ZENworks 2020 Update 2

Riferimento sulle novità

Agosto 2021

Note legali

Per ulteriori informazioni sulle note legali, i marchi, le dichiarazioni di non responsabilità, le garanzie, le esportazioni e altre limitazioni di utilizzo, i diritti del governo degli Stati Uniti, le norme sui brevetti e la conformità FIPS, consultare https://www.novell.com/company/legal/.

Le sole garanzie valide per prodotti e servizi di Micro Focus, le sue affiliate e i concessori di licenza ("Micro Focus") sono specificate nelle dichiarazioni esplicite di garanzia che accompagnano tali prodotti e servizi. Nulla di quanto riportato nel presente documento deve essere interpretato come garanzia aggiuntiva. Micro Focus non sarà da ritenersi responsabile per errori tecnici o editoriali contenuti nel presente documento né per eventuali omissioni. Le informazioni di questo documento sono soggette a modifiche senza preavviso.

Sommario

Informazioni sulla Guida

Questo *Riferimento sulle novità di ZENworks* descrive le nuove funzioni disponibili nella release di ZENworks 2020 Update 2. Nella guida sono incluse le sezioni seguenti:

Destinatari

Questa guida è destinata agli amministratori di ZENworks.

Feedback

È possibile inviare i propri commenti e suggerimenti relativi a questa guida e agli altri documenti forniti con questo prodotto. Per inserire i commenti, **utilizzare l'apposita funzione** disponibile in fondo a ogni pagina della documentazione online.

Documentazione aggiuntiva

ZENworks è supportato da altra documentazione (in formato PDF e HTML) che può essere consultata e implementata nel prodotto. Ulteriore documentazione è disponibile sul sito Web della documentazione di ZENworks.

1 Novità di ZENworks 2020 Update 2

Le seguenti sezioni descrivono le nuove funzioni e i miglioramenti apportati in ZENworks 2020 Update 2:

Supporto delle piattaforme

In questa versione sono supportate le seguenti nuove piattaforme:

- CentOS come dispositivo gestito
- macOS 11 (Big Sur) come dispositivo gestito
- Android 11
- iOS 14
- SLES 15 SP2
  - SLES 15 SP2 (server primario)
  - SLES 15 SP2 (dispositivo gestito - Incluso SLES per SAP)
  - SLED 15 SP2 (dispositivo gestito)
- Nuove piattaforme RHEL e Scientific Linux
  - Scientific Linux 7.7 e 7.8
  - RHEL 7.8 e 8.2

Installazione e upgrade

Poiché l'obiettivo di ZENworks è quello di adottare un'architettura più affidabile e flessibile e di allinearsi agli standard Micro Focus, sono stati introdotti alcuni miglioramenti al processo di installazione e upgrade in ZENworks 2020 Update 2. Le modifiche introdotte in questa versione sono le seguenti:

Installazione di Docker e di Docker Compose

Prima di eseguire l'upgrade o l'installazione di ZENworks 2020 Update 2 su un server primario Linux, è necessario installare Docker e Docker Compose sul server. Per ulteriori informazioni su Docker, vedere https://docs.docker.com/.

Migrazione dei dati dei server a un nuovo percorso di file

Dopo aver eseguito l'upgrade a ZENworks 2020 Update 2 in un server primario Windows, Appliance o Linux, i dati del server ZENworks come MSI, RPM, log e file di configurazione precedentemente presenti nel percorso dei file Novell verranno trasferiti al nuovo percorso Micro Focus.

Ad esempio, in un server Linux, i file di configurazione precedentemente salvati in: `/etc/opt/novell/zenworks` saranno ora disponibili in `/etc/opt/microfocus/zenworks`. In modo analogo, in un server Windows, i file di configurazione presenti in: `C:\Programmi (x86)\Novell\ZENworks\conf` sono ora disponibili in `C:\Programmi (x86)\Micro Focus\ZENworks\conf`

I file e i dati correlati all'agente ZENworks permangono nell'ubicazione Novell precedente.

Ridenominazione dei servizi del server ZENworks

Dopo aver eseguito l'upgrade a ZENworks 2020 Update 2 in un server primario Windows, Appliance o Linux, alcuni servizi del server ZENworks, tra cui ZENServer, ZENLoader e ZENJoinProxy, verranno rinominati da Novell in Micro Focus. Ad esempio, in un server Linux, `novell-zenserver.service` verrà rinominato in `microfocus-zenserver.service`.

