リモート管理リファレンス

Novell® ZENworks® 10 Configuration Management SP3

10.3

2010 年 3 月 30 日

www.novell.com

保証と著作権

米国 Novell, Inc. およびノベル株式会社は、本書の内容または本書を使用した結果について、いかなる保証、表明または約束も行っていません。また、本書の商品性、および特定の目的への適合性について、いかなる明示的または黙示的な保証も否認し、排除します。また、本書の内容は予告なく変更されることがあります。

米国 Novell, Inc. およびノベル株式会社は、すべてのノベル製ソフトウェアについて、いかなる保証、表明または約束も行っていません。また、ノベル製ソフトウェアの商品性、および特定の目的への適合性について、いかなる明示的または黙示的な保証も否認し、排除します。米国 Novell, Inc. およびノベル株式会社は、ノベル製ソフトウェアの内容を変更する権利を常に留保します。

本契約の下で提供される製品または技術情報はすべて、米国の輸出規制および他国の商法の制限を受けます。お客様は、すべての輸出規制を遵守し、製品の輸出、再輸出、または輸入に必要なすべての許可または等級を取得するものとします。お客様は、現在の米国の輸出除外リストに掲載されている企業、および米国の輸出管理規定で指定された輸出禁止国またはテロリスト国に本製品を輸出または再輸出しないものとします。お客様は、取引対象製品を、禁止されている核兵器、ミサイル、または生物化学兵器を最終目的として使用しないものとします。ノベル製ソフトウェアの輸出に関する詳細については、Novell International Trade Services の Web ページ (http://www.novell.com/info/exports/) を参照してください。弊社は、お客様が必要な輸出承認を取得しなかったことに対し如何なる責任も負わないものとします。

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

オンラインマニュアル: 本製品とその他の Novell 製品の最新のオンラインマニュアルにアクセスするには、Novell マニュアルの Web ページ (http://www.novell.com/documentation) を参照してください。

Novell の商標

Novell の商標一覧については、「商標とサービスの一覧 (http://www.novell.com/company/legal/trademarks/tmlist.html)」を参照してください。

サードパーティ資料

サードパーティの商標は、それぞれの所有者に帰属します。

目次

このガイドについて

『*Novell ZENworks 10 Configuration Management リモート管理リファレンス*』には、リモート管理に関する情報が含まれています。このガイドの情報は、次のように構成されます。

対象読者

このガイドは、Novell® ZENworks® の管理者を対象としています。

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。オンラインマニュアルの各ページの下部にあるユーザコメント機能を使用するか、または Novell Documentation Feedback サイト (http://www.novell.com/documentation/feedback.html) にアクセスして、ご意見をお寄せください。

追加のマニュアル

ZENworks Configuration Management 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 10 Configuration Management SP3 まマニュアル (http://www.novell.com/documentation/zcm10/) を参照してください。

マニュアルの表記規則

Novell のマニュアルでは、「より大きい」記号 (>) を使用して手順内の操作と相互参照パス内の項目の順序を示します。

商標記号 (®、™ など) は、Novell の商標を示します。アスタリスク (*) は、サードパーティの商標を示します。

パス名の表記に円記号 (\) を使用するプラットフォームとスラッシュ (/) を使用するプラットフォームがありますが、このマニュアルでは円記号を使用します。Linux* など、スラッシュを使用するプラットフォームの場合は、必要に応じて円記号をスラッシュに置き換えてください。

概要

1

Novell® ZENworks® Configuration Management を使用すると、管理コンソールからリモートでデバイスを管理できます。リモート管理では、次が可能です。

- 管理対象デバイスをリモートで管理する
- 管理対象デバイス上で実行可能ファイルをリモートで実行する
- 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する
- 管理対象デバイス上の問題を診断する
- 電源が切断されている管理対象デバイスをリモートから起動する

次のセクションを参照してください。

1.1 リモート管理の用語

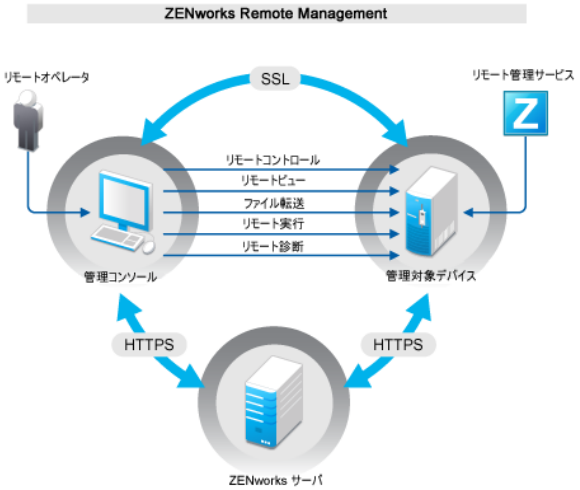
用語	説明
管理対象デバイス	リモートから管理するデバイス。デバイスをリモートから管理するには、リモート管理コンポーネントがインストールされていることおよびリモート管理サービスがそのデバイスで実行されていることを確認してください。
管理サーバ	ZENworks Configuration Management サーバをインストールするデバイス。
管理コンソール	デバイスを管理するためのインタフェース。リモート操作を実行するには、コンソールにリモート管理ビューアをインストールする必要があります。
管理者	リモート管理ポリシーおよび設定を設定し、リモート管理権限をリモートオペレータに付与することができるユーザ。
リモート管理サービス	リモートオペレータがデバイス上でリモート操作を実行できるようにする管理対象デバイスコンポーネント。
リモート管理ビューア	管理対象デバイス上でリモートオペレータがリモート操作を実行できるようにする管理コンソールアプリケーション。リモートオペレータが管理対象デバイスデスクトップを表示したり、ファイルを転送したり、管理対象デバイス上でアプリケーションを実行できるようにします。
リモート管理リスナー	リモートオペレータが管理対象デバイスユーザからのリモートアシスタント要求を受託できるようにする管理コンソールアプリケーション。

用語	説明
リモート管理プロキシ	リモート管理操作要求をリモート管理ビューアから管理対象デバイスに転送するプロキシサーバ。このプロキシは、プライベートネットワーク上、あるいは NAT (Network Address Translation) 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管理対象デバイスにビューアが直接アクセスできない場合に役に立ちます。前提条件として、プロキシを Windows 管理対象デバイスまたは Linux デバイス (プライマリサーバ、サテライトデバイス) にインストールする必要があります。

1.2 リモート管理操作の理解

管理者は、リモート管理を使用して、デバイスのあるサイトに行くことなくデバイスを制御できます。これによって、人材と組織が費やす時間や費用を節約できます。たとえば、管理者または組織のヘルプデスクは、ユーザのワークステーションまで実際に出向かなくても管理対象デバイスの問題を分析してリモートから解決できます。このため、問題解決に要する時間が短縮され、生産性が向上します。

図 1-1 *リモート管理操作*



以降の一連のセクションを読むと、リモート管理で行うさまざまな操作を理解できます。

- 12 ページのセクション 1.2.1「リモートコントロール」
- 13 ページのセクション 1.2.2「リモートビュー」
- 13 ページのセクション 1.2.3「リモート実行」
- 13 ページのセクション 1.2.4「リモート診断」
- 13 ページのセクション 1.2.5「ファイル転送」
- 14 ページのセクション 1.2.6「リモートウェイクアップ」

1.2.1 リモートコントロール

リモート制御を使用すると、管理コンソールから管理対象デバイスをリモートで制御してユーザを支援したり、デバイスの問題を解決したりすることができます。

リモートコントロール機能は、管理コンソールと管理対象デバイスの間に接続を確立します。リモートコントロール接続を使用すると、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。詳細については、53 ページのセクション 3.1「リモートコントロールセッションの管理」を参照してください。

1.2.2 リモートビュー

リモートビュー機能では、リモートで管理対象デバイスに接続して、管理対象デバイスを制御するのではなく、表示することができます。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ことを確認できます。詳細については、57 ページのセクション 3.2「リモートビューセッションの管理」を参照してください。

1.2.3 リモート実行

リモート実行機能により、管理コンソールから管理対象デバイス上のプログラムをシステム権限で実行できます。アプリケーションをリモートで実行するには、[リモート実行] ウィンドウに実行可能ファイルの名前を指定します。たとえば、regedit コマンドを実行して、管理対象デバイスで登録エディタを開くことができます。詳細については、58 ページのセクション 3.3「リモート実行セッションの管理」を参照してください。

1.2.4 リモート診断

リモート診断では、管理対象デバイスの問題をリモートで診断して分析できます。デスクトップを稼動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。詳細については、58 ページのセクション 3.4「リモート診断セッションの管理」を参照してください。

診断機能では、管理対象デバイス上の問題の診断と解決に役立つ、リアルタイムの情報が提供されます。管理対象デバイス上のデフォルト診断アプリケーションには次のものが含まれます。

- システム情報
- コンピュータ管理
- サービス
- レジストリエディタ

1.2.5 ファイル転送

ファイル転送では、管理コンソールおよび管理対象デバイス上で次のようなさまざまなファイル操作を実行できます。

- 管理コンソールと管理対象デバイス間でのファイルのコピー
- ファイルまたはフォルダの名前変更
- ファイルまたはフォルダの削除
- フォルダの作成
- ファイルおよびフォルダのプロパティの表示
- 管理コンソール上で関連付けられているアプリケーションを持つファイルを開く

詳細については、60 ページのセクション 3.5「ファイル転送セッションの管理」を参照してください。

重要 : ファイル転送プログラムを使用すると、管理対象デバイス上のネットワークドライブにアクセスできます。

1.2.6 リモートウェイクアップ

リモートウェイクアップを使用すると、ネットワーク内の電源が切断されている単一のまたは複数のノードの電源をリモートから入れることができます (ただし、ノード上のネットワークカードのリモートウェイクアップが有効にされている必要があります)。詳細については、63 ページのセクション 3.7「リモートデバイスのウェイクアップ」を参照してください。

1.3 リモート管理機能の理解

次のセクションは、さまざまなリモート管理機能の理解の支援となります。

- 14 ページのセクション 1.3.1「可視信号」
- 14 ページのセクション 1.3.2「不正侵入者検出」
- 15 ページのセクション 1.3.3「セッションの暗号化」
- 15 ページのセクション 1.3.4「可聴ビープ音」
- 15 ページのセクション 1.3.5「キーボードとマウスのロック」
- 15 ページのセクション 1.3.6「画面の空白」
- 15 ページのセクション 1.3.7「異常終了」
- 15 ページのセクション 1.3.8「スクリーンセーバーを無効にする」
- 15 ページのセクション 1.3.9「自動セッション終了」
- 16 ページのセクション 1.3.10「エージェント側で開始される接続」
- 16 ページのセクション 1.3.11「セッションコラボレーション」
- 16 ページのセクション 1.3.12「リモート管理監査」

1.3.1 可視信号

管理対象デバイスデスクトップ上に、デバイスがリモートで管理されていることをユーザに通知する可視表示を提供します。可視信号は、リモートオペレータおよびリモートセッションのタイプやセッションの開始時刻などセッションの詳細を示します。ユーザは特定のリモートセッションを終了するか、または信号ダイアログボックスを閉じてすべてのリモートセッションを終了することができます。

1.3.2 不正侵入者検出

不正侵入者検出機能により、管理対象デバイスがハックされる危険性が大幅に低下します。リモートオペレータが指定の回数内 (デフォルトは 5 回) に管理対象デバイスにログインできなかった場合は、リモート管理サービスがブロックされ、ブロックを解除しない間はどのリモートセッション要求も受け入れなくなります。

1.3.3 セッションの暗号化

リモートセッションは、セキュアソケットレイヤ (TLSv1 プロトコル) を使用して保護されます。

1.3.4 可聴ビープ音

管理対象デバイスでリモートセッションがアクティブな場合は、リモート管理ポリシーで設定されたように管理対象デバイスで定期的にビープ音を生成できます。

1.3.5 キーボードとマウスのロック

リモートセッション中に管理対象デバイスのキーボードとマウスコントロールをロックして、管理対象デバイスユーザがセッションに介入できないようにすることができます。

注 : Windows Vista 管理対象デバイスでは、Aero テーマを有効にしていると、マウスとキーボードのロック機能が動作しません。

1.3.6 画面の空白

リモートセッション中に管理対象デバイス上の画面をブランクにして、セッション中にリモートオペレータによって実行されているアクションをユーザが参照できないようにすることができます。管理対象デバイスのキーボードとマウスのコントロールもロックされます。

注 : リモートセッション中にタブレット PC 管理対象デバイスの画面を空白にすると、セッションのパフォーマンスが低下する。

1.3.7 異常終了

リモートセッションが突然切断された場合に、管理対象デバイスをロックするか、または管理対象デバイス上のユーザをログアウトすることができます。

1.3.8 スクリーンセーバーを無効にする

リモートセッション中に管理対象デバイス上のパスワード保護されたスクリーンセーバーを無効にすることができます。

注 : この機能は、Windows Vista*、Windows Server 2008、および Windows 7 管理対象デバイスでは使用できません。

1.3.9 自動セッション終了

リモートセッションが指定された時間非アクティブである場合に、リモートセッションが自動的に終了します。

1.3.10 エージェント側で開始される接続

管理対象デバイス上のユーザがリモートオペレータに助けを求めることができるようにします。リモートオペレータのリストを事前設定してユーザが利用できるようにすることができます。詳細については、44 ページのセクション 2.8.2「管理対象デバイスからのセッションの開始」を参照してください。

注 : この機能は現在 Windows でのみサポートされています。

1.3.11 セッションコラボレーション

この機能により、数人のリモートオペレータが協力し合って、共同リモートセッションを実施できます。マスタリモートオペレータは、他のリモートオペレータをセッションに招待したり、問題を解決するためにリモートコントロール権限を別のリモートオペレータに委任したり、リモートオペレータからコントロールを再取得したり、リモートセッションを終了したりできます。詳細については、55 ページのセクション 3.1.2「セッションコラボレーション」を参照してください。

1.3.12 リモート管理監査

管理対象デバイス上で実行されたそれぞれのリモートセッションの監査レコードを生成できます。監査ログは管理対象デバイス上で維持され、ユーザが参照することができます。

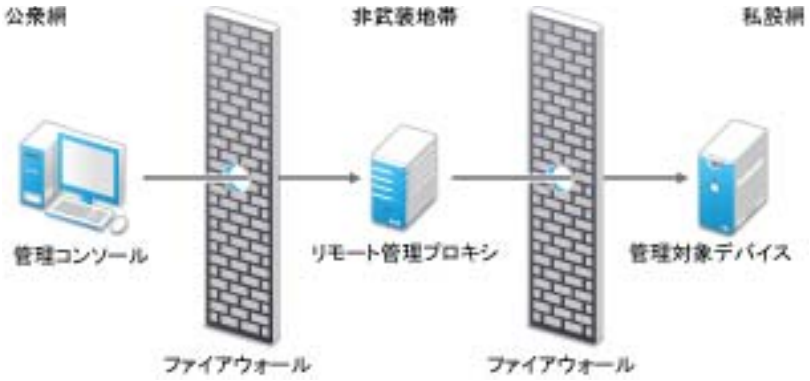
1.4 リモート管理プロキシの理解

プライベートネットワーク上、あるいは NAT (Network Address Translation) 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管理対象デバイスではリモート管理操作を実行できません。これは、NAT ファイアウォールが外部ネットワークからデバイスの IP アドレスを隠し、デバイスへの接続要求をブロックするためです。このようなデバイスをリモートで管理するには、リモート操作をリモート管理プロキシ経由でルーティングする必要があります。

管理コンソールからリモートセッションを開始する際に、プロキシを介してリモート操作をルーティングする詳細については、37 ページの 「デバイスコンテキストからリモート管理セッションを開始する」のプロキシ経由のルートを参照してください。

デバイスコンテキストからリモートセッションを開始する際に、プロキシを介してリモート操作をルーティングする詳細については、39 ページの 「ユーザコンテキストからリモート管理セッションを開始する」のプロキシ経由のルートを参照してください。

図 1-2　リモート管理プロキシ



プロキシは、非武装地帯 (DMZ) に置かれたデバイスにインストールする必要があります。プロキシをインストールするデバイスは、管理コンソールを持つパブリックネットワークからアクセスでき、プライベートネットワークにあるデバイスにアクセスできる必要があります。リモート管理プロキシのインストールの詳細については、49 ページのセクション 2.10「リモート管理プロキシのインストール」を参照してください。

リモート管理プロキシは、デフォルトでリモート管理ビューアからの受信リモート管理要求をポート 5750 でリスンし、要求をデバイスに転送します。

リモート管理のセットアップ 2

次の各セクションでは、Novell® ZENworks® 10 Configuration Management のリモート管理コンポーネントの生産環境への展開について説明します。

2.1 リモート管理設定の環境設定

［リモート管理の設定］は、管理対象デバイスでのリモート管理サービスの動作または実行を決める複数のルールです。この設定には、リモートセッション中のポート、セッション設定、およびパフォーマンス設定用の設定が含まれます。これらの設定は、ゾーン、フォルダ、およびデバイスレベルで適用できます。

次のセクションでは、異なるレベルでのリモート管理設定について説明します。

2.1.1 ゾーンレベルでのリモート管理設定

デフォルトでは、リモート管理設定をゾーンレベルで設定すると、すべての管理対象デバイスに適用されます。

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. ［管理ゾーン設定］パネルで、［*デバイス管理*］をクリックし、［*リモート管理*］をクリックします。
3. ［*リモート管理サービスをポートで実行*］を選択し、リモート管理サービスがそのポートで実行されるようにポートを指定します。

   デフォルトでは、リモート管理サービスはポート番号 5950 上でリスンします。
4. セッション設定オプションを選択します。

フィールド	詳細
リモートセッションの開始時に、ビューアの DNS 名を検索する	リモート管理サービスを有効にして、リモートセッションの開始時に管理コンソールの DNS 名を検索できるようにします。 この DNS 名は、監査ログに保存され、リモートセッション中のセッション情報に含めて表示されます。このオプションを選択しなかったか、リモート管理サービスでコンソール名を検索できなかった場合は、コンソール名に［*不明*］と表示されます。 ネットワークの逆 DNS ルックアップが有効でない場合は、この設定を無効にしてリモートセッションの開始に大きな遅延が出ることを防ぐことをお勧めします。
管理対象デバイスにユーザがログインしていない場合は、リモートセッションを許可	ポリシーでリモート操作が許可されているがデバイスにログインしているユーザがいないときに、リモートオペレータがデバイスをリモート管理できるようにします。デフォルトではこのオプションが選択されています。

5 リモートセッション中のパフォーマンスを改善する次のオプションから選択します。

フィールド	詳細
壁紙を抑制	リモートセッション中の管理対象デバイスの壁紙を抑制します。抑制することで、壁紙のビットマップデータがリモート管理コンソールに繰り返し送信されなくなるので、リモートセッションのパフォーマンスが向上します。
最適化ドライバを有効にする	デフォルトですべての管理対象デバイスにインストールされている、最適化ドライバを有効にします。このオプションを選択すると、リモートセッション中に、管理対象デバイスの画面で変更された部分だけがキャプチャされ、リモート管理コンソールで更新され、リモートセッションのパフォーマンスが向上します。

