします。

zman ユーティリティで inventory-scan-now コマンドを使用してデバイスをスキャンすることもできます。詳細については、『*ZENworks コマンドラインユーティリティリファレンス*』の「インベントリコマンド」を参照してください。

デバイスインベントリの表示

1 ZENworks コントロールセンターで、［デバイス］タブをクリックします。

2 インベントリを表示したいデバイスが見つかるまで Servers または Workstations フォルダを移動します。

3 デバイスをクリックして詳細を表示します。

4 ［インベントリ］タブをクリックします。

［インベントリ］ページには、ハードウェアインベントリの概要が表示されます。インベントリ情報の詳細を表示するには、［ハードウェア / ソフトウェアのインベントリの詳細］をクリックします。

インベントリレポートの生成

ZENworks Asset Managementha は、いくつかの標準レポートを含んでいます。また、インベントリ情報の異なるビューを提供するためにカスタムレポートを作成することができます。

1 ZENworks コントロールセンターで、［レポート］タブをクリックします。

2 ［インベントリ標準レポート］パネルで、［ソフトウェアアプリケーション］をクリックします。

3 ［オペレーティングシステム］レポートをクリックしてレポートを生成します。

レポートの下部にあるオプションを使用して、生成されたレポートを Microsoft Excel スプレッドシート、CSV (カンマ区切り値) ファイル、PDF ファイル、または PDF Graph ファイルとして保存できます。

詳細の参照場所

インベントリの詳細については、『*ZENworks Asset Inventory リファレンス*』を参照してください。

ソフトウェア使用状況の監視

デバイスについてインベントリを行った後で、デバイスのアプリケーションの使用状況を表示するレポートを実行できます。ZENworks Asset Management には、製品別、ユーザ別、デバイス別のアプリケーション使用状況に関する標準レポートが組み込まれています。また、より詳細な、より

重点を絞った情報を提供するようにレポートをカスタマイズすることもできます。たとえば、Asset Management には過去 90 日間使用されていないアプリケーションを表示する、事前定義済みのカスタムレポートも組み込まれています。

特定のアプリケーションの使用状況を表示するレポートを実行するには、次の手順に従います。

1 ZENworks コントロールセンターで、［アセット管理］タブをクリックし、次に［ソフトウェア使用状況］タブをクリックします。

2 ［ソフトウェア使用状況標準レポート］パネルで、［アプリケーション使用状況］をクリックすると、アプリケーション使用状況レポートの一覧が表示されます。

3 このパネルで、［製品別ローカルアプリケーション使用状況］をクリックします。

レポートは、デバイスにインストールされている、ソフトウェア制作会社別にグループ化されたすべての製品を表示します。

4 確認対象の製品の制作会社を検索し、［インストール］カラムの数をクリックすると、インストールされている製品が表示されます。

得られたレポートには、各製品の現在のインストール数、インストール数のうち使用されているものの数、最後に使用された日時などの使用状況情報が示されます。

5 レポートの対象期間を変更する場合、または表示された製品の一覧 (全製品、使用している製品、または使用していない製品) を変更する場合は、レポートの最下部にある［期間の変更］/［フィルタ］をクリックします。

他にも、標準および事前定義済みのカスタムレポートなど、使用できるものがたくさんあります。アプリケーション使用状況レポートの詳細については、『*ZENworks Asset Management リファレンス*』の「レポート」を参照してください。

ライセンスコンプライアンスの監視

ZENworks Asset Management では、購入したソフトウェアライセンス数をインベントリスキャン中に検出された実際のソフトウェアインストール数と比較して、組織がソフトウェア使用許諾に従っているかどうかを監視できます。

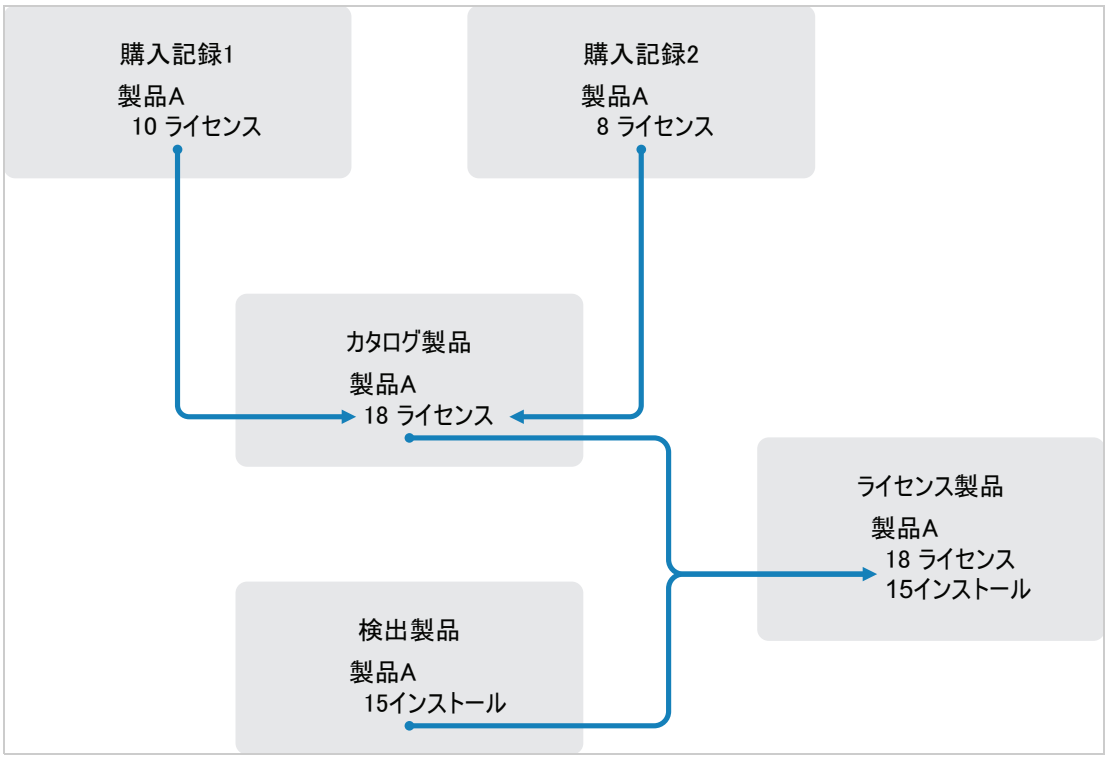
Asset Management ライセンスコンプライアンスは、強力で柔軟なツールです。この結果、ライセンスコンプライアンスを設定する際に複数のアプローチと方法を使用できます。次のセクションでは、ライセンスコンプライアンスを監視する製品をすばやく設定するため、最小限の説明で基本的な手順を説明します。この基本シナリオを把握したら、『*ZENworks Asset Management リファレンス*』の「ライセンスコンプライアンス」を参照して、詳細な情報と手順を理解してください。

- 66 ページの 「ライセンスコンプライアンスコンポーネント」
- 68 ページの 「インストールされた製品の検出」
- 68 ページの 「カタログ製品と購買記録の作成」
- 69 ページの 「ライセンス製品の作成」
- 71 ページの 「コンプライアンスデータの表示」
- 72 ページの 「詳細の参照場所」

ライセンスコンプライアンスコンポーネント

コンプライアンス監視の実行を開始する前に、次の例とそれに続くテキストで説明されているように、関連するコンポーネントやその機能について把握する必要があります。

図 8-1 ライセンスコンプライアンスコンポーネント



- 管理ゾーン内のデバイスをスキャンして、インストールされたソフトウェア製品のリストを収集します。これらは、*検出製品*と呼びます。上記の例では、インベントリスキャンで、ProductA が 15 個のデバイスにインストールされていることがわかります。
- 組織で購入したソフトウェア製品を示す*カタログ製品*を作成します。一般に、各カタログ製品は特定の製作会社の部品番号に対応します。上記の例では、ProductA だけがカタログ製品です。ただし、ProductA、ProductA Upgrade、ProductB などのカタログ製品がある場合もあります。
- ソフトウェア製品の購入注文または請求書を示す*購入記録*を作成します。ライセンス購入記録の各細目には、カタログ製品と購入数量が表示されます。カタログ製品が複数の購入記録にリストされている場合、そのカタログ製品の総ライセンス数は両方の購入記録の購入数量に等しいです。上記の例において、1 つの購入記録には ProductA の 10 個のライセンスがあり、もう 1 つの購入記録には 8 個のライセンスがあります。ProductA の総ライセンス数は 18 です。
- *ライセンス製品*を作成し、検出された対応製品とカタログ製品をライセンス製品に関連付けます。これを行うことで、製品のライセンス数やインストール数が示された単一のライセンス製品を確認できます。その結果、製品の使用状況が製品ライセンス契約に準拠しているかどうかがすぐに示されます。上記の例で、ProductA のライセンス数は 18 個で、15 個のデバイスにインストールされているので、ProductA はライセンス契約にコンプライアンスしています。

インストールされた製品の検出

管理ゾーンのデバイスをスキャンしてインストールされている製品 (［検出製品］と呼ばれる) についての情報を収集していない場合は、64 ページの 「ソフトウェアインベントリおよびハードウェアインベントリの収集」の手順を完了してください。

製品を検出した後、監視するコンプライアンスを選択します。

1 ZENworks コントロールセンターで、［アセット管理］タブをクリックし、次に［ライセンス管理］タブをクリックします。

2 ［ライセンス管理］パネルで、［検出された製品］をクリックし、［検出された製品］リストを表示します。

3 リストを参照して、使用する検出製品を選択します。

製品は、［インストール済み数量］列に少なくとも 1 つのインストールが表示されている必要があります。可能な場合、購入注文または請求書を使用できる製品を選択します。これによって、実際の情報を使用したシナリオが完了します。この方法を採用しない場合は、実際の購入ごとに購入情報を作成できます。後で使用できるように、選択した製品を記録しておいてください。

4 次のセクションの68 ページの 「カタログ製品と購買記録の作成」に進みます。

カタログ製品と購買記録の作成

検出製品から、製品のインストール情報が得られます。製品購入についての情報を取得するには、カタログ製品と購買記録を作成します。

カタログ製品はソフトウェア製品を示します。購買記録からカタログ製品に購入した製品ライセンス数が入力されます。

次の手順では、68 ページの 「インストールされた製品の検出」で選択した検出製品に対してカタログ製品と購買記録を作成する方法を説明します。

1 ZENworks コントロールセンターで、［アセット管理］タブをクリックし、次に［ライセンス管理］タブをクリックします。

2 カタログ製品を作成する :

2a ［ライセンス管理］パネルで、［カタログ製品］をクリックします。

2b ［新規］>［カタログ製品］の順にクリックして、新規カタログ製品の作成ウィザードを起動します。

2c 次のフィールドに入力します。

製造元 : ソフトウェア制作会社をリストから選択します。リストに正しい製造元がない場合は、製造元名を入力します (例、Novell、Symantec、Microsoft など)。

製品名 : 製品の名前を入力します。製品は、購入したソフトウェア製品パッケージ (SKU) を示す必要があります。たとえば、購入パッケージは「Product A Single License」または「Product A 10-Pack」となります。カタログ製品を作成している製品の請求記録がある場合、請求書の製品名を使用します。

パッケージ別ライセンス : 製品パッケージに含まれるライセンス数を指定します。

製品タイプ – 注 : これらのフィールドは、オプションです。これらを使用して製品をさらに絞り込むことができます。

除外 : このチェックボックスは選択しません。

2d ［次へ］をクリックして［概要］ページを表示してから、［完了］をクリックして、製品を［カタログ製品］リストに追加します。

2e ［ライセンス管理］(ページの最上部にあるブレッドクラムパスにある) をクリックし、［ライセンス管理］ページに戻ります。

3 購買記録を作成する :

3a ［ライセンス管理］パネルで、［購入記録］をクリックします。

3b ［新規］>［購入記録］の順にクリックし、新規購入記録の作成ウィザードを起動します。

3c 次のフィールドを入力します。

PO 番号 : ソフトウェア製品購入と関連付けられた購入注文番号または請求書番号を指定します。この製品に対する発注書または請求書がない場合は、任意の番号を使用します。

注文日付 : ソフトウェアの購入日付を選択します。

受信者 – 販売者 : これらのフィールドは、オプションです。これらを使用して購入記録を詳しく確認することができます。

3d ［次へ］をクリックして［概要］ページを表示します。

3e ［追加のプロパティの定義］ボックスを選択してから、［完了］をクリックして、購入記録を作成し、その［購入詳細］ページを表示します。

3f ［追加］をクリックして、［購入詳細の追加］ダイアログボックスを表示してから、次のフィールドを入力します。

製品名 : をクリックして、ステップ 2 で作成したカタログ製品を参照し、選択します。

数量 : 購入製品の数量を指定します。たとえば、選択したカタログ製品が ProductA 10 パックで、購入注文が ProductA 10 パック 5 個の場合は、5 を指定します。

ユニット MSRP - 増値 : これらのフィールドは、必須です。メーカー希望小売価格 (MSRP)、支払った価格 (ユニット単位)、および増値を指定します。［総額］フィールドを空白にすると、ウィザードから［購入数量］と［単価］を掛け合わせた数値が入力されます。

請求書番号 - コメント : これらのフィールドは、オプションです。これらを使用して購入をさらに特定することができます。

3g ［OK］をクリックします。

4 次のセクションの「ライセンス製品の作成」に進みます。

Asset Management では、購入情報を電子ファイルからインポートすることもできます。処理中に、購買記録の他、購買記録に含まれるソフトウェア製品のカタログ製品も作成されます。詳細については、『*ZENworks Asset Management リファレンス*』の「ライセンスコンプライアンス」を参照してください。

ライセンス製品の作成

ソフトウェア製品のコンプライアンス設定の最終手順では、ライセンス製品を作成し、検出された製品とカタログ製品とに関連付けます。これによって、ライセンスコンプライアンスステータスの判定に必要なインストールとライセンスの情報がライセンス製品に指定されます。

次の手順では、自動調整ウィザードでライセンス製品を作成し、検出された製品とカタログ製品とに関連付ける方法を説明します。

1 ZENworks コントロールセンターで、［アセット管理］タブをクリックし、次に［ライセンス管理］タブをクリックします。

2 ［ライセンス管理］パネルで、［ライセンスされた製品］をクリックします。

3 ［ライセンス製品］パネルで、**［アクション］ > ［自動調整済み : ライセンス製品の作成］**の順にクリックして、自動調整ウィザードを起動します。次の表からの情報を使用してフィールドに入力し、ウィザードを完了します。

［ウィザード］ページ	**詳細**
検出された製品フィルタ	自動調整ウィザードは、既存の検出製品からライセンス製品を作成します。検出製品を検索するには、次の手順に従います。 1. **［以下に指定した製品］**オプションをクリックします。 2. **［選択］**リストで、検出製品の製造元を選択します。 3. **［製品］**フィールドに、検出製品の名前を入力します。
作成するライセンス製品の選択	［検出された製品フィルタ］で指定した情報に基づいて、このページには検出された製品と、それに対して作成されるライセンス製品が表示されます。 ウィザードでは、［製造元］フィールドと［製品］フィールドを比較して、カタログ製品と検出製品の照合を試みます。作成したカタログ製品と検出した製品をウィザードで照合できた場合、カタログ製品もリストされます。ライセンス製品と関連付けるカタログ製品を選択します。 ウィザードでカタログ製品と検出製品を照合できなかった場合、ウィザードを終了してからカタログ製品を手動で割り当てる必要があります。
宛先フォルダ	新しいライセンス製品を配置するフォルダを選択します。 フィールドのデフォルト値は現在のフォルダです (自動調整ウィザードを起動したフォルダ)。別のフォルダを指定するには、 をクリックして、フォルダを参照して選択します。既存のフォルダを指定します。選択ダイアログを使用して新規フォルダを作成することはできません。
ライセンスエンタイトルメント	各ライセンス製品には、少なくとも 1 つのエンタイトルメントとライセンスモデルが必要です。 エンタイトルメントは通常、使用許諾契約です。多くの場合、1 つのライセンス製品にはエンタイトルメントが 1 つしかありません。ただし、複数のエンタイトルメントを許可することで、複数の使用許諾契約があるライセンス製品のコンプライアンスを判定できます。たとえば、同一製品で、フルライセンス契約とアップグレードライセンス契約を指定できます。同一製品に対して 2 つのライセンス製品を作成するのではなく、2 種類のエンタイトルメントを持つ 1 つのライセンス製品を作成できます。 ライセンスモデルは、ライセンスの計上方法を指定します。ライセンスは、インストール、ユーザ、またはデバイス単位で計上できます。 このシナリオでは、説明として**［インストールごと］**を指定し、ライセンスモデルとして**［インストールごと］**を選択します。これによって、製品のインストールごとにライセンスが使用されます。
自動調整作成サマリ	データを確認します。

4 まだこの操作を行っていない場合は、**［完了］**をクリックしてライセンス製品を作成し、［ライセンスされた製品］リストに追加します。

5 自動調整ウィザードでカタログ製品をライセンス製品と関連付けられない場合は、次の手順に従います。

5a ライセンス製品をクリックします。

5b［ライセンスエンタイトルメント］タブをクリックします。

5c［エンタイトルメント］パネルで、エンタイトルメントをクリックします。

5d［所有権の証明］タブをクリックします。

5e［カタログ製品］パネルで、［追加］をクリックします。

5f カタログ製品を選択し、［OK］をクリックして［カタログ製品］パネルに追加します。

［カタログ製品］パネルに、カタログ製品の購入数量が表示されます。これは、購入したカタログ製品の単位数です (購買記録に従う)。ライセンス数量も表示され、これは購入した単位に含まれるライセンスの合計数です。

6 コンプライアンスの監視に関する情報については、次のセクション、「コンプライアンスデータの表示」に進みます。

コンプライアンスデータの表示

ライセンス製品のコンプライアンスステータスの確認に使用できるビューは 2 つあります。［ライセンスされた製品］ページを表示して、すべての製品のコンプライアンスステータスの概要を把握したり、ソフトウェアコンプライアンスレポートを生成してさらに詳細な情報を確認したりすることができます。

