ZENworks 2020 Update 2
新機能リファレンス

2021 年 8 月

保証と著作権

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

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

この『*ZENworks 新機能リファレンス*』では、ZENworks 2020 Update 2 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 2 の新機能」

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 2 の新機能

次の各セクションでは、ZENworks 2020 Update 2 の新機能と拡張機能を説明します。

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。

- 管理対象デバイスとしての CentOS
- 管理対象デバイスとしての macOS 11 (Big Sur)
- Android 11
- iOS 14
- SLES 15 SP2
  - SLES 15 SP2 (プライマリサーバ)
  - SLES 15 SP2 (管理対象デバイス - SLES for SAP を含む)
  - SLED 15 SP2 (管理対象デバイス)
- 新しい RHEL および Scientific Linux プラットフォーム
  - Scientific Linux 7.7 および 7.8
  - RHEL 7.8 および 8.2

インストールとアップグレード

ZENworks は、より堅牢で柔軟なアーキテクチャの採用と Micro Focus 標準との適合を目指しているため、ZENworks 2020 Update 2 リリースのインストールとアップグレードプロセスにいくつかの拡張機能が導入されました。このリリースで導入された変更は次のとおりです。

Docker と Docker Compose のインストール

Linux プライマリサーバに ZENworks 2020 Update 2 をアップグレードまたはインストールする前に、Docker と Docker Compose をサーバにインストールする必要があります。Docker の詳細については、https://docs.docker.com/ を参照してください。

サーバデータの新しいファイルパスへの移行

Windows、アプライアンス、または Linux プライマリサーバで ZENworks 2020 Update 2 にアップグレードした後で、Novell ファイルパスの以前の MSI、RPM、ログ、設定ファイルなどの ZENworks サーバデータは、新しい Micro Focus ファイルパスに移行されます。

たとえば、Linux サーバの場合、以前の設定ファイル : /etc/opt/novell/zenworks は、/etc/opt/microfocus/zenworks で利用できるようになります。同様に、Windows サーバの場合、以前の設定ファイル : C:\Program Files(x86)\Novell\ZENworks\conf は、C:\Program Files (x86)\Micro Focus\ZENworks\conf で利用できるようになります。

ZENworks エージェント関連のファイルとデータは、古い Novell の場所に保持されます。

ZENworks サーバサービスの名前変更

Windows、アプライアンス、または Linux プライマリサーバで ZENworks 2020 Update 2 にアップグレードした後で、ZENServer サービス、ZENLoader サービス、ZENJoinProxy サービスなどの特定の ZENworks サーバサービスの名前が Novell から Micro Focus に変更されます。たとえば、Linux サーバの場合、novell-zenserver.service は、microfocus-zenserver.service に名前変更されます。

新しい環境変数の導入

Windows サーバの場合、新しい環境変数 %ZENSERVER_HOME% が導入され、デフォルト以外のパスのサーバインストール場所も指すようになりました (C:\Program Files(x86)\Micro Focus\ZENworks)。

TLS バージョン

ZENworks 2020 Update 2 を新規にインストールした場合、デフォルトで TLS1.2 がゾーンで有効になり、4.7 より前の Microsoft .NET バージョンがインストールされたデバイスを登録しようとすると、デバイス登録は失敗します。ただし、エージェントはデバイスにインストールされます。

既存のゾーンを ZENworks 2020 Update 2 にアップグレードする場合、TLS1.2 はデフォルトで有効になりません。ゾーンで TLS1.2 を有効にしている場合、一部の機能が期待どおりに機能しない可能性があり、ゾーン内のすべてのデバイスに Microsoft .NET 4.7 をインストールする必要があります。

ゾーンで TLS1.2 を有効にしている場合、デバイスを登録するには、デバイスに Microsoft .NET 4.7 がインストールされている必要があります。

プライマリサーバの置き換え

最初のプライマリサーバを 2 番目のプライマリサーバと置き換えるか、または既存のプライマリサーバを新しいプライマリサーバと置き換える方法に関する詳細については、『*ZENworks Disaster Recovery Reference*』の「*Replacing Primary Servers*」を参照してください。

アプライアンスへのプライマリサーバの移行

既存のプライマリサーバ (Windows または Linux) をアプライアンスサーバに移行する手順の詳細については、『*ZENworks Primary Server and Satellite Reference*』の「*Moving from a Windows or Linux Primary Server to Appliance*」を参照してください。