6 (オプション) リモート管理プロキシを設定して、管理対象デバイスでリモート操作を実行します。

管理対象デバイスがプライベートネットワーク上、あるいは 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リモート管理プロキシ経由でルーティングできます。プロキシは別々にインストールする必要があります。リモート管理プロキシのインストールの詳細については、49 ページのセクション 2.10「リモート管理プロキシのインストール」を参照してください。

タスク	詳細
リモート管理プロキシを追加する	1. ［*追加*］をクリックして、［プロキシ設定の追加］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。 **代理 :** リモート管理プロキシの IP アドレスまたは DNS 名を指定します。 **IP アドレス範囲 :** リモート管理プロキシ経由でリモート管理するデバイスの IP アドレスを指定します。次のいずれかの方法で、IP アドレスの範囲を指定できます。 ◆ CIDR(Classless Inter-Domain Routing) 表記を使用して IP アドレスの範囲を指定します。CIDR を使用すると、IP アドレスのドット付きの 10 進数の部分が、8 ビットずつの 4 つのバイトから構成される 32 ビットの 2 進数に変換されます。スラッシュの後に続く数字 (/n) は、プレフィックスの長さを表わし、アドレスの左側から数えた共有初期ビットの数です。/n の数は 0 ～ 32 のいずれかで、8、16、24、および 32 が通常使われる数です。例 : 123.45.678.12/16: 123.45 で始まるすべての IP アドレスを指定します。 123.45.678.12/24: 123.45.678 で始まるすべての IP アドレスを指定します。 ◆ IP アドレスの範囲を、**開始 IP アドレス** - **終了 IP アドレス**のフォーマットで指定します。次に例を示します。 123.45.678.12 - 123.45.678.15: 123.45.678.12 から 123.45.678.15 の範囲にあるすべての IP アドレスを指定します。
リモート管理プロキシを削除する	1. 削除するプロキシを選択します。 2. ［削除］をクリックして、［*OK*］をクリックします。

7 (オプション) アプリケーションを［*診断アプリケーション*］リストに追加することによって、リモート診断セッション中に管理対象デバイス上で起動するようにアプリケーションを設定します。デフォルトでは、次のアプリケーションがリストに含まれています。

- システム情報
- コンピュータ管理
- サービス
- レジストリエディタ

次の表に、［*診断アプリケーション*］リストのカスタマイズで実行できるタスクをリストします。

タスク	詳細
アプリケーションを追加する	1. ［*追加*］をクリックします。 2. 管理対象デバイスにアプリケーション名およびアプリケーションパスを指定します。 3. ［*OK*］をクリックします。
アプリケーションを削除する	1. 削除するアプリケーションを選択します。 2. ［削除］、［*OK*］の順にクリックします。
デフォルトのアプリケーションに戻す	1. ［*戻る*］をクリックして、［*OK*］をクリックします。

8 ［*適用*］をクリックし、［*OK*］をクリックします。

これらの変更は、デバイスが更新されたときにデバイス上で有効になります。

2.1.2 フォルダレベルでのリモート管理設定

デフォルトでは、ゾーンレベルで行ったリモート管理設定が、すべての管理対象デバイスに適用されます。ただし、1 つのフォルダ内のデバイスについてこれらの設定を変更できます。

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

2 リモート管理設定を行うフォルダ (詳細) をクリックします。

3 ［*設定*］をクリックし、［*デバイス管理*］ > ［*リモート管理*］の順にクリックします。

4 ［*上書き*］をクリックします。

5 リモート管理設定を必要に応じて編集します。

6 変更内容を適用するには、［*適用*］をクリックします。

または

ゾーンレベルでの設定にシステム設定を戻すには、［*元に戻す*］をクリックします。

7 ［*OK*］をクリックします。

これらの変更は、デバイスが更新されたときにデバイス上で有効になります。

2.1.3 デバイスレベルでのリモート管理設定

デフォルトでは、ゾーンレベルで行ったリモート管理設定が、すべての管理対象デバイスに適用されます。ただし、管理対象デバイスについてこれらの設定を変更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*］をクリックします。

2 ［*サーバ*］または［*ワークステーション*］をクリックして管理対象デバイスのリストを表示します。

3 リモート管理設定を行うデバイスをクリックします。

4 ［*設定*］をクリックし、［*デバイス管理*］ > ［*リモート管理*］の順にクリックします。

5 ［*上書き*］をクリックします。

6 リモート管理設定を必要に応じて編集します。

7 変更内容を適用するには、［*適用*］をクリックします。

または

デバイス上で以前のシステム設定に戻す場合は、［*元に戻す*］をクリックします。

デバイス上のリモート管理設定がフォルダレベルで構成されていない場合は、構成済みのフォルダレベルの設定に戻ります。その他の場合は、デフォルトのゾーンレベル設定に戻ります。

8 ［*OK*］をクリックします。

これらの変更は、デバイスが更新されたときにデバイス上で有効になります。

2.2 リモート管理リスナの有効化

リモート管理リスナを有効にして管理対象デバイスからの接続をリスンする

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

2 左ペインの［*デバイスタスク*］で、［*リモート管理リスナ*］をクリックします。

3 ［リモート管理リスナ］ダイアログボックスで、リモート接続をリスンするポートを指定します。デフォルトのポート番号は 5550 です。

4 ［*OK*］をクリックします。

通知領域に［ZENworks Remote Management リスナ］アイコンが表示されます。

2.3 リモート管理ポリシーの作成

リモート管理ポリシーでは、管理対象デバイスでのリモート管理セッションの動作または実行を設定できます。このポリシーは、リモートコントロール、リモートビュー、リモート実行、リモート診断、ファイル転送などのリモート管理操作の設定を含み、セキュリティに関する設定も制御できます。

デフォルトでは、セキュアなリモート管理ポリシーは、ZENworks Adaptive 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すると、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上書きするには、明示的にそのデバイスのリモート管理ポリシーを作成できます。

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*］リストで、［*新規*］をクリックし、［*ポリシー*］をクリックして［ポリシータイプの選択］ページを表示します。

3 ［*リモート管理ポリシー*］を選択し、［ *次へ*］をクリックして［詳細設定］ページを表示し、フィールドに入力します。

ポリシー名 : ポリシーの一意の名前を指定します。ポリシー名は、同じフォルダにある他の項目 (グループ、フォルダなど) の名前とは異なっている必要があります。

フォルダ : ポリシーを配置する ZENworks コントロールセンターフォルダの名前を入力するか、参照して選択します。デフォルトは / ポリシーですが、さらにフォルダを追加してポリシーを整理できます。

説明 : ポリシーのコンテンツの短い説明を入力します。この説明は、ZENworks コントロールセンターでポリシーの概要ページに表示されます。

4 ［*次へ*］をクリックすると、［リモート管理一般設定］ページが表示されます。デフォルト設定を受け入れる場合は、次のステップに進みます。または次の表に示す情報を参照してデフォルトの設定を変更します。

フィールド	詳細
ユーザにリモートセッション要求を許可する	管理対象デバイス上のユーザが、リモートオペレータに対してリモートセッションの実行を要求できるようにします。リモートオペレータは、リモート管理リスナが実行されていることを確認する必要があります。
管理対象デバイスにログインしている新しいユーザから権限が要求されたときにリモートセッションを終了する	リモート管理対象デバイスにログインしている新規ユーザからの許可が必要な場合、実行しているリモートセッションを終了します。
管理対象デバイス上のユーザにリモートセッション監査情報を表示する	管理対象デバイス上のユーザが、ZENworks アイコンからリモートセッションの監査情報を参照できるようにします。
ZENworks アイコンに［リモート管理］プロパティを表示する	管理対象デバイスのユーザが ZENworks アイコンによりリモート管理ポリシーに関連付けられたプロパティを参照できるようにします。
編集	リモートセッションの開始前に管理対象デバイスのユーザに表示されるメッセージを編集する 1. ［*編集*］をクリックして、［メッセージの編集］ダイアログボックスを表示します。 2. メッセージを編集します。 3. ［*OK*］をクリックします。
デフォルトの復元	デフォルトメッセージを復元する 1. ［*デフォルトの復元*］をクリックして、デフォルトメッセージに戻します。
リモートリスナの追加	リモートリスナを追加する 1. ［*追加*］をクリックします。 2. ［リモートリスナーの追加］ダイアログボックスで、管理コンソールのデバイスの DNS 名または IP アドレス、およびリモート管理リスナーがリモートセッション要求をリスンするポート番号を指定します。 3. ［*OK*］をクリックします。
リモートリスナの削除	リモートリスナを削除する 1. 削除するリモートリスナを選択します。 2. ［*削除*］をクリックします。

5 ［*次へ*］をクリックすると、［リモートコントロール設定］ページが表示されます。デフォルト設定を受け入れる場合は、次のステップに進みます。または次の表に示す情報を参照してデフォルトの設定を変更します。

フィールド	詳細
管理対象デバイスのリモートコントロールを許可	管理対象デバイスでのリモートコントロールセッションを許可します。このオプションを選択すると、ページ上の次のオプションが有効になります。このオプションを選択解除すると、デバイスでのリモートコントロール操作が無効になります。
リモートコントロールの開始前に、管理対象デバイス上のユーザからの許可を求める	リモートコントロールセッションを開始する前に、管理対象デバイスのユーザからの許可を求めることができるようにします。
リモートコントロール中に、管理対象デバイス上のユーザに可視信号が送信される	リモートコントロールセッション中に、管理対象デバイスデスクトップの右上端に可視信号が表示されます。可視信号を使用すると、管理対象デバイスのユーザはリモートコントロールセッションが実行中であることが分かります。
管理対象デバイスごとにユーザに可聴ビープ音が与えられる	リモートコントロールセッションの間、管理対象デバイスでビープ音を鳴らします。ビープ音は指定された秒数を経過後、定期的に鳴ります。
リモートコントロール中に管理対象デバイス画面を空白にする	リモートコントロール中に、管理対象デバイスの画面を空白にすることができるようにします。このオプションを選択すると、管理対象デバイスのキーボードとマウスのコントロールもロックされます。
リモートコントロール中に管理対象デバイスのマウスとキーボードをロックする	リモートコントロール中に、管理対象デバイスのマウスとキーボードをロックできるようにします。
リモートコントロール中にスクリーンセーバを自動的にロック解除する	管理対象デバイスでリモートコントロールセッションを開始する前に、リモートコントロールビューアからパスワードで保護されたスクリーンセーバのロックを解除できるようになります。
Automatically Terminate Remote Control Session After Inactivity of [ ] Minutes ([ ] 分間アクティブでない場合にリモートコントロールセッションを自動終了する)	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、指定した時間非アクティブであった場合にセッションが終了されます。

6 ［*次へ*］をクリックすると、［リモートビュー設定］ページが表示されます。デフォルト設定を受け入れる場合は、次のステップに進みます。または次の表に示す情報を参照してデフォルトの設定を変更します。

フィールド	詳細
管理対象デバイスをリモートで表示できる	管理対象デバイスでのリモートビューセッションを許可します。このオプションを選択すると、ページ上の次のオプションが有効になります。このオプションを選択解除すると、デバイスでのリモートビュー操作が無効になります。
リモートビューの開始前に、管理対象デバイス上のユーザからの許可を求める	リモートビューセッションを開始する前に、管理対象デバイスのユーザからの許可を求めることができるようになります。

フィールド	詳細
リモートビュー中に、管理対象デバイス上のユーザに可視信号が送信される	リモートビューセッション中に、管理対象デバイスデスクトップの右上隅に可視信号が表示されます。可視信号を表示することで、管理対象デバイスのユーザは、リモートビューセッションが進行中であることを認識できます。
Give Audible Beep to User on Managed Device Every [ ] Seconds During Remote View (リモートビュー中、[ ] 秒ごとに管理対象デバイスのユーザに可聴ビープ音を鳴らす)	リモートビューセッションの間に、管理対象デバイスでビープ音を鳴らします。ビープ音は指定された秒数を経過後、定期的に鳴ります。

7 ［次へ］をクリックすると、［リモート診断設定］ページが表示されます。デフォルト設定を受け入れる場合は、次のステップに進みます。または次の表に示す情報を参照してデフォルトの設定を変更します。

フィールド	詳細
リモートによる管理対象デバイスの診断を許可	管理対象デバイスでのリモート診断セッションを許可します。このオプションを選択すると、ページ上の次のオプションが有効になります。このオプションを選択解除すると、デバイスでのリモート診断操作が無効になります。
リモート診断の開始前に、管理対象デバイス上のユーザからの許可を求める	リモート診断セッションの開始前に管理対象デバイスのユーザからの許可をリモートオペレータが求めるようにします。
リモート診断中に、管理対象デバイス上のユーザに可視信号が送信される	リモート診断セッション中に、管理対象デバイスデスクトップの右上隅に可視信号が表示されます。可視信号を表示することで、管理対象デバイスのユーザは、リモート診断セッションが進行中であることを認識できます。
Give Audible Beep to User on Managed Device Every [ ] Seconds During Remote Diagnostics (リモート診断中、[ ] 秒ごとに管理対象デバイスのユーザに可聴ビープ音を鳴らす)	リモート診断セッションの間、管理対象デバイスでビープ音を鳴らします。ビープ音は指定された秒数を経過後、定期的に鳴ります。
リモート診断中に管理対象デバイス画面を空白にする	リモート診断中に、管理対象デバイスの画面を空白にすることができるようにします。管理対象デバイスのキーボードおよびマウスは、リモート診断セッション中は常にロックされます。また、このオプションを選択すると、管理対象デバイスで可視信号が無効化されます。
再起動の前に [ ] 秒間警告メッセージを表示する時間 (秒)	リモート診断セッションの開始時に管理対象デバイスのユーザに対して、すべての既存のアプリケーションを保存するよう警告メッセージが表示されます。この警告メッセージは、リモートオペレータがリモート診断セッション中にシステム再起動を開始するときに、ユーザが未保存のデータを失わないように、一定時間表示されます。

フィールド	詳細
Automatically Terminate Remote Diagnostics Session After Inactivity of [ ] Minutes ([ ] 分間非アクティブであった場合、リモート診断セッションを自動的に終了する)	リモート診断セッションが、指定した時間非アクティブであった場合にセッションが終了されます。

8 ［*次へ*］をクリックすると、［リモート実行設定］ページが表示されます。デフォルト設定を受け入れる場合は、次のステップに進みます。または次の表に示す情報を参照してデフォルトの設定を変更します。

フィールド	詳細
プログラムが管理対象デバイス上でリモートで実行されることを許可する	管理対象デバイスでのプログラムのリモート実行を許可します。このオプションを選択すると、ページ上の次のオプションが有効になります。このオプションを選択解除すると、デバイスでのリモート実行操作が無効になります。
リモート実行の開始前に、管理対象デバイス上のユーザからの許可を求める	リモート実行セッションの開始前に管理対象デバイスのユーザからの許可をリモートオペレータが求めるようにします。
リモート実行中に、管理対象デバイス上のユーザに可視信号が送信される	リモート実行セッション中に、管理対象デバイスデスクトップの右上端に可視信号が表示されます。可視信号を使用すると、管理対象デバイスのユーザはリモート実行セッションが実行中であることが分かります。
Automatically Terminate Remote Diagnostics Session After Inactivity of [ ] Minutes ([ ] 分間非アクティブであった場合、リモート診断セッションを自動的に終了する)	リモート実行セッションが、指定した時間非アクティブであった場合にセッションが終了されます。

9 ［*次へ*］をクリックすると、［ファイル転送設定］ページが表示されます。デフォルト設定を受け入れる場合は、次のステップに進みます。または次の表に示す情報を参照してデフォルトのセキュリティ設定を変更します。

フィールド	詳細
管理対象デバイスでファイル転送を許可	管理コンソールと管理対象デバイス間でのファイルを転送を可能にします。このオプションを選択すると、ページ上の次のオプションが有効になります。このオプションを選択解除すると、デバイスでのファイル転送操作が無効になります。
ファイル転送の開始前に、管理対象デバイス上のユーザからの許可を求める	ファイル転送セッションの開始前に管理対象デバイスのユーザからの許可をリモートオペレータが求めるようにします。
ファイル転送中に、管理対象デバイス上のユーザに可視信号が送信される	ファイル転送セッション中に、管理対象デバイスデスクトップの右上端に可視信号が表示されます。可視信号を使用すると、管理対象デバイスのユーザはファイル転送セッションが実行中であることが分かります。

フィールド	詳細
管理対象デバイスからファイルをダウンロード可能	リモートオペレータが管理対象デバイス上のファイルを開き、それらのファイルを管理コンソールに転送することができます。このオプションを選択していない場合、リモートオペレータは管理コンソースから管理対象デバイスへのみファイルを転送できます。
ファイル転送ルートディレクトリ	ファイル転送セッション中に、リモートオペレータが管理対象デバイスのディレクトリを確認できるように指定します。リモートオペレータは、このディレクトリとそのサブディレクトリについてのみ、ファイルを転送できます。デフォルトのディレクトリはマイコンピュータです。つまり、リモートオペレータは、管理対象デバイスの全ファイルシステム内のファイルを確認し、転送することができます。

10 ［*次へ*］をクリックすると、［セキュリティの設定］ページが表示されます。デフォルト設定を受け入れる場合は、次のステップに進みます。または次の表に示す情報を参照してデフォルトのセキュリティ設定を変更します。

パスワード認証

フィールド	詳細
パスワードベースの認証を有効にする	リモートオペレータがパスワードを使用して管理対象デバイスからの認証を受けられるようにします。パスワードタイプ設定を設定する場合に、このオプションを選択します。
最小パスワード長	パスワードの最小長を指定できるようになります。デフォルトでは、6 文字です。
セッションのパスワード	管理対象デバイスのユーザに、新しいリモートセッションを開始する前に、パスワードを設定するように指示するには、このオプションを選択します。パスワードは管理対象デバイスに保存されず、現在のセッションのみで有効なので、このオプションをお勧めします。
永続的なパスワード	ZENworks パスワードと VNC パスワードを設定する場合にこのオプションを選択します。ZENworks パスワードのほうが VNC パスワードより安全であるため、ZENworks パスワードを設定することをお勧めします。このパスワードは、管理者がリモート管理ポリシーを通じて設定するか、管理対象デバイスユーザが ZENworks アイコンから設定することができます。このオプションを選択すると、後続のオプションが有効になります。 ユーザが ZENworks アイコンからパスワードを設定できるようにするには、［*ユーザが管理対象デバイスのデフォルトのパスワードを上書きすることを許可する*］オプションを選択します。