- 71 ページの 「コンプライアンスステータスの概要を確認する」
- 71 ページの 「ソフトウェアコンプライアンスレポートを生成する」

コンプライアンスステータスの概要を確認する

1 ZENworks コントロールセンターで、［アセット管理］タブをクリックし、次に［ライセンス管理］タブをクリックします。

2 ［ライセンス管理］パネルで、［ライセンスされた製品］をクリックし、［ライセンスされた製品］ページを表示します。

［ライセンスされた製品］リストには、すべてのライセンス製品と現在のコンプライアンスステータスが示されます。

- ソフトウェア製品は正しくライセンスされています。購入ライセンスの数はインストール数と同じです。
- このソフトウェア製品は必要以上のライセンスが取得されています。購入ライセンス数はインストール済みの数よりも多いです。
- このソフトウェア製品はライセンス数が不足しています。購入ライセンス数はインストール済みの数よりも少ないです。

ソフトウェアコンプライアンスレポートを生成する

1 ZENworks コントロールセンターで、［アセット管理］タブをクリックし、次に［ライセンス管理］タブをクリックします。

2 ［ライセンス管理］パネルで、［ライセンス管理レポート］をクリックします。

3 ［ライセンス管理の標準レポート］パネルで、［ソフトウェアコンプライアンス］をクリックします。

4 このパネルで、［コンプライアンスレポート］をクリックします。

ライセンス別のコンプライアンスデータが示されているレポートが表示されます。データはコンプライアンスステータス、製造元と値、または人口統計の条件別にフィルタできます。特定のライセンス製品のコンプライアンスの詳細を確認するには、［ライセンス数量］を展開します。その他のレポートの情報については、『*ZENworks Asset Management リファレンス*』を参照してください。

詳細の参照場所

前のセクションで説明したシナリオでは、ZENworks Asset Management で使用できるライセンスコンプライアンス機能のほんの一部を紹介しました。詳細については、『*ZENworks Asset Management リファレンス*』の「ライセンスコンプライアンス」を参照してください。

ライセンスの割り当て

ZENworks Asset Management では、組織内でライセンスを割り当てて、ライセンスの所有権と配布を追跡できます。ライセンスはデバイス単位または人口統計単位 (サイト、部署、コストセンター) に割り当てられます。

*デバイス割り当て*は、ライセンスを特定のデバイスに割り当てます。そのデバイスには、製品がインストールされていても、インストールされていなくても構いません。たとえば、製品 A の 10 ライセンスを購入したとします。これらのライセンスは、デバイスにインストールする前でも、ターゲットデバイスに割り当てることができます。

*統計割り当て*は、1 つまたは複数のライセンスをサイト、部署、またはコストセンターに割り当てることです。統計を割り当てられ、製品がインストールされたデバイスは、その割り当てに関連付けられたインストールとして表示されます。たとえば、製品 A の 15 ライセンスを購入し、それを部署 Q に割り当てたとします。部署 Q に割り当てられているデバイスは 20 台です。20 台のデバイスうち、12 台のデバイスで製品 A がインストールされました。このため、DepartmentQ の割り当てとして、15 本のライセンスが割り当てられ、12 本がインストールされています。

次の手順では、ライセンスをデバイスに割り当てる方法を説明します。ライセンスを人口統計に割り当てる方法については、『*ZENworks Asset Management リファレンス*』の「ライセンスの割り当て」を参照してください。

1 ZENworks コントロールセンターで、［アセット管理］タブをクリックします。

2 ［ライセンス管理］ページで、［ライセンスされた製品］をクリックします。

3 ［ライセンスされた製品］リストで、ライセンスを割り当てるライセンス製品をクリックします。

4 デフォルトでは、デバイス割り当てだけが製品ライセンスの所有権を追跡できます。ライセンスを人口統計に割り当てるには、ユーザは次の手順を実行して、製品の人口統計割り当てを有効化する必要があります。

4a ［全般］タブをクリックします。

4b ［ライセンス割り当ての設定］パネルで、次のフィールドに入力します。

統計割り当ての有効化 : このオプションを選択します。

統計割り当てタイプ : シングルライセンス製品に関するすべての統計割り当ては、同じタイプでなければなりません。この製品に使用したいタイプを選択します (［サイト］、［部署］、［コストセンター］)。

今後の購買記録のインポートによって、統計データのライセンス割り当てを更新します :

製品の今後の購買記録のインポート時に、購買記録の統計データに基づいて、割り当てられたライセンス数量を自動的に更新する場合は、このオプションを選択します。

たとえば、製品が部署割り当てを使用するとします。部署 Q に割り当てられたライセンスを含む購買記録をインポートします。それらのライセンスが部署 Q の統計割り当てとして追加されます。

必要な場合は、新規割り当ての作成も行われます。たとえば、購買記録に、部署 Z(製品 A の割り当てリストにない新しい部署) に割り当てられた製品 A のライセンスが含まれている場合は、部署 Z の新規割り当てが作成されます。

割り当てられた数量 : デバイスまたは人口統計のどちらかに割り当てられたライセンスの総数を表示します。

4c ［適用］をクリックして変更内容を保存します。

5 ［ライセンス割り当て］タブをクリックします。

6 (オプション) 製品はインストールされていますが、割り当てられたライセンスのないデバイスを表示するには、［デバイス割り当て］パネルで、［割り当てられていないインストール数］の数字をクリックします。

7 ライセンスの割り当て先デバイスに製品がインストールされている場合は、［追加］> ［Devices with Product Installed (製品がインストールされているデバイス)］の順にクリックします。

または

ライセンスの割り当て先デバイスに製品がインストールされていない場合は、［追加］> ［任意のデバイス］の順にクリックします。

［デバイスの検索］ダイアログボックスが表示されます。

8 ［デバイスタイプ］フィールドで、［管理対象デバイス］、［インベントリ済みデバイス］、［Managed or Inventoried Devices (管理対象またはインベントリ済みデバイス)］、［ZAM マイグレートデバイス］、［すべて］のいずれを検索するか選択します。

デバイスタイプが不明な場合は、［すべて］を選択します。

9 検索を制限するには、フィルタを使用して、検索条件を作成します。

フィルタを作成しない場合は、すべてのデバイス (または製品がインストールされているすべてのデバイス) が、最大表示数まで表示されます。

10 検索で表示するデバイスの最大数を指定します。

11 検索結果のダイアログボックスに表示するカラムを選択します。複数のフィールドを選択する場合は、<Ctrl> キーを使用します。

12 ［検索］をクリックすると、検索結果が一覧表示された［デバイスの選択］ダイアログボックスが表示されます。

13 ライセンスを割り当てたいデバイスを選択して、［OK］をクリックします。

割り当てに関する次の情報が表示されます。

- **マシン名、ログイン名、IP アドレス :** デバイスの標準情報 (デバイスのインベントリ取得時にログインしていたユーザのログイン名など)。
- **サイト、部署、コストセンター :** デバイスの統計データ 1 つまたは複数のフィールドが空の場合、その情報はデバイスのインベントリデータに含まれていません。
- **インストール済み数量 :** デバイス上のライセンス製品のインストール数。通常は、1 になります。

- **重複した割り当て**：デバイスのインストールが統計割り当てにも含まれている場合は、チェックマークが付きます。
- **割り当てられていないインストール数**：統計割り当てまたはデバイス割り当てによりライセンスを割り当てられていないインストールの数を表示します。この数字をクリックすると、インストールのリストが表示されます。

9 環境設定の管理

次のセクションでは、ZENworks Configuration Management を使用する実行可能なタスクについて説明します。使用を計画している環境と機能によって、すべてのタスクを実行する方法を知っておくことが必要になる場合があります。学習対象は、任意の順序でレビューできます。

環境設定の管理の有効化

管理ゾーンのインストール時に、ライセンスキーを入力するか、評価をオンにして Configuration Management を起動しなかった場合は、次の手順を実行してください。

1. ZENworks コントロールセンターで、［環境設定］をクリックします。
2. ［ライセンス］パネルで、［ZENworks 2017 Configuration Management］をクリックします。
3. ［製品の評価 / アクティブ化］を選択して、以下のフィールドに入力します。

   使用評価 : このオプションを選択すると、60 日の評価期間が有効になります。60 日の評価期間終了後に製品を継続的に使用するには、製品ライセンスキーを申請しなければなりません。

   製品ライセンスキー : Configuration Management 用に購入したライセンスキーを指定します。製品ライセンスを購入するには、Novell ZENworks Configuration Management 製品サイト (http://www.novell.com/products/zenworks/configurationmanagement) を参照してください。
4. ［OK］をクリックします。

ZENworks Agent での Configuration Management の有効化

ZENworks Agent がデバイス上で環境設定の管理を実行するには、適切なエージェント機能が有効になっている必要があります。これらの機能 (バンドル管理、イメージ管理、ポリシー管理、リモート管理、およびユーザ管理) は、ZENworks Configuration Management (フルライセンスまたは評価版) が有効化される場合、デフォルトで有効になっています。

機能が有効になっていることを確認する必要があります。または、特定の機能を使用したくない場合は、それらの機能を無効化できます。方法については、37 ページの 「ZENworks Agent 機能の設定」を参照してください。

ソフトウェアの配布

ZENworks Configuration Management はソフトウェアの配布に高い柔軟性を提供します。アプリケーションおよび個別ファイルの配布、デバイス上の既存のファイルへの単なる変更、デバイス上のアプリケーションのインストール、削除、およびロールバックを行うことができます。

ソフトウェアはバンドルを使用して配布されます。バンドルは、すべてのファイル、構成設定、インストール指示などから構成され、デバイス上のアプリケーションまたはファイルを展開および管理する必要があります。バンドルをデバイスに割り当てるとき、定義したスケジュール (配布、起動、および可用性) に従って、バンドルをデバイスにインストールして、実行することができます。

作成できるバンドルには 4 つのタイプがあります。

- **iOS バンドル :** iOS デバイス上でアプリケーションを設定および管理できます。
- **Linux バンドル :** Linux デバイス上でアプリケーションを設定および管理できます。
- **Linux 依存バンドル :** ソフトウェアパッケージを Linux デバイスで利用できるようにして、パッケージ依存性を解決します。
- **Macintosh バンドル :** Macintosh デバイス上でアプリケーションを設定および管理できます。
- **「プレブート」バンドル :** オペレーティングシステムがデバイスで起動する前に、管理対象および管理対象外デバイス上で一連のタスクを実行できます。
- **Windows バンドル :** Windows デバイスでアプリケーションを設定および管理できます。

ZENworks が各 Google サーバおよび Apple サーバと同期を取るとすぐに、Android バンドル (企業の Android 関連の仕事用アプリ) および Apple VPP バンドルが自動的に作成されます。ただし、追加の Android バンドルまたは Apple VPP バンドルを作成できます。詳細については、「Integrating ZENworks with Android Enterprise」を参照してください。

バンドルに含まれているソフトウェアは、ZENworks サーバリポジトリにアップロードされます。これにより、ZENworks サーバが、他のネットワーク場所にアクセスする必要なくソフトウェアを配布することができます。

Windows、Linux、および Macintosh デバイスへのソフトウェアの配布について説明した次のビデオをご覧ください。

- ZENworks による Windows ソフトウェアの展開
- ZENworks による Linux ソフトウェアの展開
- ZENworks による Mac の管理 : エージェントの展開
- ZENworks による Mac の管理 : 標準化されたアプリケーション展開

バンドルの作成

ソフトウェアバンドルを作成するには、新しいバンドルの作成ウィザードを使用します。バンドルの作成の手助けに加えて、ウィザードでは、デバイスおよびユーザへの割り当てと配布、起動および可用性スケジュールの作成を行うことができます。

1 ZENworks コントロールセンターで、［バンドル］タブをクリックします。

2 ［バンドル］パネルで、［新規作成］>［バンドル］の順にクリックして新しいバンドルの作成ウィザードを起動します。

3 プロンプトに従ってバンドルを作成します。

ウィザードの各ページで［ヘルプ］ボタンをクリックすると、そのページの詳細情報が表示されます。

ウィザードを完了すると、バンドルが［バンドル］パネルに追加されます。バンドルをクリックすると、バンドルの詳細の表示および変更を行うことができます。

4 次のセクションの「バンドルの追加」に進みます。

zman ユーティリティで bundle-create コマンドを使用してソフトウェアバンドルを作成することもできます。詳細については、『*ZENworks コマンドラインユーティリティリファレンス*』の「バンドルコマンド」を参照してください。

バンドルの追加

バンドルの作成後、インストールしたいデバイスに割り当てる必要があります。デバイスまたはユーザに対して割り当てることができます。

1 ［バンドル］パネルで、割り当てたいバンドルの横のチェックボックスをオンにして選択します。

2 ［アクション］>［デバイスへの割り当て］の順にクリックします。

または

［アクション］>［ユーザへの割り当て］の順にクリックします。

3 プロンプトに従ってバンドルを割り当てます。

ウィザードの各ページで［ヘルプ］ボタンをクリックすると、そのページの詳細情報が表示されます。

ウィザードを完了すると、割り当てられたデバイスやユーザがバンドルの［関係］ページに追加されます。バンドルをクリックすると割り当てが表示されます。

zman ユーティリティで bundle-assign コマンドを使用してバンドルを割り当てることもできます。詳細については、『*ZENworks コマンドラインユーティリティリファレンス*』の「バンドルコマンド」を参照してください。

詳細の参照場所

ソフトウェアの配布の詳細については、『*ZENworks Software Distribution リファレンス*』を参照してください。

アプリのモバイルデバイスへの配布の詳細については、『*ZENworks 2017 Mobile Management Reference*』を参照してください。

ポリシーの適用

ZENworks Configuration Management では、ポリシーを使用して任意の数の管理対象デバイスに割り当てることのできる一連の環境設定を作成することができます。これによって、デバイスに一貫した環境設定が与えられ、各デバイスを個別に設定する必要がなくなります。

ZENworks Configuration Management ポリシーを使用すると、外部サービス、パペットポリシー関連の設定、Internet Explorer のお気に入り、Windows グループポリシー、ローカルファイル権利、A/C 電源管理設定、プリンタ、SNMP サービス設定、ローミングプロフィールを管理し、ダイナミックローカルユーザアカウントを設定し、管理されたデバイス上で管理できるようになります。また、管理対象デバイスのリモート管理セッションの動作または実行を設定したり、ZENworks Explorer の動作および機能を制御したり、集中管理したりすることもできます。

次のセクションに、ユーザまたは管理対象デバイスに作成および割り当て可能な Windows 環境設定ポリシーのリストを記載しています。

- **ブラウザブックマークポリシー :** Windows デバイスおよびユーザに対して Internet Explorer のお気に入りを設定します。
- **ダイナミックローカルユーザポリシー :** Windows XP、Windows Vista、Windows 7 ワークステーション、および Windows 2003、Windows 2008、Windows 2008 R2 ターミナルサーバで作成されたユーザを、ユーザが Novell eDirectory に正常に認証された後に設定します。
- **ローカルファイル権利ポリシー :** NTFS ファイルシステムにあるファイルまたはフォルダの権利を設定します。

  このポリシーは、ローカルとドメインのユーザおよびグループに対する基本的な許可および詳細な許可を設定するために使用できます。これにより、管理者が管理対象デバイスにカスタムグループを作成することができます。
- **電源管理ポリシー :** 管理対象デバイスで電源管理設定を行います。

  電源管理ポリシーの設定方法を説明したビデオをご覧ください。
- **プリンタポリシー :** Windows デバイスおよびユーザのローカル、SMB、HTTP、TCP/IP、CUPS、および iPrint プリンタを設定します。
- **リモート管理ポリシー :** 管理対象デバイスのリモート管理セッションの動作または実行を設定します。ポリシーには、リモート管理操作、セキュリティなどのプロパティが含まれます。リモート管理ポリシーは、ユーザと管理対象デバイスに割り当てることができます。
- **ローミングプロファイルポリシー :** ユーザが自分のプロファイルを保存するパスを設定できます。

  ユーザプロファイルには、セッション間で維持されるユーザのデスクトップ設定、および個人の環境設定に関する情報が含まれます。

ネットワークパスに保存されているユーザプロファイルは、ローミングプロファイルと呼びます。ユーザがマシンにログオンするたびに、ユーザのプロファイルがネットワークパスからロードされます。これにより、ユーザはマシンを移動しても、常に自分の設定を使用することができます。

- **SNMP ポリシー :** 管理対象デバイスに SNMP パラメータを設定します。
- **Windows グループポリシー :** グループポリシーを Windows デバイスおよびユーザ向けに設定します。
- **ZENworks Explorer の環境設定ポリシー :** ZENworks Explorer の動作および機能を集中管理できるようにします。

次のセクションに、ユーザまたは管理対象デバイスに作成および割り当て可能な Linux 環境設定ポリシーのリストを記載しています。

- **外部サービスポリシー :** Linux 管理対象デバイスで、YUM、ZYPP、または MOUNT のリポジトリ向けに外部サービスを設定します。これにより、管理者が管理対象デバイス上で、これらのリポジトリからソフトウェアパッケージまたは更新ファイルをダウンロードしてインストールすることができます。
- **パペットポリシー :** 管理対象デバイスでのパペットマニフェストやモジュールの実行方法を指定したり、スクリプトファイルをアップロードしたり、デバイス上でスクリプトのドライ実行を行うかどうかを指定します。

