ZENworks 2020 Update 2

Neue Funktionen – Referenz

August 2021

Rechtliche Hinweise

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

Inhalt

Allgemeines zu diesem Handbuch

In diesem Handbuch *ZENworks What's New Reference* (ZENworks: Neue Funktionen – Referenz) werden die neuen Funktionen in der Version ZENworks 2020 Update 2 beschrieben. Dieses Handbuch besteht aus den folgenden Abschnitten:

Zielgruppe

Dieses Handbuch richtet sich an ZENworks-Administratoren.

Rückmeldungen

Wir freuen uns über Ihre Hinweise, Anregungen und Vorschläge zu diesem Handbuch und den anderen Teilen der Dokumentation zu diesem Produkt. Über die Funktion **Thema kommentieren**, die Sie unten auf jeder Seite der Online-Dokumentation finden, können Sie uns Ihre Vorschläge und Meinung mitteilen.

Weitere Dokumentation

Im Lieferumfang von ZENworks finden Sie weitere Dokumentationen (im PDF- und HTML-Format), die Informationen zum Produkt und zu dessen Implementierung beinhalten. Weitere Dokumentation finden Sie auf der Dokumentations-Website zu ZENworks.

1 Neue Funktionen in ZENworks 2020 Update 2

In den folgenden Abschnitten werden die neuen Funktionen und Verbesserungen in ZENworks 2020 Update 2 beschrieben:

Unterstützte Plattformen

Die folgenden neuen Plattformen werden in dieser Version unterstützt:

- CentOS als verwaltetes Gerät
- macOS 11 (Big Sur) als verwaltetes Gerät
- Android 11
- iOS 14
- SLES 15 SP2
  - SLES 15 SP2 (Primärserver)
  - SLES 15 SP2 (verwaltetes Gerät – mit SLES für SAP)
  - SLED 15 SP2 (verwaltetes Gerät)
- Neue RHEL- und Scientific Linux-Plattformen
  - Scientific Linux 7.7 und 7.8
  - RHEL 7.8 und 8.2

Installation und Aufrüstung

ZENworks erhält eine robustere, flexiblere Architektur und wird gemäß den Micro Focus-Standards angepasst. Der Installations- und Aufrüstungsvorgang in ZENworks 2020 Update 2 wurde daher entsprechend überarbeitet. Mit dieser Version werden die folgenden Änderungen eingeführt:

Installieren von Docker und Docker Compose

Bevor Sie ZENworks 2020 Update 2 auf einem Linux-Primärserver aufrüsten können, müssen Sie Docker und Docker Compose auf dem Server installieren. Weitere Informationen zu Dockers finden Sie unter https://docs.docker.com/.

Migrieren der Serverdaten in einen neuen Dateipfad

Nach dem Aufrüsten auf ZENworks 2020 Update 2 auf einem Windows-, Appliance- oder Linux-Primärserver werden ZENworks-Serverdaten (z. B. MSIs, RPMs, Protokolle und Konfigurationsdateien), die sich bislang im Novell-Dateipfad befanden, in den neuen Micro Focus-Dateipfad verschoben.

Die Konfigurationsdateien, die auf einem Linux-Server bislang unter `/etc/opt/novell/zenworks` gespeichert waren, befinden sich jetzt beispielsweise in `/etc/opt/microfocus/zenworks`. Die Konfigurationsdateien, die auf einem Windows-Server bislang unter `C:\Programme (x86)\Novell\ZENworks\conf` gespeichert waren, befinden sich jetzt entsprechend in `C:\Programme (x86)\Micro Focus\ZENworks\conf`.

Die Dateien und Daten für den ZENworks-Agenten verbleiben am bisherigen Novell-Speicherort.

Umbenennen der ZENworks-Serverdienste

Nach dem Aufrüsten auf ZENworks 2020 Update 2 auf einem Windows-, Appliance- oder Linux-Primärserver werden bestimmte ZENworks-Serverdienste (z. B. die Dienste ZENServer, ZENLoader und ZENJoinProxy) von Novell in Micro Focus umbenannt. Auf einem Linux-Server wird beispielsweise der Dienst `novell-zenserver.service` in `microfocus-zenserver.service` umbenannt.