フィールド	詳細
ZENworks パスワード	ZENworks パスワードをクリアする 1. ［*パスワードをクリア*］をクリックします。 2. ［*適用*］をクリックし、［*OK*］をクリックします。 ZENworks パスワードを設定する 1. ［*パスワードを設定する*］をクリックします。 2. パスワードを入力します。パスワードの最大長は 255 文字です。 3. ［*適用*］をクリックし、［*OK*］をクリックします。
VNC のパスワード	VNC のパスワードをクリアする 1. ［*パスワードをクリア*］をクリックします。 2. ［*適用*］をクリックし、［*OK*］をクリックします。 VNC のパスワードを設定する 1. ［*パスワードを設定する*］をクリックします。 2. パスワードを入力します。パスワードの最大長は 8 文字です。 3. ［*適用*］をクリックし、［*OK*］をクリックします。

不正侵入者検出

フィールド	詳細
不正侵入者検出を有効にする	無効な、または許可されていない、管理対象デバイスでもリモートセッションの起動要求を検出できるようにするには、このオプションを選択します。このオプションを選択すると、［不正侵入者検出］セクションの後続のオプションが有効になります。
Suspend Accepting Connections After [ ] Successive Invalid Attempts (無効な試行が [ ] 回連続した場合に接続受諾を一時停止)	管理対象デバイスのリモート管理サービスがブロックされるまでに、リモートオペレータに許可される連続する無効な最大試行回数を指定します。デフォルトでは、試行回数は 5 回です。
Automatically Start Accepting Connections After [ ] Minutes ([ ] 分後に接続受諾を自動開始)	リモート管理エージェントが管理対象デバイスとの接続を自動的に受け入れるまでの時間を指定します。リモート管理サービスを手動でブロック解除するには、ZENworks Adaptive Agent アイコンをダブルクリックして、［*セキュリティの設定*］をクリックします。次に、［*侵入者検出によって現在ブロックされている場合は、接続の受諾を許可します*］*をクリックします。*デフォルトでは、10 分です。

セッションのセキュリティ

フィールド	詳細
セッションの暗号化を有効にする	SSL 暗号化 (TLSv1 プロトコル) を使用したセッション暗号化を有効にします。このオプションを選択すると、［セッションのセキュリティ］セクションの後続のオプションが有効になります。

フィールド	詳細
リモート管理コンソールに SSL 証明書がない場合は、接続を許可する	ZENworks コントロールセンターからリモートセッションを起動すると、リモートオペレータの証明書が自動的に生成されます。この証明書は認証の間使用されます。SSL 証明書がない恐れのある ZENworks コントロールセンター外で起動されたリモート管理コンソールからの接続を許可するには、このオプションを選択します。
最大 [ ] レベルをビューア証明書チェーンで許可する	Novell 権およびパスワードベースの認証スキームが、SSL で暗号化されたチャンネルで行われます。このチャンネルを確立するには、ビューアは証明書を提供する必要があります。この証明書は、中間またはルート認証局により署名されることで、証明書チェーンを作成します。 このプロパティは、ビューアの証明書チェーンで許可される最大レベル数を定義します。ZENworks 内部認証局が使用されている場合 (デフォルトでインストールされます)、ZENworks コントロールセンターからリモートセッションを起動するときに、2 レベルのビューア証明書チェーンが自動的に作成されます。

異常終了

フィールド	詳細
デバイスのロック	リモートセッションが異常終了した場合に、管理対象デバイスをロックします。
ユーザのログオフ	リモートセッションが異常終了した場合に、管理対象デバイスのユーザをログオフします。

11 ［*次へ*］をクリックし、［概要］ページを表示します。

12 ［*終了*］をクリックし、ポリシーを今すぐ作成するか、［*作成後に詳細を設定*］を選択し、ポリシー割り当て、施行、ステータス、およびポリシーの属するグループなどの追加情報を指定します。

2.4 リモートオペレータ権限の設定

権限をリモートオペレータに割り当てると、管理対象デバイスでリモートセッションを実行できます。リモートオペレータは、デバイス固有の権限およびユーザ固有の権限を持つことができます。

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 ［管理者］パネルから、リモート管理権限を割り当てる管理者の名前をクリックします。

3 ［割り当てられた権限］パネルで、［*追加*］をクリックしてから［*リモート管理権*］をクリックします。［リモート管理権］ダイアログボックスが表示されます。

4 権限を割り当てるデバイスまたはユーザを選択します。

次の表にリモート管理権についての説明を示します。

リモート管理権限	詳細
リモートコントロール	デバイスをリモートからコントロールする権限をリモートオペレータに割り当てます。
リモートビュー	デバイスをリモートから参照する権限をリモートオペレータに割り当てます。
リモート診断	デバイスをリモートから診断する権限をリモートオペレータに割り当てます。
リモート実行	リモートからデバイス上でアプリケーションを実行する権限をリモートオペレータに割り当てます。
ファイルの転送	デバイスとの間でファイルを転送する権限をリモートオペレータに割り当てます。
リモート管理サービスのブロック解除	不正侵入者を検出したためにロックされたリモート管理サービスをブロック解除する権限をリモートオペレータに割り当てます。

注 : リモート管理の権限は権限ベースの認証に対してのみ適用可能です。ただし、リモート管理ポリシーが許可されている場合、パスワードベース認証を使用してリモート操作を実行できます。

5 ［*OK*］をクリックします。

2.5 リモート管理パスワードの設定

次のセクションでは、管理対象デバイスに対するリモート管理サービスのリモート管理パスワードの設定について説明します。

- 31 ページのセクション 2.5.1「ZENworks コントロールセンターを使用したリモート管理パスワードのセットアップ」
- 32 ページのセクション 2.5.2「ZENworks Adaptive Agent を使用したリモート管理パスワードのセットアップ」
- 33 ページのセクション 2.5.3「ZENworks コントロールセンターを使用したリモート管理パスワードのクリア」
- 33 ページのセクション 2.5.4「ZENworks Adaptive Agent を使用したリモート管理パスワードのクリア」

2.5.1 ZENworks コントロールセンターを使用したリモート管理パスワードのセットアップ

管理者は、リモート管理ポリシーの作成時またはポリシー作成後に、［セキュリティの設定］ページでリモート管理パスワードを設定できます。

リモート管理ポリシーの作成中にパスワードを設定する方法は、23 ページのセクション 2.3「リモート管理ポリシーの作成」を参照してください。

リモート管理ポリシーのパスワードを編集するには、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*］をクリックします。

2 リモート管理ポリシーをクリックし、次に［*設定*］タブをクリックします。

3 ［セキュリティ設定］パネルで、パスワードを選択し、新しいパスワードと置換します。

4 ［*適用*］をクリックします。

5 ［概要］ページまたは［共通タスク］でこのポリシーのバージョンをカウントアップして、管理対象デバイスのパスワードの変更内容を更新します。

リモート管理ポリシー作成後にパスワードを設定するには、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*］をクリックします。

2 リモート管理ポリシーをクリックし、次に［*設定*］タブをクリックします。

3 ［セキュリティ設定］パネルで、［*パスワードベースの認証を有効にする*］を選択し、次に［*ローカルに保存*］を選択します。

4 ［*パスワードの設定*］をクリックし、パスワードを指定します。リモート管理ポリシーの作成時にすでにパスワードが設定されている場合は、パスワードを編集できます。パスワードを編集するには、パスワードを選択し、新しいパスワードと置換します。

5 ［*適用*］をクリックします。

6 ［概要］ページまたは［共通タスク］でこのポリシーのバージョンをカウントアップして、管理対象デバイスのパスワードの変更内容を更新します。

2.5.2 ZENworks Adaptive Agent を使用したリモート管理パスワードのセットアップ

管理対象デバイスのユーザは、その管理対象デバイスで有効なリモート管理ポリシーによって、［*ユーザが管理対象デバイスのデフォルトのパスワードを上書きすることを許可する*］オプションが有効にされている場合は、リモート管理サービスのパスワードを設定できます。このパスワードはリモート管理ポリシーに設定されているパスワードより優先されます。

管理対象デバイスでパスワードを設定する

1 ［*ZENworks Adaptive Agent*］アイコンをクリックして［ZENworks Adaptive Agent］ウィンドウを表示します。

2 左ペインで［*リモート管理*］にナビゲートし、［*セキュリティ*］をクリックします。

3 右ペインで［*パスワードの設定*］をクリックして次のパスワードを設定します。

- **ZENworks パスワード (推奨):** ZENworks 認証で使用されます。パスワードの長さは最大 255 文字です。
- **VNC のパスワード :** オープンソース VNC ビューアとの相互運用性を目的とする VNC 認証に使用されます。パスワードの長さは最大 8 文字です。

4 ［*OK*］をクリックします。

2.5.3 ZENworks コントロールセンターを使用したリモート管理パスワードのクリア

ポリシーを使用して設定されたリモート管理パスワードをクリアするには、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*］をクリックします。
2. リモート管理ポリシーをクリックし、次に［*設定*］タブをクリックします。
3. ［セキュリティの設定］パネルで［*パスワードをクリア*］、［*適用*］の順にクリックします。
4. ［概要］ページまたは［共通タスク］でこのポリシーのバージョンをカウントアップして、管理対象デバイスのポリシーに変更内容が更新されるようにします。

管理対象デバイスユーザによって設定されたリモート管理パスワードをクリアする手順 :

1. ZENworks コントロールセンターで、［*ポリシー*］をクリックします。
2. リモート管理ポリシーをクリックし、次に［*設定*］タブをクリックします。
3. ［セキュリティの設定］パネルで［*ユーザが管理対象デバイスのデフォルトのパスワードを上書きすることを許可する*］オプションを選択解除してから、［*適用*］をクリックします。
4. ［概要］ページまたは［共通タスク］でこのポリシーのバージョンをカウントアップして、管理対象デバイスのポリシーに変更内容が更新されるようにします。

2.5.4 ZENworks Adaptive Agent を使用したリモート管理パスワードのクリア

管理対象デバイスのユーザは、以前に自身が設定したリモート管理パスワードをリセットできます。

1. ［*ZENworks Adaptive Agent*］アイコンをクリックして［ZENworks Adaptive Agent］ウィンドウを表示します。
2. 左ペインで［*リモート管理*］にナビゲートし、［*セキュリティ*］をクリックします。
3. 右ペインで［*パスワードをクリア*］をクリックしてパスワードをクリアします。
4. ［*OK*］をクリックします。

ユーザによってパスワードが設定されていないため、ポリシーに設定されたパスワードが有効になります。

2.6 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は、リモートオペレータが管理対象デバイス上でリモート操作を実行できるようにする管理コンソールアプリケーションです。リモートオペレータが管理対象デバイスデスクトップを表示したり、ファイルを転送したり、管理対象デバイス上でアプリケーションを実行できるようにします。

リモート管理ビューアをインストールするには、管理対象デバイス上でリモート管理操作を実行しているときに、ZENworks コントロールセンターに表示される［*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ます。このリンクが表示されるのは、管理対象デバイスでリモート管理操作を初めて実行し、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。

リモート管理ビューアの以前のバージョンがデバイスにインストール済みの場合は、［*リモート管理ビューアのアップグレード*］リンクが表示されます。このリンクをクリックして、デバイスにインストールされたビューアのバージョンをアップグレードします。

注 : SLES 11 (SUSE® Linux Enterprise Server 11) または SLED 11 (SUSE Linux Enterprise Desktop 11) にリモート管理ビューアをインストールするには、依存する glitz パッケージが必要です。該当する glitz パッケージを openSUSE® Web サイト (http://software.opensuse.org/112/en) からインストールする必要があります。

Windows の場合 :

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. 左のナビゲーションペインで、［*ZENworks ツールのダウンロード*］をクリックします。
3. ZENworks ダウンロードページの左のナビゲーションページで、［*管理ツール*］をクリックします。
4. novell-zenworks-rm-viewer-<*バージョン*>.msi をクリックします。
5. (条件付き)Internet Explorer* を使用して ZENworks コントロールセンターを起動した場合は、次の手順のいずれかを実行します。
   - ［*実行*］をクリックしてビューアをインストールします。
   - ［*保存*］をクリックして、ファイルを一時的に適当な場所に保存します。ファイルをダブルクリックしてビューアをインストールします。
6. (条件付き)Firefox を使用して ZENworks Control Center を起動した場合は、［*ファイルの保存*］をクリックして、ファイルを適当な場所に一時的に保存し、ファイルをダブルクリックしてビューアをインストールします。

Linux の場合 :

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. 左のナビゲーションペインで、［*ZENworks ツールのダウンロード*］をクリックします。
3. ZENworks ダウンロードページの左のナビゲーションページで、［*管理ツール*］をクリックします。
4. novell-zenworks-rm-viewer-<*バージョン*>.noarch.rpm をクリックします。
5. ビューアを今すぐインストールするか、ビューアの RPM ファイルを保存して後でインストールするかを指定します。
   - ビューアをすぐにインストールするには、［*Open With(開くアプリケーション)*］をクリックしてリモート管理ビューアを zen-installer で開き、ルートパスワードを指定して［*OK*］をクリックします。

- ビューア RPM ファイルをデフォルトのダウンロードディレクトリに保存して後でインストールするには、［*Save to Disk(ディスクに保存する)*］をクリックします。RPM をインストールするには、次のいずれかの手順を実行します。
  - ビューアの RPM ファイルをクリックしてルートパスワードを指定し、［*OK*］をクリックします。
  - 次のコマンドをスーパーユーザまたはルートユーザとして実行します。

    rpm -ivh novell-zenworks-rm-viewer-< バージョン >.noarch.rpm

2.7 リモート管理ビューアのアップグレード

以前のバージョンのリモート管理ビューアがすでにインストールされている Windows 管理対象デバイスでリモート管理操作を実行する場合は、ZENworks コントロールセンターに［*リモート管理ビューアのアップグレード*］リンクが表示されます。このリンクをクリックして、デバイスにインストールされたビューアのバージョンをアップグレードします。

Linux デバイス上のリモート管理ビューアを Novell ZENworks 10 Configuration Management SP2 (10.2) から Novell ZENworks 10 Configuration Management SP3 (10.3) 以上にアップグレードするには、次のコマンドをスーパーユーザまたはルートユーザとして実行します。

rpm -Uvh --nopostun novell-zenworks-rm-viewer-<version>.noarch.rpm

または、古いバージョンの novell-zenworks-rm-viewer-10.x.x.rpm をアンインストールし、新しいバージョンをインストールします。ビューアのインストールの詳細については、33 ページのセクション 2.6「リモート管理ビューアのインストール」を参照してください。

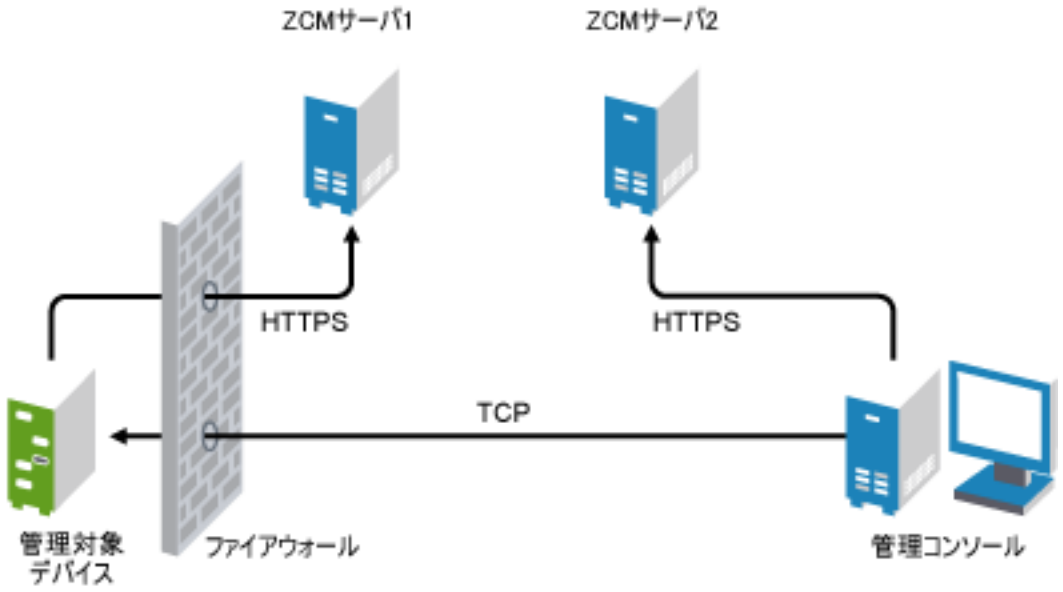
2.8 リモート管理操作の開始

リモート管理操作は、次の方法で開始できます。

2.8.1 管理コンソールからのセッションの開始

このシナリオでは、リモートセッションは管理コンソールの管理者によって開始されます。管理コンソールは通常、エンタープライズのネットワーク内に配置されており、管理対象デバイスはエンタープライズのネットワーク内部または外部のどちらにでも配置できます。次の図は、管理コンソールから管理対象デバイスで開始されるリモートセッションを示しています。

図 2-1 コンソールで開始されたセッション



リモート管理エージェントは、管理対象デバイスのブート時に自動的に起動されます。デフォルトのリモート管理ポリシーは、デバイスの展開時に管理対象デバイスで作成されます。このデフォルトポリシーを使用して権利ベース認証モードでのみリモートでデバイスを管理できます。新規のリモート管理ポリシーを作成する場合、新しいポリシーはデフォルトポリシーを上書きします。

パブリックネットワークによって相互接続した複数の NAT 対応プライベートネットワークにわたって ZENworks 管理ゾーンセットアップを広げた場合、これらのプライベートネットワークのゲートウェイで DNS_ALG を展開する必要があります。DNS_ALG は、ZENworks コンポーネントによって開始された DNS ルックアップクエリにより、ホスト名に対応した正しいプライベートアドレスが返されるようにし、管理コンソールと管理対象デバイス間の通信を実現します。DNS_ALG の詳細については、DNS ALG RFC - 2694 (http://www.ietf.org/rfc/rfc2694) を参照してください。

DNS 名を使用してデバイスをリモート管理するには、ダイナミック DNS サービスがネットワークに展開されていることを確認します。

リモートオペレータは、次のいずれかの方法でセッションを開始することができます。

- 36 ページの 「ZENworks コントロールセンターでのリモート管理操作の開始」
- 42 ページの 「スタンドアロンモードでのリモート管理操作の開始」
- 43 ページの 「コマンドラインオプションを使用してのリモート管理操作の開始」

ZENworks コントロールセンターでのリモート管理操作の開始

デバイスコンテキストまたはユーザコンテキストからさまざまなリモート管理操作を開始できます。

- 37 ページの 「デバイスコンテキストからリモート管理セッションを開始する」
- 39 ページの 「ユーザコンテキストからリモート管理セッションを開始する」

デバイスコンテキストからリモート管理セッションを開始する

デバイス上のリモート管理セッションを開始する方法

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*］または［*ワークステーション*］をクリックしてから、リモート管理するデバイスを選択します。［*適用*］をクリックしてから、実行するリモート管理操作を選択します。