次のセクションに、ゾーンに登録されたモバイルデバイスに適用されるポリシーの一覧を示します。

- **モバイルデバイス制御ポリシー :** モバイルデバイスのさまざまな機能へのユーザアクセスを許可または制限できます。
- **モバイル電子メールポリシー :** モバイルデバイスにある企業用電子メールアカウントを管理できます。
- **モバイル登録ポリシー :** モバイルデバイスを登録できるユーザ、ユーザが登録できるモバイルデバイス、モバイルデバイスの登録に使用するモード、およびデバイスの場所と名前付けを強制できます。
- **モバイルセキュリティポリシー :** デバイスのパスワード制限の設定、暗号化の設定、およびアイドル時間の設定を行います。
- **モバイルコンプライアンスポリシー :** デバイスに適用されたルールにデバイスが適合するようになります。
- **Android エンタープライズ登録ポリシー :** ユーザは Android エンタープライズプログラムの一環として仕事用プロファイルモードまたは仕事用管理デバイスモードで自分の Android デバイスを登録できるようになります。
- **iOS Intune アプリ保護ポリシー :** アプリでの切り取り、コピー、および貼り付けアクションの制限や Intune アプリにアクセスするための PIN の使用の適用など、Microsoft Intune アプリでの制限を適用します。

ポリシーの作成

ポリシーを作成するには、新規ポリシーの作成ウィザードを使用します。ポリシーの作成の手助けに加えて、ウィザードでは、デバイスおよびユーザへの割り当てと、ポリシーを直ちに実施するかまたはデバイスが情報を更新するまで待機するかどうかの決定を行うことができます。

1 ZENworks コントロールセンターで、［ポリシー］タブをクリックします。

2 ［ポリシー］パネルで、［新規］>［ポリシー］の順にクリックして、［Select Platform(プラットフォームの選択)］ページを表示します。

3 ポリシーのカテゴリを選択し、［次へ］をクリックして、［ポリシーカテゴリの選択］ページを表示します。

4 作成するポリシーのカテゴリを選択して、［次へ］をクリックします。

5 提供されているポリシーのリストからポリシーの種類を選択してください。画面のプロンプトに従ってポリシーを作成します。

ウィザードの各ページで［ヘルプ］ボタンをクリックすると、そのページの詳細情報が表示されます。

ウィザードを完了すると、ポリシーが［ポリシー］パネルに追加されます。ポリシーをクリックしてポリシーの詳細を表示し、割り当てを修正できます。

zman ユーティリティで policy-create コマンドを使用してポリシーを作成することもできます。詳細については、『*ZENworks コマンドラインユーティリティリファレンス*』の「ポリシーコマンド」を参照してください。

ポリシーの割り当て

ポリシーの作成後、適用したいデバイスに割り当てる必要があります。デバイスまたはユーザに対して割り当てることができます。

1 ［ポリシー］パネルで、割り当てたいポリシーの横のチェックボックスをオンにして選択します。

2 ［アクション］>［デバイスへの割り当て］の順にクリックします。

または

［アクション］>［ユーザへの割り当て］の順にクリックします。

3 プロンプトに従ってポリシーを割り当てます。

ウィザードの各ページで［ヘルプ］ボタンをクリックすると、そのページの詳細情報が表示されます。

ウィザードを完了すると、割り当てられたデバイスやユーザがポリシーの［関係］ページに追加されます。ポリシーをクリックするとポリシーの割り当てが表示されます。

zman ユーティリティで policy-assign コマンドを使用してポリシーを割り当てることもできます。詳細については、『*ZENworks コマンドラインユーティリティリファレンス*』の「ポリシーコマンド」を参照してください。

詳細の参照場所

ポリシーの適用の詳細については、『*ZENworks Configuration Policies リファレンス*』を参照してください。

モバイルデバイスへのポリシーの適用の詳細については、『*ZENworks 2017 Mobile Management Reference*』を参照してください。

イメージングデバイス

ZENworks Configuration Management には、オペレーティングシステムが起動される前に、デバイスでタスクを実行できるプレブートサービスが含まれています。Preboot Services を使用して、起動時に自動または手動で次の操作をデバイスに対して実行できます。

- バッシュプロンプトで発行できるコマンドを含む ZENworks イメージングスクリプトを実行する
- デバイスのハードドライブおよびその他のストレージデバイスのイメージを取得する
- イメージをデバイスに復元する
- 既存のイメージが複数のデバイスに適用されるセッションに参加する (マルチキャストにより)
- ImageX を使用して、WIM イメージを取得または復元する
- Symantec GHOST を使用して、GHOST イメージを取得または復元する

これらのタスクのいくつかを自動的に実行するには、単に PXE (Preboot Execution Environment) をデバイスで有効にするだけです。その後でプレブート可能なタスクを ZENworks コントロールセンターで設定し、デバイスに割り当てます。これにより、デバイスが起動する際にこれらのタスクを自動的に実装できます。

タスクを手動で実装するには、起動中にユーザによる介入が必要であるようにデバイスを設定できます。

ZENworks コントロールセンターを使用して、tftp ディレクトリ変更をプライマリサーバから他のイメージングサーバ (イメージング役割を持つ、プライマリサーバまたはサテライトデバイス) に複製することもできます。

- 81 ページの 「Preboot Services の設定」
- 84 ページの 「イメージの取得」
- 86 ページの 「イメージの適用」
- 89 ページの 「詳細の参照場所」

Preboot Services の設定

Preboot Services を使用するには、次のセクションのタスクを完了する必要があります。

- 81 ページの 「デバイスでの PXE の有効化」
- 82 ページの 「イメージングサーバの設定」
- 82 ページの 「サードパーティのイメージング設定の設定」
- 84 ページの 「サードパーティ NTFS ドライバ設定の構成」

デバイスでの PXE の有効化

Preboot Services では、イメージを取得または適用するすべての管理対象デバイスで PXE (Preboot Execution Environment) を有効化しておく必要があります。

PXE がデバイスで有効になっているかどうかを確認するには、デバイスを再起動して、ブートオプション (大部分のデバイスでは <F12> キー) を選択します。ネットワークのブートオプションが表示されている場合は PXE が有効になっています。

デバイスで PXE が有効になっていない場合は、デバイスの BIOS を編集して PXE を有効にします。デバイスが起動するたびに PXE 環境を確実に使用できるようにするには、ブート順を変更して、NIC (Network Interface Card) オプションが他のブートオプションより前に表示されるようにします。

イメージングサーバの設定

イメージングサーバとは、デバイスの PXE エンジンが接続する PXE サーバです。ZENworks サーバをイメージングサーバとして機能させるには、ZENworks サーバで Novell Proxy DHCP Service を起動させるだけです。サービスを開始するときには、スタートアップタイプを手動から自動に変更して、サーバが再起動したときに必ず開始するように設定する必要があります。

サードパーティのイメージング設定の設定

サードパーティのイメージングソリューションを使用する場合は、ZENworks コントロールセンターでサードパーティのイメージング設定を行う必要があります。ZENworks は、次のサードパーティのイメージングツールをサポートします。

- WIM イメージファイル形式および配布に WINPE を使用する Microsoft ImageX
- GHOST イメージファイル形式および WINPE を配布に使用する Symantec GHOST

ZENworks のサードパーティのイメージングでは、ブート方式に PXE のみをサポートします。

サードパーティのイメージングを設定するには、次の手順に従います。

1 イメージングサーバに ZENworks Configuration Management をインストールします。

ZENworks のインストール方法の詳細については、「Windows での ZENworks プライマリサーバのインストール」(『*ZENworks 2017 サーバインストールガイド*』) を参照してください。

2 ZENworks コントロールセンターでのサードパーティのイメージングの設定 .

2a ZENworks コントロールセンターを実行しているデバイスに、Microsoft Windows 自動インストールキット (WAIK) または Windows アセスメント & デプロイメントキット (WADK) がインストールされていることを確認します。

2b ZENworks コントロールセンターで、**［環境設定］**タブをクリックします。

2c **［管理ゾーンの設定］**パネルで、**［デバイス管理］** > **［起動前サービス］** > **［サードパーティのイメージング設定］**パネルの順にクリックします。

2d **［32 ビットアップロード設定］**の場合 :

WinPE ベースのディストリビューションのアップロード (Windows AIK / Windows ADK が必要): アイコンをクリックして、WIM イメージングファイルをアップロードします。［WIM イメージングファイルのアップロード］ダイアログボックスで、次の手順を行います。

1. 32 ビットの winpe.wim ファイルをアップロードするには、次の手順に従います。

WAIK から実行する場合 : インストール先ディレクトリで Windows AIK\Tools\PETools\x86 フォルダを参照して winpe.wim ファイルを選択します。

WADK から実行する場合 : インストール先ディレクトリで Windows Kits\<*version*>\Assessment and Deployment Kit\Windows Preinstallation Environment\x86\en-us フォルダを参照して winpe.wim ファイルを選択します。

<*version*> は、Windows オペレーティングシステムのバージョンです。

注 : winpe.wim ファイルを再アップロードすると、このファイルの以前のインスタンスがサーバから上書きされます。

2. ［OK］をクリックします。

   これにより、ZENworks コントロールセンターにアクセスするデバイスにサーバからイメージングファイルがダウンロードされ、イメージングファイルを使用して winpe.wim が再構築された後、デバイスからサーバにファイルがアップロードされます。ファイルのダウンロードおよびアップロードの進捗が［ステータス］フィールドに表示されます。

WIM イメージング (ImageX.exe) をサポートするためにイメージ X ファイルをアップロード :

1. アイコンをクリックして、ZENworks コントロールセンターにアクセスできるデバイス上で Microsoft イメージングエンジン (imagex.exe) を参照して選択します。
2. サードパーティのイメージング設定を設定した後、［適用］をクリックします。
3. 管理ゾーン内のすべてのプライマリサーバとイメージング役割を持つサテライトでのコンテンツの複製ステータスを表示するには、［ステータス］をクリックします。ステータスが［使用可能］である場合にのみ、イメージング操作を開始するようにします。

注 : 32 ビットと 64 ビットの両方のイメージ X ファイルをアップロードする場合、異なるインスタンスでアップロードするようにしてください。

Ghost イメージング (Ghost32.exe) をサポートするために Ghost 11.5 以降のファイルをアップロード :

1. アイコンをクリックして、ZENworks コントロールセンターにアクセスできるデバイス上で Symantec GHOST エンジン (ghost32.exe) を参照して選択します。
2. サードパーティのイメージング設定を設定した後、［適用］をクリックします。
3. 管理ゾーン内のすべてのプライマリサーバとイメージング役割を持つサテライトでのコンテンツの複製ステータスを表示するには、［ステータス］をクリックします。ステータスが［使用可能］である場合にのみ、イメージング操作を開始するようにします。

2e ［64 ビットアップロード設定］の場合 :

WinPE ベースのディストリビューションのアップロード (Windows AIK / Windows ADK が必要): アイコンをクリックして、WIM イメージングファイルをアップロードします。［WIM イメージングファイルのアップロード］ダイアログボックスで、次の手順を行います。

1. 64 ビットの winpe.wim ファイルを WADK からアップロードするには、インストール先ディレクトリで Windows Kits\<*version*>\Assessment and Deployment Kit\Windows Preinstallation environment\amd64\en-us フォルダを参照して winpe.wim ファイルを選択します。

   <*version*> は、Windows オペレーティングシステムのバージョンです。

2. ［OK］をクリックします。

   これにより、ZENworks コントロールセンターにアクセスするデバイスにサーバからイメージングファイルがダウンロードされ、イメージングファイルを使用して winpe.wim が再構築された後、デバイスからサーバにファイルがアップロードされます。ファイルのダウンロードおよびアップロードの進捗が［ステータス］フィールドに表示されます。

WIM イメージング (ImageX.exe) をサポートするためにイメージ X ファイルをアップロード :

1. アイコンをクリックして、ZENworks コントロールセンターにアクセスできるデバイス上で Microsoft イメージングエンジン (imagex.exe) を参照して選択します。
2. サードパーティのイメージング設定を設定した後、［適用］をクリックします。
3. 管理ゾーン内のすべてのプライマリサーバとイメージング役割を持つサテライトでのコンテンツの複製ステータスを表示するには、［ステータス］をクリックします。ステータスが［使用可能］である場合にのみ、イメージング操作を開始するようにします。

注 : 32 ビットと 64 ビットの両方のイメージ X ファイルをアップロードする場合、異なるインスタンスでアップロードするようにしてください。

Ghost イメージング (Ghost64.exe) をサポートするために Ghost 11.5 以降のファイルをアップロード :

1. アイコンをクリックして、ZENworks コントロールセンターにアクセスできるデバイス上で Symantec GHOST エンジン (ghost64.exe) を参照して選択します。
2. サードパーティのイメージング設定を設定した後、［適用］をクリックします。
3. 管理ゾーン内のすべてのプライマリサーバとイメージング役割を持つサテライトでのコンテンツの複製ステータスを表示するには、［ステータス］をクリックします。ステータスが［使用可能］である場合にのみ、イメージング操作を開始するようにします。

3 デバイスの PXE を有効にします。

4 イメージングサーバまたは別のネットワークサーバに標準の DHCP サーバが配置してあることを確認してください。

サードパーティ NTFS ドライバ設定の構成

最新の高性能 NTFS ドライバをダウンロードしてシステムに保存することができます。管理ゾーンに含まれるすべてのプライマリサーバにおけるコンテンツの複製ステータスを表示できます。ステータスが［使用可能］である場合、サードパーティ NTFS ドライバを使用してイメージング操作を開始できます。

これらの設定を行うには、左側のペインで［環境設定］をクリックして、［環境設定］タブを表示します。このタブが展開されない場合は、［管理ゾーンの設定］をクリックし、［デバイス管理］>［起動前サービス］の順にクリックして、［起動前サービス］ページを表示します。

イメージの取得

デバイス上で ZENworks イメージを取得および復元するには ZENworks イメージングを使用し、サードパーティのイメージを取得および復元するには ZENworks サードパーティイメージングユーティリティを使用します。このユーティリティでは、Windows イメージングフォーマット (WIM) または Ghost イメージングフォーマットを使用して、ローカルデバイスまたはサーバ上でイメージの取得および復元を行うことができます。

1 ZENworks コントロールセンターで、［デバイス］タブをクリックします。

2 イメージを取得したいデバイスが見つかるまで Servers または Workstations フォルダを移動します。

3 デバイスをクリックして詳細を表示します。

4 左ナビゲーションパネルにあるタスクリストで、［イメージの取得］をクリックして、イメージの取得ウィザードを起動します。

5 ［ファイル情報］ページで、次のフィールドに入力し、［次へ］をクリックします。

ZENworks イメージングでは、次を指定します。

イメージ形式 : デバイス用に取得されるイメージの形式を選択します。

サーバおよびファイルパス : アイコンをクリックして、［サーバとパス情報］ダイアログボックスを表示します。次のオプションを設定します。

- **サーバオブジェクト /IP/DNS:** アイコンをクリックして、イメージングサーバの役割に昇格するオブジェクト、IP アドレス、またはプライマリサーバまたはデバイスの DNS 名を参照して選択します。
- **サーバ上のファイルパス :** アイコンをクリックして、イメージファイルを参照して選択します。イメージファイルには、.zmg という、有効な ZENworks のイメージファイルであることを示す拡張子が含まれる必要があります。

注 : Linux 用に DHCP を使用する複数の検索ドメインが設定されており、サーバが Windows で動作している場合は、指定したファイルシステムを参照できません。

サードパーティイメージングでは、次を指定します。

イメージファイル用の共有ネットワークパス : 共有ネットワークパスを指定します。wim または .gho ファイルを保存する共有ネットワークパスを指定します。ディレクトリは、Windows 共有または Linux SMB または CIFS 共有にしてください。

Novell File Upload 拡張機能をこのデバイスにインストールしていない場合は、インストールするディレクトリを参照してアップロードする前にインストールする必要があります。

イメージファイル名 : 次のファイルを保存するファイル名を指定します .wim または .gho ファイルを保存するファイル名を指定します。このオプションは、Windows イメージングフォーマットでのみ表示されます (.wim) および Ghost イメージングフォーマット (.gho)。

ネットワーク資格情報 : をクリックして、.wim ファイルを持つデバイスにアクセスするために使用されるネットワーク資格情報を参照して選択します。このオプションは、Windows イメージフォーマット (.wim) および GHOST イメージ形式 (.gho) でのみ表示されます。

圧縮の使用 : 圧縮が必要です。次のうちのいずれかを選択してください :

- **バランス :** 再イメージングのスピードの平均とイメージファイルが利用できるディスク領域の間で自動的に圧縮をバランスします。このオプションは、ZENworks イメージ形式でのみ表示されます
- **なし :** このオプションは、Windows イメージ形式および GHOST イメージ形式にのみ表示されます。
- **スピード重視 :** 再イメージング時間が最短になるように圧縮を最適化します。CPU 速度が問題になる場合は、このオプションを使用します。
- **容量重視 :** ディスク領域を節約するようにイメージファイルのサイズを最小化するように圧縮を最適化します。このオプションを選択すると、再イメージング処理が長くなる可能性があります。

［バランス］は ZENworks イメージ形式のデフォルトオプションです。そして［スピード重視］は Windows イメージ形式と GHOST イメージ形式のデフォルトオプションです。

イメージバンドルの作成 : このフィールドは選択解除したままにしてください。

6 ［イメージファイルサマリ］ページの情報を確認し、［終了］をクリックし、次に［OK］をクリックします。

イメージングタスクは Preboot Services によって完了されるため、デバイスのイメージはデバイスが次に再起動されたときに取得されます。［イメージングワーク］パネルはデバイスの［サマリ］ページにあり、ワークがスケジュールされていることを示します。ワークが完了すると、このパネルからタスクが削除されます。

7 デバイスを直ちに再起動してイメージングワークを開始するには、左ナビゲーションパネルの［ワークステーションの再起動 / シャットダウン］(または［サーバの再起動 / シャットダウン］) をクリックします。

イメージの取得に必要な時間は、デバイスのドライブのサイズに依存します。

イメージの適用

イメージをデバイスに適用するには、新しいバンドルの作成 ウィザードを使用してイメージングバンドルを作成します。バンドルには適用したいイメージが含まれます。バンドルの作成の手助けに加えて、ウィザードでは、デバイスへの割り当てを行うことができます。イメージングバンドルを作成した後に、イメージングワークを開始します。

- 86 ページの 「ZENworks イメージバンドルの作成」
- 87 ページの 「サードパーティのイメージバンドルの作成」
- 88 ページの 「イメージングワークの開始」