Einführung einer neuen Umgebungsvariablen

Auf einem Windows-Server wird die neue Umgebungsvariable `%ZENSERVER_HOME%` eingeführt, die auch bei einem nicht standardmäßigen Pfad auf den Speicherort der Serverinstallation verweist (`C:\Program Files(x86)\Micro Focus\ZENworks`).

TLS-Version

Wenn Sie ZENworks 2020 Update 2 neu installiert haben, ist TLS 1.2 in der Zone standardmäßig aktiviert. Wenn Sie dann versuchen, Geräte mit einer Microsoft .NET-Version vor 4.7 zu registrieren, schlägt die Geräteregistrierung fehl. Der Agent wird jedoch auf dem Gerät installiert.

Wenn Sie eine vorhandene Zone auf ZENworks 2020 Update 2 aufrüsten, wird TLS 1.2 nicht standardmäßig aktiviert. Wenn Sie TLS 1.2 in der Zone aktivieren, arbeiten einige Funktionen möglicherweise nicht ordnungsgemäß. Installieren Sie daher Microsoft .NET 4.7 in jedem Fall auf allen Geräten in der Zone.

Wenn Sie TLS 1.2 in der Zone aktiviert haben, muss Microsoft .NET 4.7 auf dem Gerät installiert sein, damit es registriert werden kann.

Ersetzen von Primärservern

Weitere Informationen zum Ersetzen des ersten Primärservers durch den zweiten Primärserver bzw. zum Ersetzen eines vorhandenen Primärservers durch einen neuen Primärserver finden Sie unter *Replacing Primary Servers* (Ersetzen von Primärservern) im Handbuch *ZENworks Disaster Recovery Reference* (ZENworks: Referenz für die Notfallwiederherstellung).

Verschieben eines Primärservers auf eine Appliance

Weitere Informationen zum Verschieben eines vorhandenen Primärservers (Windows oder Linux) auf einen Appliance-Server finden Sie unter *Moving from a Windows or Linux Primary Server to Appliance* (Wechsel von einem Windows- oder Linux-Primärserver auf Appliance) im Handbuch *ZENworks Primary Server and Satellite Reference* (ZENworks: Referenz für Primärserver und Satelliten).

ZENworks Configuration Management

Verwaltung von Windows 10-Geräten

ZENworks 2020 Update 2 bietet neue Funktionen, mit denen Sie den gesamten Lebenszyklus von Windows 10-Geräten über den integrierten MDM-Agenten auf diesen Geräten verwalten. Bei Anwendungsfällen, die über die Funktionen auf Windows 10-Geräten hinausgehen, können Sie zudem den ZENworks-Agenten auf Geräten installieren, die mit den Windows 10 MDM-Agenten arbeiten.

Weitere Informationen zu den einzelnen Funktionen in diesem Abschnitt finden Sie im Handbuch Windows MDM Reference (Referenz zu Windows MDM).

Neue Funktionen:

Konfigurationsfunktionen

Sie können den Windows-Benachrichtigungsdienst (WNS) nunmehr für das Senden von Push-Benachrichtigungen an Geräte konfigurieren, die mit Windows Modern Management verwaltet werden.

Registrierungsfunktionen

Die folgenden Registrierungsfunktionen wurden eingeführt.

Registrierungsmethoden: Windows 10-Geräte können anhand der folgenden Methoden bei ZENworks registriert werden.

- Registrierung mit Bereitstellungspaket (PPKG)
- Azure Active Directory (Azure AD)-Beitritt
- AutoPilot-Registrierung

Bereitstellung des ZENworks-Agenten: Sie können nunmehr den ZENworks-Agenten auf Windows 10-Geräten bereitstellen, die bereits mit dem MDM-Registrierungsmodus registriert wurden.

Konfiguration der Nutzungsbedingungen: Sie können die Nutzungsbedingungsrichtlinie zu Geräten zuweisen, sodass der Inhalt der Nutzungsbedingungen auf dem Agenten angezeigt wird, während Windows 10-Geräte entweder über den Azure AD-Beitritt oder die AutoPilot-Registrierung registriert werden.

Verwaltungsfunktionen

Die folgenden Verwaltungsfunktionen wurden eingeführt:

Bereitstellung von Windows 10 MDM-Bundles: Sie können nunmehr die folgenden Bundles auf Windows 10 MDM-Geräten bereitstellen:

HINWEIS: Diese Bundles werden auf experimenteller Basis unterstützt und dürfen lediglich zu Evaluierungszwecken genutzt werden.