   または

   左ペインの［*デバイスタスク*］で、実行するリモート管理操作を選択します。

   次のリモート操作を使用できます。

   - **リモートコントロール :**［リモート管理］ダイアログボックスが表示され、管理対象デバイスに対してリモートコントロール操作、リモートビュー操作、およびリモート実行操作を実行できます。
   - **リモート診断 :**［リモート診断］ダイアログボックスが表示され、管理対象デバイスに対してリモート診断操作を実行できます。
   - **ファイルの転送 :**［ファイルの転送］ダイアログボックスが表示され、管理対象デバイスに対してファイルの転送操作を実行できます。
3. 表示されるダイアログボックスのオプションに入力します。次の表に、選択可能なさまざまなオプションを示します。

フィールド	詳細
デバイス	リモートで管理するデバイスのホスト名または IP アドレスを指定します。
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を選択します。このオプションは［リモート管理］ダイアログボックスでのみ使用できます。
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。このオプションは［リモート診断］ダイアログボックスでのみ使用できます。
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。次の認証モードを使用できます。 ◆ 権限ベース認証 ◆ パスワードベース認証
ポート	リモート管理サービス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。このモードでは、デフォルトでリモートコントロール操作用に選択されます。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権限を取得します。 ◆ 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 続いて起動されるセッションは、リモートビューセッションです。 **注 :** 協同モードは Linux ではサポートされていません。 ◆ **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。このモードでは、デフォルトでリモート表示操作用に選択されます。 このオプションは［リモート管理］ダイアログボックスでのみ使用できます。
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。
キャッシング有効化	リモート管理セッションデータのキャッシングを有効にしてパフォーマンスを向上させます。このオプションは、リモート制御操作、リモートビュー操作、およびリモート診断操作で使用できます。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大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、リモート制御操作、リモートビュー操作、およびリモート診断操作で使用できます。

フィールド	詳細
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 (ZCC) を起動した場合はデスクトップであり、Mozilla* FireFox* から ZCC 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リモート管理プロキシ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、あるいは 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リモート管理プロキシ経由でルーティングできます。このオプションは現在 Windows でのみサポートされています。 次のフィールドに入力します。 **代理 :** リモート管理プロキシの 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がこのフィールドに指定されます。別のプロキシを指定できます。 **プロキシポート :** リモート管理プロキシ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。 **注 :** リモート管理監査は、管理コンソールの IP アドレスではなくリモート管理プロキシを実行しているデバイスの IP アドレスを表示します。
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、PFX です。PFX フォーマットを使用している場合、鍵と証明書の両方が同じファイルにある必要があります。このファイルを鍵と証明書の両方の入力として指定する必要があります。 **キャッシュパスの有効化 :** プライマリキーと証明書のパスを管理コンソールにキャッシュできるようにします。 このオプションは現在 Windows でのみサポートされています。

4 ［*OK*］をクリックして、選択したリモート操作を起動します。

ユーザコンテキストからリモート管理セッションを開始する

リモートセッションを実行することにより、管理対象デバイスにログインしているユーザを支援する手順 :

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

2 ［*ユーザソース*］をクリックします。

3 リモート管理する管理対象デバイスにログインしているユーザを選択します。

4 ［*アクション*］をクリックしてから、実行するリモート管理操作を選択します。

次の操作を使用できます。

- **リモートコントロール :**［リモート管理］ダイアログボックスが表示され、管理対象デバイスに対してリモートコントロール操作、リモートビュー操作、およびリモート実行操作を実行できます。
- **リモート診断 :**［リモート診断］ダイアログボックスが表示され、管理対象デバイスに対してリモート診断操作を実行できます。
- **ファイルの転送 :**［ファイルの転送］ダイアログボックスが表示され、管理対象デバイスに対してファイルの転送操作を実行できます。

5 表示されるダイアログボックスのオプションに入力します。次の表に、選択可能なさまざまなオプションを示します。

フィールド	詳細
デバイス	リモートで管理するデバイスのホスト名または IP アドレスを指定します。
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を選択します。このオプションは［リモート管理］ダイアログボックスでのみ使用できます。
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。このオプションは［リモート診断］ダイアログボックスでのみ使用できます。
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。次の認証モードを使用できます。 ◆ 権限ベース認証 ◆ パスワードベース認証
ポート	リモート管理サービス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。このモードでは、デフォルトでリモートコントロール操作用に選択されます。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権限を取得します。 ◆ 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 続いて起動されるセッションは、リモートビューセッションです。 **注 :** 協同モードは Linux ではサポートされていません。 ◆ **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。このモードでは、デフォルトでリモート表示操作用に選択されます。 このオプションは［リモート管理］ダイアログボックスでのみ使用できます。
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。
キャッシング有効化	リモート管理セッションデータのキャッシングを有効にしてパフォーマンスを向上させます。このオプションは、リモート制御操作、リモートビュー操作、およびリモート診断操作で使用できます。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大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、リモート制御操作、リモートビュー操作、およびリモート診断操作で使用できます。

フィールド	詳細
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 (ZCC) を起動した場合はデスクトップであり、Mozilla* FireFox* から ZCC 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リモート管理プロキシ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、あるいは 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リモート管理プロキシ経由でルーティングできます。このオプションは現在 Windows でのみサポートされています。 次のフィールドに入力します。 **代理 :** リモート管理プロキシの 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がこのフィールドに指定されます。別のプロキシを指定できます。 **プロキシポート :** リモート管理プロキシ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。 **注 :** リモート管理監査は、管理コンソールの IP アドレスではなくリモート管理プロキシを実行しているデバイスの IP アドレスを表示します。
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、PFX です。PFX フォーマットを使用している場合、鍵と証明書の両方が同じファイルにある必要があります。このファイルを鍵と証明書の両方の入力として指定する必要があります。 **キャッシュパスの有効化 :** プライマリキーと証明書のパスを管理コンソールにキャッシュできるようにします。 このオプションは現在 Windows でのみサポートされています。

6 ［*OK*］をクリックすると選択したリモート操作が起動します。

スタンドアロンモードでのリモート管理操作の開始

リモート管理操作をスタンドアロンモードで開始する前に、リモート管理ビューアをインストールします。ビューアのインストールの詳細については、33 ページのセクション 2.6「リモート管理ビューアのインストール」を参照してください。

スタンドアロンモードでリモート管理操作を開始するには、次の手順に従います。

1. nzrViewer.exe ファイルをダブルクリックして ZENworks Remote Management クライアントを起動します。
2. 表示された［ZENworks Remote Management の接続］ウィンドウに、管理対象デバイスの DNS 名または IP アドレスと、ポート番号を指定します。「*IP アドレス~~ ポート*」というフォーマットを使用してください。たとえば、「10.0.0.0~~1000」です。
3. リモート管理プロキシの DNS 名または IP アドレスとポート番号を次の形式で指定します。
   - *IP アドレス~~ ポート*. 例 :10.0.0.0~~5750
   - *IP アドレス~ ポート*例 :10.0.0.0~50
4. ［*接続*］をクリックします。

   認証が正常に実行されると、リモートセッションが開始されます。デフォルトでは、リモートコントロールセッションが起動されます。

コマンドラインオプションを使用してのリモート管理操作の開始

コマンドラインからリモート管理操作を開始する前に、リモート管理ビューアをインストールします。ビューアのインストールの詳細については、33 ページのセクション 2.6「リモート管理ビューアのインストール」を参照してください。

コマンドラインオプションを使用してリモート管理操作を開始するには、次の手順に従います。

1. コマンドプロンプトで、現在のディレクトリをビューアがインストールされているディレクトリに変更します。ビューアは、デフォルトで、<*User_Application_Data_Folder*>\Novell\ZENworks\Remote Management\bin ディレクトリにインストールされます。
2. 次のコマンドを実行します。

   nzrViewer [*/options<parameters if any>*][*IP address of the managed device*] [*~~port*]

   管理対象デバイスのデフォルトポートは、5950 です。

   使用できるコマンドラインオプションについては、45 ページのセクション 2.9.1「リモート操作を起動するコマンドラインオプション」を参照してください。
3. ［*接続*］をクリックします。

   認証が正常に実行されると、リモートセッションが開始されます。コマンドラインでリモート操作のタイプを指定しないと、デフォルトでリモートコントロールセッションが起動されます。

ただし、コマンドラインオプションを使用してリモート管理操作を起動する場合、次の制限があります。

- コマンドラインオプションの key、cert、および CAcert を、SSL 認証の nzrViewer コマンドで指定したくない場合は、リモート管理ポリシーのセキュリティ設定で［*リモート管理コンソールに SSL 証明書がない場合は、接続を許可する*］オプションが有効になっているようにします。ただし、デバイスのセキュリティが低下するため、これは推奨されません。
- 管理対象デバイスが管理ゾーンに含まれる場合、ビューアが提示する証明書が有効で署名済みであり、CA に関連付けられていることを確認してください。そうでない場合、SSL 認証が失敗します。

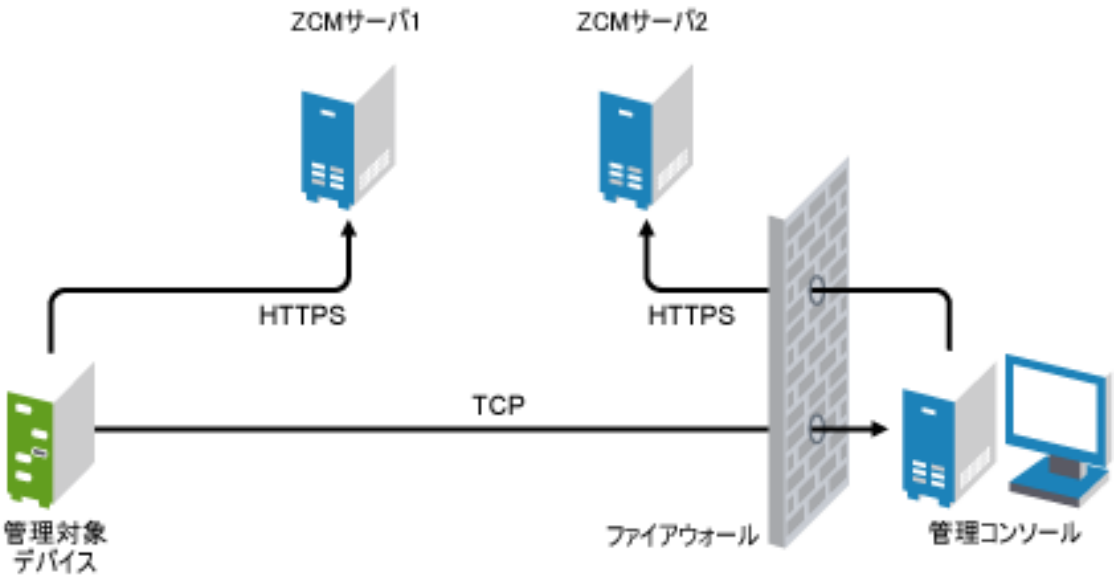
注 : ZENworks コントロールセンター (ZCC) からリモートセッションを起動すると、ZCC が自動的に証明書を生成し、ビューアに渡してセッションを起動します。証明書の有効期間は 4 日間だけです。

- 管理対象デバイスはビューアが指定する証明書を使用して、リモートオペレータを特定します。ビューアが証明書を指定しない場合、ユーザは特定されず、許可メッセージ、表示信号、監査ログで*不明*と記録されます。

2.8.2 管理対象デバイスからのセッションの開始

このシナリオでは、リモートセッションは管理対象デバイスのユーザによって開始されます。これは管理コンソールが管理対象デバイスと接続できない場合に便利です。次の図は、管理対象デバイスのユーザによって開始されたリモートセッションを示しています。

図 2-2 *エージェントで開始されたセッション*



管理対象デバイスのユーザは、次の場合にデバイスでリモートセッションを実行するようリモートオペレータに要求できます。

- リモートオペレータが、ユーザからのリモートセッション要求をリスンするためのリモート管理リスナを起動している。
- リモート管理ポリシーで、[*ユーザにリモートセッション要求を許可する*] オプションが有効化されている。
- リモート管理リスナがリモート接続をリスンするためのポートは、管理コンソールファイアウォールで開いている必要がある。デフォルトのポートは 5550 です。

セッションを要求する

1. 通知領域にある ZENworks アイコンをダブルクリックします。
2. 左ペインで [*リモート管理*] にナビゲートし、[*一般*] をクリックします。
3. [*リモート管理セッションの要求*] をクリックして、[セッションの要求] ダイアログボックスを表示します。

状況によっては、リモートオペレータによるリモート管理セッションを要求する場合や、リモートオペレータからセッションの開始を要求される場合があります。[*リモート管理セッションを要求*] オプションがリンクテキストとして表示されない場合、オプションは無効です。

4 [*リモート操作のリスニング*] リストで、リモートオペレータを選択してリモートセッションを開きます。

または

リモートオペレータが表示されていない場合は、[*接続要求*] フィールドにオペレータの接続情報を設定します。

5 [*操作*] フィールドで、開く操作のタイプ (リモートコントロール、リモートビュー、リモート診断、ファイル転送、またはリモート実行) を選択します。

各操作の詳細については、12 ページのセクション 1.2「リモート管理操作の理解」を参照してください。

6 [*要求*] をクリックして、セッションを起動します。

パブリックネットワークからプライベートネットワークへの接続を許可する場合は、DNS アプリケーションレベルゲートウェイ (DNS_ALG) を展開してください。DNS_ALG の詳細については、RFC 2694 (http://www.ietf.org/rfc/rfc2694) を参照してください。

2.9 リモート管理操作の開始に関するオプション

リモート管理操作をコマンドラインから開始する際には、リモートセッションの動作を制御するオプションを指定できます。たとえば、remotecontrol オプションを指定すると、リモート管理操作がデバイスで開始され、notoolbar オプションを指定すると、表示ウィンドウのツールバーが非表示になります。

デバイス上でリモート管理操作を開始すると、リモート管理は、内部的に一定のオプションを使用します。たとえば、zenrights オプションは、認証スキームが ZENworks 権限認証になるように指定します。これらの内部オプションは、リモート管理の操作をデバイス上で開始するのにコマンドラインを使用する場合には指定しないでください。内部的に使用されるオプションの詳細については、48 ページのセクション 2.9.2「リモート操作の開始に関する内部オプション」を参照してください。

リモート管理オプションの詳細については、次の各セクションを確認してください。

- 45 ページのセクション 2.9.1「リモート操作を起動するコマンドラインオプション」
- 48 ページのセクション 2.9.2「リモート操作の開始に関する内部オプション」

2.9.1 リモート操作を起動するコマンドラインオプション

リモート操作を制御するには、次のコマンドラインオプションを使用します。

表 2-1 *リモート操作を起動するコマンドラインオプション*

コマンドラインオプション	パラメータ	説明
listen	*port*	リスナが指定されたポートでリモートセッション要求をリスンできるようにします。デフォルトでは、ポートは 5550 です。

コマンドラインオプション	パラメータ	説明
restricted		ツールバーおよびシステムメニューを非表示にします。
viewonly		管理対象デバイスでリモート表示操作を起動します。
remotecontrol		管理対象デバイスでリモートコントロール操作を起動します。
ftponly		管理対象デバイスでファイル転送操作を起動します。
remoteexecute		管理対象デバイスでリモート実行操作を起動します。
diagnostics	*appname*	管理対象デバイスでリモート診断操作を起動します。appname パラメータが指定されると、管理対象デバイスではそのアプリケーションが起動されます。
filecompressionlevel	*level*	ファイル転送操作時の速度および圧縮率を上げるため、ファイル圧縮処理を最適化する方法を提供します。アッシュレベルは 0 まで 9 あります。 ◆ 0 は圧縮しないことを示します。 ◆ 1 は速度が一番速いことを示します。 ◆ 9 は圧縮率が一番高いことを示します。 圧縮レベルが指定されていないと、デフォルトの圧縮レベル 6 が使用されます。これは速度と圧縮の両方を最適化した値です。
noencrypt		非暗号化モードでリモートセッションを起動します。
fullscreen		管理対象デバイスでフルスクリーンモードでリモート操作を起動します。
notoolbar		表示ウィンドウのツールバーを非表示にします。
exclusive		排他モードでリモートセッションを起動します。
8bit		セッションデータをレンダリングするのに使用する色の深さを指定します。
shared		共有接続を有効にし、デスクトップをすでに使用している他のクライアントと共有できるようにします。デフォルトでは、このオプションは True です。
collaborate		コラボレーションモードでリモートセッションを起動します。このオプションは Linux ではまだサポートされていません。
noshared		非共有接続を有効にし、サーバの設定に応じて、接続されている他のクライアントを切断するかまたは接続を拒否します。
swapmouse		マウスのボタンを切り替えます。
nocursor		管理対象デバイスのマウスポインタだけを表示します。ローカルのマウスポインタは表示されません。
dotcursor		ローカルのマウスポインタをドットとして表示します。デフォルトでは、このオプションは True です。
smalldotcursor		ローカルのマウスポインタを小さなドットとして表示します。
normalcursor		ローカルのマウスポインタをデフォルトの形で表示します。

コマンドラインオプション	パラメータ	説明
belldeiconify		ビューアでビープ音を鳴らす、ベル文字の転送を許可します。このオプションによって、ベル文字が受信されるときに最大化される VNCviewer を最小化します。
emulate3		ボタンが 2 つあるマウスを使用しているユーザは、両方のボタンを同時に押下することによって真ん中のボタンをエミュレートできます。デフォルトでは、このオプションは True です。
noemulate3		3 つボタンのマウスをエミュレートしません。
nojpeg		ロッシーな JPEG 圧縮を使用不可にします。これはエンコーダの効率が低下するためお勧めしません。完璧な画像品質を求めるためどうしても必要な場合にのみこのオプションを使用してください。
nocursorshape		リモートのカーソル移動を処理するカーソルシェイプの更新を無効にします。カーソルシェイプの更新を使用すると、リモートカーソル移動での遅延を減らすことができ、帯域幅の使用量を大幅に改善できます。
noremotecursor		リモートカーソルを表示しません。
fitwindow		表示ウィンドウのスクロールバーを非表示にします。
scale	*percentage*	指定されたスケールのパーセンテージまで表示ウィンドウを拡大縮小します。
emulate3timeout	*ms*	3 つボタンマウスをエミュレートするタイムアウト時間を指定します。
disableclipboard		クリップボードへのデータのコピーを使用不可にします。
delay		表示領域をレンダリングし、時間の更新を取得するまで指定された時間待機します。
loglevel	*n*	記録する情報のレベルを指定します。
console		コンソールウィンドウに情報を記録します。
logfile	*filename*	情報が記録されるログファイルの名前。
config	*filename*	事前定義された環境設定をロードするのに使用する環境設定ファイルの名前。
key	*filename*	秘密鍵が保存されているファイルの名前。このキーは、管理対象デバイスでの SSL ハンドシェークの際に使用されます。 **重要 :** キーと cert オプションは、同時に使用される必要があります。これらのオプションを nzrViewer コマンドと一緒に使用する場合、セキュリティ上の理由により、リモート管理ポリシーのセキュリティ設定で［*リモート管理コンソールに SSL 証明書がない場合は、接続を許可する*］オプションを無効化する必要があります。