Windows 7 イメージおよび Linux イメージのデバイスへの展開について説明した次のビデオをご覧ください。

- ZENworks による Windows 7 イメージの展開
- ZENworks による Linux の展開

ZENworks イメージバンドルの作成

ZENworks イメージをデバイスに復元するには、ZENworks イメージバンドルを作成する必要があります。

1 ZENworks コントロールセンターで、［バンドル］タブをクリックします。

2 ［バンドル］パネルで、［新規作成］ > ［バンドル］の順にクリックして新しいバンドルの作成 ウィザードを起動します。

3 ［バンドルタイプの選択］ページで、［プレブートバンドル］を選択し、［次へ］をクリックします。

4 ［バンドルカテゴリの選択］ページで、［ZENworks イメージ］を選択して、［次へ］をクリックします。

5 次の表からの情報を使用してフィールドに入力し、ウィザードを完了します。

［ウィザード］ページ	詳細
詳細の定義ページ	タスクの名前を指定します。名前には次の無効な文字を使用することはできません。/ \ * ? : " ' < > | ` % ~

[ウィザード] ページ	詳細
ZENworks イメージファイルの選択ページ	イメージファイルを選択するには、次の手順に従います。 1. をクリックして、[サーバとパス情報] ダイアログボックスを表示します。 2. 次のフィールドに入力します。 **デバイスオブジェクト、IP、または DNS:** イメージを保存した ZENworks サーバを選択します。 **サーバ上のファイルパス:** イメージファイルを参照して選択します。イメージファイルの標準保存ディレクトリは、\Novell\ZENworks\work\content-repo\images です。 3. [OK] をクリックします。
[サマリ] ページ	[次へ] をクリックしてウィザードを続行し、バンドルを目的のデバイスに割り当てます。
[バンドルグループ] ページ	イメージバンドルはグループに割り当てないでください。[次へ] をクリックしてこのページをスキップしてください。
[割り当ての追加] ページ	イメージを適用するデバイスを選択します。
[スケジュール] ページ	スケジュールをイメージバンドルに割り当てないでください。[次へ] をクリックしてこのページをスキップしてください。
[完了] ページ	[完了] をクリックして、バンドルを作成して選択したデバイスに割り当てます。

サードパーティのイメージバンドルの作成

サードパーティのイメージを復元するには、サードパーティのイメージバンドルを作成する必要があります。

1 ZENworks コントロールセンターで、[バンドル] タブをクリックします。

2 [バンドル] パネルで、[新規作成] > [バンドル] の順にクリックして新しいバンドルの作成ウィザードを起動します。

3 [バンドルタイプの選択] ページで、[プレブートバンドル] を選択し、[次へ] をクリックします。

4 [バンドルカテゴリの選択] ページで、[サードパーティのイメージ] を選択して、[次へ] をクリックします。

5 次の表からの情報を使用してフィールドに入力し、ウィザードを完了します。

[ウィザード] ページ	詳細
詳細の定義ページ	タスクの名前を指定します。名前には次の無効な文字を使用することはできません。/ \ * ? : " ' < > | ` % ~

[ウィザード] ページ	詳細
[サードパーティのイメージファイルの選択] ページ	サードパーティのイメージファイルを選択するには、次の手順に従います。 1. バンドルで使用されるイメージのタイプを選択します。 ZENworks Configuration Management では、Windows イメージ形式 (.wim) と GHOST イメージ形式 (.gho) のみを使用できます。 2. .wim または .gho ファイルを持つ共有ネットワークディレクトリを指定します。ディレクトリは、Windows 共有または Linux SMB または CIFS 共有にしてください。 3. をクリックして、.wim または .gho ファイルを持つデバイスにアクセスするために使用するネットワーク資格情報を参照して選択します。 4. WIM バンドルをアドオンイメージとして使用する場合は、**[WIM をアドオンとして復元]** を選択し、次のオプションを設定します。 **イメージ番号 (WIM のみ):** 復元するイメージのインデックス番号を選択します。 **アドオンイメージを復元するパス :** アドオンイメージを復元するデバイスのロケーションを指定します。 5. **[OK]** をクリックします。
[サマリ] ページ	**[次へ]** をクリックしてウィザードを続行し、バンドルを目的のデバイスに割り当てます。
[バンドルグループ] ページ	イメージバンドルはグループに割り当てないでください。**[次へ]** をクリックしてこのページをスキップしてください。
[割り当ての追加] ページ	イメージを適用するデバイスを選択します。
[スケジュール] ページ	スケジュールをイメージバンドルに割り当てないでください。**[次へ]** をクリックしてこのページをスキップしてください。
[完了] ページ	**[完了]** をクリックして、バンドルを作成して選択したデバイスに割り当てます。

イメージングワークの開始

1 ZENworks コントロールセンターで、**[デバイス]** タブをクリックします。

2 イメージを適用するデバイスが見つかるまで Servers または Workstations フォルダを移動します。

3 デバイスをクリックして詳細を表示します。

4 左ナビゲーションパネルにあるタスクリストで、**[割り当てられたイメージングバンドルの適用]** をクリックして、ワークをスケジュールします。

イメージングタスクは Preboot Services によって完了されるため、イメージはデバイスが次に再起動されたときにデバイスに適用されます。［イメージングワーク］パネルはデバイスの［サマリ］ページにあり、ワークがスケジュールされていることを示します。ワークが完了すると、このパネルからタスクが削除されます。

5 デバイスを直ちに再起動してイメージングワークを開始するには、左ナビゲーションパネルの**［ワークステーションの再起動 / シャットダウン］**(または **［サーバの再起動 / シャットダウン］**) をクリックします。

詳細の参照場所

イメージングおよび Preboot Services の詳細については、『*ZENworks Preboot Services およびイメージングリファレンス*』を参照してください。

デバイスのリモート管理

ZENworks Configuration Management は、デバイスをリモートで管理できるリモート管理機能を提供します。リモート管理では、次の操作をサポートします。

リモート操作	説明	追加の詳細
リモートコントロール	管理コンソールから管理対象デバイスをリモートコントロールできます。これにより、ユーザをサポートし、問題の解決を支援できます。ユーザがデバイスで実行できるすべての操作を実行できます。 Windows デバイスのリモートコントロールの詳細については、92 ページの 「Windows デバイスでのリモートコントロール、リモートビュー、およびリモート実行操作の実行」を参照してください。 Linux デバイスのリモートコントロールの詳細については、96 ページの 「Linux デバイスでのリモートコントロール、リモートビュー、およびリモートログイン操作の実行」を参照してください。	
リモートビュー	管理対象デバイスをコントロールするのではなく、管理対象デバイスに接続して管理対象デバイスを表示できるようにします。これは、ユーザに発生した問題を解決する際に役立ちます。 たとえば、管理対象デバイスのユーザが特定の操作を実行している様子を監視し、その実行方法が間違っていないかどうかを確認できます。 Window デバイスのリモート表示の詳細については、92 ページの 「Windows デバイスでのリモートコントロール、リモートビュー、およびリモート実行操作の実行」を参照してください。 Linux デバイスのリモート表示の詳細については、96 ページの 「Linux デバイスでのリモートコントロール、リモートビュー、およびリモートログイン操作の実行」を参照してください。	

リモート操作	説明	追加の詳細
リモート実行	管理コンソールから管理対象デバイスですべての実行可能ファイルを実行できます。リモートでアプリケーションを実行するには、［リモート実行］ダイアログボックスで実行名を指定します。アプリケーションが管理対象デバイス上のシステムパスにない場合は、アプリケーションの完全なパスを指定します。 たとえば、regedit コマンドを実行して、管理対象デバイスでレジストリエディタを開くことができます。［リモート実行］ダイアログボックスには、コマンド実行のステータスが表示されます。 Windows デバイスのリモート実行の詳細については、92 ページの 「Windows デバイスでのリモートコントロール、リモートビュー、およびリモート実行操作の実行」を参照してください。	この操作は、Windows 管理対象デバイスでのみサポートされています。
リモート診断	管理対象デバイス上の問題を診断し、分析できます。これにより、問題の解決に要する時間が短縮されると共に、問題の発生しているデバイスまで技術者が出向くことなく、問題を抱えているユーザを支援できるようになります。デスクトップを稼働させたまま診断を実行できるため、ユーザ側の生産性も向上します。 デバイスのリモート診断の詳細については、94 ページの 「リモート診断操作の実行」を参照してください。	この操作は、Windows 管理対象デバイスでのみサポートされています。
ファイル転送	管理コンソールと管理対象デバイス間でファイルを転送できます。 ファイル転送操作の詳細については、95 ページの「ファイル転送操作の実行」を参照してください。	この操作は、Windows 管理対象デバイスでのみサポートされています。
リモートログイン	管理コンソールから管理対象デバイスにログインし、管理対象デバイス上のユーザの操作なしで新しいグラフィカルセッションを開始できます。ただし、管理対象デバイス上のユーザには、リモートログインセッションを表示できません。 Linux デバイスのリモートログインの詳細については、96 ページの 「Linux デバイスでのリモートコントロール、リモートビュー、およびリモートログイン操作の実行」を参照してください。	この操作は、Linux 管理対象デバイスでのみサポートされています。 非 root ユーザの資格情報を使用してデバイスにログインする必要があります。
リモート SSH	リモート Linux デバイスに安全に接続でき、デバイス上で安全にコマンドを実行できます。 Linux デバイスのリモートログインの詳細については、97 ページの 「Linux デバイスでのリモート SSH 操作の実行」を参照してください。	この操作は、Linux 管理対象デバイスでのみサポートされています。

次のセクションでは、リモート管理の設定および各操作の実行方法について説明します。

- 91 ページの 「リモート管理ポリシーの作成」
- 92 ページの 「リモート管理設定」

- 92 ページの 「Windows デバイスでのリモートコントロール、リモートビュー、およびリモート実行操作の実行」
- 94 ページの 「リモート診断操作の実行」
- 95 ページの 「ファイル転送操作の実行」
- 96 ページの 「Linux デバイスでのリモートコントロール、リモートビュー、およびリモートログイン操作の実行」
- 97 ページの 「Linux デバイスでのリモート SSH 操作の実行」
- 97 ページの 「詳細の参照場所」


デバイスのリモート管理について説明したビデオをご覧ください。

リモート管理ポリシーの作成

デフォルトでは、セキュアなリモート管理ポリシーは、ZENworks Agent がリモート管理コンポーネントと共に展開されるときに、管理対象デバイスに作成されます。デフォルトポリシーを使用してデバイスをリモートで管理できます。デフォルトポリシーを使用すると、デバイスに対するすべてのリモート管理操作を実行できます。デフォルトポリシーを上書きするには、デバイスに明示的にリモート管理ポリシーを作成します。

リモート管理ポリシーは、デバイスまたはユーザに対して割り当てることができます。

リモート管理ポリシーを作成するには、次の手順に従います。

1 ZENworks コントロールセンターで、［ポリシー］タブをクリックします。

2 ［ポリシー］パネルで、［新規］>［ポリシー］の順にクリックして新規ポリシーの作成ウィザードを起動します。

3 ［Windows 環境設定ポリシー］を選択し、［次へ］をクリックします。

4 プロンプトに従ってリモート管理ポリシーを作成します。

ウィザードの各ページで［ヘルプ］ボタンをクリックすると、そのページの詳細情報が表示されます。ウィザードを完了すると、ポリシーが［ポリシー］パネルに追加されます。ポリシーをクリックすると、ポリシーの詳細の表示および割り当ての変更、スケジュールなどを行うことができます。

5 ユーザおよびデバイスへのリモート管理ポリシーの割り当て

5a ［ポリシー］パネルで、ポリシーの横のチェックボックスをオンにします。

5b ［アクション］>［デバイスへの割り当て］の順にクリックします。

または

［アクション］>［ユーザへの割り当て］の順にクリックします。

5c プロンプトに従ってポリシーを割り当てます。

ウィザードの各ページで［ヘルプ］ボタンをクリックすると、そのページの詳細情報が表示されます。

ウィザードを完了すると、割り当てられたデバイスやユーザがポリシーの［関係］ページに追加されます。ポリシーをクリックするとポリシーの割り当てが表示されます。

リモート管理設定

［設定］ページのリモート管理設定では、リモート管理ポート、セッションパフォーマンス、および使用可能な診断アプリケーションなどを指定できます。

設定は事前定義されており、最も一般的な設定が提供されています。設定を変更するには、次の手順を実行します。

1 ZENworks コントロールセンターで、［環境設定］タブをクリックします。

2 ［管理ゾーンの設定］パネルで、［デバイス管理］>［リモート管理］の順にクリックします。

3 必要に応じて、設定を変更します。

各ページで［ヘルプ］ボタンをクリックすると、そのページの詳細情報が表示されます。

4 設定の変更が終わったら、［適用］または［OK］をクリックして変更を保存します。

Windows デバイスでのリモートコントロール、リモートビュー、およびリモート実行操作の実行

1 ZENworks コントロールセンターで、［デバイス］タブをクリックします。

2 管理するデバイスが見つかるまで Servers または Workstations フォルダを移動します。

3 デバイスの前にあるチェックボックスをクリックしてデバイスを選択します。

4 左ナビゲーションパネルにあるタスクリストで、［リモートコントロールワークステーション］または［リモートコントロールサーバ］をクリックして、［リモート管理］ダイアログボックスを表示します。

5 ［リモート管理］ダイアログボックスで、次のフィールドに入力します。

デバイス : リモートで管理するデバイスの名前または IP アドレスを指定します。

Always default to IP address for all devices (すべてのデバイスについて常に IP アドレスを使用する): システムで DNS 名の代わりにデバイス IP アドレスを表示したい場合は、これを選択します。

［OK］をクリックすると、リモートコントロール操作の実行中にデバイスにアクセスするために指定した値がシステムに保存されます。以降のリモートコントロール操作時には、デバイスまたはリモートオペレータに応じて、これらの値の一部が自動的に選択されます。

説明 : 管理対象デバイスで実行するリモート操作のタイプ (［リモートコントロール］、［リモートビュー］、または［リモート実行］) を選択します。

認証 : 管理対象デバイスを認証するために使用するモードを選択します。オプションには次の 2 つがあります。

- **パスワード :** パスワードベース認証を提供して、リモートコントロール操作を実行します。ユーザが管理対象デバイスで設定したパスワードか、または管理者がリモート管理ポリシーのセキュリティ設定で設定したパスワードを正しく入力する必要があります。ユーザが設定したパスワードは、管理者が設定したパスワードより優先されます。
- **権利 :** このオプションは、リモート操作を実行する管理対象デバイスを選択した場合のみ使用できます。選択した管理対象デバイスで目的のリモート操作を実行するリモート管理権が管理者より割り当てられている場合、セッション開始時に自動的にアクセス権を取得します。

ポート : リモート管理エージェントがリスンするポート番号を指定します。デフォルトのポート番号は 5950 です。

セッションモード : 次のいずれかのセッションモードを選択します。

- **コラボレート :** コラボレーションモードでリモートコントロールセッションとリモート表示セッションを起動できます。ただし、管理対象デバイスで、最初にリモートビューセッションを起動することはできません。リモートコントロールセッションを管理対象デバイスで最初に起動した場合、次に示すマスタリモートオペレータのすべての権限が得られます。
  - 他のリモートオペレータにリモートセッションに参加するように呼びかける
  - リモートコントロール権をリモートオペレータに委任する
  - コントロールをリモートオペレータから再取得する
  - リモートセッションを終了する

  コラボレーションモードで管理対象デバイスのリモートコントロールセッションが確立すると、管理対象デバイスのその他のリモートセッションはリモートビューセッションになります。
- **共有 :** 複数のリモートオペレータで同時に管理対象デバイスをコントロールできます。
- **排他的 :** 管理対象デバイスに対する排他的なリモートセッションを使用できます。セッションが排他モードで開始されると、他のリモートセッションは、管理対象デバイスで開始できなくなります。

セッションの暗号化 : SSL 暗号化 (TLSv1 プロトコル) を使用してリモートセッションのセキュリティを保持します。

キャッシング有効 : リモート管理セッションのデータのキャッシングを有効にして、パフォーマンスを高めます。このオプションは、リモート管理操作に対してのみ利用できます。このオプションは、現在 Windows でのみサポートされています。

帯域幅の動的な最適化の有効化 : 使用可能なネットワーク帯域幅の検出を有効にし、それに従ってセッション設定を調整してパフォーマンスを強化します。このオプションは、リモート管理操作に対してのみ利用できます。

ログを有効にする : セッションおよびデバッグ情報を novell-zenworks-vncviewer.txt ファイルに記録します。ファイルのデフォルトの保存場所は、Internet Explorer から ZENworks コントロールセンターを起動した場合はデスクトップで、Mozilla FireFox から ZENworks コントロールセンターを起動した場合は Mozilla のインストールディレクトリです。

プロキシ経由のルート : 管理対象デバイスのリモート管理操作をプロキシサーバ経由でルーティングできるようにします。管理対象デバイスがプライベートネットワーク上、または NAT (ネットワークアドレス変換) を使用するファイアウォールまたはルータの反対側にある場合、デバイスのリモート管理操作はプロキシサーバ経由でルーティングされます。次のフィールドに入力します。

- **代理 :** プロキシサーバの DNS 名または IP アドレスを指定します。デフォルトで、デバイスのリモート操作を実行するように［プロキシ設定］パネルで設定されたプロキシサーバが、このフィールドに指定されます。別のプロキシサーバを指定できます。
- **プロキシポート :** プロキシサーバがリスンするポート番号を指定します。デフォルトでは、ポートは 5750 です。

識別用に次のキーペアを使用します : 内部認証局 (CA) が展開されている場合、次のオプションは表示されません。外部 CA が展開されている場合、次のフィールドに値を入力してください。

- **秘密鍵 :** ［参照］をクリックして、リモートオペレータの秘密鍵を参照して選択します。

- **証明書 :** ［参照］をクリックして、秘密鍵に対応する証明書を参照して選択します。この証明書は、ゾーンに設定された認証局にチェーンされている必要があります。