Introduzione di una nuova variabile di ambiente

Per i server Windows è stata introdotta la nuova variabile di ambiente `%ZENSERVER_HOME%` che punta all'ubicazione di installazione del server anche per il percorso non di default (`C:\Programmi (x86)\Micro Focus\ZENworks`.)

Versione di TLS

Se ZENworks 2020 Update 2 è stato installato di recente, per default, TLS 1.2 verrà abilitato nella zona e, quando si tenta di registrare un dispositivo con Microsoft .NET 4.7 e versioni successive, la registrazione ha esito negativo. Tuttavia, l'agente viene installato nel dispositivo.

Se si esegue l'upgrade di una zona esistente a ZENworks 2020 Update 2, TLS 1.2 non viene abilitato di default. Se si abilita TLS 1.2 nella zona, alcune funzioni potrebbero non funzionare come previsto ed è necessario verificare di installare Microsoft .NET 4.7 in tutti i dispositivi nella zona.

Se TLS 1.2 è stato abilitato nella zona, per poter registrare il dispositivo è necessario installarlo con Microsoft .NET 4.7.

Sostituzione dei server primari

Per maggiori dettagli sulla sostituzione del primo server primario con il secondo oppure sulla sostituzione di un server primario esistente con uno nuovo, vedere *Replacing Primary Servers* (Sostituzione dei server primari) in *ZENworks Disaster Recovery Reference* (Riferimento per il disaster recovery di ZENworks).

Spostamento di un server primario in un server Appliance

Per maggiori dettagli sulla procedura per spostare un server primario (Windows o Linux) esistente in un server Appliance, vedere *Moving from a Windows or Linux Primary Server to Appliance* (Spostamento di un server primario Windows o Linux ad Appliance) in *ZENworks Primary Server and Satellite Reference* (Riferimento per server primari e satelliti ZENworks).

ZENworks Configuration Management

Gestione dei dispositivi Windows 10

In ZENworks 2020 Update 2 sono state aggiunte nuove funzionalità che consentono di gestire l'intero ciclo di vita dei dispositivi Windows 10 utilizzando l'agente MDM integrato in questi dispositivi. Per gestire i casi di utilizzo al di fuori delle funzionalità dei dispositivi Windows 10, è inoltre possibile distribuire l'agente ZENworks nei dispositivi che utilizzano gli agenti MDM Windows 10.

Per ulteriori informazioni sulle singole funzionalità elencate in questa sezione, vedere Windows MDM Reference (Riferimento per MDM di Windows).

Di seguito sono riportate le nuove funzionalità:

Funzionalità di configurazione

È ora possibile configurare Servizi notifica Push Windows per l'invio di notifiche push ai dispositivi Windows amministrati tramite la gestione moderna di Windows.

Funzionalità di registrazione

Sono state introdotte le seguenti funzionalità di registrazione:

Metodi di registrazione: è possibile registrare i dispositivi Windows 10 in ZENworks mediante i seguenti metodi:

- Registrazione dei pacchetti di provisioning (PPKG)
- Aggiunta ad Azure Active Directory (Azure AD)
- Registrazione con AutoPilot

Distribuzione dell'agente ZENworks: è ora possibile distribuire l'agente ZENworks nei dispositivi Windows 10 già registrati mediante la modalità MDM.

Configurazione delle Condizioni per l'utilizzo: è possibile assegnare la policy delle Condizioni per l'utilizzo ai dispositivi per aggiungere il relativo contenuto da visualizzare nell'agente durante la registrazione dei dispositivi Windows 10 mediante le modalità Aggiunta ad Azure AD o Autopilot.

Funzionalità di gestione

Sono state introdotte le seguenti funzionalità di gestione:

Distribuzione di pacchetti MDM Windows 10: è ora possibile distribuire i seguenti pacchetti nei dispositivi MDM Windows 10:

Nota: il supporto per questi pacchetti è su base sperimentale e deve essere utilizzato solo per scopi di valutazione.

- Utilizzando il pacchetto del programma di installazione MSI MDM Windows 10, distribuire un pacchetto MSI nei dispositivi MDM Windows 10.
- Utilizzando il pacchetto CSP MDM Windows 10, distribuire Configuration Service Provider (CSP) per implementare varie configurazioni disponibili tramite CSP su dispositivi MDM Windows 10.

