Readme zu ZENworks 2017 Update 4

Januar 2019

Die Informationen in dieser Readme-Datei beziehen sich auf ZENworks 2017 Update 4.

Neue Funktionen in ZENworks 2017 Update 4

Weitere Informationen zu den neuen Funktionen in dieser Version finden Sie in ZENworks Neue Funktionen – Referenz.

Planen der Bereitstellung von ZENworks 2017 Update 4

Beachten Sie die folgenden Richtlinien, wenn Sie die Bereitstellung von ZENworks 2017 Update 4 in Ihrer Verwaltungszone planen:

- Wenn Sie die Festplattenverschlüsselung nutzen und der Agent zur vollständigen Festplattenverschlüsselung von einer Version vor ZENworks 2017 Update 1 aktualisiert werden soll, MÜSSEN Sie die Datenverschlüsselungsrichtlinie auf den verwalteten Geräten entfernen, bevor Sie sie auf ZENworks 2017 Update 4 aktualisieren können.

  Wenn Sie den Agenten zur vollständigen Festplattenverschlüsselung von ZENworks 2017 Update 1 oder 2017 Update 2 auf ZENworks 2017 Update 4 aktualisieren, behalten Sie die Festplattenverschlüsselungsrichtlinie bei. Vor der Systemaktualisierung ist keine Änderung erforderlich.

  Weitere Informationen zum Aktualisieren der vollständigen Festplattenverschlüsselung in ZENworks 2017 Update 4 von einer Version vor ZENworks 2017 Update 1 finden Sie unter ZENworks 2017 – Full Disk Encryption Update Reference (ZENworks 2017 Update – Referenz zur Aktualisierung der vollständigen Festplattenverschlüsselung).

- Sie müssen zuerst die Primärserver, dann die Satellitenserver und schließlich die verwalteten Geräte auf ZENworks 2017 Update 4 aufrüsten. Die verwalteten Geräte und die Satellitenserver dürfen erst dann aufgerüstet werden (und es dürfen erst dann neue ZENworks 2017 Update 4-Agenten in die Zone aufgenommen werden), wenn alle Primärserver in der Zone auf ZENworks 2017 Update 4 aufgerüstet wurden.

  HINWEIS: Die Agenten erhalten unter Umständen inkonsistente Daten aus der Zone, bis alle Primärserver aufgerüstet sind. Dieser Schritt muss daher so rasch wie möglich erledigt werden – im Idealfall unmittelbar nach dem Aufrüsten des ersten Primärservers.

- Sie können Version 2017 Update 4 auf den folgenden Geräten direkt bereitstellen:

Gerätetyp	Betriebssystem	Mindestens erforderliche ZENworks-Version
Primärserver	Windows und Linux	ZENworks 2017 (oder höher)
Satellitenserver	Windows, Linux und Mac	ZENworks 11.x (oder höher)
Verwaltete Geräte	Windows	ZENworks 11.x (oder höher)
	Linux	ZENworks 11.x (oder höher)
	Mac	ZENworks 11.2 (oder höher)

- Nach dem Aufrüsten auf ZENworks 2017 Update 4 wird das System neu gebootet. In den folgenden Szenarien ist jedoch ein zweimaliger Neustart erforderlich:
  - Wenn Sie von 11.x auf ZENworks 2017 oder höher (2017 Update 1, Update 2, Update 3 oder Update 4) mit aktivierter Endpoint Security aktualisieren, muss das Gerät ein zweites Mal neu gestartet werden, damit der ZESNETAccess-Treiber geladen wird.
  - Wenn ein verwaltetes Gerät mit Windows 10 und aktivierter Client-Selbstverteidigung von 11.4.x auf ZENworks 2017 oder höher (2017 Update 1 , Update 2, Update 3 oder Update 4) aktualisiert werden soll, müssen Sie die Client-Selbstverteidigung in ZENworks Control Center deaktivieren, das verwaltete Gerät neu starten und dann die Aktualisierung ausführen, wobei ein zweiter Neustart erforderlich ist.
  - Wenn eine Datenverschlüsselungsrichtlinie auf einem verwalteten Gerät gilt und der Agent zur vollständigen Festplattenverschlüsselung von einer Version vor ZENworks 2017 Update 1 auf ZENworks 2017 Update 4 aktualisiert werden soll, müssen Sie zunächst die Richtlinie entfernen, das Gerät entschlüsseln und dann neu starten. Anschließend können Sie das Gerät auf 2017 Update 4 aktualisieren, wobei ein zweiter Neustart erforderlich ist.