  鍵および証明書のサポートするフォーマットは、DER、PEM です。

リモート管理ビューアのインストール : ［リモート管理ビューアのインストール］リンクをクリックして、リモート管理ビューアをインストールします。このリンクが表示されるのは、管理対象デバイスで初めてリモート管理セッションを実行している場合、またはリモート管理ビューアが管理対象デバイスにインストールされていない場合だけです。

6 ［OK］をクリックして、セッションを起動します。

リモート診断操作の実行

1 ZENworks コントロールセンターで、［デバイス］タブをクリックします。

2 管理するデバイスが見つかるまで Servers または Workstations フォルダを移動します。

3 デバイスの前にあるチェックボックスをクリックしてデバイスを選択します。

4 左側のナビゲーションペインのタスクリストで、［リモート診断］をクリックして［リモート診断］ダイアログボックスを表示します。

5 ［リモート診断］ダイアログボックスで、次のフィールドに入力します。

デバイス : リモートで診断するデバイスの名前または IP アドレスを指定します。

Always default to IP address for all devices (すべてのデバイスについて常に IP アドレスを使用する): システムで DNS 名の代わりにデバイス IP アドレスを表示したい場合は、これを選択します。

［OK］をクリックすると、リモートコントロール操作の実行中にデバイスにアクセスするために指定した値がシステムに保存されます。以降のリモートコントロール操作時には、デバイスまたはリモートオペレータに応じて、これらの値の一部が自動的に選択されます。

アプリケーション : リモートで診断するデバイスで起動するアプリケーションを選択します。

認証 : 管理対象デバイスを認証するために使用するモードを選択します。オプションには次の 2 つがあります。

- **パスワード :** リモート診断操作を実行するパスワードベース認証を提供します。ユーザが管理対象デバイスで設定したパスワードか、または管理者がリモート管理ポリシーのセキュリティ設定で設定したパスワードを正しく入力する必要があります。ユーザが設定したパスワードは、管理者が設定したパスワードより優先されます。
- **権利 :** このオプションは、リモート操作を実行する管理対象デバイスを選択した場合のみ使用できます。選択した管理対象デバイスで目的のリモート操作を実行するリモート管理権が管理者より割り当てられている場合、セッション開始時に自動的にアクセス権を取得します。

ポート : リモート管理エージェントがリスンするポート番号を指定します。デフォルトのポート番号は 5950 です。

セッションモード : リモート診断操作には適用されません。

セッションの暗号化 : SSL 暗号化 (TLSv1 プロトコル) を使用してリモートセッションのセキュリティを保持します。

キャッシング有効 : リモート管理セッションのデータのキャッシングを有効にして、パフォーマンスを高めます。このオプションは、現在 Windows でのみサポートされています。

帯域幅の動的な最適化の有効化 : 使用可能なネットワーク帯域幅の検出を有効にして、それに応じてセッションの設定を調製し、パフォーマンスを高めます。

ログを有効にする : セッションおよびデバッグ情報を novell-zenworks-vncviewer.txt ファイルに記録します。ファイルのデフォルトの保存場所は、Internet Explorer から ZENworks コントロールセンターを起動した場合はデスクトップで、Mozilla FireFox から ZENworks コントロールセンターを起動した場合は Mozilla のインストールディレクトリです。

プロキシ経由のルート : 管理対象デバイスのリモート管理操作をプロキシサーバ経由でルーティングできるようにします。管理対象デバイスがプライベートネットワーク上、または NAT (ネットワークアドレス変換) を使用するファイアウォールまたはルータの反対側にある場合、デバイスのリモート管理操作はプロキシサーバ経由でルーティングされます。次のフィールドに入力します。

- **代理 :** プロキシサーバの DNS 名または IP アドレスを指定します。デフォルトで、デバイスのリモート操作を実行するように［プロキシ設定］パネルで設定されたプロキシサーバが、このフィールドに指定されます。別のプロキシサーバを指定できます。
- **プロキシポート :** プロキシサーバがリスンするポート番号を指定します。デフォルトでは、ポートは 5750 です。

6 ［OK］をクリックして、セッションを起動します。

ファイル転送操作の実行

1 ZENworks コントロールセンターで、［デバイス］タブをクリックします。

2 管理するデバイスが見つかるまで Servers または Workstations フォルダを移動します。

3 デバイスの前にあるチェックボックスをクリックしてデバイスを選択します。

4 左側のナビゲーションペインのタスクリストで、［ファイル転送］をクリックして［ファイル転送］ダイアログボックスを表示します。

5 ［ファイル転送］ダイアログボックスで、次のフィールドに入力します。

デバイス : アクセスするデバイスの名前または IP アドレスを指定します。

Always default to IP address for all devices (すべてのデバイスについて常に IP アドレスを使用する): システムで DNS 名の代わりにデバイス IP アドレスを表示したい場合は、これを選択します。［OK］をクリックすると、リモートコントロール操作の実行中にデバイスにアクセスするために指定した値がシステムに保存されます。以降のリモートコントロール操作時には、デバイスまたはリモートオペレータに応じて、これらの値の一部が自動的に選択されます。

認証 : 管理対象デバイスを認証するために使用するモードを選択します。オプションには次の 2 つがあります。

- **パスワード :** パスワードベース認証を提供して、操作を実行します。ユーザが管理対象デバイスで設定したパスワードか、または管理者がリモート管理ポリシーのセキュリティ設定で設定したパスワードを正しく入力する必要があります。ユーザが設定したパスワードは、管理者が設定したパスワードより優先されます。
- **権利 :** このオプションは、リモート操作を実行する管理対象デバイスを選択した場合のみ使用できます。選択した管理対象デバイスで目的のリモート操作を実行するリモート管理権が管理者より割り当てられている場合、セッション開始時に自動的にアクセス権を取得します。

ポート : リモート管理エージェントがリスンするポート番号を指定します。デフォルトのポート番号は 5950 です。

セッションモード : ファイル転送操作には適用されません。

セッションの暗号化 : SSL 暗号化 (TLSv1 プロトコル) を使用してリモートセッションのセキュリティを保持します。

ログを有効にする : セッションおよびデバッグ情報を novell-zenworks-vncviewer.txt ファイルに記録します。ファイルのデフォルトの保存場所は、Internet Explorer から ZENworks コントロールセンターを起動した場合はデスクトップで、Mozilla FireFox から ZENworks コントロールセンターを起動した場合は Mozilla のインストールディレクトリです。Linux 管理コンソールでは、ファイルの保存場所は、ログインしたユーザのホームディレクトリです。

プロキシ経由のルート : 管理対象デバイスのリモート管理操作をプロキシサーバ経由でルーティングできるようにします。管理対象デバイスがプライベートネットワーク上、または NAT (ネットワークアドレス変換) を使用するファイアウォールまたはルータの反対側にある場合、デバイスのリモート管理操作はプロキシサーバ経由でルーティングされます。次のフィールドに入力します。

- **代理 :** プロキシサーバの DNS 名または IP アドレスを指定します。デフォルトで、デバイスのリモート操作を実行するように［プロキシ設定］パネルで設定されたプロキシサーバが、このフィールドに指定されます。別のプロキシサーバを指定できます。
- **プロキシポート :** プロキシサーバがリスンするポート番号を指定します。デフォルトでは、ポートは 5750 です。

6 ［OK］をクリックして、セッションを起動します。

Linux デバイスでのリモートコントロール、リモートビュー、およびリモートログイン操作の実行

1 ZENworks コントロールセンターで、［デバイス］タブをクリックします。

2 管理するデバイスが見つかるまで Servers または Workstations フォルダを移動します。

3 デバイスの前にあるチェックボックスをオンにして、Linux デバイスを選択します。

4 ［アクション］>［リモートコントロール］の順にクリックし、［リモート管理］ダイアログボックスを表示します。

5 ［リモート管理］ダイアログボックスで、次のフィールドに入力します。

デバイス : リモートで管理するデバイスの名前または IP アドレスを指定します。

Always default to IP address for all devices (すべてのデバイスについて常に IP アドレスを使用する): システムで DNS 名の代わりにデバイス IP アドレスを表示したい場合は、これを選択します。

［OK］をクリックすると、リモートコントロール操作の実行中にデバイスにアクセスするために指定した値がシステムに保存されます。以降のリモートコントロール操作時には、デバイスまたはリモートオペレータに応じて、これらの値の一部が自動的に選択されます。

説明 : 管理対象デバイスで実行するリモート操作のタイプ (［リモートコントロール］、［リモートビュー］、または［リモートログイン］) を選択します。

ポート : リモート管理エージェントがリスンするポート番号を指定します。デフォルトでは、ポート番号はリモートコントロール操作とリモートビュー操作に 5950、リモートログイン操作に 5951 です。

ログを有効にする : セッションおよびデバッグ情報を novell-zenworks-vncviewer.txt ファイルに記録します。ファイルのデフォルトの保存場所は、Internet Explorer から ZENworks コントロールセンターを起動した場合はデスクトップで、Mozilla FireFox から ZENworks コントロールセンターを起動した場合は Mozilla のインストールディレクトリです。Linux 管理コンソールでは、ファイルの保存場所は、ログインしたユーザのホームディレクトリです。

プロキシ経由のルート：管理対象デバイスのリモート管理操作をプロキシサーバ経由でルーティングできるようにします。管理対象デバイスがプライベートネットワーク上、または NAT (ネットワークアドレス変換) を使用するファイアウォールまたはルータの反対側にある場合、デバイスのリモート管理操作はプロキシサーバ経由でルーティングされます。次のフィールドに入力します。

- **代理**：プロキシサーバの DNS 名または IP アドレスを指定します。デフォルトで、デバイスのリモート操作を実行するように［プロキシ設定］パネルで設定されたプロキシサーバが、このフィールドに指定されます。別のプロキシサーバを指定できます。
- **プロキシポート**：プロキシサーバがリスンするポート番号を指定します。デフォルトでは、ポートは 5750 です。

リモート管理ビューアのインストール：［リモート管理ビューアのインストール］リンクをクリックして、リモート管理ビューアをインストールします。このリンクが表示されるのは、管理対象デバイスで初めてリモート管理セッションを実行している場合、またはリモート管理ビューアが管理対象デバイスにインストールされていない場合だけです。

6 ［OK］をクリックして、セッションを起動します。

Linux デバイスでのリモート SSH 操作の実行

1 ZENworks コントロールセンターで、［デバイス］タブをクリックします。

2 管理するデバイスが見つかるまで Servers または Workstations フォルダを移動します。

3 デバイスの前にあるチェックボックスをオンにして、Linux デバイスを選択します。

4 ［アクション］>［リモート SSH］の順にクリックし、［リモート SSH］ダイアログボックスを表示します。

5 ［リモート SSH］ダイアログボックスで、次のフィールドに入力します。

デバイス：リモートから接続するデバイスの名前または IP アドレスを指定します。デバイスが同じネットワークにない場合、デバイスの IP アドレスを指定する必要があります。

ユーザ名：リモートデバイスにログインするために使用するユーザ名を指定します。デフォルトでは、これはルートです。

ポート：リモート SSH サービスのポート番号を指定します。デフォルトのポート番号は 22 です。

［OK］をクリックすると、Remote SSH Java Web Start Launcher を起動するように求められます。［はい］をクリックして証明書を受け入れ、［実行］をクリックします。デバイスへの接続を続行するには、［はい］をクリックします。管理対象デバイスに接続するためにパスワードの入力が求められます。

6 ［OK］をクリックして、セッションを起動します。

詳細の参照場所

デバイスのリモート管理の詳細については、『*ZENworks 2017 Remote Management リファレンス*』を参照してください。

ソフトウェアインベントリおよびハードウェアインベントリの収集

ZENworks Configuration Management を使用して、デバイスからソフトウェアおよびハードウェアの情報を収集できます。個々のデバイスのインベントリを表示し、特定の基準に基づいてインベントリレポートを生成できます。

たとえば、特定のプロセッサ、メモリ、およびディスク容量要件を持つソフトウェアアプリケーションを配布したい場合があります。2 つのレポート、1 つは要件を満たすすべてのデバイスが一覧表示されたレポート、もう 1 つは要件を満たしていないデバイスが一覧表示されたレポートを作成します。レポートに基づいて、ソフトウェアを準拠デバイスに配布し、非準拠デバイスにアップグレード計画を作成します。レポートに基づいて、ソフトウェアを準拠デバイスに配布し、非準拠デバイスにアップグレード計画を作成します。

デフォルトでは、デバイスは毎月 1 日の AM1:00 に自動的にスキャンされます。スケジュールおよびその他多くの［インベントリ］環境設定を ZENworks コントロールセンターの［環境設定］タブで変更することができます。

- 98 ページの 「デバイススキャンの開始」
- 98 ページの 「デバイスインベントリの表示」
- 99 ページの 「インベントリレポートの生成」
- 99 ページの 「詳細の参照場所」

デバイススキャンの開始

デバイスのスキャンはいつでも開始できます。

1. ZENworks コントロールセンターで、［デバイス］タブをクリックします。
2. スキャンするデバイスが見つかるまで Servers または Workstations フォルダを移動します。
3. デバイスをクリックして詳細を表示します。
4. 左ナビゲーションパネルにあるタスクリストで、［サーバインベントリスキャン］または［ワークステーションインベントリスキャン］をクリックしてスキャンを開始します。

   ［クイックタスクステータス］ダイアログボックスにはタスクの状態が表示されます。タスクが完了したら、［インベントリ］タブをクリックしてスキャンの結果を表示します。

zman ユーティリティで inventory-scan-now コマンドを使用してデバイスをスキャンすることもできます。詳細については、『*ZENworks コマンドラインユーティリティリファレンス*』の「インベントリコマンド」を参照してください。

デバイスインベントリの表示

1. ZENworks コントロールセンターで、［デバイス］タブをクリックします。
2. スキャンするデバイスが見つかるまで Servers または Workstations フォルダを移動します。
3. デバイスをクリックして詳細を表示します。
4. ［インベントリ］タブをクリックします。

インベントリレポートの生成

ZENworks Configuration Management は、いくつかの標準レポートを含んでいます。さらに、カスタムレポートを作成してインベントリ情報の各種のビューを提供することもできます。

1 ZENworks コントロールセンターで、タブをクリックします。

2 ［インベントリ標準レポート］パネルで、［ソフトウェアアプリケーション］をクリックします。

3 ［オペレーティングシステム］レポートをクリックしてレポートを生成します。

レポートの下部にあるオプションを使用して、生成されたレポートを Microsoft Excel スプレッドシート、CSV (カンマ区切り値) ファイル、PDF ファイル、または PDF Graph ファイルとして保存できます。

詳細の参照場所

インベントリの詳細については、『*ZENworks Asset Inventory リファレンス*』を参照してください。

Linux 管理

Linux 管理を使用すると、既存環境内にある Linux の組み込みおよび拡張を容易に行えます。この製品は、ポリシー重視の自動化を使用して、Linux リソースを導入、管理、および維持します。自動化されたインテリジェントなポリシーにより、デスクトップのロックダウン、イメージ作成、リモート管理、インベントリ管理、およびソフトウェア管理などの Linux システムのライフサイクル全体を集中管理できます。その結果、この製品は包括的な Linux 管理ソリューションになり、Linux システムの管理に必要なオーバーヘッドを大幅に削減することで、IT にかかる手間を解消できます。

次のいずれかを使用して、Linux デバイスにパッチを適用することができます。

- パッチ管理
- Linux パッケージ管理

パッチ管理

パッチ管理は ZENworks に完全に統合された機能で、エージェントベースのパッチ、脆弱性パッチ、およびコンプライアンス管理ソリューションを提供します。

パッチ管理では、次の機能を提供します。

- 署名を使用して必要なパッチを判断し、簡単なレポーティング用に報告する
- デバイス上に常に存在するように特定のパッチのための必須ベースラインを実装する
- SLES および RHEL の配布のみにパッチを適用する

詳細については、121 ページの第 12 章「パッチ管理」を参照してください。

Linux パッケージ管理

Linux パッケージ管理は、Linux デバイス (サーバおよびデスクトップ) 用の ZENworks Configuration Management のパッケージ管理機能の処理を目的としています。

Linux パッケージ管理では、次の機能を提供します。

- エンタープライズレベルで多数の Linux デバイス用のパッケージをパッチ適用、インストール、および更新するために単一点管理を提供する
- ZENworks バンドルとしてパッチおよびパッケージの、UN、RHN、RCE および YUM リポジトリから更新ファイルとパッケージをミラーリングするこれらのバンドルをパッケージ管理用の Linux 管理対象デバイスに割り当てることができます。
- デルタ RPM が利用可能かつ適用可能な場合は常に、管理対象デバイスでデルタ RPM のダウンロードをサポートし、それによってパッチ適用時に必要な帯域幅を削減する
- ミラーリングするカタログ、パッケージ、およびバンドルを選択可能
- OES サーバにパッチを適用可能

モバイルデバイスの管理

ZENworks コントロールセンターには［モバイル管理の開始］ページがあります。このページを使用して、ゾーン内のモバイルデバイスを登録および管理するために必要なタスクを実行できます。

［モバイル管理の開始］ページにアクセスするには、次の手順に従います。

1 ZENworks コントロールセンターで、［モバイル管理］(左のナビゲーションペイン内) をクリックします。

このページの各設定タスクには、完了ステータスを示す または のマークが付いたアイコンと、タスクを完了するページへのリンクが 1 つ以上含まれます。

また、各タスクに対して表示される アイコンをクリックするか、各ページの右上隅にある［ヘルプ］リンクをクリックして、タスクの詳細を参照できます。

2 デバイスをゾーンに登録するために必要な［設定］タスクを完了します。その後、［次の内容］セクションに表示されたタスクを完了して、デバイスを管理できます。

これらの各タスクの詳細については、『ZENworks 2017 Mobile Management Reference』を参照してください。

モバイルデバイスの登録

iOS DEP デバイスの登録

DEP デバイスの登録はエンドユーザにとって簡単です。DEP プロファイルを変更することで、ユーザがデバイスアクティベーションのプロンプトのほとんどをスキップするようにできるからです。DEP デバイスを登録する前に、次の前提条件を満たしていることを確認してください。