- Mit dem Bundle "Windows 10 MDM – MSI installieren" stellen Sie ein Microsoft Installer-(MSI-)Paket auf Windows 10 MDM-Geräten bereit.
- Mit dem "Windows 10 MDM – CSP-Bundle" verteilen Sie Konfigurationsdienstanbieter (CSPs) zur Bereitstellung verschiedener über CSPs verfügbarer Konfigurationen auf Windows 10 MDM-Geräten.

Starten von Schnellaufgaben: Die folgenden Schnellaufgaben werden auf Windows 10 MDM-Geräten unterstützt:

- Gerät löschen
- Registrierung des Geräts aufheben
- Gerät stilllegen
- Gerät wieder in Betrieb nehmen
- Gerät verloren
- Geräteregistrierung aufheben

Weitere Funktionen

Die folgenden weiteren Funktionen wurden für die Windows 10 MDM-Funktion eingeführt:

- Windows 10-Geräte unterstützen den automatischen Abgleich.

- Der Vorgang für die Neuzusammenstellung der Zertifizierungsstelle stellt nunmehr Zertifikate für Windows 10 MDM-Geräte aus.
- Die Einstellung "MS-Graph-API" wurde in "Azure-MDM-Anwendung" umbenannt und muss neu konfiguriert werden, damit die Optimierungen aus dieser Version in Kraft treten.

Erste Schritte mit Modern Management

Die Seite "Erste Schritte" für die mobile Verwaltung wurde überarbeitet und um die Registrierung und Verwaltung von Windows 10 MDM-Geräten ergänzt. Weitere Informationen finden Sie im Handbuch Modern Management Reference (Referenz zu Modern Management).

ZENworks Imaging

Image-Wiederherstellung anhand des Bundle-Namens unter WinPE: In ZENworks 2020 Update 1 (und früher) unterstützte die WinPE-Distribution die Image-Wiederherstellung mit dem IMG-Befehl und Angabe des Image-Namens. Der Befehl erkannte jedoch nicht, ob das Bundle mit dem Befehl übergeben wurde. Ab ZENworks 2020 Update 2 werden die IMG-Bundle-Befehle in der WinPE-Distribution unterstützt. Weitere Informationen finden Sie im Handbuch Preboot Services and Imaging (Preboot-Dienste und Imaging).

Neues Tool zum Lesen von ZENworks-Image-Informationen: Das zmginfo-Tool liefert Informationen zu einem Image. Dies ist insbesondere dann von Nutzen, wenn sich mehrere Images im Inhalts-Repository oder im freigegebenen Pfad befinden und Sie aus Zeitgründen Informationen zu den einzelnen Images zusammenstellen müssen. Mit dem zmginfo-Tool können Sie wahlweise grundlegende oder vollständige Informationen zum Image abrufen. Mit zmginfo können Administratoren die Bundle-XML erstellen, die als Bundle importiert werden kann; hiermit lassen sich alle Linux-Basis-Images in WinPE-Basis-Images konvertieren.

Weitere Informationen finden Sie im Handbuch Preboot Services and Imaging (Preboot-Dienste und Imaging).

ZENworks-Fernverwaltung

Fernsteuerung eines Geräts mit aktiver RDP-Sitzung: Sie können nunmehr eine Fernsitzung auf einem Gerät mit aktiver RDP-Sitzung starten, so wie dies bereits mit einer normalen Fernverwaltungs-Sitzung möglich ist. Weitere Informationen finden Sie im Handbuch Remote Management Reference (Referenz zur Fernverwaltung).

Aufzeichnen einer Fernverwaltungssitzung (experimentelle Unterstützung): Die Benutzer auf dem verwalteten Gerät können die Fernverwaltungssitzung aufzeichnen. Weitere Informationen finden Sie im Handbuch Remote Management Reference (Referenz zur Fernverwaltung).

Mobile Management

Aktivieren von Gerätezuweisungen für Android-Bundles: Android-Bundles für genehmigte Play Store-Apps, die bislang auf Benutzerzuweisungen beschränkt waren, können nunmehr auch Geräten zugewiesen werden. Weitere Informationen finden Sie im Handbuch Mobile Management Reference (Referenz zur mobilen Verwaltung).