Avvio di task rapidi: i seguenti task rapidi sono supportati nei dispositivi MDM Windows 10:

- Elimina dispositivo
- Annulla registrazione del dispositivo
- Disattiva dispositivo
- Annulla la disattivazione permanente del dispositivo
- Dispositivo perso
- Annulla registrazione dispositivo

Altre funzioni

Di seguito sono elencate altre funzionalità introdotte per la funzione MDM Windows 10:

- I dispositivi Windows 10 supportano la riconciliazione automatica.
- Il processo Nuova creazione CA emette ora certificati nei dispositivi MDM Windows 10.
- L'impostazione API MS Graph è stata rinominata in Applicazione Azure MDM e deve essere riconfigurata per poter usufruire dei nuovi miglioramenti introdotti in questa versione.

Introduzione alla gestione moderna

La pagina introduttiva alla gestione dei dispositivi mobili è stata aggiornata per includere la registrazione e la gestione dei dispositivi MDM Windows 10. Per ulteriori informazioni, vedere Modern Management Reference (Riferimento per Gestione moderna).

Imaging di ZENworks

Ripristino dell'immagine mediante il nome del pacchetto in WinPE: in ZENworks 2020 Update 1 e versioni precedenti, la distribuzione di WinPE supporta il ripristino dell'immagine fornendo il relativo nome mediante il comando IMG, che non riconosce se il pacchetto è stato passato tramite il comando. A partire da ZENworks 2020 Update 2, i comandi di pacchetto IMG sono supportati nella distribuzione di WinPE. Per ulteriori informazioni, vedere la guida Preboot Services and Imaging (Servizi di preavvio e imaging).

Nuovo strumento per la lettura delle informazioni sull'immagine ZENworks: lo strumento zmginfo consente di raccogliere informazioni su un'immagine. Si tratta di uno strumento particolarmente utile se si dispone di più immagini nell'archivio contenuti o nel percorso condiviso ed è necessario raccogliere informazioni su ognuna di esse per risparmiare tempo. Con lo strumento zmginfo è possibile raccogliere informazioni di base o complete sull'immagine. Mediante zmginfo un admin può creare il pacchetto XML che può essere importato e utilizzato per convertire tutte le immagini di base Linux in immagini di base winpe.

Per ulteriori informazioni, vedere la guida Preboot Services and Imaging (Servizi di preavvio e imaging)

Gestione remota ZENworks

Controllo remoto di un dispositivo con una sessione RDP attiva: è ora possibile avviare una sessione remota su un dispositivo con una sessione RDP attiva esattamente come una normale sessione di gestione remota. Per ulteriori informazioni, vedere la guida Remote Management Reference (Riferimento per Gestione remota).

Registrazione di una sessione di gestione remota (supporto sperimentale): consente agli utenti sul dispositivo gestito di registrare la sessione di gestione remota. Per ulteriori informazioni, vedere la guida Remote Management Reference (Riferimento per Gestione remota).

Gestione mobile

Abilitazione di assegnazioni dispositivo per pacchetti Android: i pacchetti Android creati per le app approvate del Play Store, in precedenza limitati alle assegnazioni utente, possono ora essere assegnati anche ai dispositivi. Per ulteriori informazioni, vedere Mobile Management Reference (Riferimento per Gestione mobile).

Provisioning delle app di sistema: mediante la funzione Pacchetti è possibile abilitare o disabilitare le app di sistema sui dispositivi Android. Le app di sistema sono app integrate e preinstallate sul dispositivo. Per ulteriori informazioni, vedere Mobile Management Reference (Riferimento per Gestione mobile).

Introduzione alla gestione moderna: la pagina introduttiva alla gestione dei dispositivi mobili è stata aggiornata per includere la registrazione e la gestione dei dispositivi MDM Windows 10. In questa pagina sono state inoltre incluse funzioni aggiuntive associate alla registrazione e alla gestione dei dispositivi Apple e Android. Per ulteriori informazioni, vedere Modern Management Reference (Riferimento per Gestione moderna).

Modifica dell'ubicazione dei log dei dispositivi Android: l'ubicazione dei log delle app ZENworks sui dispositivi Android è stata modificata in `Android/data/com.novell.zapp/files/Documents/zapp.log`. Per condividere questi log, è necessario distribuire l'app Files nei dispositivi Android.

