

ZENworks 2020 新機能リファレンス

2019年10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。

© Copyright 2008 - 2019 Micro Focus or one of its affiliates.

Micro Focus、関連会社、およびライセンサ (「Micro Focus」) の製品およびサービスに対する保証は、当該製品およびサービスに付属する保証書に明示的に規定されたものに限られます。本書のいかなる内容も、当該保証に新たに保証を追加するものではありません。Micro Focus は、本書に技術的または編集上の誤りまたは不備があっても責任を負わないものとします。本書の内容は、将来予告なしに変更されることがあります。

目次

このガイドについて	5
1 ZENworks 2020 Update 3	7
1.1 新しいプラットフォームのサポート	7
1.2 サポートされていないプラットフォームと機能	8
1.2.1 サポートされていないプラットフォーム	8
1.2.2 サテライトサーバとしての 32 ビットデバイスの昇格をサポートしない	8
1.3 セキュリティ (パッチ管理、ZFDE および ZESM)	9
1.3.1 CVE を使用したソフトウェアセキュリティの脆弱性に対するパッチ適用	9
1.3.2 新しいセキュリティのはじめにページ	9
1.3.3 ユーザインタフェース関連の変更	9
1.3.4 セキュリティダッシュボード	10
1.3.5 パッチスキャンの開始クイックタスク	11
1.3.6 シャットダウン時のパッチの適用	11
1.3.7 エンドポイントセキュリティ	11
1.4 ZENworks Configuration Management	12
1.4.1 インストールとアップグレード	12
1.4.2 バンドル管理	12
1.4.3 モバイル管理	13
1.4.4 プレブートイメージング	14
1.4.5 リモート管理	14
1.4.6 デバイス管理	14
1.4.7 ZENworks エージェント	15
1.4.8 データベース管理	16
1.4.9 その他の機能	17
1.5 レポートティング	17
1.5.1 レポートティングにおける Vertica ドメインのサポート	17

このガイドについて

この『ZENworks 新機能リファレンス』では、ZENworks 2020 リリースの新機能について説明します。このガイドは、次の章で構成されています。

- ◆ [7 ページの第 1 章「ZENworks 2020 Update 3」](#)

対象読者

このガイドは、ZENworks 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。オンラインヘルプの各ページの下部にある、[\[このトピックに関するコメント\]](#)機能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。その他のマニュアルについては、[ZENworks マニュアル Web サイト](#)を参照してください。

1 ZENworks 2020 Update 3

次の各セクションでは、ZENworks 2020 の新機能と拡張機能について説明します。

- ◆ 7 ページのセクション 1.1 「新しいプラットフォームのサポート」
- ◆ 8 ページのセクション 1.2 「サポートされていないプラットフォームと機能」
- ◆ 9 ページのセクション 1.3 「セキュリティ (パッチ管理、ZFDE および ZESM)」
- ◆ 12 ページのセクション 1.4 「ZENworks Configuration Management」
- ◆ 17 ページのセクション 1.5 「レポートिंग」

1.1 新しいプラットフォームのサポート

このリリースでは、次の新しいプラットフォームがサポートされています。

- ◆ ZENworks アプライアンス : SLES 12 SP4 オペレーティングシステムに基づく
- ◆ プライマリサーバ :
 - ◆ Windows: Windows Server 2019
 - ◆ Linux: SLES 15 および SLES 15 SP1
- ◆ 管理対象デバイス :
 - ◆ Windows: Windows 10 (バージョン 1903)
 - ◆ Linux: RHEL 6.6 ~ 7.3、Scientific Linux 6.6 ~ 7.3、SLES/SLED 15、および SLES/SLED 15 SP1、OpenSUSE Leap 15 SP1
- ◆ データベース :
 - ◆ PostgreSQL 11.4 (組み込みデータベース)
 - ◆ PostgreSQL 11.1 (外部データベース)
 - ◆ Microsoft SQL Server 2019
 - ◆ Oracle 18cR1 および Oracle 19c
- ◆ 管理ブラウザ : Firefox ESR 60
- ◆ モバイル
 - ◆ iOS 13
 - ◆ Android 10

注: このリリースにサポートされるプラットフォームについては、『ZENworks 2020 のシステム要件』ドキュメントを参照してください。

1.2 サポートされていないプラットフォームと機能

- ◆ 8 ページのセクション 1.2.1 「サポートされていないプラットフォーム」
- ◆ 8 ページのセクション 1.2.2 「サテライトサーバとしての 32 ビットデバイスの昇格をサポートしない」

