ZENworks 2017 Update 4 Readme

2019 年 1 月

この Readme ファイルでは、ZENworks 2017 Update 4 リリースに関する情報を提供します。

ZENworks 2017 Update 4 の新機能

このリリースに含まれる新機能の詳細については、『ZENworks 新機能リファレンス』を参照してください。

ZENworks 2017 Update 4 の展開の計画

管理ゾーン内での ZENworks 2017 Update 4 の展開を計画するには、次のガイドラインを使用します。

- ディスク暗号化を使用している場合に、ZENworks 2017 Update 1 より前のバージョンから Full Disk Encryption Agent を更新するには、ZENworks 2017 Update 4 に更新する前に、管理対象デバイスからディスク暗号化ポリシーを削除する必要があります。

  ZENworks 2017 Update 1 または 2017 Update 2 から ZENworks 2017 Update 4 に Full Disk Encryption Agent を更新するには、ディスク暗号化ポリシーをそのまま残してください。システム更新前に変更する必要はありません。

  ZENworks 2017 4 より前のバージョンから ZENworks 2017 Update へ Full Disk Encryption を更新する方法の詳細については、『ZENworks 2017 Update 1 - Full Disk Encryption Update Reference』を参照してください。

- まずプライマリサーバをアップグレードし、次にサテライトサーバ、最後に管理対象デバイスという順番で ZENworks 2017 Update 4 にアップデートする必要があります。ゾーン内のすべてのプライマリサーバが ZENworks 2017 Update 4 にアップグレードされるまで、管理対象デバイスおよびサテライトサーバをアップグレードしないでください (または、新しい 2017 Update 4 エージェントをゾーンに追加しないでください)。

  注 : プライマリサーバがすべてアップグレードされるまで、エージェントは整合性のないデータを受け取る可能性があります。したがって、このプロセスのこの部分はできる限り短時間で実行することをお勧めします。理想的には、最初のプライマリサーバのアップグレード直後に実行します。

- 次のデバイスにバージョン 2017 Update 4 を直接展開することができます。

デバイスタイプ	オペレーティングシステム	ZENworks の最小バージョン
プライマリサーバ	Windows および Linux	ZENworks 2017 以上のバージョン
サテライトサーバ	Windows、Linux、および Mac	ZENworks 11.x 以上のバージョン
管理対象デバイス	Windows	ZENworks 11.x 以上のバージョン
	Linux	ZENworks 11.x 以上のバージョン
	Mac	ZENworks 11.2 以上のバージョン

- ZENworks 2017 Update 4 へのアップグレードが完了すると、システムは再起動します。ただし、次の場面では再起動が 2 回必要になります。
  - Endpoint Security が有効な状態で 11.x から ZENworks 2017 以上のバージョン (2017 Update 1、Update 2、Update 3、または Update 4) に更新する場合は、再度再起動して ZESNETAccess ドライバをロードする必要があります。
  - 管理対象デバイスがクライアントセルフディフェンスが有効な Windows 10 を使用していて、11.4.x から ZENworks 2017 以上のバージョン (2017 Update1、Update2、Update 3、または Update 4) にアップグレードする場合は、ZENworks コントロールセンターでクライアントセルフディフェンスを無効にして管理対象デバイスを再起動してから、更新を実行して、再度デバイスを再起動する必要があります。
  - 管理対象デバイスにディスク暗号化ポリシーが適用されている場合に、Full Disk Encryption Agent を ZENworks 2017 Update 1 より前のバージョンから ZENworks 2017 Update 4 に更新するには、最初にポリシーを削除してデバイスを復号化する必要があり、このときデバイスを再起動する必要があります。その後、デバイスを 2017 Update 4 にアップデートし、このときに 2 回目の再起動を実行する必要があります。

  重要 : 11.x より前のバージョンが実行されている管理対象デバイスは、まず 11.x にアップグレードする必要があります。システムは 11.x へのアップグレード後に再起動し、ZENworks 2017 Update 4 システム更新の展開時にもう一度再起動します。