Gestione pacchetti

Nel workflow Copia relazioni è stata introdotta l'opzione **Continua in caso di errore**. Durante la copia delle relazioni da un dispositivo a un altro set di oggetti, se si verifica un errore, l'operazione prosegue per gli oggetti rimanenti. I dettagli degli errori vengono visualizzati al termine dell'operazione, insieme a un'opzione per esportare i dettagli dell'operazione per riferimento e azioni future. Per ulteriori informazioni, vedere Software Distribution Reference (Riferimento per la distribuzione software).

Varie

Possibilità per gli utenti di utilizzare la versione più recente del pacchetto puppet-agent: in precedenza, ZENworks forniva il pacchetto puppet-agent all'interno della build, consentendo agli utenti di utilizzare la policy Puppet. Tuttavia, con la pubblicazione costante di aggiornamenti alla versione di puppet-agent successivamente al rilascio di ZENworks, gli utenti non riuscivano a utilizzare la versione più recente del pacchetto puppet-agent. A partire da questa versione, per rendere effettiva la policy Puppet sui dispositivi gestiti da Linux con ZENworks 2020 Update 2 e versioni successive, è necessario verificare che il pacchetto puppet-agent sia installato sui dispositivi. Per ulteriori informazioni, vedere Configuration Policies Reference (Riferimento per le policy di configurazione).

Miglioramenti per la sicurezza in ZENworks

I miglioramenti per la sicurezza introdotti in questa versione consentono di registrare e comunicare in modo sicuro con i dispositivi anche in una rete perimetrale (DMZ).

- Se ZENworks 2020 Update 2 è stato installato di recente, per default, le impostazioni di sicurezza sono abilitate in tutti i server primari.
- Se si esegue l'upgrade dei server primari, le impostazioni di sicurezza sono disabilitate per default.
- Se è stato aggiunto un nuovo server primario alla zona, dopo l'upgrade a ZENworks 2020 Update 2, per default, le impostazioni di sicurezza sono abilitate.

È necessario eseguire il seguente comando zman per abilitare le impostazioni:

- `zman ssassc` (Security-Set-Agent-Server-Secure-Communication) è stato introdotto per abilitare o disabilitare l'autenticazione per le comunicazioni tra l'agente ZENworks e i server ZENworks.

Per ulteriori informazioni sui miglioramenti per la sicurezza introdotti in questa versione, vedere ZENworks Securing Devices Reference (Riferimento per la sicurezza dei dispositivi ZENworks).

Registrazione dei dispositivi

Preapprovazione della registrazione dei dispositivi

I dispositivi preapprovati sono i dispositivi approvati dagli amministratori che faranno parte della zona. Si tratta di una funzione particolarmente utile se sono presenti dispositivi preapprovati durante la registrazione in massa di un set noto di dispositivi. Viene inoltre utilizzata per consentire la riconciliazione dei dispositivi noti, se necessaria.

Utilizzo della chiave di autorizzazione

Una chiave di autorizzazione può essere utilizzata dall'agente ZENworks per autorizzare in modo automatico la registrazione nella zona e per eventuali comunicazioni con il server durante l'installazione.

Protezione della registrazione di dispositivi gestiti e iOA

Per registrare agenti iOA o dispositivi gestiti più recenti nella zona, è necessario specificare una chiave di autorizzazione durante la registrazione dei dispositivi o verificare che il dispositivo sia incluso nell'elenco dei dispositivi approvati.

Comunicazioni dei dispositivi

Utilizzo di OSP per le comunicazioni dei dispositivi e il login a ZCC

Per la maggior parte delle funzioni, ZENworks utilizza ora il protocollo O-Auth per stabilire l'identità degli utenti. È stato quindi introdotto un nuovo servizio denominato OSP che viene utilizzato per il login a ZCC e le comunicazioni tra servizi e tra dispositivo e server.

Protezione della raccolta e del trasferimento del contenuto tra dispositivi, server primari e server satellite

Con l'introduzione di questa nuova funzione di sicurezza, i processi end-to-end di raccolta e trasferimento del contenuto tra dispositivi, server primari e server satelliti vengono eseguiti tramite SSL. A tale scopo, è necessario configurare l'impostazione in ZCC oppure utilizzare i comandi zman introdotti di recente.

Protezione delle comunicazioni dei servizi Web tra dispositivi e server primari o satellite

Per proteggere ulteriormente le comunicazioni dei servizi Web tra l'agente ZENworks e i server primari e satellite ZENworks, sono stati introdotti miglioramenti per la sicurezza alle chiamate dei servizi Web in questa versione.