1.2.1 サポートされていないプラットフォーム

ZENworks 2020 では、次のプラットフォームはサポートされていません。

- ◆ サポートされていないプライマリサーバプラットフォーム
 - ◆ Windows 2008 および 2008 R2
 - ◆ RHEL (すべてのバージョン)
 - ◆ Windows 2003
 - ◆ SLES 11 SP3 以前
 - ◆ SLES 12 SP2 以前
- ◆ サポートされていないサテライトサーバプラットフォーム
 - ◆ Windows Vista
 - ◆ Windows XP
 - ◆ SLES 11 SP3 以前
 - ◆ SLED 11 SP3 以前
 - ◆ RHEL 6.8 以前
- ◆ サポートされていないデータベースプラットフォーム
 - ◆ Sybase Anywhere (すべてのバージョン)
 - ◆ Oracle 11.x
 - ◆ Microsoft SQL Server 2008 バージョン (R2 および SP3)

1.2.2 サテライトサーバとしての 32 ビットデバイスの昇格をサポートしない

ZENworks では、32 ビットデバイスをサテライトサーバの役割に昇格させたり、既存の 32 ビットサテライトサーバに新しい役割を追加したりすることができなくなりました。ただし、ZENworks では引き続き既存の 32 ビットサテライトサーバをサポートします。

1.3 セキュリティ (パッチ管理、ZFDE および ZESM)

新しいセキュリティ機能では、脆弱性ベースのビューを使用してデバイスのセキュリティステータスを迅速に把握できるようすることにより、多くの管理者が直面するセキュリティの課題に対処します。この機能を使用して、管理者はゾーン内のデバイスに影響を与える脆弱性を簡単に特定して修復できます。これは、次により実現されます。

- ◆ 9 ページのセクション 1.3.1「CVE を使用したソフトウェアセキュリティの脆弱性に対するパッチ適用」
- ◆ 9 ページのセクション 1.3.2「新しいセキュリティのはじめにページ」
- ◆ 9 ページのセクション 1.3.3「ユーザインタフェース関連の変更」
- ◆ 10 ページのセクション 1.3.4「セキュリティダッシュボード」
- ◆ 11 ページのセクション 1.3.5「パッチスキャンの開始クイックタスク」
- ◆ 11 ページのセクション 1.3.6「シャットダウン時のパッチの適用」
- ◆ 11 ページのセクション 1.3.7「エンドポイントセキュリティ」

1.3.1 CVE を使用したソフトウェアセキュリティの脆弱性に対するパッチ適用

セキュリティの観点から、ソフトウェアの脆弱性を追跡する主な方法は Common Vulnerabilities and Exposures (CVE) です。ZENworks では CVE を介してデバイスの脆弱性を追跡できるようになりました。CVE はパッチにマップされるため、パッチを手動で選択する必要なしに、脆弱性を簡単に修復できます。CVE ダッシュレットを使用して脆弱性を修復することができます。

詳細については、『[CVE Reference](#)』を参照してください。

1.3.2 新しいセキュリティのはじめにページ

新しい [はじめに] ページでは、ゾーン内のセキュリティを設定および追跡するプロセスを簡素化し、利用可能なデバイスにパッチを適用することにより脆弱性を修復できます。このページを使用して脆弱性を軽減することができるとともに、デバイスを暗号化および保護することもできます。

詳細については、『[ZENworks Security Reference](#)』を参照してください。

1.3.3 ユーザインタフェース関連の変更

- ◆ 次の UI の変更により、管理者は、ZENworks によって提供されるすべてのセキュリティ機能間を簡単に移動できるようになりました。
 - ◆ パッチ管理、デバイス暗号化、およびデバイスのセキュリティ保護機能が新しい [セキュリティ] タブ内でグループ化されるようになりました。