- システム更新をインストールする前に、次の場所に十分な空きディスク容量があることを確認してください。

場所	説明	ディスク容量
Windows: `%zenworks_home%\install\downloads` **Linux:** `opt/novell/zenworks/install/downloads`	エージェントのパッケージを維持するため	5.7GB
Windows: `%zenworks_home%\work\content-repo` **Linux:** `/var/opt/novell/zenworks/content-repo`	zip ファイルをコンテンツシステムにインポートするため	5.7GB
エージェントキャッシュ	ZENworks サーバを更新するために必要な、該当するシステム更新コンテンツをダウンロードするため	1.5GB
システム更新ファイルがコピーされる場所。これは、システム更新 zip ファイルをインポートするために使用される ZENworks サーバにのみ適用されます。	ダウンロードしたシステム更新 zip ファイルを保存するため	5.7GB

ZENworks 2017 Update 4 のダウンロードと展開

ZENworks 4 のダウンロードと展開の方法については、『*ZENworks 2017 Update System Updates Reference*』を参照してください。

管理ゾーンが、ZENworks 2017 より前のバージョンのプライマリサーバで構成されている場合、これらのプライマリサーバすべてを ZENworks 2017 にアップグレードした後でのみ、プライマリサーバに ZENworks 2017 Update 4 を展開できます。手順については、『*ZENworks アップグレードガイド*』を参照してください。

管理タスクについては、ZENworks 2017 Update 4 のマニュアルのサイトを参照してください。

重要 : ゾーン内のすべての結合プロキシサテライトサーバが更新されるまで、Remote Management (RM) Viewer を更新しないでください。結合プロキシ経由で Remote Management を実行するには、RM Viewer のバージョンと結合プロキシのバージョンが同じであることを確認してください。

ZENworks 2017 Update 4 アップデートをダウンロードして展開する前に、必ず 1 ページの「ZENworks 2017 Update 4 の展開の計画」を読んでください。

重要 : ZENwork アップデートの展開中に、準備ステージで、プライマリサーバの ZENworks Updater Service (ZeUS) はその更新に含まれている新しいパッケージで置き換えられます。

ゾーン内のすべてのプライマリサーバが ZENworks 2017 にアップグレードされるまで、ZENworks 2017 Update 4 を展開しない

この更新では、データベースのスキーマを変更する必要があります。最初のパッチインストール中は、サービスはマスタまたは専用のプライマリサーバでのみ実行されます。これは、データベース内で変更中のテーブルに他のプライマリサーバがアクセスしないようにするためです。

マスタまたは専用のプライマリサーバが更新されると、残りのサーバでサービスが再開され、アップデートが同時に適用されます。

注 : アップデート中に手動でサーバ上のサービスを停止または開始する必要はありません。サービスは自動的に停止および開始されます。

システム更新を延期して管理対象デバイスからログアウトしても、システム更新はデバイスに適用されます。

ZENworks 2017 Update 4 がインストールされた管理ゾーンでサポートされる管理対象デバイスとサテライトサーバのバージョンのリストについては、「Supported Managed Devices and Satellite Server Versions」を参照してください。

ZENworks 2017 Update 4 で解決された問題

このリリースでは、前のリリースで見つかった複数の問題が解決されています。解決された問題のリストについては、サポートナレッジベースの TID 7023612 を参照してください。

ZENworks 2017 Update 4 で引き続き存在する問題

ZENworks 2017 Update 4 より前のバージョンで明らかになった問題のうち、一部は依然として解決されていません。詳細については、次の Readme ドキュメントを参照してください。

- ZENworks 2017 Readme
- ZENworks 2017 Update 1 Readme
- ZENworks 2017 Update 2 Readme
- ZENworks 2017 Update 3 Readme