前提条件

- ZCCでDEPサーバを追加し、AppleポータルでZENworks MDMサーバと仮想MDMサーバをリンクします。
- Apple ポータルで仮想 MDM サーバにデバイスを割り当てます。これらのデバイスは、ZENworks によって検出され、ZCC に入力されます。
- (オプション)デバイスにユーザを割り当てます(DEP登録中にこのユーザのみをデバイスに関連付ける場合)。

- (オプション)DEP プロファイル設定を変更して、登録プロセスを強化します。
- (条件付き)DEPプロファイルを変更する場合は、変更されたDEPプロファイルがAppleポータルに正しく割り当てられていることを確認してください。

追加として :

- モバイル登録ポリシーを割り当てます。
- (条件付き) 別のユーザによってリタイアされたデバイスを再登録する場合は、以前のデバイスオブジェクトが ZCC で削除されていることを確認します。
- (オプション) モバイル電子メールポリシーを割り当てて、デバイス上の電子メールアカウントを設定します。

これらの各タスクの詳細については、『ZENworks 2017 Mobile Management Reference』を参照してください。

手順

セットアッププロンプトに従って、デバイスを登録します。ユーザが Wi-Fi 設定を行った後、ユーザの資格情報でデバイスにログインします。デバイスが特定のユーザに割り当てられている場合、このユーザのみの資格情報を指定する必要があります。さもないと、登録が失敗します。

デバイスが登録されると、ZCC 内のデバイスの［Deployment Status (展開ステータス)］を表示できます。展開ステータスは［Discovered (検出済み)］から［Managed (管理済み)］に変更されているはずです。このステータスは、デバイスの概要ページで表示できます。

Apple Configurator を使用した iOS デバイスの登録

Apple Configurator は、管理者がビジネスや教育の設定で iOS デバイスを導入する際に役立つ Mac OS X ツールです。Apple Configurator を使用すると、デバイスの再割り当てが迅速かつ簡単になり、次のユーザがコンテンツのクリーンなスレートで開始できるようになります。

前提条件

- モバイル登録ポリシーを割り当てます。
- Apple Enrollment URL をコピーします。これによりデバイスの登録先となる MDM サーバを指定します。これを取得するには、ZCC で、［設定］>［インフラストラクチャ管理］>［MDM サーバ］の順に移動します。MDM サーバを選択して、［Apple Enrollment URL］をクリックします。
- (オプション) モバイル電子メールポリシーを割り当てて、デバイス上の電子メールアカウントを設定します。

これらの各タスクの詳細については、『ZENworks 2017 Mobile Management Reference』を参照してください。

手順

1 USB ポートを介してデバイスを Mac に接続します。

2 右クリックして［Prepare (準備)］を選択するか、Apple Configurator のメニューバーから［Prepare (準備)］を選択します。

3 ［設定］ドロップダウンメニューで［Manual (手動)］を選択します。［次へ］をクリックします。

4 デバイスの登録先となる MDM サーバを選択します。ドロップダウンメニューに保存された MDM サーバがない場合は、［New Server (新しいサーバ)］を選択します。

5 サーバの名前を指定し、ZCC からコピーした Apple Enrollment URL を貼り付けます。これを取得するには、ZCC で、［設定］>［インフラストラクチャ管理］>［MDM サーバ］の順に移動します。MDM サーバを選択して、［Apple Enrollment URL］をクリックします。URL をコピーし、Apple Configurator の［Define an MDM Server (MDM サーバの定義)］ページに貼り付けます。この MDM サーバは、後で使用するために保存されます。

6 デバイスを監視対象として設定する場合は、［Supervise device (デバイスの監視)］を選択します。［Allow devices to pair with other computers (デバイスと他のコンピュータとのペアリングを許可する)］チェックボックスが自動的に有効になります。

7 これらのデバイスを監視する組織を選択します。

8 デバイスの登録中に特定のセットアップ手順をスキップする場合は、［Setup Assistant (設定アシスタント)］ドロップダウンメニューから適切なオプションを選択します。デバイスの登録中に表示される設定項目を確認します。

9 ［Prepare (準備)］をクリックして、接続されたデバイスを準備します。

準備段階の後、iOS デバイスは出荷時の設定にリセットされます。デバイスがリセットされた後で、Apple Configurator の［Configure iOS Setup Assistant (iOS 設定アシスタントの設定)］ページでの構成に基づいて iOS デバイスに表示されるプロンプトに従います。Wi-Fi パスワードを入力すると、ユーザはユーザの資格情報の入力を求められます。

ZENworks User Portal を使用した iOS デバイスの登録

このシナリオでは、ZENworks 管理ゾーンに iOS デバイスを完全管理デバイスとして登録する方法を説明します。このタイプの登録では、デバイス上に MDM プロファイルが作成されます。このプロファイルを使用して、デバイス上に制限を適用したり、アプリを展開したりできます。

前提条件

- ZENworks が iOS バージョン 8 以降が実行されているデバイスをサポートしている。
- ユーザソースがモバイルデバイスの登録用に構成および有効化されている。
- 登録ポリシーが作成されて、ユーザに割り当てられている。
- プライマリサーバに MDM 役割が割り当てられている。
- iOS デバイスのプッシュ通知。
- ZENworks が Exchange ActiveSync アカウントの電子メールを同期できるようにするため、ActiveSync サーバが設定されている必要がある。さらに、ZENworks サーバが ActiveSync サーバのプロキシサーバとして設定されたモバイル電子メールポリシーを作成して割り当てます。これにより、ZENworks は、デバイスで送受信される企業用電子メールを管理できるようになります。
- プライベートモードで実行されている Safari ブラウザを使用した iOS デバイスの登録は、iOS バージョン 11 以降のみでサポートされます。

手順

1 *ZENworks_server_address*/zenworks-eup を入力します。ここで、*ZENworks_server_address* はデバイス上の Safari ブラウザにおける ZENworks MDM サーバの DNS 名または IP アドレスです。

ZENworks User Portal のログイン画面が表示されます。

2 ユーザのユーザ名とパスワードを入力します。ユーザが属するユーザソースで［簡易登録を許可］オプションが選択されている場合、登録ドメインを指定する必要はありません。選択されていない場合は、登録ドメインを指定します。

ZENworks User Portal には、ユーザに関連付けられているすべてのデバイスが表示されます。

3 右上隅の［登録］をタップして、デバイスの登録オプションを表示します。

4 ［管理対象デバイス専用］をタップして、［デバイスの登録オプション］画面を表示します。デバイス所有権 (企業または個人) の指定をユーザに許可するようにモバイルデバイス登録ポリシーが設定されている場合、その情報の入力を求めるプロンプトが表示されます。適切なデバイス所有権オプションを選択して、［OK］をクリックします。

5 ［証明書のダウンロード］をタップして、［プロファイルをインストール］画面を表示します。

6 ［インストール］をタップし、プロンプトに従って証明書をインストールし、［管理対象デバイスとして登録］画面に戻ります。

7 (条件付き) デバイス上の登録証明書を有効にします。このステップは、iOS バージョン 10.3 以降で実行されるデバイスに表示されます。証明書を有効にするには :

7a デバイス上の［設定］メニューに移動して、［一般］をクリックします。

7b ［情報］をクリックします。

7c ［証明書信頼設定］をクリックします。

7d 画面に表示されるルート証明書を有効にします。

8 ［管理対象デバイスとして登録］画面で［プロファイルのダウンロード］をタップして、［プロファイルをインストール］画面を表示します。［インストール］をタップし、プロンプトに従ってプロファイルをインストールし、［管理対象デバイスとして登録］画面に戻ります。

9 ［ホーム］をタップして、ホームページに戻ります。デバイスは［マイデバイス］リストに［登録が進行中］という状態で表示されています。ブラウザを更新して、状態を［Device is Active (デバイスはアクティブです)］に更新する必要があります。

これにより、ZCC の［デバイス情報］ページで登録モードを参照できます。デバイス情報を表示するには、ZCC の左側のナビゲーションペインから、［デバイス］> ［モバイルデバイス］の順にクリックして (またはモバイル登録ポリシーで設定されているフォルダに移動して)、適切なデバイスを選択します。登録は［iOS MDM］と表示されます。

10 ユーザまたはデバイスに割り当てられているモバイル電子メールポリシーに基づいて、デバイスに自動的に電子メールアカウントが設定されます。

基本モードでの Android デバイスの登録

このシナリオでは、ZENworks 管理ゾーンに Android デバイスを完全管理デバイスとして登録する方法を説明します。これは、基本モードの登録であり、これらのデバイス上では特定のポリシー制限のみを適用できます。Android デバイスをより適切に管理するには、仕事用プロファイルモードまたは仕事用管理デバイスモードでこのデバイスを登録することをお勧めします。

前提条件

モバイルデバイスを完全管理デバイスまたは電子メール専用デバイスとして登録する前に、次の前提条件を満たしていることを確認する必要があります。

- ZENworksが登録の基本モード用にAndroidバージョン4.1以降のデバイスをサポートしている。
- ユーザソースがモバイルデバイスの登録用に構成および有効化されている。
- 登録ポリシーが作成されて、ユーザに割り当てられている。
- プライマリサーバに MDM 役割が割り当てられている。
- Android デバイスのプッシュ通知。
- ZENworks が Exchange ActiveSync アカウントの電子メールを同期できるようにするため、ActiveSync サーバが設定されている必要がある。さらに、ZENworks サーバが ActiveSync サーバのプロキシサーバとして設定されたモバイル電子メールポリシーを作成して割り当てます。

これらの各タスクの詳細については、『ZENworks 2017 Mobile Management Reference』を参照してください。

手順

1 *ZENworks_server_address*/zenworks-eup を入力します。ここで、*ZENworks_server_address* は Android デバイス上の Google Chrme ブラウザにおける ZENworks MDM サーバの DNS 名または IP アドレスです。

注 : 必ず Google Chrome を使用してください。組み込みのインターネットブラウザはサポートされません。

ZENworks User Portal のログイン画面が表示されます。

2 ユーザのユーザ名とパスワードを入力します。ユーザが属するユーザソースで［簡易登録を許可］オプションが選択されている場合、登録ドメインを指定する必要はありません。選択されていない場合は、登録ドメインを指定します。

3 右上隅の［登録］をタップして、デバイスの登録オプションを表示します。

4 ［管理対象デバイス専用］をタップします。

5 ［アプリのダウンロード］をタップします。Google Play ストアにリダイレクトされ、ユーザが［インストール］をクリックして、ZENworks Agent アプリをダウンロードする必要があります。インストールが完了したら、［開く］をクリックします。

6 ［Activate this Device Administrator (このデバイス管理者を有効にする)］をクリックし、ユーザがこの画面に表示されている操作を実行してデバイスを管理できるようにします。

7 アプリをダウンロードして起動する際に表示される、関連する許可を受諾します (Android M 以降のバージョンに該当)。ZENworks Agent アプリのログイン画面が表示されます。

8 フィールドに入力して、［サインイン］をタップします。

- **［ユーザ名］、［パスワード］、［ドメイン］、［サーバ URL］**：最初に ZENworks User Portal にログインする際に使用したものと同じユーザ名、パスワード、および登録ドメイン (必要な場合) と、ZENworks MDM サーバのサーバ URL を使用します。この情報は、ステップ 4 で表示される ZENworks User Portal から入手できます。

デバイス所有権 (企業または個人) の指定をユーザに許可するようにモバイル登録ポリシーが設定されている場合、その情報の入力を求めるプロンプトが表示されます。［OK］をタップします。デバイスが自動的にゾーンに登録されます。

ZENworks Agent アプリのホーム画面が表示され、デバイスが登録されてアクティブであることが示されます。

9 ZCC でデバイス情報を表示します。デバイス情報を表示するには、ZCC の左側のナビゲーションペインから、［デバイス］>［モバイルデバイス］の順にクリックして (またはモバイル登録ポリシーで設定されているフォルダに移動して)、適切なデバイスを選択します。登録モードは［Android アプリ］と表示されます。

10 ZENworks Agent アプリの登録後にユーザに送信された電子メールに基づいて、デバイス上に電子メールアカウントを設定します。これには企業用電子メールアカウントの設定が含まれます。この電子メールには、電子メールクライアントの Web アプリケーションまたは他の任意のデバイスからアクセスできます。この情報を使用して、ユーザは企業用電子メールを送受信するデバイスに手動で電子メールアカウントを設定する必要があります。ZENworks からこれらの電子メール通知を送信できるようにするため、SMTP サーバを設定する必要があります。

企業用電子メールアカウントを設定すると、デバイスが登録されて、ZENworks Agent アプリの登録完了時に最初に作成されたデバイスオブジェクトに合わせて自動的に調整されます。ZCC の［デバイス情報］ページの登録モードが［Android アプリ + ActiveSync］に変わります。

仕事用プロファイルモードでの Android デバイスの登録

仕事用プロファイルモードでは、デバイス上に企業アプリと企業データを格納するための専用コンテナが作成されます。これにより、企業データのみを管理できるようになります。このモードは、BYOD (職場への個人デバイスの持ち込み) シナリオ向けです。

前提条件

必須設定

- Android エンタープライズサブスクリプションを作成する。
- モバイル登録ポリシーを作成し、割り当てる。
- Android プロファイル登録ポリシーを作成し、割り当てる。
- Androidバージョンが5.0以降(仕事用プロファイルモードの場合)または6.0以降(仕事用管理デバイスモードの場合) であることを確認する。

オプション設定

- デバイスを登録するようユーザを招待します。

これらの各タスクの詳細については、『ZENworks 2017 Mobile Management Reference』を参照してください。

手順

このセクションで詳述されているシナリオでは、初めて ZENworks にデバイスを登録するユーザを対象にしています。基本モード (Android アプリのみ) でデバイス登録を終えていて、仕事用プロファイルモードでも登録したい場合は、「既存ユーザのための仕事用プロファイルの登録」を参照してください。

手順

1. Google Play ストアから ZENworks Agent アプリをインストールします。または、招待用レターに記載されている手順に従って、ZENworks Agent アプリをダウンロードできます。
2. インストール後に、［開く］をクリックします。ZENworks Agent の短い説明が表示されます。［続行］をクリックします。
3. ［Activate this Device Administrator (このデバイス管理者を有効にする)］をクリックして、アプリを使用したデバイス管理を有効にします。
4. 次の項目を指定して、アプリにログインします。

   ユーザ名、パスワード、ドメイン、サーバ URL: ユーザ名、パスワード、登録ドメイン (ユーザの［簡易登録を許可］が無効になっている場合) を、ZENworks MDM サーバのサーバ URL と一緒に指定します。ユーザは招待用レターからこの情報を取得できます。
5. モバイル登録ポリシーでユーザの所有権の指定が許可されている場合は、デバイス所有権 (企業または個人) を指定します。［［OK］］をタップします。
6. 残りの画面に表示されるプロンプトに従うと、デバイスで自動的に仕事用プロファイルが設定され、ZENworks に登録されます。ZENworks Agent アプリのホーム画面に、デバイスが登録され、アクティブになったことが示されます。
7. ZCC でデバイス情報を表示します。ZCC の左側ナビゲーションペインから［デバイス］>［モバイルデバイス］の順にクリックします (またはモバイル登録ポリシーで設定されているフォルダに移動します)。［概要］ページで適切なデバイスをクリックし、詳細を表示します。登録モードは［Android アプリ］として表示され、［仕事用プロファイルモード］も有効になっています。

デバイスが登録された後、ZENworks Agent アプリとその他のシステムアプリにバッジアイコンが付きます。これにより、仕事用アプリと個人用アプリを区別できます。

既存ユーザのための仕事用プロファイルの登録

基本モード (Android アプリのみ) で ZENworks への登録を終えていて、仕事用プロファイルモードで登録したいユーザには、Android プロファイル登録ポリシーを割り当てます。

モバイル登録ポリシーを割り当てられたユーザのデバイスには、通知が送られます。ここで、ZENworks Agent アプリを開いたときに仕事用プロファイルを設定するよう指示されます。

ユーザは、［設定］をクリックし、プロンプトに従って、仕事用プロファイルを設定します。デバイスは仕事用プロファイルを自動的に設定します。

仕事用管理デバイスモードでの Android デバイスの登録

仕事用管理デバイスモードは、管理者がデバイス全体を管理するために使用できます。これにより、そのデバイスは企業での使用のみに制限されます。このモードは主に企業所有のデバイス向けです。

前提条件

必須設定

- Android エンタープライズサブスクリプションを作成する。
- モバイル登録ポリシーを作成し、割り当てる。
- Android プロファイル登録ポリシーを作成し、割り当てる。
- Androidバージョンが5.0以降(仕事用プロファイルモードの場合)または6.0以降(仕事用管理デバイスモードの場合) であることを確認する。

手順

1 言語設定や Wi-Fi 設定などの初期設定画面に従います。

2 ［電子メール ID］フィールドが表示された設定画面で、AFW 識別子 (afw#zenworks) を指定します。

3 ［Android エンタープライズ］ページで **［次へ］** をクリックし、ZENworks アプリのインストールを続行します。

ZENworks Agent アプリはデバイス上に自動的にダウンロードされます。

4 **［インストール］** をクリックして、デバイス上にアプリをインストールし、プロンプトに従ってデバイスの設定を完了します。

5 残りの画面に表示されるプロンプトに従って、仕事用管理デバイスを設定します。これでデバイスが設定されましたが、まだ仕事用管理デバイスとして登録されていません。

6 次の詳細情報を指定してアプリにログインします。

ユーザ名、パスワード、ドメイン、サーバ URL: ユーザ名、パスワード、登録ドメイン (ユーザの **［簡易登録を許可］** が無効になっている場合) を、ZENworks MDM サーバのサーバ URL と一緒に指定します。