ZENworks Configuration Management

Windows 10 デバイスの管理

ZENworks 2020 Update 2 リリースでは、これらのデバイスに組み込まれた MDM エージェントを使用して、Windows 10 デバイスのライフサイクル全体を管理する新機能が追加されました。Windows 10 デバイスの機能以外のユースケースに対処するため、Windows 10 MDM エージェントを使用するデバイスに ZENworks エージェントを展開することもできます。

このセクションに一覧にされている各機能の詳細については、『Windows MDM Reference』を参照してください。

新機能は次のとおりです。

設定機能

Windows Modern Management で管理されている Windows デバイスにプッシュ通知を送信するように Windows 通知サービス (WNS) を設定できるようになりました。

登録機能

以下の登録機能が導入されました。

登録方法 : Windows 10 デバイスは次の方法を使用して、ZENworks に登録できます。

- プロビジョニングパッケージ (PPKG) 登録
- Azure Active Directory (Azure AD) 参加
- AutoPilot 登録

ZENworks Agent の展開 : MDM モードの登録を使用してすでに登録されている Windows 10 デバイスに ZENworks Agent を展開できるようになりました。

利用規約の設定 : 利用規約ポリシーをデバイスに割り当てて、Azure AD 参加または AutoPilot 登録のいずれかを使用して Windows 10 デバイスを登録する際にエージェントに表示される利用規約コンテンツを追加できます。

管理機能

以下の管理機能が導入されました。

Windows 10 MDM バンドルの展開 : 以下のバンドルを Windows 10 MDM デバイスに展開できるようになりました。

注 : これらのバンドルのサポートは実験を目的としており、評価目的でのみ使用する必要があります。

- Windows 10 MDM - Install MSI バンドルを使用して、Microsoft インストーラ (MSI) パッケージを Windows 10 MDM デバイスに展開します。
- Windows 10 MDM CSP バンドルを使用して、構成サービスプロバイダ (CSP) を配布し、Windows 10 MDM デバイス上に CSP を介して使用可能なさまざまな構成を展開します。

クイックタスクの開始 : 次のクイックタスクが、Windows 10 MDM デバイスでサポートされています。

- デバイスを削除する
- デバイスの登録解除
- デバイスをリタイアする
- デバイスのリタイア解除
- 紛失したデバイス
- デバイスの登録解除

その他の機能

Windows 10 MDM 機能に導入されたその他の機能の一部は次のとおりです。

- Windows 10 デバイスは自動調整をサポートしています。
- CA 再作成プロセスが Windows 10 MDM デバイスに証明書を発行するようになりました。
- MS Graph API 設定は、Azure MDM アプリケーションに名前変更されているため、このリリースで導入された新しい拡張機能を利用するには、再構成する必要があります。

Getting Started with Modern Management (Modern Management の導入)

モバイル管理の［はじめに］ページが一新され、Windows 10 MDM デバイスの登録と管理も含まれるようになりました。詳細については、『Modern Management Reference』を参照してください。

ZENworks Imaging

WinPE でのバンドル名を使用したイメージの復元 : ZENworks 2020 Update 1 以前のバージョンでは、WinPE ディストリビューションは、IMG コマンドを使用してイメージ名を指定することでイメージの復元をサポートしていましたが、バンドルがコマンドを通過したかどうかをコマンドは認識しませんでした。ZENworks 2020 Update 2 以降、IMG バンドルコマンドは WinPE ディストリビューションでサポートされています。詳細については、『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。

ZENworks イメージ情報を読み込むための新しいツール : イメージに関する情報を収集するのに役立つ zmginfo ツール。これは、コンテンツリポジトリまたは共有パスに複数のイメージがあり、時間を節約するために各イメージに関する情報を収集する必要がある場合に特に役立ちます。zmginfo ツールを使用して、イメージに関する基本情報または完全な情報を収集できます。管理者は zmginfo を使用して、バンドルとしてインポートしてすべての linux ベースイメージを winpe ベースイメージに変換するために使用できるバンドル xml を作成できます。

詳細については、『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。

ZENworks Remote Management

アクティブな RDP セッションを持つデバイスのリモート管理 : 通常のリモート管理セッションと同様に、アクティブな RDP セッションを持つデバイスでリモートセッションを起動できるようになります。詳細については、『Remote Management リファレンス』を参照してください。

リモート管理セッションの記録 (実験的サポート): 管理対象デバイスのユーザがリモート管理セッションを記録できるようにします。詳細については、『Remote Management リファレンス』を参照してください。

モバイル管理

Android バンドルのデバイス割り当ての有効化 : 以前はユーザの割り当てに制限されていた承認済みの Play ストアアプリ用に作成された Android バンドルを、デバイスにも割り当てることができるようになりました。詳細については、『Mobile Management Reference』を参照してください。