既知の問題

このセクションでは、ZENworks 2017 Update 4 の使用時に発生する可能性がある問題について説明します。

- 5 ページの 「モバイルデバイス制御ポリシーの一部として設定された明るさの割合を Android デバイスに適用できない」
- 5 ページの 「Android P (9.0) デバイスではダイレクトブートはサポートされていない」
- 5 ページの 「デバイスのキーガード設定が、ZENworks Agent アプリが前のバージョンから 17.4.0 バージョンにアップグレードされたデバイスで機能しない」
- 5 ページの 「デバイスのキーガード設定が仕事用プロファイルモードで登録された Android Lollipop および Marshmallow デバイスに適用できない」
- 6 ページの 「デバイスのロック解除クイックタスクが仕事用プロファイルモードで登録された Android Lollipop および Marshmallow デバイスに適用できない」
- 6 ページの「ZENworks をアップデートした後で、novell-zenworks-xplat-uninstall RPM で ZDC に不正なバージョンが表示される」
- 6 ページの 「Intel AMT デバイスフォルダ名の不要な文字」

- 6 ページの 「信頼できないアクセス制御ルールがエンドポイントセキュリティファイアウォールポリシーが適用されたデバイス上のネットワークトラフィックをブロックしていない」
- 6 ページの「Windows v1709、v1803、または v1809 にアップグレードした後で、ZENworks Passive Mode ログインが機能しない」
- 7 ページの 「クイックタスクおよびシステムアップデートが ZENworks Agent で実行されない」
- 8 ページの「novell-proxydhcp サービスが RHEL 7.5 および 7.6 イメージングサテライトサーバで機能しない場合がある」

モバイルデバイス制御ポリシーの一部として設定された明るさの割合を Android デバイスに適用できない

特定の明るさの割合値が **[明るさの割合設定]** フィールドで定義されているモバイルデバイス制御ポリシーは、Android 仕事用管理デバイスに割り当てられるが、その後、明るさ値はデバイスには適用されず、エラーメッセージ「App not supported (アプリがサポートされていない)」がポリシーステータスメッセージに表示されます。

解決策 : ありません。

Android P (9.0) デバイスではダイレクトブートはサポートされていない

Google で確認されているように、ダイレクトブート機能は Android P デバイスでは機能しません。

解決策 : ありません。

デバイスのキーガード設定が、ZENworks Agent アプリが前のバージョンから 17.4.0 バージョンにアップグレードされたデバイスで機能しない

デバイス上の ZENworks Agent アプリが 17.4.0 バージョンにアップグレードされた場合、割り当てられたモバイルデバイス制御ポリシーの一部として有効なデバイスのキーガード設定が、デバイス上で機能しません。

解決策 : ZCC で **[登録解除]** クイックタスクを使用してデバイスの登録を解除し、再登録します。同じモバイルデバイス制御ポリシーを再割り当てします。デバイスのキーガード設定がデバイス上で正常に有効化されます。

デバイスのキーガード設定が仕事用プロファイルモードで登録された Android Lollipop および Marshmallow デバイスに適用できない

デバイスのキーガード設定がモバイルデバイス制御ポリシーの一部として有効になっている場合、仕事用プロファイルモードで登録された Android Lollipop および Marshmallow デバイスにポリシーを適用できません。ポリシーのステータスが ZCC で失敗と表示され、「You can not set trust agent configuration for a managed profile (管理対象プロファイル用に信頼できるエージェント設定を設定できません)」というエラーメッセージがデバイスのログに表示されます。

解決策 : ありません。

デバイスのロック解除クイックタスクが仕事用プロファイルモードで登録された Android Lollipop および Marshmallow デバイスに適用できない

デバイスのロック解除クイックタスクが仕事用プロファイルモードで登録された Android Lollipop および Marshmallow デバイスに適用できません。クイックタスクのステータスが ZCC で失敗と表示され、「You cannot reset password for managed profile (管理対象プロファイルのパスワードをリセットできません)」というエラーがデバイスのログに表示されます。

解決策 : ありません。

ZENworks をアップデートした後で、novell-zenworks-xplat-uninstall RPM で ZDC に不正なバージョンが表示される

ZENworks 管理ゾーンがアップグレードされた後で、novell-zenworks-xplat-uninstall RPM で ZDC に不正なバージョンが表示されます。

解決策 : ありません。

更新アクションがプライマリサーバで実行されるまで待機します。

Intel AMT デバイスフォルダ名の不要な文字

[ZCC]> [デバイス]> [検出済み] タブで、「Intel AMT デバイス」というフォルダ名に不要な文字が表示されます。

解決策 : ありません。

信頼できないアクセス制御ルールがエンドポイントセキュリティファイアウォールポリシーが適用されたデバイス上のネットワークトラフィックをブロックしていない

アクセス制御リスト (ACL) がファイアウォールポリシーの 1 つ以上の信頼できない ACL ルールで設定されている場合、ルールパラメータに基づくネットワークアクセスがブロックされません。