  WICHTIG: Verwaltete Geräte mit einer Version vor 11.x müssen zunächst auf 11.x aktualisiert werden. Das System wird nach erfolgter Aktualisierung auf 11.x und dann ein zweites Mal beim Bereitstellen der Systemaktualisierung auf ZENworks 2017 Update 4 neu gestartet.

- Stellen Sie vor der Installation der Systemaktualisierung sicher, dass für folgende Ordner ausreichend Festplattenspeicher verfügbar ist:

Standort	Beschreibung	Festplattenspeicher
Windows: `%zenworks_home%\install\downloads` **Linux:** `opt/novell/zenworks/install/downloads`	Zum Beibehalten der Agentenpakete.	5,7 GB
Windows: `%zenworks_home%\work\content-repo` **Linux:** `/var/opt/novell/zenworks/content-repo`	Zum Importieren der ZIP-Datei in das Inhaltssystem.	5,7 GB
Agentencache	Zum Herunterladen des Inhalts der zutreffenden Systemaktualisierung für den ZENworks-Server.	1,5 GB
Ordner, in den die Datei mit der Systemaktualisierung kopiert wird. Betrifft nur den ZENworks-Server, auf den die ZIP-Datei mit der Systemaktualisierung importiert wird	Zum Speichern der heruntergeladenen ZIP-Datei mit der Systemaktualisierung.	5,7 GB

Herunterladen und Bereitstellen von ZENworks 2017 Update 4

Anweisungen zum Herunterladen und Bereitstellen von ZENworks 4 finden Sie im Handbuch *ZENworks System Updates Reference* (ZENworks 2017 Update 1 – Referenz zu Systemaktualisierungen).

Wenn sich Primärserver mit einer Version vor ZENworks 2017 in Ihrer Verwaltungszone befinden, können Sie ZENworks 2017 Update 4 erst dann auf diesen Primärservern bereitstellen, wenn alle Primärserver auf ZENworks 2017 aktualisiert wurden. Anweisungen finden Sie im *ZENworks-Aufrüstungshandbuch*.

Weitere Informationen zu den Verwaltungsaufgaben finden Sie auf der Dokumentations-Site zu ZENworks 2017 Update 4.

WICHTIG: Den Fernverwaltungs-Viewer (RM-Viewer, Remote Management) dürfen Sie erst aktualisieren, nachdem alle Join Proxy-Satellitenserver der Zone aktualisiert wurden. Die Fernverwaltung über Join Proxy ist nur möglich, wenn die Version des RM-Viewers und die Join Proxy-Version identisch sind.

Lesen Sie vor dem Herunterladen und Bereitstellen der Aktualisierung auf ZENworks 2017 Update 4 unbedingt „Planen der Bereitstellung von ZENworks 2017 Update 4“, auf Seite 1.

WICHTIG: Beim Bereitstellen der ZENworks-Aktualisierung wird der ZENworks Updater Service (ZeUS) auf Primärservern in der Vorbereitungsphase durch ein neues Paket aus der Aktualisierung ersetzt.

Stellen Sie ZENworks 2017 Update 4 erst dann bereit, wenn alle Primärserver der Zone auf ZENworks 2017 aktualisiert wurden.

Für diese Aktualisierung muss das Datenbankschema geändert werden. Bei der ursprünglichen Patch-Installation werden diese Dienste nur auf dem Master-Server oder auf einem dedizierten Primärserver ausgeführt. So ist gewährleistet, dass andere Primärserver nicht auf die Tabellen zugreifen, die in der Datenbank geändert werden.

Sobald der Master-Server oder der dedizierte Primärserver aktualisiert wurde, werden die Dienste auf den verbleibenden Servern wieder aufgenommen und die Aktualisierung wird auf allen Servern gleichzeitig angewendet.

HINWEIS: Sie müssen die Dienste während der Aktualisierung nicht manuell auf den Servern anhalten oder starten. Die Dienste werden automatisch angehalten und gestartet.

Wenn Sie eine Systemaktualisierung zurückstellen, wird die Systemaktualisierung auf das Gerät angewendet, sobald Sie sich beim verwalteten Gerät abmelden.

Eine Liste der unterstützten Versionen der verwalteten Geräte und Satellitenserver in einer Verwaltungszone mit ZENworks 2017 Update 4 finden Sie unter Unterstützte Versionen der verwalteten Geräte und Satellitenserver.

Behobene Probleme in ZENworks 2017 Update 4

Einige der in früheren Versionen festgestellten Probleme wurden in dieser Version behoben. Eine Liste der behobenen Probleme finden Sie unter TID 7023612 in der Support-Knowledgebase.