システムアプリのプロビジョニング : バンドル機能を使用すると、Android デバイスでシステムアプリを有効または無効にできます。システムアプリは、すでにデバイス上に事前インストールされた組み込みアプリです。詳細については、『Mobile Management Reference』を参照してください。

Modern Management の［はじめに］ : モバイル管理の［はじめに］ページが一新され、Windows 10 MDM デバイスの登録と管理も含まれるようになりました。また、Apple および Android デバイスの登録と管理に関連付けられている特定の追加機能もこのページに含まれています。詳細については、『Modern Management Reference』を参照してください。

Android デバイスログの場所の変更 : Android デバイス上の ZENworks アプリログの場所が Android/data/com.novell.zapp/files/Documents/zapp.log に変更されました。これらのログを共有するには、Android デバイスに Files アプリを展開する必要があります。

バンドル管理

関係のコピーワークフローに新しい **[エラー発生時に続行する]** オプションが導入されました。あるデバイスから別のオブジェクトセットに関係をコピーしているときにエラーが発生した場合、残りのオブジェクトに対して操作が続行されます。エラーの詳細は、操作の最後に表示され、さらに参照してアクションを実行するために操作の詳細をエクスポートするオプションも表示されます。詳細については、『ソフトウェア配布リファレンス』を参照してください。

その他

お客様が最新バージョンの puppet-agent パッケージを使用できるようにする : 以前に、ZENworks では、ビルドの一部として、ユーザがパペットポリシーを使用できるようにする、puppet-agent パッケージを提供していました。しかし、ZENworks リリース後に puppet-agent バージョンの継続的な更新を行うことにより、ユーザは puppet-agent パッケージの最新バージョンを使用できなくなりました。このリリース以降、Linux 管理対象デバイスの ZENworks 2020 Update 2 以降でパペットポリシーを有効にするには、puppet-agent パッケージがデバイスにインストールされていることを確認する必要があります。詳細については、『Configuration Policies リファレンス』を参照してください。

ZENworks のセキュリティ拡張機能

このリリースで導入されたセキュリティ拡張機能により、DMZ 環境でも安全にデバイスを登録し、通信することができます。

- ZENworks 2020 Update 2 を新たにインストールした場合、デフォルトでセキュリティ設定がすべてのプライマリサーバで有効になります。
- プライマリサーバをアップグレードする場合は、セキュリティ設定がデフォルトで無効になります。
- ゾーンに新しいプライマリサーバを追加した場合は、ZENworks 2020 Update 2 にアップグレードした後、デフォルトでセキュリティ設定が有効になります。

設定を有効にするには、次の zman コマンドを実行する必要があります。

- zman ssassc (Security-Set-Agent-Server-Secure-Communication) が、ZENworks Agent と ZENworks サーバ間の通信の認証を有効または無効にするために導入されました。

このリリースで導入されたセキュリティ拡張機能の詳細については、『ZENworks Securing Devices Reference』を参照してください。

デバイス登録

デバイス登録の事前承認

事前承認済みデバイスは、管理者によってゾーンの一部として承認されたデバイスです。これは、既知のデバイスセットを一括登録する際にデバイスを事前承認する必要がある場合に特に役立ちます。必要に応じて、既知のデバイスを調整するために使用することもできます。

認証キーの使用

認証キーは、ZENworks エージェントがゾーンへの登録とインストール中のサーバとの通信を認証するために使用できます。

管理対象デバイスと iOA デバイス登録のセキュリティ保護

より新しい iOA エージェントまたは管理対象デバイスをゾーンに登録するには、デバイス登録中に認証キーを指定するか、デバイスが事前承認済みデバイスリストに含まれていることを確認する必要があります。

デバイス通信

ZCC ログインを含むデバイス通信に OSP を使用

ZENworks では、ほとんどの機能に対してユーザ ID を確立するために O-Auth プロトコルを使用するように切り替えました。したがって、OSP と呼ばれる新しいサービスが導入され、ZCC へのログイン、サービス間通信、およびデバイスとサーバ間の通信に使用されます。

デバイス、プライマリサーバ、およびサテライトサーバ間のコンテンツとコレクションのセキュリティ保護

この新しいセキュリティ機能の導入により、管理対象デバイス、プライマリサーバ、およびサテライトサーバ間でのコンテンツのエンドツーエンドのコレクションと転送が SSL を介して行われます。これは、ZCC 内で設定を構成するか、または新たに導入された zman コマンドを使用することで実現できます。