仕事用管理デバイスはデバイス上で自動的に設定されます。

ZCC でデバイス情報を表示します。ZCC の左側ナビゲーションペインから **［デバイス］** > **［モバイルデバイス］** の順にクリックします (またはモバイル登録ポリシーで設定されているフォルダに移動します)。**［概要］** ページで適切なデバイスをクリックし、詳細を表示します。登録モードは **［Android アプリ］** として表示され、**［仕事用管理デバイスモード］** も有効になっています。

ActiveSync 専用デバイスの登録

前提条件

モバイルデバイスを完全管理デバイスまたは電子メール専用デバイスとして登録する前に、次の前提条件を満たしていることを確認する必要があります。

- ZENworksがActiveSync 12.1以降のバージョンが実行されているデバイスをサポートしている。
- ユーザソースがモバイルデバイスの登録用に構成および有効化されている。
- 登録ポリシーが作成されて、ユーザに割り当てられている。
- プライマリサーバに MDM 役割が割り当てられている。

- Android デバイスのプッシュ通知。
- ZENworks が Exchange ActiveSync アカウントの電子メールを同期できるようにするため、ActiveSync サーバが設定されている必要がある。さらに、ZENworks サーバが ActiveSync サーバのプロキシサーバとして設定されたモバイル電子メールポリシーを作成して割り当てます。

手順

このシナリオでは、ZENworks 管理ゾーンにデバイスを電子メール専用デバイスとして登録する方法を説明します。このシナリオで詳しく説明するのは、iOS デバイスを電子メール専用デバイスとして登録する方法です。

1. *ZENworks_server_address*/zenworks-eup を入力します。ここで、*ZENworks_server_address* はデバイス上のブラウザにおける ZENworks MDM サーバの DNS 名または IP アドレスです。

   ZENworks User Portal のログイン画面が表示されます。

2. ZENworks User Portal にユーザ名とパスワードを入力します。ユーザが属するユーザソースで［簡易登録を許可］オプションが選択されている場合、登録ドメインを指定する必要はありません。選択されていない場合は、登録ドメインを指定します。
3. 右上隅の［登録］をタップして、デバイスの登録オプションを表示します。
4. ［電子メール専用］をタップして、［電子メール専用として登録］画面を表示します。表示される情報を使用して、ユーザの電子メールアカウントを作成します。

   ユーザが電子メールアカウントを設定した後、登録プロセスを完了する必要があることを示す電子メールがユーザに送信されます。この電子メールの内容を ZCC で編集できます。そのためには、［設定］>［管理ゾーンの設定］>［イベントとメッセージング］>［電子メール通知］の順に移動します。関連する電子メールをクリックして、内容を編集します。
5. 電子メールに記載されている ZENworks End User Portal へのリンクをクリックするか、ステップ 1 で説明する手順で ZENworks End User Portal にアクセスします。

   ZENworks User Portal の［マイデバイス］リストにデバイスが表示されます。この時点では、デバイスは ZENworks 管理ゾーンに追加されていますが、登録は保留中です。
6. ［登録の完了］をタップします。

   デバイス所有権 (企業または個人) の指定をユーザに許可するようにモバイル登録ポリシーが設定されている場合、その情報の入力を求めるプロンプトが表示されます。デバイスで、必要な登録情報を入力して［OK］をタップします。

   ［マイデバイス］リストが更新され、デバイスは登録済みでアクティブであると表示されます。
7. 別のアカウントからこのユーザに電子メールを送信して、デバイスが電子メールを受信することを確認します。

   デバイスが ZENworks 管理ゾーンに登録されると、デバイスの登録モードは、ZCC の［デバイス情報］ページに［ActiveSync］と表示されます。デバイス情報を表示するには、ZCC の左側のナビゲーションペインから、［デバイス］>［モバイルデバイス］の順にクリックして (またはモバイル登録ポリシーで設定されているフォルダに移動して)、適切なデバイスを選択します。

10 Endpoint Security Management

ZENworks Endpoint Security Management は、管理対象デバイスにセキュリティポリシーの集中管理機能を提供することによってエンドポイントセキュリティを簡素化します。リムーバブルストレージデバイス、無線ネットワーク、およびアプリケーションへのデバイスのアクセスを制御できます。また、暗号化によってデータを保護し、ファイアウォールの実施 (ポート、プロトコル、および制御リスト) を介してネットワーク通信を保護することができます。また、その場所に基づいてエンドポイントデバイスのセキュリティを変更できます。

次のセクションでは、Endpoint Security Management を使用して、会社オフィスであっても、自宅であっても、空港ターミナルであってもデバイスのセキュリティを保護する方法について説明します。

エンドポイントセキュリティ管理の有効化

管理ゾーンのインストール時に、ライセンスキーを入力するか、評価をオンにして Endpoint Security Management を起動しなかった場合は、次の手順を実行してください。

1. ZENworks コントロールセンターで、［環境設定］をクリックします。
2. ［ライセンス］パネルで、［ZENworks 2017 Endpoint Security Management］をクリックします。
3. ［製品の評価 / アクティブ化］を選択して、以下のフィールドに入力します。

   使用評価 : このオプションを選択すると、60 日の評価期間が有効になります。60 日の評価期間終了後に製品を継続的に使用するには、製品ライセンスキーを申請しなければなりません。

   製品ライセンスキー : エンドポイントセキュリティ管理用に購入したライセンスキーを指定します。製品ライセンスを購入するには、ZENworks Endpoint Security Management 製品サイト (http://www.novell.com/products/zenworks/endpointsecuritymanagement) を参照してください。
4. ［OK］をクリックします。

エンドポイントセキュリティエージェントの有効化

ZENworks Agent では、デバイス登録、コンテンツの配布、デバイスのソフトウェア更新を行います。

ZENworks Endpoint Security Management (フルライセンスまたは評価版) が有効化されている場合は、デバイスには ZENworks Agent の他に、Endpoint Security Agent もインストールされます。Endpoint Security Agent は、デバイス上のセキュリティポリシー設定を実施します。

Endpoint Security Agent が有効になっていることを確認する必要があります。方法については、37 ページの 「ZENworks Agent 機能の設定」を参照してください。

場所の作成

デバイスのセキュリティ要件は、場所ごとに異なります。たとえば、空港内にあるデバイスと、企業ファイアウォール内のオフィスにあるデバイスでは、個々のファイアウォール制限が異なります。

デバイスのセキュリティ要件をその場所に合ったものにするため、Endpoint Security Management はグローバルポリシーと場所ベースのポリシーの両方をサポートしています。グローバルポリシーは、デバイスの場所とは無関係に適用されます。場所ベースのポリシーは、デバイスの現在の場所が、ポリシーに関連付けられた場所の条件を満たす場合にのみ適用されます。たとえば、会社オフィスの場所ベースポリシーを作成し、これをラップトップに割り当てた場合、このポリシーは、ラップトップの場所が会社オフィスであるときにのみ適用されます。

場所ベースのポリシーを使用する場合は、最初に、自分の会社や組織に合った場所を定義する必要があります。場所とは、特定のセキュリティ要件が設定されているプレースやプレースタイプを意味します。たとえば、オフィス、自宅、または空港でデバイスを使用する場合のセキュリティ要件は異なります。

場所はネットワーク環境に応じて定義されます。ニューヨークと東京にオフィスがあると仮定してください。両方のオフィスには同じセキュリティ要件が設定されています。したがって、「オフィス」場所を作成し、ニューヨークオフィスと東京オフィスの 2 つのネットワーク環境に関連付けます。これらの環境はそれぞれ、ゲートウェイ、DNS サーバ、およびワイヤレスアクセスポイントの一連のサービスによって明示的に定義されます。Endpoint Security Agent は、その現在の環境がニューヨークオフィスのネットワーク、または東京オフィスのネットワークに合致していると判断した場合は常に、その場所を「オフィス」に設定し、「オフィス」場所に関連付けられているセキュリティポリシーを適用します。

場所の作成方法の詳細については、34 ページの 「場所の作成」を参照してください。

セキュリティポリシーの作成

セキュリティポリシーは 11 種類あります。

デバイスのセキュリティ設定は、Endpoint Security Agent が適用するセキュリティポリシーによって制御されます。セキュリティ関連の機能範囲を制御するセキュリティポリシーは 8 種類あります。組織のニーズに応じてポリシーの一部、または全部を使用することができます。

ポリシー	目的
アプリケーション制御	アプリケーションの実行をブロックするか、またはアプリケーションへのインターネットアクセスを拒否します。インターネットアクセスがブロックまたは拒否されるアプリケーションを指定します。

ポリシー	目的
通信ハードウェア	次の通信ハードウェアを無効にします : 1394-Firewire、IrDA-Infrared、Bluetooth、シリアル / パラレル、ダイヤルアップ、有線、および無線。各通信ハードウェアは個別に構成されます。これは一部のハードウェアタイプ (Bluetooth やダイヤルアップなど) を無効にし、その他を有効なままにできることを意味します。
データの暗号化	リムーバブルストレージデバイス上のファイルのデータ暗号化を有効にします。
ファイアウォール	ポート、プロトコル、ネットワークアドレス (IP および MAC) を無効にすることによって、ネットワーク接続を制御します。
Scripting(スクリプト作成)	デバイス上でスクリプト (JScript または VBScript) を実行します。スクリプトの実行を開始するトリガを指定できます。トリガは、エンドポイントセキュリティエージェントのアクション、場所の変更、または時間間隔に基づいて実行されます。
ストレージデバイス制御	CD/DVD ドライブ、フロッピードライブ、およびリムーバブルストレージドライブへのアクセスを制御します。各ストレージデバイスタイプは個別に設定されます。それは有効にも無効にもできることを意味します。
USB 接続	リムーバブルストレージデバイス、プリンタ、入力デバイス (キーボード、マウスなど) の USB デバイスへのアクセスを制御します。個別のデバイスまたはデバイスのグループを指定できます。たとえば、特定のプリンタへのアクセスを無効にして、すべての Sandisk USB デバイスへのアクセスを有効にできます。
VPN 強制	デバイスの場所に基づいて、VPN 接続を実施します。たとえば、デバイスの場所が不明な場合は、すべてのインターネットトラフィックがルーティングされる VPN 接続を強制できます。
Wi-Fi	無線アダプタの無効化、無線接続のブロック、無線アクセスポイントへの接続の制御などを行います。

上記のセキュリティポリシー以外に、以下のセキュリティポリシーは Endpoint Security Agent の保護と設定をサポートします。この 2 つのポリシーは、その特性により、最初に作成して割り当てることをお勧めします。

ポリシー	目的
セキュリティの設定	エンドポイントセキュリティエージェントが変更されたり、アンインストールされないように保護します。 ZENworks エージェントセキュリティ設定を行う方法については、39 ページの 「ZENworks Agent のセキュリティの設定」を参照してください。
場所割り当て	デバイスまたはユーザに許可されている場所のリストを提供します。Endpoint Security Agent は、現在のネットワーク環境を評価して、許可されている場所のいずれかと一致するかどうかを確認します。一致する場合、その場所はセキュリティ場所になり、エージェントはその場所に関連付けられているすべてのセキュリティポリシーを適用します。リスト内のどの場所とも一致しない場合は、不明な場所に関連付けられているセキュリティポリシーが適用されます。 場所ベースのポリシーを使用する場合は、ロケーション割り当てポリシーが各デバイスやユーザに割り当てられていることを確認する必要があります。デバイス、またはデバイスのユーザに場所割り当てポリシーが割り当てられていない場合は、Endpoint Security Agent はデバイスに場所ベースのポリシーを適用することができません。

セキュリティポリシーを作成するには、次の手順に従います。

1. ZENworks コントロールセンターで、［ポリシー］をクリックして、［ポリシー］ページを表示します。
2. ［ポリシー］パネルで、［新規］>［ポリシー］の順にクリックして新規ポリシーの作成ウィザードを起動します。
3. ［Select Platform(プラットフォームの選択)］ページで、［Windows］を選択して、次に［次へ］をクリックします。
4. ［ポリシーカテゴリの選択］ページで、［Windows Endpoint セキュリティポリシー］を選択して、［次へ］をクリックします。
5. ［ポリシータイプの選択］ページで、作成するポリシーのタイプを選択して、［次へ］をクリックします。

   場所を作成し、場所ベースのポリシーを使用する予定の場合は、1 つ以上の場所割り当てポリシーを作成してデバイスやデバイスのユーザに割り当てる必要があります。割り当てておかないと、作成した場所をデバイスが使用できず、場所ベースのポリシーが適用されません。
6. ［詳細の定義］ページで、ポリシーに名前を入力し、ポリシーを配置するフォルダを選択します。

   名前は選択したフォルダ内にあるすべてのポリシーの間で固有でなければなりません。
7. (条件付き) ［継承と場所割り当て］ページが表示されたら、以下の設定を行い、［次へ］をクリックします。
   - **継承 :** このポリシーに、ポリシー階層で上位に割り当てられたポリシータイプと同じ設定を継承させるには、［ポリシー階層からの継承］の設定を選択したままにします。たとえば、このポリシーをデバイスに割り当て、別のポリシー (同じタイプ) をデバイスのフォルダに割り当てた場合、このオプションを有効にすると、このポリシーは、デバイスの

フォルダに割り当てられたポリシーの設定を継承できるようになります。このポリシーにポリシー設定を継承させたくない場合は、［ポリシー階層からの継承］設定の選択を解除します。

- **場所割り当て：**ポリシーは、グローバルにすることも、場所ベースにすることもできます。グローバルポリシーは、場所とは無関係に適用されます。場所ベースのポリシーは、デバイスがポリシーに割り当てられた場所内にあることを検知した場合にのみ適用されます。

  グローバルまたは場所ベースのいずれのポリシーかを選択します。場所ベースを選択する場合は、［追加］をクリックし、ポリシーを割り当てる場所を選択し、次に［OK］をクリックしてリストに追加します。

8 ポリシー特有の設定を行い、［概要］ページに達するまで［次へ］をクリックします。

ポリシー設定に関する詳細は、ZENworks コントロールセンターで［ヘルプ］>［現在のページ］の順にクリックします。

9 ［概要］ページで、情報が正しいことを確認してください。間違っている場合は、［戻る］ボタンをクリックして該当するウィザードページに戻り、変更します。正しい場合は、以下のいずれかのオプションを選択し (必要に応じて)、次に［完了］をクリックします。

- **サンドボックスとして作成：**サンドボックスバージョンとしてポリシーを作成する場合に、このオプションを選択します。サンドボックスバージョンは、発行するまでユーザやデバイスから分離されています。たとえば、サンドボックスバージョンをユーザやデバイスに割り当てることはできますが、発行して初めて適用されます。
- **作成後に詳細を設定：**ポリシーのプロパティページを表示するには、このオプションを選択します。これらのページでは、ポリシー設定を変更し、ユーザやデバイスに割り当てることができます。

ユーザおよびデバイスへのポリシーの割り当て

ポリシーの作成後、ポリシーをデバイスやデバイスユーザに割り当てて、デバイスに適用する必要があります。

1 ［ポリシー］パネルで、割り当てるポリシーの横のチェックボックスをオンにします。

2 ［アクション］>［デバイスへの割り当て］の順にクリックします。

または

［アクション］>［ユーザへの割り当て］の順にクリックします。

3 プロンプトに従ってポリシーを割り当てます。

ウィザードの各ページで［ヘルプ］ボタンをクリックすると、そのページの詳細情報が表示されます。

ウィザードを完了すると、割り当てられたデバイスやユーザがポリシーの［関係］ページに追加されます。ポリシーをクリックするとポリシーの割り当てが表示されます。

ゾーンへのポリシーの割り当て

セキュリティポリシーを管理ゾーンに割り当てることができます。デバイスに適用する有効なポリシーを決定するときに、ユーザ割り当て済みおよびデバイス割り当て済みのポリシーがすべて評価された後でゾーンポリシーが評価されます。次の状況について考えてみます。

- ファイアウォールポリシーがデバイスまたはデバイスのユーザに (直接でも、グループやフォルダを通じてでも) 割り当てられていません。ゾーンファイアウォールポリシーが、デバイスの有効なポリシーになり、デバイスで適用されています。
- ファイアウォールポリシーが、デバイスおよびデバイスのユーザに割り当てられています。両方のポリシーが評価および統合され、デバイスに適用する有効なファイアウォールポリシーが決定されます。ユーザ割り当ておよびデバイス割り当てポリシーから有効なポリシーが決定された後、1) 有効なファイアウォールポリシーで未設定の値、2) 追加の値 (複数値のポート / プロトコルルールテーブルなど) を提供するために、ゾーンファイアウォールポリシーが使用されます。

3 つのレベルでゾーンポリシーを定義できます。これを使用して、管理ゾーン内の別々のデバイスに異なるゾーンポリシーを割り当てられます。

- **管理ゾーン :** デバイスフォルダまたはデバイスレベルで別のゾーンポリシーを指定しない限り、管理ゾーンで割り当てたポリシーがすべてのデバイスのゾーンポリシーになります。
- **デバイスフォルダ :** デバイスフォルダで定義したポリシーは、管理ゾーン (および親デバイスフォルダ) レベルに優先し、サブフォルダまたは個々のデバイスに別のゾーンポリシーを指定しない限り、フォルダ構造内に含まれるすべてのデバイスのゾーンポリシーになります。
- **デバイス :** 個々のデバイスに対して定義したポリシーは、管理ゾーンおよびデバイスフォルダレベルに優先し、デバイスのゾーンポリシーになります。

次の手順は、管理ゾーンでのポリシーの割り当て方法を示したものです。

1. ZENworks コントロールセンターで、［環境設定］をクリックして、［環境設定］ページを表示します。
2. ［管理ゾーンの設定］パネルで、［Endpoint Security Management］をクリックします。
3. ［ゾーンポリシー設定］ページを表示するには、［ゾーンポリシー設定］をクリックしてします。
4. ［追加］をクリックし、ゾーンに割り当てるポリシーを参照して選択します。次に［OK］をクリックしてリストに追加します。
5. ポリシーの追加を完了したら、［OK］をクリックします。