Weiterhin bestehende Probleme in ZENworks 2017 Update 4

Einige der in Versionen vor ZENworks 2017 Update 4 festgestellten Probleme wurden noch nicht behoben. Weitere Informationen hierzu finden Sie in folgenden Readme-Dokumenten:

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

Bekannte Probleme

Dieser Abschnitt enthält Informationen zu Problemen, die während des Programmbetriebs von ZENworks 2017 Update 4 auftreten können:

Die Helligkeitseinstellung (in Prozent) aus der Richtlinie zur Mobilgerätesteuerung kann bei Android-Geräten nicht angewendet werden

Wenn eine Richtlinie zur Mobilgerätesteuerung mit einem bestimmten Helligkeitswert im Feld **Bildschirmhelligkeit (%) festlegen** einem verwalteten Android-Unternehmensgerät zugewiesen wird, tritt der Helligkeitswert auf dem Gerät nicht in Kraft und in den Richtlinienstatusmeldungen wird die Fehlermeldung „App nicht unterstützt“ angezeigt.

Behelfslösung: Keine.

Die Direct Boot-Funktion wird bei Geräten mit Android P (9.0) nicht unterstützt

Wie Google bestätigt hat, ist die Direct Boot-Funktion auf Android P-Geräten nicht funktionsfähig.

Behelfslösung: Keine.

Die Einstellungen für die Tastensperrfunktionen funktionieren nicht auf Geräten, auf denen die ZENworks-Agenten-App von einer früheren Version auf Version 17.4.0 aufgerüstet wird

Nach dem Aufrüsten der ZENworks-Agenten-App auf einem Gerät auf Version 17.4.0 funktionieren die Einstellungen für die Tastensperrfunktion aus der zugewiesenen Richtlinie zur Mobilgerätesteuerung nicht auf dem Gerät.

Behelfslösung: Heben Sie die Geräteregistrierung mit der Schnellaufgabe **Geräteregistrierung aufheben** im ZCC auf und registrieren Sie das Gerät erneut. Weisen Sie dieselbe Richtlinie zur Mobilgerätesteuerung erneut zu. Die Einstellungen für die Tastensperrfunktionen werden auf dem Gerät fehlerfrei aktiviert.

Die Einstellungen für die Tastensperrfunktionen werden auf Geräten mit Android Lollipop und Marshmallow, die im Arbeitsprofilmodus registriert sind, nicht angewendet

Wenn die Einstellungen für die Tastensperrfunktionen im Rahmen der Richtlinie zur Mobilgerätesteuerung aktiviert sind, wird die Richtlinie auf Geräten mit Android Lollipop und Marshmallow, die im Arbeitsprofilmodus registriert sind, nicht angewendet. Im ZCC wird für die Richtlinie der Status „Fehler“ angezeigt und in den Geräteprotokollen wird die Fehlermeldung „Sie können keine Trust-Agentenkonfiguration für ein verwaltetes Profil festlegen“ eingetragen.

Behelfslösung: Keine.

Die Schnellaufgabe „Gerät entsperren“ wird auf Geräten mit Android Lollipop und Marshmallow, die im Arbeitsprofilmodus registriert sind, nicht angewendet

Die Schnellaufgabe „Gerät entsperren“ wird auf Geräten mit Android Lollipop und Marshmallow, die im Arbeitsprofilmodus registriert sind, nicht angewendet. Im ZCC wird für die Schnellaufgabe der Status „Fehler“ angezeigt und in den Geräteprotokollen wird die Fehlermeldung „Sie können das Passwort für ein verwaltetes Profil nicht zurücksetzen“ eingetragen.

Behelfslösung: Keine.

Nach dem Aktualisieren von ZENworks zeigt die RPM „novell-zenworks-xplat-uninstall“ eine fehlerhafte Version im ZDC an

Nach dem Aufrüsten der ZENworks-Verwaltungszone zeigt die RPM „novell-zenworks-xplat-uninstall“ eine fehlerhafte Version im ZDC an.

Behelfslösung: Keine.

Warten Sie ab, bis die Aktualisierungsaktion auf dem primären Server ausgeführt wird.

Unerwünschte Zeichen im Ordnernamen „Intel AMT-Geräte“

Auf der Registerkarte **ZCC** > **Geräte** > **Ermittelt** werden im Ordnernamen **Intel AMT-Geräte** unerwünschte Zeichen angezeigt.

Behelfslösung: Keine.

Die Zugriffssteuerungsregel „Nicht verbürgt“ blockiert nicht den Netzwerkverkehr auf Geräten, auf denen die Endpoint Security-Firewall-Richtlinie erzwungen wird

Wenn eine Zugriffssteuerungsliste (ACL) mit mindestens einer ACL-Regel „Nicht verbürgt“ in der Firewall-Richtlinie konfiguriert ist, wird der Netzwerkzugriff gemäß den Regelparametern nicht blockiert.