デバイスとプライマリサーバまたはサテライトサーバ間の Web サービス通信のセキュリティ保護

ZENworks Agent とプライマリサーバまたはサテライトサーバ間の Web サービス通信のセキュリティ保護を強化するため、このリリースでは、Web サービスコールにセキュリティ拡張機能が導入されました。

Microsoft データ暗号化ポリシーのドライブの除外

管理対象デバイスでポリシーが適用されている場合、リムーバブルデータドライブを Microsoft データ暗号化ポリシーのドライブタイプ別に暗号化から除外できるようになりました。

マルウェア対策

ZENworks Antimalware は、ZENworks コントロールセンターの［セキュリティ］グループ下の ZENworks Endpoint Security Management の新しいコンポーネントです。マルウェア対策は、最新のすべてのマルウェア脅威から管理対象デバイスを保護する圧縮ソリューションです。ゾーン内のデバイスに展開されると、マルウェア対策エージェントはマルウェア対策クラウドサービスからマルウェアシグネチャファイルの更新を継続的に受信し、オンアクセススキャンとオンデマンドスキャンの両方を使用してマルウェア感染を検出します。感染したファイルは駆除されるまで検疫されます。

このセクションのトピックの詳細については、次のマニュアルを参照してください。

- 『ZENworks Endpoint Security Antimalware Reference』

マルウェアから保護 - はじめにページ

セキュリティの［はじめに］ページには、「マルウェアから保護」というタイトルの追加のタブ付きページが含まれています。このページを単一アクセスポイントとして使用して、ZENworks Antimalware が提供する必要があるすべての機能を設定、展開、およびカスタマイズできます。

Antimalware Update Entitlement

Antimalware Update Entitlement は、マルウェア対策ポリシーをデバイスに展開するために必要です。Endpoint Security Management を評価モードで有効にすると、その評価期間の間、エンタイトルメントは自動的に有効になります。

Windows Endpoint セキュリティポリシー

マルウェア対策の展開、カスタマイズ、および継続性を管理するために、次の 4 つの新しいポリシーが使用されます。

マルウェア対策強制ポリシー: これは、管理対象デバイスにマルウェア対策エージェントをインストールする基本ポリシーです。このポリシーは、任意の他のマルウェア対策ポリシーを使用するために展開する必要があります。オンアクセス、フル、クイック、外部デバイス、コンテキストオンデマンドスキャンを含む、すべてのタイプのマルウェアスキャンの設定が含まれます。検疫動作や、スキャンから除外するコンテンツの定義の設定も含まれます。

ポリシーの展開時にエンドユーザの権利と通知のデフォルト設定が維持されている場合、エンドユーザはエンドポイントのエージェントステータスコンソールにアクセスすることができ、これにより独自のスキャンを開始したり、スキャンとエージェントの更新ステータスを表示したり、ポリシーで制御されるエージェントアクティビティの通知を受信したりできます。

マルウェア対策スキャン除外ポリシー: マルウェア対策には、ビルトインスキャン除外とカスタムスキャン除外の両方があり、任意のマルウェア対策ポリシーに追加できます。スキャン除外ポリシーは、他のマルウェア対策ポリシーも同じデバイスに割り当てられている場合にデバイス割り当てで使用されます。これにより、ゾーン全体にスキャン除外をより簡単な方法で伝播できます。特定のスキャンタイプに対して除外を有効または無効にできます。

マルウェア対策カスタムスキャンポリシー: カスタムスキャンポリシーは、特定の脅威が疑われる場合に管理対象デバイスのローカルドライブをスキャンしたり、それらのデバイス上の特定の場所をスキャンしたりするためのより対象を絞ったアプローチに使用されます。マルウェア対策強制ポリシー用に設定されたゾーンスケジュールを使用するのではなく、独自のスケジュールがあります。

マルウェア対策ネットワークスキャンポリシー: ネットワークスキャンポリシーも、より対象を絞ったアプローチに使用されますが、ネットワークドライブ上のフォルダとファイルのスキャンに明示的に使用されます。また、独自のスケジュールがあり、ネットワークの場所に対する認証用の追加設定が含まれます。

マルウェア対策セキュリティダッシュレット

マルウェアの脅威、マルウェアスキャン、およびマルウェアシグネチャの更新を監視するために、デフォルトでセキュリティダッシュボードに設定された 4 つの新しいダッシュレットが提供されています。