- ◆ 管理ゾーン設定には、パッチ管理とエンドポイントセキュリティ設定を含む新しいセキュリティリストがあります。
- ◆ ZCC の左側のナビゲーションメニューにあるパッチ管理機能は、セキュリティ機能に置き換えられました。
- ◆ 選択したパッチに関連する包括的な情報を表示します。パッチオブジェクトのページには、次のタブが含まれます。
 - ◆ パッチ情報：パッチに関する詳細、パッチで対処される CVE、およびパッチの置き換えの詳細。これらはレポートおよび調査目的に役立ちます。
 - ◆ 関係：パッチポリシー、改善の展開、および選択したパッチに関連付けられたバンドルに関する情報。
 - ◆ デバイス：パッチによって影響を受けるデバイス、最後にパッチスキャンが実行された時刻、パッチステータス、割り当てられた改善、割り当てをインストールしたソースの名前 (ZENworks またはその他)、および割り当てがデバイスにインストールされた時刻に関する情報。
- ◆ デバイスの脆弱性ステータスに関する包括的な情報を表示します。[デバイス] ページで、適用可能なパッチ、パッチポリシーの割り当て、デバイスに行われたパッチ改善の割り当てに関する情報を表示できます。パッチがいつインストールされたか、ZENworks または別のソースによってインストールされたかどうかとも特定できます。

1.3.4 セキュリティダッシュボード

新しいセキュリティダッシュボードでは、ゾーンの脆弱性ステータスを監視し、セキュリティダッシュボードを使用して脆弱性を修復することができます。これらのダッシュレットは、重要な CVE とパッチ、および環境における影響を追跡するためにカスタマイズできます。セキュリティダッシュレットには、次のものが含まれます。

- ◆ パッチトラッカー：[パッチトラッカー] ダッシュレットでは、単一のパッチまたは複数の関連付けられたパッチを追跡し、脆弱なデバイスの現在のパッチステータスを表示できます。脆弱なデバイスを特定した後で、改善の展開クイックタスクを使用して、これらのデバイスに必要なパッチを適用することができます。[パッチトラッカー] ダッシュレット内のトレンドチャートは、特定の期間の間に分析および追跡することができます。
- ◆ CVE トラッカー：[CVE トラッカー] ダッシュレットでは、単一の、または複数の関連した CVE を追跡できます (NVD 問題の CVE ID)。指定された CVE については、適用可能なデバイスの合計数を追跡したり、依然として脆弱であるデバイスを特定したりできます。脆弱なデバイスを特定した後で、改善の展開クイックタスクを使用して、これらのデバイスに必要なパッチを適用することができます。ダッシュレットの [脆弱性トレンド] セクションで、選択した CVE の脆弱性トレンドを特定の期間、分析および追跡することができます。
- ◆ CVE 重大度分布：[CVE 重大度分布] ダッシュレットには、重大度に基づいてグループ化された、ゾーン内のデバイスに適用可能なすべての CVE が表示されます。要件に基づいて、対処する必要がある脆弱性を特定し、優先順位をつけるためにデータを簡単

にフィルタし、ソートすることができます。脆弱性を修復するには、デバイスを選択して、改善の展開クイックタスクを実行することで必要なパッチを適用することができます。

- ◆ 上位 CVE: [上位 CVE] ダッシュレットは、デフォルトで、最近発行された CVE に基づいて上位 CVE を表示します。フィルタを変更して、脆弱なデバイスの最大数または重大度評価に基づいて上位 CVE を表示することができます。要件に基づいて、対処する必要がある脆弱性を特定し、優先順位をつけるためにデータを簡単にフィルタし、ソートすることができます。脆弱性を修復するには、デバイスを選択して、改善の展開クイックタスクを実行することで必要なパッチを適用することができます。

詳細については、『[CVE Reference](#)』の「[ZENworks Patch Management Reference](#)」を参照してください。

1.3.5 パッチスキャンの開始クイックタスク

選択したデバイスに対してこのクイックタスクを開始すると、ZENworks では、スケジュール設定したスキャンを待機することなく、選択したデバイスに必要なパッチでプライマリサーバを更新し、パッチがキャッシュやインストールに対して特定できるようにします。

詳細については、『[ZENworks Patch Management Reference](#)』の「[Initiating a Patch Scan](#)」を参照してください。

1.3.6 シャットダウン時のパッチの適用

この機能により、管理者はデバイスのシャットダウン時にパッチポリシーを展開できるようになるため、エンドユーザの通常の操作に影響を及ぼすことなく、エンドユーザのデバイス上で、組織によって必要とされるパッチの展開が可能になります。現在、この機能は、Windows 管理対象デバイスでのみ使用可能です。

詳細については、『[ZENworks Patch Management Reference](#)』の「[Patch Policy Reboot Behavior](#)」セクションを参照してください。