Behelfslösung: Blockieren Sie den Netzwerkzugriff mit nativen Firewall-Portkonfigurationen.

Die ZENworks-Anmeldung im passiven Modus funktioniert nach dem Aufrüsten auf Windows Version 1709, 1803 oder 1809 nicht mehr

Nach dem Aufrüsten des Geräts auf Windows 10 Version 1709 (Fall Creator Update), 1803 oder Windows 10 1809 (April 2018 Update) funktioniert die Anmeldung bei ZENworks im passiven Modus nicht mehr.

Behelfslösung: Beachten Sie die Informationen im Artikel TID 7022478 in der Micro Focus-Knowledgebase.

Schnellaufgaben und Systemaktualisierungen werden für ZENworks-Agenten nicht durchgeführt

Wenn Sie einem ZENworks-Agenten eine Schnellaufgabe oder eine Systemaktualisierung zuweisen, wird die zugewiesene Aufgabe oder Aktualisierung nicht für den Agenten durchgeführt und im ZeUS-Protokoll wird der Fehler **TaskNotifier, "503 vom Server erhalten** eingetragen.

Bestätigen Sie den Fehler „TaskNotifier, "503 vom Server erhalten“ wie folgt:

1. Im Agenten in der Technikeranwendung (mit der rechten Maustaste auf das **ZENworks-Symbol** klicken, **Technikeranwendung** auswählen) sollte die Protokollierung auf **Fehler, Warnung, Info, Debuggen** eingestellt sein.
2. Ändern Sie den Protokollierumfang auf dem Agenten und weisen Sie die gewünschten Schnellaufgaben oder eine Systemaktualisierung zu.
3. Die Fehlermeldung **TaskNotifier, "503 vom Server erhalten** wird in die Datei `zeus-messages.log` (Speicherort: `%ZENWORKS_HOME%\ZeUS\logs\`) eingetragen.

Der Fehler **TaskNotifier, "503 vom Server erhalten** weist darauf hin, dass der Server die Verbindung verweigert hat, weil die Standardkapazität (10.000) nahezu erschöpft ist.

Dieser Fehler tritt auf, wenn die Anzahl der Agenten, die eine Verbindung zu einem Server herstellen, höher ist als die Anzahl unter *maxConnections* in der Datei `server.xml`. Standardmäßig liegt der Wert für *maxConnections* bei 10.000.

Lösung:

Tragen Sie die Anzahl im Parameter *maxConnections* in die Datei `server.xml` ein.

So tragen Sie die Anzahl unter „maxConnections“ in die Datei „server.xml“ ein:

1. Ergänzen Sie die folgende Zeile in der Datei „server.xml“ mit dem Parameter „maxConnections="20000"“:

   <!-- Nicht-SSL-HTTP/1.1-Connector an Port 80 definieren --> <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" />

   HINWEIS: Der Wert für den Parameter „maxConnections“ liegt standardmäßig bei 10.000 und wird nicht in der Datei „server.xml“ aufgeführt. Wenn der Wert 10.000 nicht ausreicht, tragen Sie den Parameter ein und erhöhen Sie die Anzahl entsprechend der Anzahl der Agenten in der Zone. In diesem Beispiel liegt der Wert für „maxConnections“ bei 20.000.

   ---

2. Starten Sie die ZENworks-Services neu.

Der Dienst „novell-proxydhcp“ funktioniert auf Imaging-Satellitenservern mit RHEL 7.5 und 7.6 nicht

Der Dienst *novell-proxydhcp* funktioniert unter Umständen unter RHEL 7.5 und 7.6 nicht, da der durch *den* Dienst benötigte Port 67 vom Dienst *dnsmasq* verwendet wird.

Behelfslösung: Führen Sie den Befehl `systemctl disable libvirtd.service` aus und starten Sie das Gerät neu:

Weitere Dokumentation

In diesem Dokument finden Sie spezielle Informationen zu ZENworks 2017 Update 4. Eine Liste weiterer Dokumentation zu ZENworks 2017 finden Sie auf der *Dokumentations-Website zu ZENworks 2017*.

Rechtliche Hinweise

Informationen zu rechtlichen Hinweisen, Marken, Haftungsausschlüssen, Gewährleistungen, Ausfuhrbeschränkungen und sonstigen Nutzungseinschränkungen, Rechten der US-Regierung, Patentrichtlinien und Erfüllung von FIPS finden Sie unter http://www.novell.com/company/legal/.