デバイスマルウェアステータス: このダッシュレットには、選択した検出期間におけるゾーン内の個々のデバイスのマルウェアステータスが表示されます。

デバイスの前回のマルウェアスキャン: このダッシュレットには、マルウェアの脅威に対するゾーン内のデバイスのヘルスが表示されます。デフォルトでは、指定された期間にデバイスで実行されたあらゆるタイプのスキャンに関する情報が表示されます。

上位マルウェアの脅威: このダッシュレットには、ゾーン内における上位マルウェアの脅威のリストが表示されます。デフォルトでは、上位マルウェアの脅威は、感染したデバイス数に基づいて表示されます。

デバイスマルウェアシグネチャのバージョン: このダッシュレットには、ゾーン内のデバイスにインストールされたマルウェアシグネチャのバージョンとマルウェア対策エージェントのバージョンのリストが表示されます。

デバイスのマルウェア対策ページ

このページは、デバイスが選択されるときにアクセスされる新しいタブです。マルウェアの脅威のスナップショットステータス、スキャンスケジュール、および選択したデバイスの検疫済みファイル情報を提供します。また、ファイルに対して特定のアクションを実行したり、スキャンを開始したり、デバイス上のマルウェア対策エージェントとマルウェアシグネチャのバージョンを更新したりすることもできます。

Malware Threat Details (マルウェア脅威の詳細) ページ

このページには、デバイスの［マルウェア対策］ページの［マルウェアの脅威］セクションにあるマルウェア脅威リンクをクリックしてアクセスできます。このページには、選択した脅威に関する詳細と脅威に感染したデバイスの詳細が表示されます。

マルウェア対策クイックタスク

ZENworks コントロールセンターの［デバイス］グループで、マルウェア対策エージェントがインストールされている 1 つ以上のデバイスを選択すると、選択したデバイスで 5 つの新しいクイックタスクを実行できます。これらには、次のクイックタスクが含まれます。

- マルウェアスキャンの開始
- マルウェアシグネチャの更新
- マルウェア対策エージェントの更新
- マルウェア検疫からのファイルの復元
- マルウェア検疫からのファイルの削除

マルウェア対策 zac コマンド

マルウェア対策には、このコンポーネントに固有のいくつかの新しい zac コマンドが付属しています。これらには、デバイスのマルウェアスキャンの開始、マルウェア対策エージェントのマルウェアステータスの確認、エージェントのインストール、更新または削除、検疫からのファイルの削除などを実行するコマンドが含まれます。

マルウェア対策ゾーン設定ページ

3 つの新しいゾーン設定ページがメインの ZENworks 設定ページのセキュリティグループに含まれるようになりました。これらの各ページには、カスタマイズ可能なデフォルト設定が含まれます。ページは次のとおりです。

マルウェア対策エージェントスケジュール : マルウェアスキャンおよびマルウェアシグネチャの更新用スケジュールを設定します。デバイスフォルダおよびデバイスレベルでこのスケジュールを上書きできます。

マルウェア対策エージェントの通知 : 管理対象デバイス上のマルウェア対策エージェントで表示されるアラートと通知を設定します。デバイスフォルダおよびデバイスレベルでこれらの設定を上書きできます。

マルウェア対策設定 : マルウェア対策サーバとして使用する ZENworks プライマリサーバを定義します。このサーバは、マルウェア対策コンポーネントを展開するために手動で設定する必要があります。また、マルウェア対策エージェントの保守スケジュールも設定します。

Ondemand Content Configuration (オンデマンドコンテンツ設定) ページ

メインの ZENworks 設定ページのバンドル、ポリシー、およびコンテンツグループにこの新しいゾーン設定ページが含まれるようになりました。ゾーン内のコンテンツ配布のコンテンツダウンロード率とコンテンツキャッシュサイズを管理します。これには現在、マルウェア対策シグネチャファイルとマルウェア対策エージェントの更新が含まれています。

マルウェア対策サービスステータス

マルウェア対策サービスステータスには、ZCC 診断ページからアクセスできるようになりました。

Antimalware データベース

Antimalware データベースは ZENworks 2020 Update 2 の新機能です。その目的は、マルウェア対策ページとマルウェア対策セキュリティダッシュレットを介してマルウェア対策の監視機能のデータを提供することです。設定すると、このデータベースは ZENworks データベースと同期されるため、同じデータベースタイプである必要があります。例 : PostgreSQL、Microsoft SQL Server、または Oracle。

Antimalware データベースは ZENworks コントロールセンターの［セキュリティ］の［マルウェアから保護］ - ［はじめに］ページから設定されます。Antimalware データベースが、まだ存在していない外部データベースを使用して設定される場合は、setup.exe ファイルを使用して CLI コマンドからデータベースを作成できます。