Bereitstellung von System-Apps: Mit der Bundle-Funktion können Sie System-Apps auf Android-Geräten aktivieren oder deaktivieren. System-Apps sind integrierte Anwendungen, die bereits auf dem Gerät vorinstalliert sind. Weitere Informationen finden Sie im Handbuch Mobile Management Reference (Referenz zur mobilen Verwaltung).

Erste Schritte mit Modern Management: Die Seite "Erste Schritte" für die mobile Verwaltung wurde überarbeitet und um die Registrierung und Verwaltung von Windows 10 MDM-Geräten ergänzt. Auch zusätzliche Funktionen für die Registrierung und Verwaltung von Apple- und Android-Geräten wurden in diese Seite aufgenommen. Weitere Informationen finden Sie im Handbuch Modern Management Reference (Referenz zu Modern Management).

Bearbeiten des Protokollspeicherorts auf Android-Geräten Der Speicherort der ZENworks-App-Protokolle auf Android-Geräten lautet nunmehr `Android/data/com.novell.zapp/files/Documents/zapp.log`. Zum Freigeben dieser Protokolle müssen Sie die App Dateien auf Android-Geräten installieren.

Bundle-Verwaltung

Der Workflow "Beziehungen kopieren" wurde um die neue Funktion **Bei Fehler fortfahren** erweitert. Wenn beim Kopieren von Beziehungen von einem Gerät in einen anderen Objektsatz ein Fehler auftritt, wird der Vorgang für die verbleibenden Objekte fortgesetzt. Am Ende des Vorgangs werden die Fehlerdetails angezeigt und es wird eine Option angeboten, mit der die Details als Referenz und als Ausgangspunkt für weitere Maßnahmen exportiert werden können. Weitere Informationen finden Sie im Handbuch: Software Distribution Reference (Referenz zur Softwareverteilung).

Sonstige

Verwendung der aktuellen Version des Puppet-Agentenpakets für Kunden: ZENworks hat das Puppet-Agentenpaket bislang als Teil des Builds bereitgestellt, sodass die Benutzer die Puppet-Richtlinie nutzen konnten. Angesichts der fortlaufenden Aktualisierungen der Puppet-Agentenversion nach der Veröffentlichung von ZENworks waren die Benutzer nicht in der Lage, die jeweils aktuelle Version des Puppet-Agentenpakets zu nutzen. Ab dieser Version gilt: Damit die Puppet-Richtlinie auf verwalteten Linux-Geräten mit ZENworks 2020 Update 2 (oder höher) wirksam wird, muss das Puppet-Agentenpaket auf den Geräten installiert sein. Weitere Informationen finden Sie im Handbuch Configuration Policies Reference (Referenz für Konfigurationsrichtlinien).

Sicherheitsoptimierungen in ZENworks

Durch die Sicherheitsoptimierungen in dieser Version können Sie auf sichere Weise Geräte registrieren und mit den Geräten kommunizieren, selbst in einer DMZ-Umgebung.

- Wenn Sie ZENworks 2020 Update 2 neu installiert haben, sind die Sicherheitseinstellungen standardmäßig auf allen Primärservern aktiviert.
- Wenn Sie die Primärserver aufrüsten, werden die Sicherheitseinstellungen standardmäßig deaktiviert.
- Wenn Sie einen neuen Primärserver in die Zone eingefügt haben, werden die Sicherheitseinstellungen nach der Aufrüstung auf ZENworks 2020 Update 2 standardmäßig aktiviert.

Sie müssen die Einstellungen mit dem folgenden zman-Befehl aktivieren:

- Mit `zman ssassc` (Security-Set-Agent-Server-Secure-Communication) wird nunmehr die Authentifizierung für die Kommunikation zwischen dem ZENworks-Agenten und den ZENworks-Servern aktiviert oder deaktiviert.

Weitere Informationen zu den Sicherheitsoptimierungen in dieser Version finden Sie im Handbuch ZENworks Securing Devices Reference (Referenz zum ZENworks-Geräteschutz).

Geräteregistrierung

Vorabgenehmigung der Geräteregistrierung

Vorab genehmigte Geräte wurden von den Administratoren als Bestandteil der Zone genehmigt. Dies ist insbesondere dann von Nutzen, wenn Sie eine bekannte Gruppe von Geräten vorab genehmigen müssen, die per Massenvorgang registriert werden sollen. Bei Bedarf ist damit auch der Abgleich bekannter Geräte möglich.