解決策 : ネイティブなファイアウォールポート設定を使用してネットワークアクセスをブロックします。

Windows v1709、v1803、または v1809 にアップグレードした後で、ZENworks Passive Mode ログインが機能しない

デバイスを Windows 10 v1709 (Fall Creator アップデート)、v1803 または Windows 10 v1809 (April 2018 アップデート) にアップグレードした後で、ZENworks へのパッシブモードログインが機能しません。

解決策 : Micro Focus ナレッジベースの TID 7022478 を参照してください。

クイックタスクおよびシステムアップデートが ZENworks Agent で実行されない

クイックタスクおよびシステムアップデートが ZENworks Agent に割り当てられる場合、割り当てられたタスクまたはアップデートがエージェントで実行されず、「TaskNotifier, "Got 503 from Server (TaskNotifier、「サーバから 503 を取得しました」)」というエラーが ZeUS ログに記録されます。

「TaskNotifier, "Got 503 from Server (「TaskNotifier、「サーバから 503 を取得しました」)」というエラーを確認するには、次を実行します。

1. エージェントの技術者アプリケーションで (**[ZENworks Icon]** を右クリックし、**[技術者アプリケーション]** を選択して)、ロギングを **[Errors, Warning, Info, Debug (エラー、警告、情報、デバッグ)]** に設定する必要があります。
2. エージェントのログレベルを変更した後で、クイックタスクまたはシステムアップデートを割り当てます。
3. 「TaskNotifier, "Got 503 from Server (「TaskNotifier、「サーバから 503 を取得しました」)」というエラー メッセージが `zeus-messages.log` ファイル (場所 : `%ZENWORKS_HOME%\ZeUS\logs\`) に記録されます。

「TaskNotifier, "Got 503 from Server (「TaskNotifier、「サーバから 503 を取得しました」)」というエラーは、デフォルト容量 (10000) として接続を拒否されたサーバがほぼフルであることを示しています。

このエラーは、`server.xml` ファイルの「maxConnections」数と比較して、サーバに接続しているエージェント数が多い場合に発生します。デフォルトで、「maxConnections」数は 10000 です。

解決策 :

`server.xml` ファイルに「maxConnections」パラメータ数を追加します。

server.xml ファイルに maxConnections 数を追加するには :

1. server.xml ファイルの次の行で、以下に示すようにパラメータ maxConnections="20000" を追加します。

   <! -- Define a non-SSL HTTP/1.1 Connector on port 80 --> <Connector acceptCount="1000" connectionTimeout="60000" maxConnections="20000" disableUploadTimeout="true" enableLookups="false" maxHttpHeaderSize="8192" maxSpareThreads="75" maxThreads="600" minSpareThreads="25" port="80" protocol="org.apache.coyote.http11.Http11NioProtocol" redirectPort="443" />

   注 : デフォルトで、パラメータ maxConnections 数は 10000 で、server.xml ファイルに一覧表示されません。10000 で十分ではない場合、パラメータを追加し、ゾーンのエージェント数に基づいて数を増やします。この例では、maxConnections 数は 20000 です。

   ---

2. ZENworks サービスを再起動します。

novell-proxydhcp サービスが RHEL 7.5 および 7.6 イメージングサテライトサーバで機能しない場合がある

「novell-proxydhcp」サービスで必要とされるポート 67 が「dnsmasq」サービスで使用されるため、novell-proxydhcp サービスが RHEL 7.5 および 7.6 で機能しない場合があります。

解決策 : `systemctl disable libvirtd.service` コマンドを実行してから、デバイスを再起動します。

その他のマニュアル

このドキュメントには、ZENworks 2017 Update 4 リリースに固有の情報が含まれています。他のすべての ZENWorks 2017 のマニュアルについては、*ZENworks 2017 マニュアルの Web サイト*を参照してください。

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。