詳細の参照場所

ZENworks Endpoint Security Management の詳細については、次のガイドを参照してください。

- *ZENworks Endpoint Security Policies リファレンス*
- *ZENworks Endpoint Security Agent リファレンス*
- *ZENworks Endpoint Security Utilities Reference*
- *ZENworks Endpoint Security Scripting Reference*

11 Full Disk Encryption

ZENworks Full Disk Encryption は、デバイスの電源がオフのときや、デバイスがハイバネーションモードのときに、不正アクセスからデバイスのデータを保護します。この操作を行うには、ディスク暗号化とプレブート認証の組み合わせを使用します。

Full Disk Encryption は、標準、ソリッドステート、および自己暗号化されたハードディスクに対してソフトウェアベースの暗号化を提供します。すべてのディスクボリューム (または選択されたディスクボリューム) は、ボリューム上の一時ファイル、スワップファイル、およびオペレーティングシステムファイルを含めすべて暗号化されます。データには、有効なユーザが正常にログインするまでアクセスできなくなり、CD/DVD やフロッピーディスク、USB ドライブなどのメディアからデバイスをブートしてもデータにアクセスすることはできません。認証済みユーザの場合は、暗号化されていないディスク上のデータにアクセスするのと同じように、暗号化されたディスク上のデータにアクセスできます。

Full Disk Encryption は、ハードディスクに対してオプションのプレブート認証を提供します。ZENworks Pre-Boot Authentication (PBA) コンポーネントは、ハードディスク上に小さな Linux パーティションとしてインストールされます。ログインは、ZENworks PBA を通じて処理されます。この PBA は、MDT チェックサムと、キーに強化暗号を使用したパスワード抽出を利用して改変から保護されています。

ZENworks PBA は Windows ログインを使用してシングルサインオンをサポートします。シングルサインオンによって、ユーザは一組の資格情報 (ユーザ / パスワードまたはスマートカード) を入力するだけで、ZENworks PBA と Windows オペレーティングシステムの両方にログインできるようになります。

Full Disk Encryption のアクティブ化

管理ゾーンのインストール時に、ライセンスキーを入力するか、評価をオンにして Full Disk Encryption をアクティブ化しなかった場合は、今すぐこれを実行する必要があります。

Full Disk Encryption を有効化するには、次の手順を実行します。

1 ZENworks コントロールセンターで、**［環境設定］** をクリックします。

2 ［ライセンス］パネルで、**［ZENworks 2017 Full Disk Encryption］** をクリックします。

3 **［製品の評価 / アクティブ化］** を選択して、以下のフィールドに入力します。

使用評価 : このオプションを選択すると、60 日の評価期間が有効になります。60 日の評価期間終了後に製品を継続的に使用するには、製品ライセンスキーを申請しなければなりません。

製品ライセンスキー : ZENworks Full Disk Encryption 用に購入したライセンスキーを指定します。製品ライセンスを購入するには、ZENworks Full Disk Encryption 製品サイト (http://www.novell.com/products/zenworks/full-disk-encryption) を参照してください。

4 ［OK］をクリックします。

Full Disk Encryption Agent の有効化

ZENworks Agent では、デバイス登録、コンテンツの配布、デバイスのソフトウェア更新を行います。

ZENworks Full Disk Encryption (フルライセンスまたは評価版) をアクティブ化すると、ZENworks Agent に加えて、Full Disk Encryption Agent もデバイスにインストールされます。Full Disk Encryption Agent は、デバイスに適用したディスク暗号化ポリシーに応じて、ディスクを暗号化処理および復号化処理する役割を果たします。

Full Disk Encryption Agent が有効化されていることを確認してください。方法については、ZENworks Agent 機能の設定を参照してください。

重要 : ZENworks Full Disk Encryption は Windows Secure Boot をサポートしていないため、Full Disk Encryption Agent をデバイスにインストールする前にこの機能を無効にする必要があります。システム要件の詳細については、*ZENworks Full Disk Encryption Agent Reference* の「System Requirements」を参照してください。

ディスク暗号化ポリシーの作成

デバイスのディスク暗号化と ZENworks プレブート認証 (オプション) の使用は、どちらもディスク暗号化ポリシーが適用されます。

ディスク暗号化ポリシーを作成するには、次の手順を実行します。

1 ZENworks コントロールセンターで、［ポリシー］をクリックして、［ポリシー］ページを表示します。

2 ［ポリシー］パネルで、［新規］>［ポリシー］の順にクリックして新規ポリシーの作成ウィザードを起動します。

3 プラットフォームの選択ページで、［Windows］を選択し、［次へ］をクリックします。

4 ［ポリシーカテゴリの選択］ページで、［Windows Full Disk Encryption Policies (Windows 完全ディスク暗号化ポリシー)］を選択して、［次へ］をクリックします。

5 ［ポリシータイプの選択］ページで、［Disk Encryption Policy (ディスク暗号化ポリシー)］を選択してから［次へ］をクリックします。

6 ［詳細の定義］ページで、ポリシーに名前を入力し、ポリシーを配置するフォルダを選択します。

名前は選択したフォルダ内にあるすべてのポリシーの間で固有でなければなりません。

7 ポリシー特有の設定を行い、［概要］ページに達するまで［次へ］をクリックします。

ポリシー設定に関する詳細は、ZENworks コントロールセンターで［ヘルプ］>［現在のページ］の順にクリックします。

8 ［概要］ページで、情報が正しいことを確認してください。間違っている場合は、［戻る］ボタンをクリックして該当するウィザードページに戻り、変更します。正しい場合は、以下のいずれかのオプションを選択し (必要に応じて)、次に［完了］をクリックします。

- **サンドボックスとして作成 :** サンドボックスバージョンとしてポリシーを作成する場合に、このオプションを選択します。サンドボックスバージョンは、発行するまでユーザやデバイスから分離されています。たとえば、サンドボックスバージョンをユーザやデバイスに割り当てることはできますが、発行して初めて適用されます。
- **作成後に詳細を設定 :** ポリシーのプロパティページを表示するには、このオプションを選択します。これらのページでは、ポリシー設定を変更し、ユーザやデバイスに割り当てることができます。

ポリシーのデバイスへの割り当て

ディスク暗号化ポリシーを作成したら、そのポリシーをデバイスに割り当てる必要があります。

ディスク暗号化ポリシーは、デバイス専用のポリシーです。デバイスおよびデバイスフォルダに割り当てることができます。デバイスグループ、ユーザ、ユーザグループ、またはユーザフォルダに割り当てることはできません。

また、デバイスに最も関連性の強いポリシーのみが適用されます。たとえば、あるデバイスと、そのデバイスのフォルダに異なるポリシーが割り当てられた場合は、そのデバイスに直接割り当てられたポリシーが適用されます。

重要 : UEFI BIOS を使用する Windows デバイスでは、ディスク暗号化ポリシーはサポートされていません。ディスク暗号化ポリシーを Windows UEFI デバイスに割り当てても、ポリシーはデバイスに適用されません。

---

1 ［ポリシー］パネルで、割り当てるディスク暗号化ポリシーの横にあるチェックボックスをオンにします。

2 ［アクション］>［デバイスへの割り当て］の順にクリックします。

3 プロンプトに従ってポリシーを割り当てます。

ウィザードの各ページで［ヘルプ］ボタンをクリックすると、そのページの詳細情報が表示されます。

ウィザードを完了すると、割り当てられたデバイスがポリシーの［関係］ページに追加されます。ポリシーをクリックするとポリシーの割り当てが表示されます。

ポリシーがデバイスに適用された後の状態について

プレブート認証を使用している場合は、デバイスにポリシーを割り当てた後、ポリシー適用とディスク暗号化のワークフローが多少異なります。以下は、デバイスにディスク暗号化ポリシーを適用するときに理解する必要がある、ディスク暗号化とプレブート認証の概念です。

ディスク暗号化

ZENworks Full Disk Encryption は、標準、ソリッドステート、および自己暗号化されたハードディスクに対してソフトウェアベースの暗号化を提供します。

Full Disk Encryption は、ディスク全体または選択したボリューム (パーティション) のセクタベースの暗号化を提供します。一時ファイル、スワップファイル、オペレーティングシステムなど、ボリューム上のすべてのファイルが暗号化されます。すべてのファイルが暗号化されるため、CD-ROM、フロッピーディスク、または USB ドライブといった外部メディアからコンピュータを起動しても、データにアクセスできません。

互換性のあるハードディスクは、IDE、SATA、または PATA インタフェース規格を備えた 3.5 または 2.5 インチのディスクです。

業界標準の暗号化アルゴリズム (AES、Blowfish、DES、または DESX) と、組織の要件を最もよく満たすキー長を選択できます。デバイスファームウェアが UEFI 用に設定されている場合、AES アルゴリズムと 256 キー長が自動的に使用されます。

注 : 標準ハードドライブを暗号化するために ZENworks Full Disk Encryption で使用される暗号モジュールは、連邦情報処理規格 (FIPS) 140-2 の認定を受けて*いません*。ただし、暗号モジュールは、FIPS 140-2 レベル 1 証明書に一致した規格を実装しています。

プレブート認証

ZENworks Full Disk Encryption は、デバイスの電源がオフのときや、デバイスがハイバネーションモードのときに、デバイスのデータを保護します。誰かが Windows オペレーティングシステムに正常にログインすると、暗号化されたボリュームは保護されなくなり、データに自由にアクセスできます。ログインセキュリティを強化するために、ZENworks Pre-Boot Authentication (PBA) を使用できます。

ZENworks PBA は、Linux ベースのコンポーネントです。ディスク暗号化ポリシーがデバイスに適用されると、ハードディスク上に Linux カーネルと ZENworks PBA を格納した 500 MB のパーティションが作成されます。

通常の操作時には、この Linux パーティションからデバイスがブートされ、ZENworks PBA がロードされます。ユーザが適切な資格情報 (ユーザ ID/ パスワードまたはスマートカード) を提出すると、PBA はすぐに終了して Windows オペレーティングシステムが起動し、それまでは非表示でアクセスできなかった Windows のドライブ上の暗号化データにアクセスできるようになります。

Linux パーティションはセキュリティ向上を目指して強化されており、ZENworks PBA は、MD5 チェックサムの使用により改ざんから保護され、認証キーの強力な暗号化を使用します。

ZENworks プレブート認証を使用することを、強くお勧めします。ZENworks PBA を使用しない場合、暗号化されたデータは Windows 認証によってのみ保護されます。

ZENworks プレブート認証の詳細については、『*ZENworks Full Disk Encryption PBA リファレンス*』を参照してください。

詳細の参照場所

ZENworks Full Disk Encryption の詳細については、次のガイドを参照してください。

- *ZENworks Full Disk Encryption Policy Reference*
- *ZENworks Full Disk Encryption Agent Reference*
- *ZENworks Full Disk Encryption PBA Reference*
- *ZENworks Full Disk Encryption Emergency Recovery リファレンス*

12 パッチ管理

パッチ管理を使用すると、ソフトウェアパッチを自動的に一貫して適用して脆弱性および問題を最小限にすることができます。

パッチ管理は、ZENworks Patch Subscription Service と定期的にインターネットで通信することにより最新パッチとフィックスで常に最新に保たれます。最初の 60 日間の評価期間後も、引き続き最新の脆弱性およびパッチ情報を毎日ダウンロードするには有料のサブスクリプションが必要になります。

新しいパッチがサブスクリプションサービスから利用可能になると、ZENworks サーバは、そのパッチに関する情報をダウンロードします。パッチはデバイスに展開するか、またはパッチを破棄することもできます。

次のセクションでは、ZENworks Patch Management を使用して、管理ゾーンでソフトウェアパッチを自動的に一貫してデバイスに適用する方法について説明します。これを行うと、古いソフトウェアやパッチが適用されていないソフトウェアで発生する可能性のある脆弱性および問題を最小限にすることができます。

パッチ管理の有効化

1 ZENworks コントロールセンターで、［環境設定］をクリックします。

2 ［ライセンス］パネルで、［ZENworks 2017 Patch Management］をクリックします。

3 ［Activate Product (製品のアクティブ化)］を選択して、次のフィールドに入力します。

製品サブスクリプションのシリアル番号 : サブスクリプションライセンスを購入したときに提供された、シリアル番号。サブスクリプションライセンスを購入しなかった場合は、トライアル用の評価コードを入力できます。60 日間の評価期間が過ぎると、引き続きサブスクリプションサービスからパッチを受け取るには、Patch Management のサブスクリプションライセンスが必要になります。このサブスクリプションライセンスを購入するには、ZENworks Patch Management 製品サイト (http://www.novell.com/products/zenworks/patchmanagement) を参照してください。

会社名 : サブスクリプションライセンスの購入に使用した、ユーザの会社名。評価に必要ではありません。

メールアドレス : 必要なときに連絡ができる、メールアドレス。評価に必要ではありません。

4 ［適用］をクリックします。

ZENworks Agent での Patch Management の有効化

ZENworks Agent がデバイスでパッチ管理操作を実行するには、エージェントのパッチ管理機能が有効になっている必要があります。パッチ管理機能は、ZENworks Patch Management (フルライセンスまたは評価版) が有効になっている場合にはデフォルトで有効になっています。

エージェントのパッチ管理機能が有効になっていることを確認する必要があります。方法については、37 ページの 「ZENworks Agent 機能の設定」を参照してください。

サブスクリプションサービスの開始

パッチの受け取りを開始する前に、ZENworks サーバのいずれかでサブスクリプションサービスを開始し、パッチのダウンロード用のデイリースケジュールを設定する必要があります。

新しいパッチがサブスクリプションサービスから利用可能になると、ZENworks サーバは自動的にパッチをダウンロードします。[パッチ] ページ (**[パッチ管理]** タブ上) には、最新のパッチと一緒にその説明およびビジネスへの影響が示されています。パッチはデバイスに展開するか、またはパッチを破棄することもできます。

パッチ管理は、ZENworks Patch Subscription Service と定期的にインターネットで通信することにより最新パッチとフィックスで常に最新に保たれます。最初の 60 日間の試用期間が過ぎると、Patch Management の最新脆弱性およびパッチ情報の日次ダウンロードを継続するには有料申し込みが必要です。

管理ゾーンに複数の ZENworks サーバがある場合は、任意の 1 つを選択して Patch Management サーバに指定することができます。パッチ管理サーバとして選択されたサーバは、新しいパッチとアップデートを毎日ダウンロードするために、インターネットに最適な状態で接続できる必要があります。

サブスクリプションサービスを開始するには、次の手順に従います。

1. ZENworks コントロールセンターで、**[環境設定]** タブをクリックします。
2. [管理ゾーン設定] パネルで、**[パッチ管理]** をクリックし、**[サブスクリプションサービス情報]** をクリックします。
3. **[サブスクリプションサービスの開始]** リストで、サブスクリプションサービスを実行する ZENworks サーバを選択して、**[サービスの開始]** をクリックします。

   サブスクリプションサービスの実行が開始されると、**[サービスの開始]** ボタンが **[実行中のサービス]** になります。
4. **[サブスクリプション通信インターバル (毎日)]** リストで、毎日パッチをダウンロードする時刻を選択します。
5. **[OK]** をクリックします。

パッチポリシーの作成

デバイスにパッチを展開する前に、ZENworks Agent は Discover Applicable Update (DAU) タスクを実行する必要があります。DAU タスクにより、ネットワークのデバイスに従って、ZENworks Agent が各パッチのステータス (パッチ適用済み、パッチ未適用、適用なし) を検出することができます。

パッチ検出サイクルは、DAU タスクがすべての管理対象デバイス (サーバとワークステーション) にスケジュールされている ZENworks サーバで毎日開始します。個々のエージェントから DAU タスクを開始することもできます。パッチ検出スキャンの結果は、ZENworks サーバの［パッチ管理］タブまたは［デバイス］タブの［パッチ］セクションで表示できます。ワークステーションがネットワークから接続解除されている場合にも結果が利用できます。

パッチを展開するには、パッチポリシーを作成するか、［Deploy Remediation (修復の展開)］を使用できます。パッチポリシーはパッチ展開プロセスを自動化するもので、［Deploy Remediation (修復の展開)］より推奨される方法です。パッチポリシーでルールを定義して、パッチのキャッシングと配布を、デバイスが必要とするパッチのみに制限できます。

次の手順は、1 つまたは複数のパッチがサブスクリプションサービスから利用可能であると想定しています。

1. ZENworks コントロールセンターで、［パッチ管理］> ［パッチポリシー］に移動します。
2. ［パッチポリシー］ページで、［新規］をクリックします。
3. プロンプトに従って、パッチポリシーを作成します。

   各ページで［ヘルプ］ボタンをクリックすると、そのページの詳細情報が表示されます。
4. パッチポリシーの作成後、パッチポリシーをクリックして、［関係］ページを選択します。
5. ［関係］パネルで［追加］をクリックして、1 つ以上のデバイスをポリシーに割り当てます。
6. ［発行］をクリックし、パッチポリシーの設定に従って、適用可能なパッチをデバイスに配布して適用します。

重要 : ゾーン全体でデバイスにパッチを適用する前に、まずテストデバイスにパッチを適用することをお勧めします。「テスト」デバイスとして設定されたデバイスは、手順 6 (ポリシーの発行) を実行することなく、割り当てられたテストデバイスにサンドボックス経由で自動的にパッチを適用します。

初めてパッチポリシーを作成する場合、［auto approve patches after successful test enforcements (強制テストの正常完了後にパッチを自動承認)］を選択し、パッチを自動承認するようにポリシーを設定することもできます。ポリシー環境設定でこのオプションを選択すると、テストデバイスの 100% がテストに合格した後、そのポリシーに割り当てられているすべてのデバイスにポリシーが自動的に発行されます (発行 (上の手順 6) が不要になります)。

詳細の参照場所

パッチ管理の設定、パッチポリシーを使用した管理ゾーン全体でのパッチ配布の自動化、および［Deploy Remediation (修復の展開)］の使用の詳細については、『*ZENworks 2017 Patch Management Reference*』を参照してください。