Verwendung des Autorisierungsschlüssels

Anhand eines Autorisierungsschlüssels kann sich der ZENworks-Agent zur Registrierung in der Zone autorisieren; dies gilt auch für die Kommunikation mit dem Server im Rahmen der Installation.

Schutz für die Registrierung von verwalteten Geräten und von iOA-Geräten

Sollen neuere iOA-Agenten oder verwaltete Geräte in der Zone registriert werden, müssen Sie entweder bei der Geräteregistrierung einen Autorisierungsschlüssel angeben oder das Gerät muss sich auf der Liste der vorab genehmigten Geräte befinden.

Gerätekommunikation

Gerätekommunikation (und ZCC-Anmeldung) über OSP

Bei den meisten Funktionen prüft ZENworks die Benutzeridentität mittlerweile mithilfe des OAuth-Protokolls. Aus diesem Grund wurde der neue OSP-Dienst eingeführt, mit dem die Anmeldung bei ZCC, die Kommunikation zwischen den Diensten und die Kommunikation zwischen Gerät und Servern erfolgt.

Schutz des Inhalts und der Erfassung zwischen Geräten, Primärservern und Satellitenservern

Mit Einführung dieser neuen Sicherheitsfunktion läuft die Ende-zu-Ende-Erfassung und -Übertragung von Inhalt zwischen verwalteten Geräten, Primärservern und Satellitenserver über SSL ab. Konfigurieren Sie hierzu die Einstellung in ZCC oder verwenden Sie die neu eingeführten zman-Befehle.

Schutz der Webdienstkommunikation zwischen Gerät und Primärserver oder Satellitenserver

Mit dieser Version wurden Sicherheitsoptimierungen für die Webdienstaufrufe eingeführt, die den Schutz der Webdienst-Kommunikation zwischen dem ZENworks-Agenten und den ZENworks-Primärservern und -Satellitenservern verstärken.

Ausschluss von Laufwerken aus der Microsoft-Datenverschlüsselungsrichtlinie

Wechseldatenträger können nunmehr von der Verschlüsselung nach Laufwerkstyp in der Microsoft-Datenverschlüsselungsrichtlinie ausgeschlossen werden, wenn die Richtlinie auf verwalteten Geräten durchgesetzt wird.

Antimalware

ZENworks Antimalware ist eine neue Komponente von ZENworks Endpoint Security Management in der Sicherheitsgruppe im ZENworks-Kontrollzentrum. Antimalware schützt als komprimierende Lösung die verwalteten Geräte vor den aktuellen Malware-Bedrohungen. Wenn der Antimalware-Agent auf Geräten in Ihrer Zone bereitgestellt wird, empfängt er fortlaufend Aktualisierungen der Malware-Signaturdateien vom Antimalware-Cloud-Service, sodass Malware-Infektionen sowohl mit On-Access- als auch mit On-Demand-Absuchen erkannt werden können. Infizierte Dateien werden bis zu ihrer Desinfektion unter Quarantäne gestellt.

Weitere Informationen zu den Themen in diesem Abschnitt finden Sie hier:

- ZENworks Endpoint Security Antimalware Reference (Referenz zu ZENworks Endpoint Security Antimalware)

Schutz gegen Malware – Seite "Erste Schritte"

Die Seite "Erste Schritte" der Sicherheit umfasst eine zusätzliche Seite "Schutz gegen Malware" mit verschiedenen Registerkarten. Auf dieser Seite können Sie sämtliche Funktionen von ZENworks Antimalware zentral konfigurieren, bereitstellen und anpassen.

Antimalware-Aktualisierungsberechtigung

Die Antimalware-Aktualisierungsberechtigung ist für die Bereitstellung der Antimalware-Richtlinien auf Geräten erforderlich. Wenn Sie Endpoint Security Management im Evaluierungsmodus aktivieren, wird die Berechtigung automatisch für die Dauer des Evaluierungszeitraums aktiviert.