コマンドラインオプション	パラメータ	説明
cert	*filename*	秘密鍵に対応する証明書が保存されているファイルの名前。 **重要 :** キーと cert オプションは、同時に使用される必要があります。これらのオプションを nzrViewer コマンドと一緒に使用する場合、セキュリティ上の理由により、リモート管理ポリシーのセキュリティ設定で［*リモート管理コンソールに SSL 証明書がない場合は、接続を許可する*］オプションを無効化する必要があります。
CAcert	*filename*	ルート証明書が保存されているファイルの名前。この証明書は、SSL ハンドシェークの際に管理対象デバイス証明書を確認するために使用されます。
encoding	*encname*	セッションで使用する目的のエンコードを指定します。エンコードのタイプは、Raw、CopyRect、RRE、CoRRE、Hextile、Zlib、および Tight です。
compresslevel	*n*	リモートセッションデータを圧縮する圧縮レベルを 0 ～ 9 で選択します。レベル 1 では、使用する CPU 時間は最小となり、圧縮率は低くなります。またレベル 9 では最大の圧縮率を実現しますが、サーバ側での CPU 時間は遅くなります。非常に遅いネットワークでは高いレベルを使用し、高速 LAN で作業する場合は低いレベルを使用してください。圧縮レベル 0 は使用しないようお勧めします。
quality	*n*	JPEG の品質を 0 から 9 の範囲で指定します。品質レベル 0 はイメージの品質は劣りますが圧縮率は非常に高くなります。レベル 9 はイメージ品質は非常に高くなりますが圧縮率は低くなります。
zenpasswd		使用される認証スキーマは、ZENworks パスワード認証であることを指定します。
locale		リソースが表示されるロケールを指定します。デフォルトでは、英語が使用されます。このオプションの値は、英語、フランス語、ドイツ語、スペイン語、ポルトガル語、日本語、イタリア語、中国語 (繁体字)、および中国語 (簡体字) です。
代理	proxy_server	リモート管理プロキシの DNS 名または IP アドレスとポート番号を次の形式で指定します。 ◆ *IP アドレス ~~ ポート* . 例 :10.0.0.0~~5750 ◆ *IP アドレス ~ ポート*例 :10.0.0.0~50 プロキシのデフォルトポートは、5750 です。

2.9.2 リモート操作の開始に関する内部オプション

次の表に、リモート管理が内部的に使用するオプションを一覧します。これらのオプションは、コマンドラインからリモート管理操作を開始する場合には、使用しないでください。

表 2-2 リモート操作の開始に関する内部オプション

オプション	説明
zenrights	認証スキームとして ZENworks 権限認証を指定します。
pipe	認証情報を指定します。

2.10 リモート管理プロキシのインストール

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リモート管理プロキシ経由でルーティングできます。プロキシは、Windows 管理対象デバイスまたは Linux デバイス (プライマリサーバまたはサテライトサーバ) にインストールできます。デフォルトでは、リモート管理プロキシは、ポート 5750 でリスンします。

リモート管理プロキシの詳細については、16 ページのセクション 1.4「リモート管理プロキシの理解」を参照してください。

Windows 管理対象デバイスまたは Linux デバイスが、それらにインストールされたプロキシを有効にするために満たす必要のあるシステム要件については、『*ZENworks 10 Configuration Management インストールガイド*』の「システム要件」を参照してください。

プロキシをインストールするには、次の手順を実行します。

Windows の場合 :

1. デバイスで Web ブラウザを開き、ZENworks ダウンロードページにアクセスします。

   https://*server*/zenworks-setup

   server は ZENworks サーバの DNS 名または IP アドレスです。
2. 左のナビゲーションペインで、［*管理ツール*］をクリックします。
3. novell-zenworks-rm-repeater-<*version*>.msi をクリックして、ファイルを一時的に適当な場所に保存します。

   version は、ZENworks 製品のバージョンです。
4. 次のコマンドを実行してプロキシアプリケーションをインストールします。

   msiexec /i novell-zenworks-rm-repeater-<*version*>.msi TARGETDIR="ZENworks_Installation_directory”

Linux の場合 :

1. デバイスで Web ブラウザを開き、ZENworks ダウンロードページにアクセスします。

   https://*server*/zenworks-setup

   server は ZENworks サーバの DNS 名または IP アドレスです。
2. 左のナビゲーションペインで、［*管理ツール*］をクリックします。
3. novell-zenworks-rm-repeater-<*version*>.noarch.rpm をクリックします。

4 プロキシを今すぐインストールするか、プロキシの RPM ファイルを保存して後でインストールするかを指定します。

- プロキシをすぐにインストールするには、[*Open With(開くアプリケーション)*] をクリックしてリモート管理プロキシを zen-installer で開き、ルートパスワードを指定して［*OK*］をクリックします。
- プロキシの RPM ファイルをデフォルトのダウンロードディレクトリに保存して後でインストールするには、[*Save to Disk(ディスクに保存する)*］をクリックします。RPM をインストールするには、次のいずれかの手順を実行します。
  - プロキシの RPM ファイルをクリックしてルートパスワードを指定し、［*OK*］をクリックします。
  - 次のコマンドをスーパーユーザまたはルートユーザとして実行します。

    rpm -ivh novell-zenworks-rm-repeater-<*version*>.noarch.rpm

リモート管理プロキシは、インストール時に自動的に実行されるように設計されています。デバイスのデフォルト設定を変更することにより、プロキシの動作をカスタマイズすることもできます。リモート管理プロキシ設定の詳細については、50 ページのセクション 2.11「リモート管理プロキシの設定」を参照してください。

2.11 リモート管理プロキシの設定

リモート管理プロキシをデバイスにインストールすると、一定の設定が、デフォルトで、デバイス上に設定されます。これらの設定は、編集することができます。

2.11.1 Windows デバイス上のリモート管理プロキシ設定

Windows デバイスでは、リモート管理プロキシのレジストリ設定は、HKLM\SOFTWARE\Novell\ZCM\Remote Management\Proxy にあります。

ClientPort: プロキシが、リモート管理ビューアからのリモートセッション要求をリッスンするために使用するポート番号を指定します。デフォルト値は「5750」です。

SessionEncryption: プロキシとリモート管理ビューア間の初期データフローを暗号化するかどうか指定します。デフォルト値は「True」です。プロキシが管理対象デバイスとの接続を確立した後は、この設定は適用できません。セッション暗号化は、リモート管理ポリシーとリモートオペレータの好みに準拠します。この設定は、True のままにしておく必要があります。これを False に設定すると、リモート管理ビューア以外の認証されていない外部プロセスがプライベートネットワーク内のデバイスに接続できるからです。

SSLClientAuthentication: 有効な証明書を持たないビューアからの接続要求をプロキシが受け入れるかどうか指定します。可能な値は、True と False です。デフォルト値は「True」です。

2.11.2 Linux プライマリサーバまたは Linux サテライトサーバ上のリモート管理プロキシ設定

Linux プライマリサーバまたは Linux サテライトサーバでは、リモート管理プロキシの設定は、/etc/opt/novell/zenworks/repeater/nzrepeater.ini ファイルにあります。次に、設定のいくつかを示します。

viewerport: リモート管理プロキシが、リモート管理ビューアからのリモートセッション要求をリッスンするために使用するポート番号を指定します。デフォルト値は「5750」です。

runasuser: プロキシがなりすますユーザを指定します。リモート管理プロキシは、リモート操作を実行するユーザ特権のみを要求します。デフォルト値は、zenworks です。ただし、異なるユーザを指定できます。

strictimpersonation: runasuser として指定されたユーザが存在しない場合、リモートセッションを root として続行するかどうか指定します。可能な値は、 t rue と f alse です。デフォルト値は、 f alse であり、runasuser として指定されたユーザが存在しない場合に、root としてリモートセッションを続行することを指定します。

sslauth: SSL を有効にするか無効にするか指定します。可能な値は、0 または 1 です。デフォルト値は、1 であり、SSL 認証を有効化することを指定します。

警告 : SSL 認証を無効にすることはお勧めできません。無効にすると、外部プロセスが、認証なしで、ネットワークデバイスにアクセスできます。

---

verifyViewerCert: リモート管理ビューアの証明書を検証する必要があるかどうか指定します。この設定は、SSL 認証が有効な場合のみ適用できます。可能な値は、0 または 1 です。デフォルト値は、1 であり、リモート管理ビューアの証明書を検証する必要があることを指定します。セッションがスタンドアロンビューアから開始される場合、リモートオペレータが、ルート認証局にチェーンされた必要な証明書を持たないことがあります。この場合は、プロキシがサーバに接続できません。

loggingenabled: デバイス上でメッセージをログするかどうか指定します。可能な値は、 t rue と f alse です。デフォルト値は、true です。

他のレジストリ設定については、/etc/opt/novell/zenworks/repeater/nzrepeater.ini ファイルを参照してください。

リモートセッションの管理

3

次の各セクションでは、Novell® ZENworks® 10 Configuration Management のリモートセッションを効率的に管理する上で役立つ情報を示します。

3.1 リモートコントロールセッションの管理

リモート管理により、管理対象デバイスをリモートで制御できます。リモートオペレータは、リモートコントロール接続を使用して、管理対象デバイスを参照するのみでなく、制御することもできます。このことは、管理対象デバイスでのユーザ支援の提供と問題の解決に役立ちます。リモートコントロールセッションの起動について詳しくは、35 ページのセクション 2.8「リモート管理操作の開始」を参照してください。

3.1.1 リモート管理ビューアのツールバーオプションの使用

次の表では、リモートコントロールセッション中にリモート管理ビューアで利用可能なさまざまなツールバーオプションについて説明しています。また、使用できる場合、ショートカットキーもリストされています。

表 3-1 *リモート管理ビューアのツールバーオプション*

オプション	ショートカットキー	機能
接続オプション 	<Ctrl>+<Alt>+<Shift>+<P>	セッションパフォーマンスを改善するフォーマットやエンコーディング、ログ、リモートカーソル処理などの様々なセッションパラメータを設定できます。
接続情報 	<Ctrl>+<Alt>+<Shift>+<I>	接続されている管理対象デバイスのホスト名、ポート、画面解像度、およびプロトコルバージョンを提供します。
全画面 	<Ctrl>+<Alt>+<Shift>+<F>	全画面モードと通常モードを切り替えることができます。

オプション	ショートカットキー	機能
画面更新要求 	<Ctrl>+<Alt>+<Shift>+<H>	［表示］ウィンドウを更新します。
Ctrl+Alt+Del を押す 		管理対象デバイスに <Ctrl>+<Alt>+<Del> キー操作を送信します。 <Ctrl>+<Alt>+<Del> 機能の Windows 7 デバイスでのシミュレーションは、現在、無効化されています。
Ctrl+Esc の送信 		管理対象デバイス上の［スタート］メニューを呼び出します。
Alt キーを押す / 離す 		このオプションをクリックしてキーボードの <ALT> キーを押すと、<ALT> キーストロークが管理対象デバイスに送信されます。
画面の消去 / 非消去 	<Ctrl>+<Alt>+<Shift>+<B>	管理対象デバイスの画面を黒くする、または表示します。デバイスの画面を消去すると、リモートオペレータが実行している操作が、デバイスにいるユーザに参照されません。管理対象デバイスのキーボードとマウスのコントロールもロックされます。 このオプションが有効になるのは、［*管理対象デバイス画面を空白にする*］オプションが、管理対象デバイスで有効なリモート管理ポリシーで有効な場合だけです。
キーボードのロック / アンロックとマウス 	<Ctrl>+<Alt>+<Shift>+<L>	管理対象デバイスのキーボードおよびマウスコントロールをロック、またはロック解除します。デバイスのマウスとキーボードのコントロールがロックされると、管理対象デバイスのユーザは、これらのコントロールを使用できません。 このオプションが有効になるのは、［*管理対象デバイスのマウスとキーボードをロックする*］オプションが、管理対象デバイスで有効なリモート管理ポリシーで有効な場合だけです。
ファイルの転送 	<Ctrl>+<Alt>+<Shift>+<T>	管理対象デバイスとファイルを受け渡しするセッションを起動します。 このオプションが有効になるのは、［*管理対象デバイスでファイル転送を許可*］オプションが、管理対象デバイスの有効なポリシーで有効な場合だけです。ファイル転送について詳しくは、60 ページのセクション 3.5「ファイル転送セッションの管理」を参照してください。

オプション	ショートカットキー	機能
コラボレーション 		管理対象デバイス上で ZENworks Remote Management Collaboration Session を起動します。このセッションにより、複数のリモートオペレータをリモート管理セッションに参加するよう招待できます。リモートコントロール権を別のリモートオペレータに委任して問題解決を支援してもらうこともできます。このオプションは現在 Windows でのみサポートされています。 セッションコラボレーションについて詳しくは、55 ページのセクション 3.1.2「セッションコラボレーション」を参照してください。
リモート実行 	<Ctrl>+<Alt>+<Shift>+<U>	管理対象デバイスでリモート実行セッションを起動します。これにより、管理対象デバイスで任意のプログラムをリモートで起動できます。 このオプションが有効になるのは、[*プログラムが管理対象デバイス上でリモートで実行されることを許可する*] オプションが、管理対象デバイスで有効なリモート管理ポリシーで有効な場合だけです。
スクリーンセーバの上書き 	<Ctrl>+<Alt>+<Shift>+<O>	リモートセッション中、管理対象デバイスでパスワードにより保護されているスクリーンセーバを無効にします。 このオプションが有効になるのは、[*リモートコントロール中にスクリーンセーバを自動的にロック解除する*] オプションが、管理対象デバイスで有効なリモート管理ポリシーで有効な場合だけです。
接続解除 	<Alt>+<F4>	リモートセッションを閉じます。

3.1.2 セッションコラボレーション

セッションコラボレーション機能では、リモート管理セッションに参加するよう、複数のリモートオペレータを招待できます。ただし、招待されるリモートオペレータは、リモートセッション要求をリスンするリモート管理リスナを起動している必要があります。リモートコントロール権を別のリモートオペレータに委任して問題解決を支援してもらい、その後コントロール権を再び取得することもできます。このオプションは現在 Windows でのみサポートされています。

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、マスタリモートオペレータの権限を取得します。セッションコラボレーションを使用して以下を行うことができます。

- 複数のリモートオペレータをリモートコントロールセッションに参加するよう招待する。
- リモートコントロール権を別のリモートオペレータに委任して問題解決を支援してもらい、その後コントロール権を再び取得する。
- リモートセッションを終了する。

セッションコラボレーションを起動するには、次の手順に従います。

1 管理対象デバイス上のリモート制御セッションをコラボレーションモードで起動します。

リモートコントロールセッション起動の詳細については、35 ページのセクション 2.8「リモート管理操作の開始」を参照してください。

2 リモート管理ビューアのツールバーにある をクリックします。［セッションコラボレーション］ウィンドウが表示されます。

［セッションコラボレーション］ウィンドウには、デバイスで有効なリモート管理ポリシーに追加されたリモートオペレータが一覧表示されます。各リモートオペレータは、色付きの円を前に付けた別々のエントリとしてリストされます。

- グレーの円は、リモートオペレータがセッションに参加していないことを示します。
- 赤い円は、リモートオペレータがセッションに参加し、リモート表示モードになっていることを示します。
- 緑の円は、リモートオペレータがセッションに参加していて、セッションのリモートコントロール権を委任されていることを示します。

リモートオペレータの追加については、23 ページのセクション 2.3「リモート管理ポリシーの作成」を参照してください。

次の表に、マスタリモートオペレータがセッションコラボレーション中に実行できるアクションをリストします。

表 3-2 *［セッションコラボレーション］ウィンドウのオプション*

タスク	手順	追加の詳細
リモートオペレータをリモートセッションに招待	1. セッションコラボレーションウィンドウにリストされたリモートオペレータを選択します。 2. ［*招待*］をクリックします。	リモートオペレータが要求を受け入れ、セッションに参加すると、リモートオペレータのグレーの円が赤に変わります。 デフォルトでは、新しいセッションは、リモート表示モードで開始されます。
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	1. リモート制御権限を委任するリモートオペレータを選択します。 2. ［*委任*］をクリックします。	選択されたリモートオペレータは、リモートコントロールモードになり、リモートオペレータの赤い円が緑に変わります。 マスタリモートオペレータは、自動的にリモートビューモードに切り替わります。
リモートオペレータからリモートコントロール権を再取得する	1. ［*コントロールの再取得*］をクリックします。	リモートオペレータは、リモートビューモードに切り替わり、リモートオペレータの緑の円が赤くなります。 マスタリモートオペレータは、自動的にリモートコントロールモードに切り替わります。

タスク	手順	追加の詳細
リモートセッションを終了する	1. リモートセッションを終了するリモートオペレータを選択します。 2. ［*終了*］をクリックします。	選択したリモートオペレータがリモートコントロールモードの場合は、操作者がリモートコントロール権を再取得します。 リモートオペレータのセッションが終了し、リモートオペレータの円の色がグレーになります。
外部リモートオペレータの招待	1. ［*外部の招待*］をクリックして、［セッションコラボレーション］ウィンドウにリストされていないリモートオペレータを、リモートセッションに参加するよう招待します。 2. リモートオペレータのデバイスの DNS 名または IP アドレス、およびポート番号を指定します。たとえば、10.0.0.0 ~~1000 とします。 3. ［*招待*］をクリックします。	

マスタリモートオペレータがリモートセッションを切断すると、すべてのリモートオペレータのセッションが終了されます。

3.2 リモートビューセッションの管理

リモートビュー機能では、リモートで管理対象デバイスに接続して、管理対象デバイスのデスクトップを表示できます。リモートビューセッションの起動について詳しくは、35 ページのセクション 2.8「リモート管理操作の開始」を参照してください。

次の表は、リモートビューセッション中にリモート管理ビューアで利用可能なさまざまなツールバーオプションについて説明しています。

表 3-3 *リモート管理ビューアのツールバーオプション*

オプション	ショートカットキー	機能
接続オプション 	<Ctrl>+<Alt>+<Shift>+<P>	セッションパフォーマンスを改善するフォーマットやエンコーディング、ログ、リモートカーソル処理などの様々なセッションパラメータを設定できます。
接続情報 	<Ctrl>+<Alt>+<Shift>+<I>	接続されている管理対象デバイスのホスト名、ポート、画面解像度、およびプロトコルバージョンを提供します。
全画面 	<Ctrl>+<Alt>+<Shift>+<F>	全画面モードと通常モードを切り替えることができます。

オプション	ショートカットキー	機能
画面更新要求 	<Ctrl>+<Alt>+<Shift>+<H>	［表示］ウィンドウを更新します。
接続解除 	<Alt>+<F4>	リモートセッションを閉じます。