1.3.7 エンドポイントセキュリティ

次のエンドポイントセキュリティポリシーには、機能拡張が示されています。

- ◆ Microsoft データ暗号化ポリシー: このポリシーには、Microsoft の Windows 暗号化ファイルシステム (EFS) の管理が追加されました。これにより、管理対象デバイス上で固定ディスクフォルダを暗号化する機能が追加されます。ポリシーが適用されると、デフォルトでフォルダを暗号化するように設定することができ、エンドユーザは自身のフォルダを暗号化できるようになります。暗号化されたフォルダは、ユーザのプロファイル外のデフォルトのポリシーフォルダであるか、ユーザのプロファイル内またはプロファイル外のユーザによって暗号化されたかどうかによって、パブリックまたはプライベートにすることもできます。この機能には、ユーザパスワードを忘れた場合に管理者が使用するための、組み込みのスタンドアロンリカバリツールもあります。
- ◆ ストレージデバイス制御: このポリシーには、Windows ポータブルデバイス (WPD) として特定するデバイスの制御が追加されました。これには、WPD メディア用に設定可能な例外リストの追加が含まれます。

1.4 ZENworks Configuration Management

- 12 ページのセクション 1.4.1 「インストールとアップグレード」
- 12 ページのセクション 1.4.2 「バンドル管理」
- 13 ページのセクション 1.4.3 「モバイル管理」
- 14 ページのセクション 1.4.4 「プレブートイメージング」
- 14 ページのセクション 1.4.5 「リモート管理」
- 14 ページのセクション 1.4.6 「デバイス管理」
- 15 ページのセクション 1.4.7 「ZENworks エージェント」
- 16 ページのセクション 1.4.8 「データベース管理」
- 17 ページのセクション 1.4.9 「その他の機能」

1.4.1 インストールとアップグレード

- 12 ページの「更新された ZENworks インストーラ」

更新された ZENworks インストーラ

更新された ZENworks 2020 インストーラにより、最初にデータを Sybase から PostgreSQL に移行してから、管理ゾーンを ZENworks 2020 にアップグレードできます。以下はインストーラに導入された追加機能です。

- ライセンスの変更: 新しいインストーラでは、ZENworks Suite ライセンスから個別ライセンスに、または個別ライセンスから ZENworks Suite ライセンスに変更するオプションがあります。
- ZENworks Diagnostic Center (ZDC) チェック: 管理ゾーンをアップグレードする前に、ZENworks および Audit データベースのヘルスを確認するためのアップグレードフローに新たなステップが導入されました。
- サービスチェック: ZENworks サービスが管理ゾーンのすべてのプライマリサーバ上で停止されているかどうかを確認するための新たなステップが導入されました。サービスが停止されていない場合、サービスがまだ実行されているすべてのプライマリサーバを一覧表示するファイルの場所を含むエラーウィンドウが表示されます。

詳細については、『ZENworks サーバインストールガイド』を参照してください。

1.4.2 バンドル管理

このリリースでは、ZENworks にバンドルダッシュボード機能といくつかのバンドル機能拡張が導入されています。

- 13 ページの「バンドルダッシュボード」
- 13 ページの「古いバンドルバージョンのクリーンアップ」
- 13 ページの「実行可能ファイルのインストールアクション」

バンドルダッシュボード

バンドルダッシュボード機能の主なメリットには次のものがあります。

- 新しい [バンドルのステータス] ダッシュレットを使用して、バンドルの正確な割り当て、配布、インストール、および起動ステータスを監視できるようになりました。
- バンドルダッシュレットでは、ステータス情報がコレクションフレームワークからではなく、プライマリサーバに直接送信されるため、ステータス情報をより迅速に提供されます。
- これらのダッシュレットは、依存チェーン内の親バンドルと子バンドル両方の完全なステータスと、割り当て、配布、インストール、および起動のバージョン固有のステータスを追跡します。
- ステータスのバージョン管理では、デバイスが再イメージされる時、またはキャッシュがクリアされる時にステータスを自動的に再調整することにより、ステータスの精度を向上させます。
- ダッシュレットデータは最適化および圧縮され、帯域幅の使用を最小限に抑えます。

詳細については、『ZENworks Software Distribution Reference』の「[Accessing the Bundle Dashboard](#)」を参照してください。