Policy cifratura dati Microsoft: esclusioni di unità

Le unità dati rimovibili possono ora essere escluse dalla cifratura per tipo di unità nella Policy cifratura dati Microsoft quando viene applicata nei dispositivi gestiti.

Antimalware

ZENworks Antimalware è un nuovo componente di ZENworks Endpoint Security Management nel raggruppamento Sicurezza all'interno del Centro di controllo ZENworks. Antimalware è una soluzione completa che protegge i dispositivi gestiti da tutte le minacce malware più recenti. In caso di distribuzione nei dispositivi della zona, l'agente antimalware riceve costantemente aggiornamenti dei file di firma malware dal servizio cloud antimalware per rilevare infezioni dannose utilizzando scansioni all'accesso e su richiesta. I file infettati vengono messi in quarantena fino alla disinfezione.

Per ulteriori informazioni sugli argomenti in questa sezione, vedere:

- ZENworks Endpoint Security Antimalware Reference (Riferimento per ZENworks Endpoint Security Antimalware)

Pagina Protezione contro il malware - Introduzione

La pagina Introduzione di Sicurezza include un'ulteriore pagina a schede denominata "Protezione contro il malware". È possibile utilizzare questa pagina come unico punto di accesso per configurare, distribuire e personalizzare tutte le funzioni offerte da ZENworks Antimalware.

Autorizzazione aggiornamento antimalware

L'Autorizzazione aggiornamento antimalware è necessaria per distribuire policy antimalware nei dispositivi. L'autorizzazione viene automaticamente abilitata per il periodo di valutazione quando si attiva Endpoint Security Management in modalità di valutazione.

Policy di sicurezza endpoint Windows

Quattro nuove policy consentono di gestire la distribuzione, la personalizzazione e la continuità dell'antimalware:

Policy di applicazione antimalware: si tratta della policy di base che installa l'agente antimalware nei dispositivi gestiti. Questa policy deve essere distribuita per l'utilizzo di qualsiasi altra policy antimalware. Include le configurazioni per tutti i tipi di scansioni antimalware, tra cui le scansioni su richiesta di tipo Scansione completa, Scansione rapida, Scansione dispositivo esterno e Scansione contestuale. Sono inoltre disponibili impostazioni per il comportamento della quarantena e la definizione del contenuto da escludere dalle scansioni.

Se le impostazioni di default per le notifiche e i diritti degli utenti finali vengono mantenute con la distribuzione della policy, gli utenti finali hanno accesso alla console di stato dell'agente sui propri endpoint e possono avviare scansioni personalizzate, visualizzare lo stato degli aggiornamenti delle scansioni e dell'agente e ricevere notifiche sull'attività degli agenti controllata dalla policy.

Policy di esclusioni da scansioni antimalware: antimalware presenta esclusioni integrate e da scansioni personalizzate che è possibile aggiungere a qualsiasi policy antimalware. La Policy di esclusioni da scansioni antimalware viene impiegata dall'assegnazione dispositivo quando anche altre policy antimalware sono assegnate agli stessi dispositivi, garantendo un processo semplificato per propagare le esclusioni da scansioni nell'intera zona. È possibile abilitare o disabilitare esclusioni per tipi specifici di scansioni

Policy di scansione personalizzata antimalware: la Policy di scansione personalizzata antimalware viene utilizzata per un approccio più mirato alla scansione delle unità locali sui dispositivi gestiti in caso di sospetto di una specifica minaccia o per destinare le scansioni a specifiche ubicazioni su questi dispositivi. Include una pianificazione specifica rispetto all'utilizzo della pianificazione di zone configurata per la Policy di applicazione antimalware

Policy di scansione di rete antimalware: anche la Policy di scansione di rete antimalware viene utilizzata per un approccio più mirato, ma è impiegata esplicitamente per la scansione di cartelle e file sulle unità di rete. Anche questa policy include una pianificazione specifica e un'ulteriore impostazione per l'autenticazione nelle ubicazioni di rete.

Dashlet di sicurezza antimalware

Quattro nuove dashlet di default nel Dashboard sicurezza consentono di monitorare le minacce, le scansioni e gli aggiornamenti delle firme malware.

Stato malware dispositivo: questa dashlet visualizza lo stato dei malware relativo a singoli dispositivi nella zona per un periodo di rilevamento selezionato.