3.3 リモート実行セッションの管理

リモート実行では、システム権限を使用して、管理デバイス上でリモートから実行可能ファイルを実行できます。管理対象デバイスでアプリケーションプログラムを実行するには、リモート実行セッションを起動します。

1 リモート実行セッションの起動

   リモート実行セッションの起動について詳しくは、35 ページのセクション 2.8「リモート管理操作の開始」を参照してください。

2 実行可能ファイル名を指定します。

   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。管理対象デバイスで実行するファイルの拡張子を指定しない場合は、リモート実行機能によって .exe 拡張子が追加されます。

3 ［*実行*］をクリックします。

指定したアプリケーションが、管理対象デバイス上の、定義したパスに存在しない場合は、アプリケーションのリモート実行が失敗します。

警告 : リモート管理モジュールは、デフォルトでは、管理デバイス上でシステム権限を持つサービスとして実行されます。したがって、リモート実行セッション中に起動されるアプリケーションは、すべてシステム権限を使用して実行されます。セキュリティ上の理由により、使用後はアプリケーションを閉じることを強くお勧めします。

3.4 リモート診断セッションの管理

リモート管理では、管理対象デバイスの問題をリモートで診断して分析できます。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。デスクトップを稼動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。

管理対象デバイスでリモート診断セッションを開始した場合は、リモート管理設定でそのデバイスの診断と問題解決のためにそのデバイスに設定された診断アプリケーションにのみアクセスできます。セッションの間、これらの診断アプリケーションは、アイコンとしてツールバーに表示されます。デフォルトでは、次の診断アプリケーションが、リモート管理設定に設定されています。

表 3-4　リモート管理ビューアのツールバーオプション

オプション	ショートカットキー	機能
接続オプション 	<Ctrl>+<Alt>+<Shift>+<P>	セッションパフォーマンスを改善するフォーマットやエンコーディング、ログ、リモートカーソル処理などの様々なセッションパラメータを設定できます。
接続情報 	<Ctrl>+<Alt>+<Shift>+<I>	接続されている管理対象デバイスのホスト名、ポート、画面解像度、およびプロトコルバージョンを提供します。
全画面 	<Ctrl>+<Alt>+<Shift>+<F>	全画面モードと通常モードを切り替えることができます。
画面更新要求 	<Ctrl>+<Alt>+<Shift>+<H>	［表示］ウィンドウを更新します。
ファイルの転送 	<Ctrl>+<Alt>+<Shift>+<T>	管理対象デバイスとファイルを受け渡しするセッションを起動します。 このオプションが有効になるのは、［*管理対象デバイスでファイル転送を許可*］オプションが、管理対象デバイスの有効なポリシーで有効な場合だけです。ファイル転送について詳しくは、60 ページのセクション 3.5「ファイル転送セッションの管理」を参照してください。
接続解除 	<Alt>+<F4>	リモートセッションを閉じます。

表 3-5　リモート診断アプリケーション

アイコン	アプリケーション
	*システム情報*
	*コンピュータ管理*
	*サービス*
	*レジストリエディタ*

リモート診断セッション中に管理対象デバイスで起動されるアプリケーションを設定できます。診断アプリケーションの設定について詳しくは、19 ページのセクション 2.1「リモート管理設定の環境設定」を参照してください。

3.5 ファイル転送セッションの管理

リモート管理により、管理コンソールと管理対象デバイスの間でのファイル転送を行うことができます。ファイル転送セッションの起動について詳しくは、35 ページのセクション 2.8「リモート管理操作の開始」を参照してください。

［ファイル転送］ウィンドウの［ローカルコンピュータ］ペインには、管理コンソールのすべてのファイルとフォルダが表示されます。［リモートコンピュータ］ペインには、リモート管理ポリシーの［*ファイル転送ルートディレクトリ*］オプションで指定したディレクトリのすべてのファイルとフォルダが表示されます。［*ファイル転送ルートディレクトリ*］をポリシーに指定していない場合、または管理対象デバイスにポリシーが関連付けられていない場合は、リモートデバイスの全ファイルシステムに対してファイル転送操作を実行できます。

次の表に、ファイル転送機能の使用方法と［ファイル転送］ウィンドウからファイルの作業を行う場合に利用できるオプションについて説明します。［*アクション*］メニューオプションはまだ Linux ではサポートされていません。ただし、ツールバーで該当するアイコンをクリックして操作を実行できます。

表 3-6 *［ファイル転送］ウィンドウのオプション*

タスク	ショートカットキー	手順	追加の詳細
新規ローカルフォルダを作成する	<Alt>+<L>	1. ［*アクション*］>［*新規ローカルフォルダ*］の順にクリックします。 または ［ローカルコンピュータ］ペインで をクリックします。 2. 画面のプロンプトに従います。	
新規リモートフォルダを作成する	＜ Alt ＞ + ＜ W ＞	1. ［*アクション*］>［*新規リモートフォルダ*］の順にクリックします。 または ［リモートコンピュータ］ペインで をクリックします。 2. 画面のプロンプトに従います。	

タスク	ショートカットキー	手順	追加の詳細
ファイルを開く		1. 関連付けられたアプリケーションで、ファイルをダブルクリックして、開きます。	
ファイルまたはフォルダの名前を変更する	＜ Alt ＞ + ＜ N ＞	1. 名前を変更するファイルまたはフォルダを選択します。 2. ［*アクション*］> ［*名前変更*］の順にクリックします。 または をクリックします。 3. 画面のプロンプトに従います。	
ファイルまたはフォルダを削除する	<Alt>+<D>	1. 削除するファイルまたはフォルダを選択します。 2. ［*アクション*］> ［*削除*］の順にクリックします。 または をクリックします。 3. 画面のプロンプトに従います。	<Shift> キーまたは <Ctrl> キーを使用して複数のファイルを選択できます。
ローカルフォルダをリフレッシュする	＜ Alt ＞ + ＜ E ＞	1. ［*アクション*］> ［*ローカルフォルダのリフレッシュ*］の順にクリックします。 または ［リモートコンピュータ］ペインでをクリックします。	
リモートフォルダをリフレッシュする	<Alt>+<M>	1. ［*アクション*］> ［*リモートフォルダの更新*］の順にクリックします。 または ［リモートコンピュータ］ペインでをクリックします。	

タスク	ショートカットキー	手順	追加の詳細
ローカルファイルをソートする		1. ［*アクション*］>［*ローカルソート*］の順にクリックします。 2. ソートタイプを選択します。名前、サイズ、または日付別にファイルをソートできます。	または、個々の列見出しをクリックしてもファイルをソートできます。
リモートファイルをソートする		1. ［*アクション*］>［*リモートソート*］の順にクリックします。 2. ソートタイプを選択します。名前、サイズ、または日付別にファイルをソートできます。	または、個々の列見出しをクリックしてもファイルをソートできます。
ファイル / フォルダをアップロードする		1. リモートコンピュータにアップロードするファイルを選択します。 2. ［リモートコンピュータ］ペインで、あて先フォルダを選択します。 3. ［*アクション*］>［*アップロード*］の順にクリックします。 または ➡をクリックします。	［*アクション*］>［*アップロード*］オプションは、ローカルコンピュータにフォーカスがある場合のみ使用できます。 <Shift> キーまたは <Ctrl> キーを使用して複数のファイルを選択できます。
ファイル / フォルダをダウンロードする	＜ Alt ＞ + ＜ O ＞	1. ローカルコンピュータにダウンロードするファイルを選択します。 2. ［ローカルコンピュータ］ペインで、あて先フォルダを選択します。 3. ［*アクション*］>［*ダウンロード*］の順にクリックします。 または ⬅をクリックします。	*［アクション］>［ダウンロード］オプションは*、リモートコンピュータにフォーカスがある場合のみ使用できます。 <Shift> キーまたは <Ctrl> キーを使用して複数のファイルを選択できます。
ファイル転送のキャンセル	<Alt>+<C>	1. ［*アクション*］>［*ファイル転送のキャンセル*］をクリックします。	［キャンセル］ボタンをクリックしてファイル転送操作をキャンセルすることもできます。

タスク	ショートカットキー	手順	追加の詳細
ファイルプロパティを表示する	＜ Alt ＞ + ＜ P ＞	1. ファイルを選択します。 2. ［*アクション*］> ［*プロパティ*］の順にクリックします。 または をクリックします。	<Shift> キーまたは <Ctrl> キーを使用して複数のファイルを選択できます。 選択したファイルまたはフォルダの累積サイズが表示されます。
親フォルダに移動する		1. をクリックして親フォルダに移動します。	

3.6 リモート管理プロキシセッションの管理

リモート管理プロキシでは、プライベートネットワークにある、あるいは NAT (Network Address Translation) 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管理対象デバイスでリモート管理操作を実行できます。

リモート管理プロキシの詳細については、16 ページのセクション 1.4「リモート管理プロキシの理解」を参照してください。

リモート管理プロキシのインストール方法の詳細については、49 ページのセクション 2.10「リモート管理プロキシのインストール」を参照してください。

リモート管理プロキシの設定方法の詳細については、50 ページのセクション 2.11「リモート管理プロキシの設定」を参照してください。

3.7 リモートデバイスのウェイクアップ

リモートウェイクアップを使用すると、ネットワーク内の電源が切断されている単一のまたは複数のノードの電源をリモートから入れることができます (ただし、ノード上のネットワークカードのリモートウェイクアップが有効にされている必要があります)。

複数の NIC(ネットワークインタフェースカード) を持つデバイスの起動は、Wake-on-LAN パケットをブロードキャストしているデバイスを含むサブネットに対して 1 つ以上の NIC が設定されている場合にのみ成功します。

3.7.1 前提条件

管理対象デバイスの起動は、次の要件を満たしてから実行する必要があります。

- 管理対象デバイス上のネットワークカードが Wake-ON-LAN をサポートしていることを確認します。次に、管理対象デバイスの BIOS 設定で Wake-ON-LAN オプションが有効になっていることも確認します。

- 管理対象デバイスが ZENworks 管理ゾーンに登録されていることを確認します。
- リモートノードがソフト電源オフ状態になっていることを確認します。ソフト電源オフ状態とは、CPU の電源が切断されていて、ネットワークインタフェースカードが最小限の電力を使用している状態です。ハードオフ状態とは異なり、ソフトオフ状態のときには、コンピュータがシャットダウンされていても、コンピュータの電源接続はオンのままになります。

3.7.2 管理対象デバイスのリモートウェイクアップ

リモートウェイクアップを実行するには、次の手順に従います。

1. ZENworks コントロールセンターで、［*デバイス*］をクリックします。
2. ［*サーバ*］または［*ワークステーション*］をクリックして管理対象デバイスのリストを表示します。
3. ウェイクアップするデバイスを選択します。
4. ［*クイックタスク*］>［*起動*］をクリックします。［起動］ダイアログボックスが表示されます。
5. 次のいずれかのオプションを選択して、管理対象デバイスにウェイクアップ要求を送信するサーバを指定します。
   - **サーバを自動的に検出する。**ZENworks では管理対象デバイスにもっとも近いプライマリサーバを自動的に検出します。サーバとリモートデバイスが異なるサブネットに属する場合は、サブネットを接続するルータがサブネット向けブロードキャストを UDP ポート 1761 で転送するよう設定されていることを確認します。
   - **次のデバイスを使用します。**［*追加*］をクリックして、起動するデバイスと同じサブネットに存在するプロキシデバイスを選択します。

     ルータがサブネット向けブロードキャストを UDP ポート 1761 で転送するよう設定されている場合、プロキシは必要ありません。
6. (オプション) 次のいずれかのオプションを選択して、ウェイクアップブロードキャストを送信するのに使用する IP アドレスを指定します。
   - **IP アドレスを自動的に検出する。**ZENworks はサブネットのデフォルトのブロードキャストアドレスを自動的に検出し、ウェイクアップブロードキャストを管理対象デバイスに送信します。
   - **次の IP アドレスを使用します。**ウェイクアップブロードキャストを管理対象デバイスに送信する IP アドレスを指定して、［*追加*］をクリックします。
7. ［*再試行の回数*］オプションで、デバイスをウェイクアップする再試行の回数を指定します。デフォルトでは、1 です。
8. ［*再試行間隔*］オプションで、2 つの再試行の間の間隔を指定します。デフォルトでは、2 分です。
9. ［*OK*］をクリックします。

［*再試行の回数*］および［再試行間隔］オプションはゾーンレベルで設定されます。これらの値は、デバイスレベルで上書きできます。

3.8 リモート管理のパフォーマンスの向上

低速リンクまたは高速リンクを通じたリモートセッション中のリモート管理のパフォーマンスはネットワークトラフィックに応じて変わります。応答時間を短縮するために、次の手順を 1 つまたは複数実行してみてください。

- 65 ページのセクション 3.8.1「管理コンソールでの手順」
- 65 ページのセクション 3.8.2「管理対象デバイス側」

3.8.1 管理コンソールでの手順

コンソールの ZENworks Remote Management の接続ウィンドウで、［*オプション*］をクリックし、次の値を設定します。

- 低速リンク経由でのリモート管理のパフォーマンスを最大化する
  - ［*8 ビット色を使用*］オプションを選択します。
  - ［*カスタム圧縮レベル*］にレベル 6 を設定します。
- ［*マウス移動イベントのブロック*］オプションを選択します。
- ［リモート管理設定］の［*壁紙を抑制*］オプションを有効にします。

3.8.2 管理対象デバイス側

- リモート管理セッションのスピードは、管理対象デバイスの処理パワーに依存します。256MB 以上の RAM を装備した Pentium* III 700MHz(以降) を使用することをお勧めします。
- 壁紙パターンは設定しません。

セキュリティ

4

次の各セクションでは、Novell® ZENworks® 10 Configuration Management のリモート管理コンポーネントを使用するときに注意する必要のあるセキュリティ関係の情報を提供します。

4.1 認証

リモートオペレータがデバイスをリモート管理するには、リモート管理サービスがデバイスにインストールされている必要があります。このサービスは、管理対象デバイスのブート時に自動的に開始されます。リモートオペレータが管理対象デバイス上のリモートセッションを開始すると、リモート管理サービスは、リモートオペレータが管理対象デバイスでリモート操作を実行するよう許可される場合に限りリモートセッションを開始します。

管理対象デバイスに対する非許可アクセスを防ぐために、管理対象デバイス上のリモート管理サービスは次の認証モードを使用します。

4.1.1 権限ベースのリモート管理認証

権限ベース認証では、管理対象デバイス上でリモートセッションを起動する権限がリモートオペレータに割り当てられます。デフォルトでは、ZENworks 管理者とスーパー管理者は、ローカルユーザまたは ZENworks ユーザがそのデバイスにログインしているかどうかによらず、すべての管理対象デバイスについてリモート操作を実行する権限を持ちます。

ユーザが管理対象デバイスにログインしていないか、管理対象デバイスにはログインしているものの ZENworks にログインしていない場合、リモートオペレータは管理対象デバイスでリモートセッションを実行するために排他的な権限を持つ必要はありません。ただし、ZENworks ユーザが管理対象デバイスにログインしている場合は、リモートオペレータは、管理対象デバイスでリモート操作を実行する排他的なリモート管理権限を持つ必要があります。権限ベース認証は安全であるため、権限ベース認証を使用することを強くお勧めします。

権限ベースの認証を使用するには、デバイスに ZENworks Adaptive Agent がインストールされている必要があります。デバイス上にリモート管理サービスをインストールするだけでは十分ではありません。

この認証モードは、スタンドアロンモードまたはコマンドラインからリモート管理操作を開始する際にはサポートされません。

4.1.2 パスワードベースのリモート管理認証

パスワードベース認証では、管理対象デバイスでリモートセッションを起動するパスワードを入力するようリモートオペレータにプロンプトが表示されます。

次の 2 種類のパスワード認証方式を使用します。

- **ZENworks パスワード :** この方式は、セキュアリモートパスワード (SRP) プロトコル (バージョン 6a) に基づきます。ZENworks パスワードの最大長は 255 文字です。
- **VNC のパスワード :** これは、従来の VNC パスワード認証方式です。VNC パスワードの最大長は、8 文字です。このパスワード方式は、本質的に脆弱であり、オープンソースコンポーネントとの相互運用性のためにのみ提供されています。

パスワードベース認証を使用する場合は、VNC パスワード方式よりも安全な ZENworks パスワード方式を使用することを強くお勧めします。

これらのパスワード方式は、次のモードで動作します。

- **セッションモード :** このモードで設定されたパスワードは、現在のセッションでのみ有効です。管理対象デバイス上のユーザは、リモートセッションの開始時にパスワードを設定し、電話などのアウトオブバンド方式でリモートオペレータに伝える必要があります。リモートオペレータは、管理対象デバイスとのリモートセッションの開始時に、表示されるセッションパスワードのダイアログボックスに正しいパスワードを入力する必要があります。ダイアログボックスが表示されてから 2 分以内にリモートオペレータが正しいパスワードを入力できない場合は、セキュリティのためにセッションが閉じられます。パスワードベース認証を使用する場合は、パスワードが現在のセッションでのみ有効であり管理対象デバイスに保存されないため、このモードの認証を使用することを強くお勧めします。
- **永続モード** このモードでは、管理者がリモート管理ポリシーを通じてパスワードを設定できます。リモート管理ポリシーのセキュリティ設定で［*ユーザが管理対象デバイスのデフォルトのパスワードを上書きすることを許可する*］オプションが選択されている場合は、管理対象デバイスのユーザが ZENworks アイコンから設定できます。

  管理対象デバイスユーザとポリシーの両方でパスワードが設定されている場合は、ユーザが設定したパスワードが、ポリシーに設定されたパスワードより優先されます。

  管理者は、ユーザがパスワードを設定できないようにすることや、ユーザが設定したパスワードをリセットすることもでき、これによりポリシーに設定したパスワードが、常に、認証時に使用されるようにすることができます。管理対象デバイスユーザの設定したパスワードのリセットについて詳しくは、33 ページのセクション 2.5.3「ZENworks コントロールセンターを使用したリモート管理パスワードのクリア」を参照してください。

4.2 パスワード強度

安全なパスワードを使用してください。次のガイドラインに注意してください。

- **長さ :** 推奨される最小長は 6 文字です。パスワードを安全にするには 8 文字以上にします。長い程安全です。最大長は、ZENworks パスワードでは 255 文字、VNC パスワードでは 8 文字です。
- **複雑性 :** パスワードを安全にするには、文字と数字を組み合わせます。このためには、大文字と小文字の両方を含み、数字を 1 つ以上含む必要があります。数字をパスワードに追加すると、パスワードの強度が向上します。特に、先頭や末尾ではなく中間に追加すると、パスワードの強度を向上できます。&、*、$、> などの特殊文字を使用すると、パスワードの強度を大幅に向上できます。通常の名前や辞書にある単語など、認識可能な語を使用しないでください。電話番号、誕生日、記念日、住所、ZIP コードなどの個人情報も使用しないでください。