古いバンドルバージョンのクリーンアップ

不要で古いバンドルバージョンをクリーンアップ可能な設定が ZCC で利用できるようになり、バンドルの不要な古いバージョンによってスペースが占有されないようになりました。

実行可能ファイルのインストールアクション

実行可能ファイルのインストールアクションにより、管理者は実行可能ファイルをアップロードし、起動オプションを指定することができます。実行可能ファイルおよび関連するファイルが管理対象デバイスにダウンロードされ、デバイス上で直接起動されます。単一アクションでアプリケーションをインストールおよび起動する機能により、管理者のプロセスが簡素化されます。

詳細については、『ZENworks Software Distribution Reference』の「[Action - Install Executable](#)」を参照してください。

1.4.3 モバイル管理

- [13 ページの「iOS 更新バンドルのサポート」](#)

iOS 更新バンドルのサポート

新しい iOS 更新バンドルを使用して、ZENworks で管理対象 iOS デバイスフリートに iOS 更新を展開できます。

詳細については、『ZENworks Mobile Management Reference』の「[Creating iOS OS Update Bundles](#)」を参照してください。

1.4.4 プレブートイメージング

- [14 ページの「Mac イメージングのサポート」](#)

Mac イメージングのサポート

NetBoot サービス機能を使用すると、管理者は既存の ZENworks プライマリサーバおよびサテライトサーバ (ZENworks 2020 にアップグレード) を Apple NetBoot サーバとして使用し、MAC アドレスとモデル詳細を使用して、NetBoot、NetRestore、および NetInstall イメージを Apple Mac デバイスに割り当てることができます。

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。

1.4.5 リモート管理

- [14 ページの「新しいリモート管理ビューア」](#)

新しいリモート管理ビューア

ZENworks では、新しくアップグレードされたリモート管理 (RM) ビューアを提供できるようになりました。新しい RM ビューアには限定的な機能があり、デバイスをリモート制御する際により優れたパフォーマンスを発揮します。したがって、要件に基づいた古いまたは新しいビューアを使用することを選択できるようになりました。このリリースでは、新しい RM ビューアへの実験段階のサポートが提供されます。

詳細については、『[ZENworks Remote Management リファレンス](#)』を参照してください。

1.4.6 デバイス管理

- [14 ページの「Windows 10 MDM のサポート」](#)
- [15 ページの「SSL を介したコレクションロールアップ」](#)

Windows 10 MDM のサポート

管理者は、Windows 10 MDM エージェントを使用して Windows 10 デバイスを管理できるようになりました。Windows MDM 一括登録機能により、Windows 10 デバイスをプロビジョニングパッケージを使用して ZENworks に一括登録することができます。ユーザ操作は最低限に抑えられます。このリリースでは、この機能は依然として開発中であり、実験段階のサポートのみが提供されます。

詳細については、『[Windows 10 MDM Enrollment Reference](#)』を参照してください。

SSL を介したコレクションロールアップ

この機能を使用すると、SSL を介したサテライトサーバ上でコレクションロールアップが可能になります。昇格するコレクションサテライトサーバごとに SSL を有効にすることを選択できます。コレクション役割が SSL で昇格される場合、サテライトサーバによりその管理対象デバイスが HTTPS を介してサテライトサーバと通信できます。また、サテライトサーバおよびプライマリサーバ通信は、サテライトサーバが ZENworks 2020 にアップグレードされた後で、HHTTPS を介して実行されます。

詳細については、『*ZENworks Primary Server and Satellite Reference*』の「[Collection Role](#)」セクションを参照してください。

重要: このリリースでは、外部認証局を使用した Mac サテライトサーバ上で、SSL を介したコレクションロールアップはサポートされていません。

1.4.7 ZENworks エージェント

- 15 ページの「ZENworks アプリケーション (ZAPP) でバンドルをお気に入りとして設定する」
- 15 ページの「ZCC で ZENworks Updater Service (ZeUS) のステータスを表示する」
- 16 ページの「デバイス上のバンドルの有意義なアクティビティの表示」

ZENworks アプリケーション (ZAPP) でバンドルをお気に入りとして設定する

ZENworks Explorer 設定ポリシーを使用して、ZAPP ウィンドウで特定のバンドルをお気に入りとして設定できます。これらのバンドルは ZAPP ウィンドウおよび ZENworks Explorer ウィンドウの左ペインに表示されるお気に入りフォルダに表示できます。ZENworks Explorer 設定ポリシーを使用して、ZAPP ウィンドウが開くときのデフォルトフォルダとしてフォルダ (すべて、お気に入り、または最終) を設定することもできます。