Windows Endpoint Security-Richtlinien

Für die Bereitstellung, Anpassung und Kontinuität von Antimalware stehen vier neue Richtlinien bereit:

Antimalware-Durchsetzungsrichtlinie: Mit dieser Basisrichtlinie wird der Antimalware-Agent auf verwalteten Geräten installiert. Diese Richtlinie muss bereitgestellt werden, damit die anderen Antimalware-Richtlinien verwendet werden können. Sie umfasst Konfigurationen für alle Malware-Absuchen, u. a. On-Access-Absuchen, vollständige Absuchen, Schnellabsuchen, Absuchen auf externen Geräten und Kontext-On-Demand-Absuchen. Auch Einstellungen für das Quarantäneverhalten und für die Definition der Inhalte, die von den Absuchen ausgeschlossen werden sollen, stehen bereit.

Wenn die Standardeinstellungen für die Endbenutzerrechte und die Benachrichtigungen beim Bereitstellen der Richtlinie beibehalten werden, können die Endbenutzer auf ihren Endpunkten auf die Agentenstatuskonsole zugreifen und damit eigene Absuchen starten, den Status von Absuchen und Agenten-Aktualisierungen abrufen sowie Benachrichtigungen zur Agentenaktivität erhalten, die durch die Richtlinie kontrolliert wird.

Antimalware-Absuchausschlussrichtlinie: Antimalware bietet sowohl integrierte als auch benutzerdefinierte Absuchausschlüsse, die Sie in die verschiedenen Antimalware-Richtlinien einbinden können. Die Absuchausschlussrichtlinie wird per Gerätezuweisung angewendet, wenn dem Gerät auch andere Antimalware-Richtlinien zugewiesen sind. So lassen sich Absuchausschlüsse einfacher in der gesamten Zone weiterleiten. Ausschlüsse können für bestimmte Absuchtypen aktiviert oder deaktiviert werden.

Richtlinie für benutzerdefinierte Antimalware-Absuche: Die Richtlinie für die benutzerdefinierte Absuche bewirkt eine stärker zielgerichtete Absuche lokaler Laufwerke oder verwalteter Geräte, wenn eine bestimmte Bedrohung vermutet wird oder wenn bestimmte Speicherorte auf diesen Geräten abgesucht werden sollen. Diese Richtlinie umfasst einen eigenen Zeitplan; der Zonenzeitplan, der für die Antimalware-Durchsetzungsrichtlinie konfiguriert ist, gilt hier nicht.

Antimalware-Netzwerkabsuchrichtlinie: Auch die Netzwerkabsuchrichtlinie ermöglicht eine stärker zielgerichtete Absuche, jedoch explizit für Ordner und Dateien auf Netzlaufwerken. Diese Richtlinie besitzt ebenfalls einen eigenen Zeitplan und bietet eine zusätzliche Einstellung für die Authentifizierung bei Speicherorten im Netzwerk.

Antimalware-Sicherheits-Dashlets

Vier neue Dashlets, die standardmäßig im Sicherheits-Dashboard voreingestellt sind, überwachen Malware-Bedrohungen, Malware-Absuchen und Aktualisierungen der Malware-Signaturen.

Geräte-Malware-Status: Dieses Dashlet zeigt den Malware-Status für einzelne Geräte in der Zone für einen ausgewählten Erkennungszeitraum.

Letzte Malware-Absuche auf dem Gerät: Dieses Dashlet zeigt den Zustand der Geräte in Ihrer Zone gegenüber Malware-Bedrohungen. Standardmäßig werden Informationen zu allen Absuchen angezeigt, die auf den Geräten in einem bestimmten Zeitraum durchgeführt wurden.

Wichtigste Malware-Bedrohungen: Dieses Dashlet zeigt die Liste der wichtigsten Malware-Bedrohungen in der Zone. Standardmäßig werden die wichtigsten Malware-Threats nach der Anzahl der infizierten Geräte angezeigt.

Geräte-Malware-Signaturversion: Dieses Dashlet zeigt die Liste der Malware-Signaturversionen und die Antimalware-Agentenversionen, die auf den Geräten in der Zone installiert sind.

Geräteseite "Antimalware"

Diese Seite wird beim Auswählen eines Geräts als neue Registerkarte geöffnet. Die Seite zeigt einen Snapshot-Status der Malware-Bedrohungen, den Absuchzeitplan und Informationen zu Dateien unter Quarantäne für das ausgewählte Gerät. Außerdem können Sie bestimmte Aktionen für Dateien ausführen, Absuchen anstoßen sowie die Version des Antimalware-Agenten und der Malware-Signaturen auf dem Gerät aktualisieren.