4.3 ポート

デフォルトでは、リモート管理サービスはポート 5950 で実行され、リモート管理リスナはポート 5550 で実行されます。ファイアウォールは、リモート管理サービスが使用するすべてのポートを許可するよう設定されていますが、リモート管理リスナが使用するポートを許可するようファイアウォールを設定する必要があります。

デフォルトでは、リモート管理プロキシは、ポート 5750 でリスンします。

4.4 Audit

ZENworks Configuration Management は、管理対象デバイスで実行された全リモートセッションのログを保持します。このログは管理対象デバイスに保管され、ユーザおよび管理者が参照できます。管理者は、そのデバイスで実行された全リモートセッションのログを参照できます。ユーザは、そのユーザがログインしているときにそのデバイスで実行された全リモートセッションのログを参照できます。

監査ログを表示するには、次の手順に従います。

1. 管理対象デバイスの通知領域にある ZENworks アイコンをダブルクリックします。
2. 左ペインで［*リモート管理*］にナビゲートし、［*セキュリティ*］をクリックします。
3. ［*監査情報の表示*］をクリックします。デバイスで実行されたリモート操作の監査情報が表示されます。

フィールド	説明
ZENworks ユーザ	リモートセッションの開始時に管理対象デバイスにログインした ZENworks ユーザの名前です。
リモートオペレータ	操作を実行したリモートオペレータの名前です。
コンソールマシン	リモート操作の実行元デバイスのホスト名です。

フィールド	説明
コンソール IP	リモート操作の実行元デバイスの IP アドレスです。 **注 :** デバイスのリモート管理操作がリモート管理プロキシ経由でルーティングされる場合は、プロキシを実行しているデバイスの IP アドレスが表示されます。
操作	実行された操作のタイプ (リモートコントロール、リモート実行、リモートビュー、リモート診断、ファイル転送) です。
開始時刻	リモート操作の開始時刻です。
終了時刻	リモート操作の完了時刻です。
ステータス	リモート操作のステータス (成功、実行中、または失敗) です。失敗の原因も表示されます。

4.5 管理対象デバイス上のユーザからの許可を求める

管理者は、デバイスでのリモート操作を開始する前に、リモートオペレータが管理対象デバイスのユーザからの許可を要求できるようリモート管理ポリシーを設定できます。

リモートオペレータが管理対象デバイスでのリモートセッションを開始すると、リモート管理サービスは、そのデバイスで有効なポリシーで、そのリモート操作について［*管理対象デバイス上のユーザからの許可を求める*］オプションが有効かどうかを確認します。このオプションが有効であり、ユーザがデバイスにログインしていない場合は、リモートセッションが続行されます。一方、このオプションが有効であり、ユーザが管理対象デバイスにログインしている場合は、リモート管理ポリシーに設定されているメッセージが、デバイスでのリモートセッションを起動する許可を要求しているユーザに表示されます。セッションは、ユーザが許可を与えた場合にのみ開始されます。

4.6 異常終了

異常終了機能では、リモートセッションが突然切断された場合に、リモート管理ポリシーのセキュリティ設定によって、管理対象デバイスをロックするか、管理対象デバイス上のユーザをログアウトさせることができます。リモートセッションは次の場合に突然終了されます。

- ネットワークの障害が発生し、リモート管理ビューアとリモート管理サーバが通信できない。
- リモート管理ビューアがタスクマネージャから突然閉じられた。
- 管理対象デバイスまたは管理コンソールで、ネットワークが使用できない。

場合によっては、リモート管理サービスがセッションの異常終了を判断するまで 1 分程度かかることがあります。

4.7 不正侵入者検出

不正侵入者検出機能により、管理対象デバイスがハックされる危険性が大幅に低下します。リモートオペレータが指定の回数 (デフォルトは 5 回) 以内に管理対象デバイスにログインできなかった場合は、リモート管理サービスがブロックされ、ブロックを解除しない間はどのリモートセッション要求も受け入れなくなります。管理者は、手動または自動で、リモート管理サービスのブロックを解除できます。

4.7.1 リモート管理サービスの自動ブロック解除

リモート管理サービスは、リモート管理ポリシーの［*[] 分後に接続受諾の自動開始*］オプションに指定した時間が過ぎると自動的にブロック解除されます。デフォルトの時間は 10 分です。デフォルトの時間は、リモート管理ポリシーのセキュリティ設定で変更できます。

4.7.2 リモート管理サービスの手動ブロック解除

管理対象デバイスまたは ZENworks コントロールセンターからリモート管理サービスを手動でブロック解除できます。

リモート管理サービスを ZENworks コントロールセンターからブロック解除するには、リモートオペレータが管理対象デバイスでのリモートコントロール権限とリモート実行権限を持つ必要があります。

1. ZENworks コントロールセンターで、［*デバイス*］をクリックします。
2. ［*サーバ*］または［*ワークステーション*］をクリックして管理対象デバイスのリストを表示します。
3. ロック解除するデバイスを選択します。
4. ［*アクション*］をクリックしてから［*リモート管理のブロック解除*］をクリックします。
5. ［*OK*］をクリックします。

管理対象デバイスからリモート管理サービスをブロック解除する

1. 管理対象デバイスの通知領域にある ZENworks アイコンをダブルクリックします。
2. 左ペインで［*リモート管理*］にナビゲートし、［*セキュリティ*］をクリックします。
3. ［*侵入者検出によって現在ブロックされている場合は、接続の受諾を許可します*］をクリックします。

4.8 リモートオペレータ ID

リモートオペレータが ZENworks コントロールセンターからリモートセッションを起動すると、管理対象デバイスでのリモートオペレータの識別を助ける証明書が自動生成されます。ただし、リモートオペレータがセッションをスタンドアロンモードで起動した場合は、証明書が生成されず、リモートオペレータは*不明ユーザ*として監査ログ、可視信号、および［ユーザ許可の要求］ダイアログボックスに表示されます。リモート管理サービスは、セキュアソケットレイヤ (SSL) ハンドシェイク中に管理コンソールから提供された証明書を使用して、リモートオペレータの ID を取得します。SSL ハンドシェイクは、VNC パスワード認証を除くすべての種類の認証で行われます。

デバイス上のリモート管理サービスは、そのデバイスで有効なポリシーで［*管理対象デバイス上のユーザに可視信号が送信される*］オプションが有効である場合、リモートオペレータの詳細を［可視信号］ダイアログボックスに表示します。リモート管理サービスは、リモートオペレータの情報をリモート管理監査ログにも記録します。

4.9 ブラウザ設定

Windows Vista デバイスで Internet Explorer を使用して ZENworks コントロールセンターを起動する場合は、セキュリティ設定でプロテクトモードをオフにしてからブラウザを再起動してください (*［ツール］> ［インターネットオプション］> ［セキュリティ］*)。

4.10 セッションのセキュリティ

ZENworks Configuration Management では、セキュアソケットレイヤ (SSL) を使用してリモートセッションを保護します。ただし、VNC パスワードベースの認証を使用して起動されたリモートセッションは安全ではありません。リモート管理ポリシーにセッション暗号化が設定されているかどうかによらず SSL ハンドシェイクが行われるため、認証処理は、保護されたチャネルを通じて行われます。

認証が完了すると、リモート管理ポリシーで［*セッションの暗号化を有効にする*］オプションが無効にされており、管理対象デバイスでのリモートセッションの開始時にリモートオペレータが［*セッション暗号化*］オプションを無効にした場合は、リモートセッションが安全でないモードに切り替わります。ただし、セッションのパフォーマンスに大きな影響はないため、セッションをセキュアモードのままにすることをお勧めします。

4.10.1 SSL ハンドシェイク

管理対象デバイスへの ZENworks Adaptive Agent のインストール時に、リモート管理サービスは 10 年間有効な自己署名証明書を 1 つ生成します。

リモートオペレータが管理対象デバイスでのリモートセッションを開始すると、リモート管理ビューアは管理対象デバイス証明書を検証するようリモートオペレータにプロンプトを表示します。証明書には、管理対象デバイスの名前、証明書発行認証局、証明書の有効性、フィンガープリントなどの詳細情報が表示されます。セキュリティ上の理由から、リモートオペレータは、証明書のフィンガープリントとアウトオブバンド方式で管理対象デバイスユーザから通知されたフィンガープリントを照合して、管理対象デバイスの資格情報を検証する必要があります。次に、リモートオペレータは次のいずれかを実行できます。

- **証明書を永続的に受諾 :** 管理コンソールにログインしているユーザが、証明書を永続的に受諾すると、このコンソールにこのユーザがログインして開始する以降のリモートセッションでは、証明書が表示されません。
- **証明書を一時的に受諾 :** 管理コンソールにログインしているユーザが、証明書を一時的に受諾すると、証明書は現在のセッションについてのみ受諾されます。このユーザがこの管理対象デバイスに対して次回接続を開始すると、証明書を検証するようプロンプトが表示されます。
- **証明書を拒否 :** 管理コンソールにログインしているユーザが証明書を拒否すると、リモートセッションが終了されます。

4.10.2 証明書の再生成

管理対象デバイスは、次の場合に新規自署証明書を再生成します。

- 管理対象デバイスの名前が変更された
- 証明書が先日付であり現在有効でない
- 証明書の期限が切れた
- 証明書の期限が切れそうである
- 証明書が存在しない

デフォルトでは、証明書は 10 年ごとに再生成されます。

トラブルシューティング

5

次の各セクションでは、Novell® ZENworks® 10 Configuration Management のリモート管理コンポーネントの使用中に発生する可能性のある状況について説明します。

- 81 ページの 「リモートコントロールセッション中に、リモート管理ビューアで［Ctrl+Alt+Del］アイコンをクリックすると、コントロールがまったくない状態の［Secure Attention Sequence］ウィンドウが表示される場合がある」
- 82 ページの 「デバイスのデスクトップは、デバイスをリモートで制御またはリモートで表示する場合に、表示されないことがある」
- 82 ページの 「Windows Vista、Windows 7、Windows Server 2008、または Windows Server 2008 R2 のデバイス上の制限されたフォルダにファイルをリモートから転送できない」
- 83 ページの 「Mozilla Firefox を介して、SUSE Linux Enterprise Server 11 デバイス上でリモートセッションを開始できない」
- 83 ページの 「Internet Explorer 8 を介して ZENworks を起動すると、［リモート管理ビューアのアップグレード］リンクが表示されない」

管理デバイスのスクリーンセーバーを無効にできない

ソース： ZENworks 10 Configuration Management、リモート管理。

説明： リモートコントロールセッションの開始より前に、管理対象サーバでパスワード保護されたスクリーンセーバーがアクティブになっていた場合は、リモートオペレータがユーザデスクトップを参照できるよう、リモート管理サービスがスクリーンセーバーを無効にしようとします。リモートオペレータは、リモート管理ツールバーの［*スクリーンセーバーの無効化*］アイコンをクリックして、リモートセッション中にスクリーンセーバーを無効にすることもできます。

考えられる原因： リモートセッションがアクティブでないためにスクリーンセーバーが起動された。

アクション： リモート管理ビューアツールバーの［*スクリーンセーバーの無効化*］アイコンをクリックします。アイコンを数回クリックしないと無効化されないことがあります。

考えられる原因： スクリーンセーバー機能の上書きは、Windows Vista、Windows 7、Windows Server 2008、または Windows Server 2008 R2 のデバイスではサポートされません。

アクション： なし。

考えられる原因： 管理対象デバイスに対して何らかのマウス移動が送信されたことによりスクリーンセーバーが中断された。

アクション： ZENworks Remote Management ビューアのオプションウィンドウで［*マウス移動イベントのブロック*］オプションを選択して、マウス移動が管理対象デバイスに送信されないようにします。

考えられる原因： 管理対象デバイスでのスクリーンセーバーの割り込みにより、管理対象デバイスの GINA (Graphical Identification and Authentication) がアクティブになった。

アクション： 管理対象デバイスにログインし直します。

リモート管理セッションで Windows 2000* Professional マシンからログオフしてログインし直すと、マシンに設定されている壁紙が復元されない

ソース： ZENworks 10 Configuration Management、リモート管理。

アクション： なし。

極めて低い色品質で実行されている管理対象デバイスでリモートセッションを起動できない

ソース： ZENworks 10 Configuration Management、リモート管理。

説明： 極めて低い色品質 (8bpp(bits per pixel) 未満) で実行されている管理対象デバイスでは、リモートコントロール、リモートビュー、またはリモート診断セッションを起動できません。

アクション： 次の手順に従って、デバイスの色品質を 16bpp 以上に上げます。

1. デスクトップを右クリックします。
2. ［*プロパティ*］をクリックします。
3. ［画面のプロパティ］ウィンドウで、［*設定*］をクリックします。
4. 適切な色品質を選択し［*OK*］をクリックします。

リモート管理ビューアを起動できない。

ソース： ZENworks 10 Configuration Management、リモート管理。

考えられる原因： リモート管理ビューアの実行可能ファイルが削除または名前変更されると、リモート管理ビューアを起動できません。

アクション： 最新バージョンの novell-zenworks-rm-viewer.msi を https://*ZENworks_server_IPaddress*/zenworks-remote-management からダウンロードして、リモート管理ビューアを再インストールします。

異常セッション終了は、Windows Vista、Windows 7、Windows Server 2008、Windows Server 2008 R2 の管理対象デバイスでは失敗する場合があります。

ソース： ZENworks 10 Configuration Management、リモート管理。

説明： リモートセッション中に、ユーザが Windows Vista、Windows 7、Windows Server 2008、または Windows Server 2008 R2 の管理対象デバイスでネットワーク接続を無効にすると、ZENworks はこれを異常終了として検出できないことがあり、デバイスをロックしなかったり、管理対象デバイス上のユーザをログアウトしないことがあります。

アクション： なし。

リモート管理リスナがバインドしているポートが管理コンソールのファイアウォールで開けられていないと、リモート管理リスナが管理対象デバイスからのリモートセッション要求を受諾できない。

ソース： ZENworks 10 Configuration Management、リモート管理。

アクション： 管理コンソールのファイアウォールでリスナのポートを開けます。

リモート管理コンポーネントの使用中に、トラブルシューティングエラーメッセージが表示される。

ソース： ZENworks 10 Configuration Management、リモート管理。

アクション : リモート管理コンポーネントの使用中に発行されるエラーメッセージをトラブルシュートするには、次のログファイルを Novell サポート (http://support.novell.com) に送信します。

- WinVNCApp.log ファイルと WinVNC.log ファイル (Windows Vista、Windows 7、Windows Server 2008、または Windows Server 2008 R2 のデバイスの場合)
- WinVNC.log ファイル (他の管理対象デバイスの場合)

ログファイルにアクセスする手順 :

1. レジストリエディタを開きます。
2. HKLM\Software\Novell\ZCM\Remote Management\Agent に移動します。
3. DebugMode という名前の DWORD を作成し、値に 2 を設定します。
4. DebugLevel という名前の DWORD を作成し、16 進値に a (10 進値の 10) を設定します。
5. リモート管理サービスを再起動します。

次のリモート管理ログファイルが、*ZENworks_installation_directory*\logs に作成されます。

- WinVNC.log
- WinVNCApp.log

ZENworks コントロールセンターを起動するデバイスでのリモート管理デバッグログの有効化方法

ソース : ZENworks 10 Configuration Management、リモート管理。

アクション : このログを有効化するには、Novell サポートナレッジベース (http://support.novell.com/search/kb_index.jsp) の TID 3418069 を参照してください。

Mirror ドライバの新しいバージョンのインストール

ソース : ZENworks 10 Configuration Management、リモート管理。

考えられる原因 : ZENworks Adaptive Agent を Windows 2003 64-bit の管理対象デバイスにインストールした場合は、ミラードライバがデバイスにインストールされません。「新しいバージョンの Mirage ドライバをインストールしてください」というメッセージが ZENworks コントロールセンターに記録されます。

デバイスでリモートセッションを実行できるが、パフォーマンスが低下する。

アクション : このメッセージは無視してください。

考えられる原因 : RDP (Remote Desktop Connection) を使用してすでに接続済みのデバイスをリモートで制御すると、「新しいバージョンの Mirage ドライバをインストールしてください」というメッセージが ZENworks コントロールセンターに記録されます。

デバイスでリモートセッションを実行できますが、パフォーマンスが低下します。

アクション : このメッセージは無視してください。

管理対象デバイスでセッション用に Novell 暗号化方式を初期化できませんでした。管理対象デバイスとこのシステムの UTC 時刻が同期していることを確認してください。問題が継続する場合は、Novell テクニカルサービスにお問い合わせください。

ソース : ZENworks 10 Configuration Management、リモート管理。

考えられる原因 : 管理対象デバイスはアップグレードまたは登録されましたが、この情報は、管理対象デバイスのレジストリ内でアップグレードされていない可能性があります。

アクション : 管理対象デバイスのアップグレード時または登録時に、次の作業を行ってください。

1. レジストリにある新規 CA 証明書のドメイン名を新しい詳細情報で更新します。

   キー : HKLM\Software\Novell\ZCM

   値 : CASubject
2. 新規ゾーンの CA 証明書を、信頼されたルート証明書ストアにインポートします。
3. 古いゾーンの CA 証明書を、信頼されたルート証明書ストアから削除します。

考えられる原因 : 管理対象デバイスが新しい管理ゾーンに移動されています。

アクション : 新しい管理ゾーンからデバイスを管理します。

regedit などのアプリケーションを 64 ビットの管理対象デバイスからリモート実行経由で起動した場合に、特定のレジストリキーにアクセスできない

ソース : ZENworks 10 Configuration Management、リモート管理。

考えられる原因 : 64 ビット管理対象デバイスでリモート実行を使用して起動したアプリケーションは、WOW (Windows On Windows) 環境で実行されます。

アクション : リモート診断を使用してアプリケーションを起動します。

Windows デバイスをリモート制御しているときに［画面の消去］オプションが失敗する

ソース : ZENworks 10 Configuration Management、リモート管理。

考えられる原因 : Windows のレガシドライバでは［画面の消去］電源オプションは許可されていません。

アクション : システム固有のグラフィックドライバをインストールする必要があります。

Windows 2000 Professional 管理対象デバイスでリモート管理セッションを起動すると、デバイスがリブートする

ソース : ZENworks 10 Configuration Management、リモート管理。

考えられる原因 : デバイスにビデオドライバがインストールされていない。

アクション : システム固有のビデオドライバをインストールする必要があります。

Internet Explorer 7 ブラウザを使用しているデバイスで、リモート管理ビューアの複数のインスタンスが起動される

ソース : ZENworks 10 Configuration Management、リモート管理。

考えられる原因 : Internet Explorer 7 ブラウザを使用しているデバイスでリモート管理操作を起動した場合、FlashGet などのダウンロードアクセラレータが管理コンソールにインストールされているとビューアの複数のインスタンスが起動されます。