詳細については、『*ZENworks Application 2020*』ガイドを参照ください。

ZCC で ZENworks Updater Service (ZeUS) のステータスを表示する

ZeUS がデバイス上でアクティブであるかどうかを、ZCC 内で表示できるようになりました。この機能を使用すると、アクセスできないデバイスに関する正確な情報を取得できません。

注: 詳細については、『*ZENworks Discovery, Deployment, and Retirement Reference*』の「[Viewing and Updating the Managed Device Details](#)」セクションを参照してください。

デバイス上のバンドルの有意義なアクティビティの表示

子バンドルに対しても実行中のアクションセット名を表示することで、デバイス上のバンドルアクティビティのより正確な進行状況が表示されるようになりました。それにより、エンドユーザはバンドルアクティビティのより正確なステータスが提供されるようになります。この機能により、お客様は進行状況ウィンドウで現在実行中のアクションおよびバンドルアイコンを表示することができます。[バンドル動作の表示] ウィンドウには、子バンドルに対しても、ZAPP 進行状況ウィンドウで表示されるのと同じ情報が表示されます。

1.4.8 データベース管理

- [16 ページの「組み込み PostgreSQL DB の自動バックアップ」](#)
- [16 ページの「Vertica を使用したパフォーマンスのアップグレード」](#)
- [16 ページの「データベースマイグレーションツール」](#)

組み込み PostgreSQL DB の自動バックアップ

このリリースの一部として、新しい反復キューアクションが導入され、組み込み ZENworks データベースの週次バックアップが実行されます。デフォルトでは、Audit データベースはバックアップされません。ただし、必要に応じて設定することができます。バックアップは毎週日曜日の午後 12 時にスケジュールされます。ただし、必要に応じてこのスケジュールの上書き、新しいスケジュールの設定、バックアップファイルの場所の変更が可能です。

詳細については、『[ZENworks 2020 System Backup](#)』ガイドを参照してください。

Vertica を使用したパフォーマンスのアップグレード

ZENworks では、Vertica データベースの機能を活用して、ステータスコンポーネントのスケラビリティおよびパフォーマンスを強化することができます。Vertica は大量のデータを分析しながらクエリのパフォーマンスとスケラビリティを向上させるため、ダッシュレット内のデータをクエリする際に発生する遅延をゾーン内で Vertica を有効にすることで軽減できます。また、パッチトラッカーおよび CVE トラッカーのダッシュレット内の履歴トレンディングデータを表示するため、ゾーン内の Vertica を有効にしておく必要があります。ZENworks は、オプションコンポーネントとして Vertica を提供します。これは、ZENworks アプライアンスでのみ使用できます。

詳細については、『[Vertica Reference](#)』を参照してください。

データベースマイグレーションツール

ZENworks 2020 以降、Sybase データベースはサポートされなくなりました。また、Sybase データは他の ZENworks サポート対象データベースに移行する必要があります。新しいデータベースマイグレーションツールを使用して、Sybase データベースは簡単に PostgreSQL に移行できます。

1.4.9 その他の機能

このリリースには、次の機能も含まれます。

- [17 ページの「メモリ調整ツール」](#)

メモリ調整ツール

ZENworks は、使用可能なデバイスメモリに基づいて、アプライアンスまたは非アプライアンスサーバで実行されているすべての ZENworks プロセスの適切なメモリを調整し割り当てる新しい設定アクションを提供します。このツールを使用して、選択したサーバで実行中のすべてのサービスの現在のメモリ調整を特定することもできます。

詳細については、『*Vertica Reference*』の「[Managing Vertica Memory Requirements](#)」セクションおよび『*ZENworks アップグレードガイド*』の「[ZENworks Server でのメモリ要件の管理](#)」セクションを参照してください。

1.5 レポートティング

- [17 ページのセクション 1.5.1 「レポートティングにおける Vertica ドメインのサポート」](#)

1.5.1 レポートティングにおける Vertica ドメインのサポート

ZENworks Reporting では、パッチおよびバンドルステータスの Vertica ドメインがサポートされるようになりました。

詳細については、『*ZENworks Reporting Universe Objects and Predefined Reports Reference*』を参照してください。