Ultima scansione malware dispositivo: questa dashlet visualizza lo stato dei dispositivi nella zona rispetto alle minacce malware. Per default, contiene informazioni su qualsiasi tipo di scansione effettuata sui dispositivi per un periodo di tempo specificato.

Principali minacce malware: questa dashlet visualizza l'elenco delle principali minacce malware nella zona. Per default, le principali minacce malware vengono visualizzate in base al numero di dispositivi infettati.

Versione firma malware dispositivo: questa dashlet visualizza l'elenco delle versioni delle firme malware e degli agenti antimalware installati sui dispositivi nella zona.

Pagina Antimalware dispositivo

Questa pagina è una nuova scheda accessibile quando viene selezionato un dispositivo. Fornisce uno snapshot sulle informazioni relative a minacce malware, pianificazioni di scansione e file in quarantena per il dispositivo selezionato. È inoltre possibile intraprendere azioni specifiche sui file, avviare scansioni e aggiornare le versioni dell'agente antimalware e delle firme malware sul dispositivo.

Pagina Dettagli minacce malware

Questa pagina è accessibile facendo clic sul collegamento di una minaccia malware nella sezione relativa alle minacce malware della pagina Antimalware di un dispositivo. Fornisce informazioni avanzate sulla minaccia selezionata e i dettagli dei dispositivi infettati.

Task rapidi antimalware

Se nel raggruppamento Dispositivi del Centro di controllo ZENworks sono selezionati uno o più dispositivi con l'agente antimalware installato, sono disponibili cinque nuovi task rapidi che è possibile eseguire sui dispositivi selezionati. I task rapidi sono i seguenti:

- Avvia scansione malware
- Aggiorna firma malware
- Aggiorna agente antimalware
- Ripristina file da quarantena antimalware
- Elimina file da quarantena antimalware

Comandi zac di Antimalware

Antimalware presenta alcuni nuovi comandi zac specifici per questo componente. Tra i vari comandi, sono disponibili quelli per avviare le scansioni antimalware sui dispositivi, verificare lo stato dei malware dell'agente antimalware, installare, aggiornare o rimuovere l'agente e cancellare i file dalla quarantena.

Pagine di configurazione delle zone di Antimalware

Nel raggruppamento Sicurezza della pagina principale di configurazione di ZENworks sono ora disponibili tre nuove pagine di configurazione delle zone. Ognuna di queste pagine include impostazioni di default che è possibile personalizzare. Le pagine sono le seguenti:

Pianificazioni agente antimalware: consente di configurare le pianificazioni per le scansioni dei malware e gli aggiornamenti delle firme malware. È possibile ignorare questa pianificazione a livello di dispositivo e cartella dispositivo.

Notifiche dell'agente antimalware: consente di configurare gli avvisi e le notifiche visualizzati dall'agente antimalware sui dispositivi gestiti. È possibile ignorare queste impostazioni a livello di dispositivo e cartella dispositivo.

Configurazione antimalware: consente di definire il server primario ZENworks da utilizzare come server antimalware, che deve essere configurato manualmente per distribuire il componente antimalware. Consente inoltre di configurare la pianificazione di manutenzione per l'agente antimalware.

Pagina di configurazione Contenuto su richiesta

Nel raggruppamento Pacchetto, policy e contenuto della pagina principale di configurazione di ZENworks è ora disponibile questa nuova pagina di configurazione delle zone. Consente di gestire la velocità di download e le dimensioni della cache per la distribuzione di contenuti nella zona, che attualmente include i file di firma antimalware e gli aggiornamenti dell'agente antimalware.

Stato del servizio antimalware

Lo stato del servizio antimalware è ora accessibile nella pagina Diagnostica di ZCC.

Database antimalware

Il database antimalware è una novità di ZENworks 2020 Update 2. Il suo scopo è quello di fornire dati per le funzionalità di monitoraggio dell'antimalware tramite la pagina Antimalware e le dashlet di sicurezza antimalware. Se configurato, si sincronizza con il database ZENworks e pertanto devono essere dello stesso tipo, ad esempio PostgreSQL, Microsoft SQL Server oppure Oracle.

Il database antimalware è configurabile dalla pagina Protezione contro il malware - Introduzione per Sicurezza nel Centro di controllo ZENworks. Se il database antimalware viene configurato mediante un database esterno ancora inesistente, è possibile crearne uno tramite interfaccia riga di comando utilizzando il file `setup.exe`.