アクション : ダウンロードアクセラレータのアドオンを一時的に無効にします。

1. Internet Explorer 7 ブラウザを起動します。
2. ［*ツール*］>［*アドオンの管理*］の順にクリックします。
3. ［*アドオンの有効化 / 無効化*］をクリックし、次にダウンロードアクセラレータのアドオンを無効化します。
4. リモート管理操作を起動します。

アクション : Firefox ブラウザを使用して操作を実行してみてください。

Windows Vista、Windows Server 2008、または Windows Server 2008 R2 のデバイスをリモートから制御中に、Ctrl-Alt-Del アイコンを使用できない

ソース : ZENworks 10 Configuration Management、リモート管理。

説明 : UAC (User Account Control) が無効にされている Windows Vistaa、Windows Server 2008、または Windows Server 2008 R2 のデバイスでリモート制御操作を開始すると、［*Ctrl-Alt-Del*］アイコンがグレー表示になります。

アクション : UAC を有効にします。

リモート管理スナップインでデフォルトセッションモードが選択されない

ソース : ZENworks 10 Configuration Management、リモート管理。

説明 : Internet Explorer を使用して ZENworks コントロールセンターを開き、デバイスでリモート管理操作を実行すると、リモート管理スナップインでデフォルトセッションモードが選択されません。ただし、セッションモードを何も選択しないと、リモートコントロール操作はデフォルトコラボレーションモードで起動され、リモートビュー操作はデフォルトの排他モードで起動されます。

アクション : セッションモードを選択してリモート操作を実行してください。

［リモート管理ビューアのインストール］リンクが、Internet Explorer 7 ブラウザを持つ Windows Vista、Windows 7、Windows Server 2008、または Windows Server 2008 R2 のデバイスでアクティブのまま残る

ソース : ZENworks 10 Configuration Management、リモート管理。

説明： Internet Explorer 7 ブラウザのある Windows Vista、Windows 7、Windows Server 2008、または Windows Server 2008 R2 のデバイスで、ActiveX* コントロールがアクティブになっていないと、［*リモート管理ビューア*］のインストールが失敗する場合があります。

アクション： Vista デバイスで次を実行して、ユーザアカウントコントロール (UAC) を有効にします。

1. ［*スタート*］>［*設定*］>［*コントロールパネル*］>［*ユーザアカウント*］>［*ユーザアカウント*］>［*Turn User Account Control On or Off(ユーザーアカウント制御 On/Off)*］の順にクリックします。
2. ［*Use User Account Control (UAC) to help protect your computer(ユーザーアカウント制御 (UAC) を使用してコンピュータを保護する)*］をオンにします。
3. ［*OK*］をクリックします。

アクション: Windows Vista デバイスで UAC をオンにしたくない場合は、Windows Vista SP1 にアップグレードする必要があります。

リモート管理ビューアのインストールに失敗する場合がある

ソース： ZENworks 10 Configuration Management、リモート管理。

説明： リモート管理ビューアのインストールに失敗する場合があります。このエラーは MSI フレームワークに起因するものです。

アクション： 次のいずれかの手順を実行します。

- ［プログラムの追加と削除］を使用してリモート管理ビューアをアンインストールし、再インストールする。
- Microsoft Windows の Installer クリーンアップユーティリティを使用してアプリケーションをクリーンアップし、再インストールする。このユーティリティは Microsoft サポート (http://support.microsoft.com/kb/290301) からダウンロードできます。

リモート管理ビューアが Windows Vista、Windows 7、Windows Server 2008、または Windows Server 2008 R2 のデバイスで起動できない

ソース： ZENworks 10 Configuration Management、リモート管理。

説明： Windows Vista、Windows 7、Windows Server 2008、または Windows Server 2008 R2 のデバイスで、リモート管理ビューアがセキュリティプロンプトを正常に完了した場合でも失敗します。

アクション： ZENworks コントロールセンターを実行しているサーバを信頼済みサイトのリストに追加して、再試行します。

リモートコントロールセッション中に、リモート管理ビューアで［Ctrl+Alt+Del］アイコンをクリックすると、コントロールがまったくない状態の［Secure Attention Sequence］ウィンドウが表示される場合がある

ソース： ZENworks 10 Configuration Management、リモート管理。

アクション : リモート管理ビューアで［*Ctrl+Alt+Del*］アイコンをクリックしてから、Esc キーを押して［Secure Attention Sequence (SAS)］ウィンドウを終了します。続いて、リモート管理ビューアでもう一度［*Ctrl+Alt+Del*］アイコンをクリックします。

デバイスのデスクトップは、デバイスをリモートで制御またはリモートで表示する場合に、表示されないことがある

ソース : ZENworks 10 Configuration Management、リモート管理。

説明 : RDP セッションを実行したデバイスをリモートで制御またはリモートで表示する場合、デバイスのデスクトップが表示されず、何も表示されないことがあります。

アクション : デバイスのデスクトップを表示するには、次の手順に従います。

1 デスクトップを手動でアンロックします。

2 次のコマンドを実行して、RDP セッションをデバイスのコンソールセッションで再起動します。

```
mstsc /console
```

Windows Vista、Windows 7、Windows Server 2008、または Windows Server 2008 R2 のデバイス上の制限されたフォルダにファイルをリモートから転送できない

ソース : ZENworks 10 Configuration Management、リモート管理。

説明 : ファイル転送操作を開始して、ユーザアカウント制御 (UAC) を有効にした Windows Vistaa、Windows 7、Windows Server 2008、または Windows Server 2008 R2 のデバイス上の制限されたフォルダに、リモートからファイルを転送した場合、操作が失敗します。

アクション : Windows Vista デバイスで次を実行して、ユーザアカウント制御 (UAC) を無効にします。

1 *［スタート］>［設定］>［コントロールパネル］>［ユーザアカウント］>［ユーザアカウント］>［Turn User Account Control On or Off(ユーザーアカウント制御 On/Off)］*の順にクリックします。

2 ［*Use User Account Control (UAC) to help protect your computer(ユーザーアカウント制御 (UAC) を使用してコンピュータを保護する)*］をオフにします。

3 ［*OK*］をクリックします。

アクション: Windows 7 デバイスで次を実行して、ユーザアカウント制御 (UAC) を無効にします。

1 *［スタート］>［コントロールパネル］>［ユーザアカウント］>*［*Change User Account Control Settings(ユーザアカウント制御設定の変更)*］の順にクリックします。

2 スライドバーを、決して通知しないという説明が表示された最も低い値 (［*Never Notify(決して通知しない)*］の方向) にスライドさせます。

3 ［*OK*］をクリックします。

4 デバイスを再起動します。

Mozilla Firefox を介して、SUSE Linux Enterprise Server 11 デバイス上でリモートセッションを開始できない

ソース： ZENworks 10 Configuration Management、リモート管理。

説明： Firefox 用のリモート管理プラグインは、/usr/lib/firefox ディレクトリ (デフォルトの Firefox インストールディレクトリでもある) にインストールされています。Firefox を SLES 11 デバイスの別のディレクトリにインストールした場合は、Firefox を使用してリモートセッションを開始するとデバイス上で失敗します。

アクション： nsZenworksPluginSample.so ファイルを /usr/lib/firefox/plugins ディレクトリから Firefox plug-ins ディレクトリにコピーします。

Internet Explorer 8 を介して ZENworks を起動すると、［リモート管理ビューアのアップグレード］リンクが表示されない

ソース： ZENworks 10 Configuration Management、リモート管理。

説明： ZENworks Configuration Management SP2 から ZENworks Configuration Management SP3 にアップグレードし、Internet Explorer 8 を介して ZENworks コントロールセンターを起動した場合、［*リモート管理ビューアのアップグレード*］リンクが ZENworks コントロールセンターで表示されません。

アクション： ［*リモート管理ビューアのアップグレード*］リンクを表示するには、次の手順を実行します。

1. Internet Explorer 8 ブラウザを起動します。
2. ［*ツール*］>［*インターネットオプション*］の順にクリックして、［インターネットオプション］ダイアログボックスを表示します。
3. ［*セキュリティ*］タブをクリックします。
4. ［*カスタムレベル*］オプションをクリックします。
5. 次の設定が有効になっていることを確認します。
   - *ActiveX コントロールとプラグインの実行*
   - *スクリプトを実行しても安全だとマークされていない ActiveX コントロールの初期化とスクリプトの実行*
6. ブラウザを再起動します。

暗号化の詳細

A

次の各セクションでは、Novell® ZENworks® 10 Configuration Management のリモート管理コンポーネントの使用中に生成されるさまざまな証明書の詳細について説明します。

A.1 管理対象デバイスの鍵ペア詳細

Certificate Generated By: Remote Management service
Certificate Generated Using: OpenSSL v0.9.8e (Novell version)
Certificate Signed By: Self-signed
Certificate Signed Using: OpenSSL v0.9.8e (Novell version)
Certificate Verified By: Remote Management viewer
Certificate Verified Using: OpenSSL v0.9.8e (Novell version)
Used By: Remote Management Service
Used For: Establishing a secure session with the Remote Management viewer
Private Key Type: RSA
Key Strength: 1024 bits
Signature Algorithm: RSA-SHA256
Validity: 10 years

A.2 リモートオペレータの鍵ペア詳細

この証明書は、内部 CA を展開する場合にのみ有効です。

Certificate Generated By: ZENworks Server hosting ZENworks Control Center
Certificate Generated Using: Bouncy Castle library (bcprov-jdk15-134.jar)
Certificate Signed By: ZENworks Server hosting ZENworks Control Center
Certificate Signed Using: Bouncy Castle library (bcprov-jdk15-134.jar)
Certificate Verified By: Remote Management Service
Certificate Verified Using: OpenSSL v0.9.8e (Novell version)
Used By: The Remote Management viewer and the Remote Management service
Used For: Establishing secure session and identifying the remote operator
Private Key type: RSA
Key Strength: 1024 bits
Signature Algorithm: RSA-SHA1
Validity: 4 days

A.3 リモート管理チケット詳細

この証明書は、権限認証でのみ有効です。

Ticket Generated By: ZENworks Server hosting ZENworks Control Center
Ticket Generated Using: Bouncy Castle library (bcprov-jdk15-134.jar)
Certificate Signed By: ZENworks Server hosting ZENworks Control Center
Ticket Signed Using: Bouncy Castle library (bcprov-jdk15-134.jar)
Certificate Verified By: Remote Management Web Service (on the ZENworks server)
Certificate Verified Using: Bouncy Castle library (bcprov-jdk15-134.jar)
Used By: The Remote Management viewer and the Remote Management Web service
Used For: Authenticating the remote operator and verifying the rights to perform an operation
Signature Algorithm: RSA-SHA1
Validity: 2 minutes

A.4 セッション暗号化の詳細

Session Established Between: Remote Management Service and Remote Management viewer
Encryption Protocol: SSL (TLSv1)
Session Cipher: AES256-SHA
SSL Authentication Mode: Mutual/Server

ベストプラクティス

B

次の各セクションでは、Novell® ZENworks® 10 Configuration Management のリモート管理コンポーネントの使用時に従うべきベストプラクティスを示します。

B.1 リモート管理リスナを閉じる

リモートオペレータが、管理対象デバイスユーザからのリモートセッション要求をリスンするリモート管理リスナを起動すると、ZENworks は、リモートオペレータが管理対象デバイスから認証を受けるために使用できるチケットを発行します。このチケットの有効期限は 2 日間です。

リモート管理リスナは、リモートオペレータがログアウトした後や、ZENworks コントロールセンターを終了した後も、実行が継続されます。チケットが引き続き有効である場合は、他のリモートオペレータが、このリスナを使用して管理対象デバイスユーザからのリモートセッション要求をリスンする可能性があります。セキュリティ上の理由から、ログアウトする前またはブラウザを閉じる前に、リモート管理リスナを終了するようにしてください。

リモート管理リスナを閉じるには、通知領域にある［*ZENworks Remote Management リスナ*］アイコンを右クリックして、［*リスニングデーモンを閉じる*］をクリックします。

B.2 リモート実行操作時に起動されたアプリケーションを閉じる

リモート管理モジュールは、デフォルトでは、管理デバイス上でシステム権限を持つサービスとして実行されます。したがって、リモート実行セッション中に起動されたアプリケーションは、すべてシステム権限を使用して実行されます。セキュリティ上の理由により、使用後はアプリケーションを閉じることを強くお勧めします。

B.3 管理対象デバイスでのリモートオペレータの識別

リモートオペレータが ZENworks コントロールセンターから管理対象デバイス上でリモートセッションを起動すると、管理対象デバイスがリモートオペレータを識別できるようにする証明書が ZENworks により自動的に生成されます (内部 CA が使用されている場合)。ただし、内部 CA が使用されている場合は、リモートオペレータが、展開済み外部 CA に関連付けられた SSL クライアント認証向けの証明書を手動で提供する必要があります。外部 CA の使用の詳細については、「35 ページのセクション 2.8「リモート管理操作の開始」」の「*識別用に次のキーペアを使用します*」を参照してください。

リモートオペレータが証明書を提供せずに管理対象デバイスでリモート操作を起動する場合は、リモートオペレータの名前が監査ログ、［可視信号］および［Ask User Permission(ユーザ権限要求)］ダイアログボックスで「*不明なユーザ*」として記録されます。リモートオペレータが確実に証明書を提供するように、リモート管理ポリシーで［*リモート管理コンソールに SSL 証明書がない場合は、接続を許可する*］を選択解除します。

B.4 リモートデスクトップ接続により、すでに接続されているデバイスでのリモート制御セッションの実行

RDP (Remote Desktop Connection) を使用してすでに接続されているデバイスをリモート制御セッションするには、次のいずれかの条件が満たされている必要があります。

- 管理対象デバイスで RDP セッションが実行中である
- デバイスでのRDPセッションの終了後に管理対象デバイスのロックが手動で解除されている

B.5 管理コンソール名の決定

リモート管理ポリシーで［*Look up viewer DNS name at the start of the remote session(リモートセッションの開始時にビューアの DNS 名をルックアップ)*］オプションが有効になっている場合は、管理対象デバイスがリモートセッションの開始時に管理コンソール名を決定しようとします。これにより、ネットワークで逆引き DNS ルックアップが有効にされてない場合はリモートセッションの開始で大幅な遅延が発生することがあります。この遅延を回避するには、ポリシーの［*Look up viewer DNS name at the start of the remote session(リモートセッションの開始時にビューアの DNS 名をルックアップ)*］を無効にします。

B.6 Windows Vista、Windows 7、Windows Server 2008、および Windows Server 2008 R2 のデバイスでの Aero テーマの使用

リモートセッションのパフォーマンスを向上させるには、画面の変化を検出するためにリモート管理でミラードライバを使用します。ミラードライバが Aero デスクトップテーマと互換性を持たない場合は、Aero テーマが有効化されたデバイスにミラードライバをロードしようとすると、デバイスでデフォルトのデスクトップテーマに切り替わります。これにより、ユーザの環境に影響が出る場合があるため、リモート管理するデバイスで Aero テーマを使用することは推奨されません。

管理対象デバイスのリモートセッション時に Aero テーマを保持したい場合は、デバイス上でミラードライバを無効にします。ミラードライバを無効にするには、デバイス上の［*最適化ドライバを有効にする*］設定を選択解除します。［最適化ドライバを有効にする］設定の詳細については、ゾーンレベルでのリモート管理設定を参照してください。

ただし、管理対象デバイスで Aero テーマを有効にすると、デバイス上のリモートセッションのパフォーマンスが低下する場合があります。

B.7 Windows Vista または Windows Server 2008 デバイスをリモート制御するときに Secure Attention Sequence (Ctrl+Alt+Del) ボタンを有効化

Windows Vista または Windows Server 2008 デバイスをリモート制御するときにリモート管理ビューアツールバーで(Ctrl+Alt+Del) アイコンを有効にするには、管理対象デバイスで UAC (User Account Control) を有効にします。

B.8 RDP を使用して Windows XP デバイスにリモート管理サービスをインストール

管理対象デバイスへのリモート管理サービスのインストール時に、ZENworks は DFMirage という名前のミラードライバをデバイスに自動的にインストールします。RDP (Remote Desktop Connection) を使用してリモート管理サービスを Windows XP デバイスにインストールする場合は、デバイスに Microsoft サポート Web サイト (http://support.microsoft.com/kb/952132) で提供されているパッチをインストールしてください。

B.9 リモート管理のパフォーマンス

低速リンクまたは高速リンクにおけるリモート管理セッション中のリモート管理パフォーマンスはネットワークトラフィックに応じて変わります。レスポンスを向上させるには、65 ページのセクション 3.8「リモート管理のパフォーマンスの向上」を参照してください。

マニュアルの更新

C

このセクションでは、Novell® Zenworks® 10 Configuration Management SP3 用の『*ZENworks Remote Management リファレンス*』で行われた文書内容の変更について説明します。ドキュメントの最新の更新情報をここで入手できます。

この製品のドキュメントは、HTML および PDF の 2 つの形式で Web にて提供されています。HTML および PDF ドキュメントにはこのセクションに一覧表示された変更が反映され、最新の状態に保たれています。

使用している PDF ドキュメントが最新のものであるかどうかを知る必要がある場合、PDF ドキュメントの表紙の発行日を参照してください。

本書では、次の更新が行われました。

- 91 ページのセクション C.1「2010 年 3 月 30 日 : SP3 (10.3)」

C.1 2010 年 3 月 30 日 : SP3 (10.3)

次の各セクションが更新されました。

場所	変更内容
12 ページの 「リモート管理プロキシ」	セクションが更新されました。
14 ページのセクション 1.3「リモート管理機能の理解」	セクションが更新されました。
31 ページのセクション 2.5「リモート管理パスワードの設定」	セクションが更新されました。
45 ページのセクション 2.9「リモート管理操作の開始に関するオプション」	セクションが追加されました。
49 ページのセクション 2.10「リモート管理プロキシのインストール」	セクションが更新されて、Linux でのリモート管理プロキシのインストールに関するサポートが追加されました。
50 ページのセクション 2.11「リモート管理プロキシの設定」	セクションが追加されました。
63 ページのセクション 3.7「リモートデバイスのウェイクアップ」	セクションが更新されて、複数の NIC を持つデバイスの起動に関する情報が追加されました。
63 ページのセクション 3.6「リモート管理プロキシセッションの管理」	セクションが追加されました。

場所	変更内容
75 ページの第 5 章「トラブルシューティング」	次のシナリオを追加しました。 ◆ 83 ページの 「Mozilla Firefox を介して、SUSE Linux Enterprise Server 11 デバイス上でリモートセッションを開始できない」 ◆ 83 ページの「Internet Explorer 8 を介して ZENworks を起動すると、［リモート管理ビューアのアップグレード］リンクが表示されない」
75 ページの第 5 章「トラブルシューティング」	次のシナリオを追加しました。 Windows Vista または Windows 7 デバイスで、制限されたフォルダにリモートからファイルを転送できない
88 ページのセクション B.6「Windows Vista、Windows 7、Windows Server 2008、および Windows Server 2008 R2 のデバイスでの Aero テーマの使用」	セクションが更新されました。