Seite "Malware-Bedrohungsdetails"

Diese Seite wird geöffnet, wenn Sie auf den Link einer Malware-Bedrohung im Abschnitt "Malware-Bedrohungen" auf der Seite "Antimalware" eines Geräts klicken. Diese Seite bietet ausführliche Informationen zur ausgewählten Bedrohung und Details zu den Geräten, die mit der Bedrohung infiziert wurden.

Antimalware-Schnellaufgaben

Wenn in der Gerätegruppe im ZENworks-Kontrollzentrum mindestens ein Gerät ausgewählt wird, auf dem der Antimalware-Agent installiert ist, stehen fünf neue Schnellaufgaben für die ausgewählten Geräte zur Auswahl. Hierzu gehören die folgenden Schnellaufgaben:

- Malware-Absuche starten
- Malware-Signatur aktualisieren
- Antimalware-Agenten aktualisieren
- Datei aus Malware-Quarantäne wiederherstellen
- Datei aus Malware-Quarantäne löschen

Antimalware-zac-Befehle

Antimalware umfasst mehrere spezielle neue zac-Befehle. Mit diesen Befehlen können Sie u. a. Malware-Absuchen starten, den Malware-Status des Antimalware-Agenten prüfen, den Agenten installieren, aktualisieren oder entfernen sowie Dateien aus der Quarantäne löschen.

Antimalware-Zonenkonfigurationsseiten

Die Sicherheitsgruppe auf der Hauptseite der ZENworks-Konfiguration umfasst nunmehr drei neue Zonenkonfigurationsseiten. Diese Seiten enthalten jeweils verschiedene Standardeinstellungen, die Sie individuell anpassen können. Folgende Seiten stehen zur Verfügung.

Antimalware-Agenten-Zeitpläne: Konfiguriert die Zeitpläne für Malware-Absuchen und für Aktualisierungen der Malware-Signaturen. Sie können diesen Zeitplan auf Geräteordner- und Geräteebene überschreiben.

Antimalware-Agenten-Benachrichtigungen: Konfiguriert die Meldungen und Benachrichtigungen, die vom Antimalware-Agenten auf verwalteten Geräten angezeigt werden. Sie können diese Einstellungen auf Geräteordner- und Geräteebene überschreiben.

Antimalware-Konfiguration: Definiert den ZENworks-Primärserver, der als Antimalware-Server fungieren soll; dieser Server muss manuell für die Bereitstellung der Antimalware-Komponente konfiguriert werden. Außerdem wird hier der Wartungszeitplan für den Antimalware-Agenten konfiguriert.

Konfigurationsseite für On-Demand-Inhalte

Diese neue Zonenkonfigurationsseite ist neuer Bestandteil der Bundle-, Richtlinien- und Inhaltsgruppen auf der Hauptseite der ZENworks-Konfiguration. Hier werden die Download-Geschwindigkeit und die Cache-Größe der Inhalte für die Inhaltsverteilung in der Zone verwaltet; hierzu gehören derzeit auch die Antimalware-Signaturdateien und die Aktualisierungen für den Antimalware-Agenten.

Antimalware-Dienststatus

Der Antimalware-Dienststatus kann nunmehr auf der ZCC-Diagnoseseite abgerufen werden.

Antimalware-Datenbank

Die Antimalware-Datenbank wurde mit ZENworks 2020 Update 2 eingeführt. Hier werden Daten für die Antimalware-Funktionen über die Antimalware-Seite und die Antimalware-Sicherheits-Dashlets bereitgestellt. Wenn die entsprechende Einstellung konfiguriert ist, wird diese Datenbank mit der ZENworks-Datenbank synchronisiert; die Datenbanken müssen also denselben Datenbanktyp aufweisen. Beispiel: PostgreSQL, Microsoft SQL Server oder Oracle.

Die Antimalware-Datenbank wird über "Schutz gegen Malware" – Seite "Erste Schritte" für die Sicherheit im ZENworks-Kontrollzentrum konfiguriert. Wenn die Antimalware-Datenbank anhand einer externen Datenbank konfiguriert werden soll, die bislang noch nicht vorhanden ist, können Sie die Datenbank mit einem CLI-Befehl über die Datei `setup.exe` erstellen.