Readme dell'Aggiornamento 1 di ZENworks 2017

Luglio 2017

Le informazioni contenute in questo Readme si riferiscono alla release dell'Aggiornamento 1 di ZENworks 2017.

1 Novità dell'Aggiornamento 1 di ZENworks 2017

Per informazioni sulle nuove funzioni incluse in questa release, vedere Novità dell'Aggiornamento 1 di ZENworks 2017.

2 Pianificazione della distribuzione dell'Aggiornamento 1 di ZENworks 2017

Per pianificare la distribuzione dell'Aggiornamento 1 di ZENworks 2017 nella zona di gestione, attenersi alle seguenti linee guida:

- Se si utilizza la cifratura disco e si desidera aggiornare l'agente FDE (Full Disk Encryption), è NECESSARIO rimuovere la policy di cifratura disco dai dispositivi gestiti prima di aggiornarli all'Aggiornamento 1 di ZENworks 2017.

  Per ulteriori informazioni sull'aggiornamento di FDE (Full Disk Encryption) in Aggiornamento 1 di ZENworks 2017, vedere ZENworks 2017 Update 1 - Full Disk Encryption Update Reference (in lingua inglese).

- Per prima cosa, è necessario eseguire l'upgrade all'Aggiornamento 1 di ZENworks 2017 dei server primari, quindi dei server satellite e infine dei dispositivi gestiti. Non eseguire l'upgrade dei dispositivi gestiti e dei server satellite (o non aggiungere nuovi agenti dell'Aggiornamento 1 2017 nella zona) se l'upgrade all'Aggiornamento 1 di ZENworks 2017 non è ancora stato eseguito su tutti i server primari.

  Nota: se sui server primari non è ancora stato eseguito l'upgrade, gli agenti potrebbero ricevere dati incoerenti dalla zona. Pertanto, questa parte del processo deve essere completata nel più breve tempo possibile, idealmente subito dopo l'upgrade del primo server primario.

- Se i dispositivi gestiti sono stati aggiornati a ZENworks 11.x o versioni successive, è possibile aggiornarli direttamente all'Aggiornamento 1 di ZENworks 2017.
- Una volta eseguito l'upgrade all'Aggiornamento 1 di ZENworks 2017, ha luogo il riavvio del sistema. Tuttavia, nei seguenti casi sarà necessario un doppio riavvio:
  - Se si esegue l'aggiornamento da 11.x a ZENworks 2017 o all'Aggiornamento 1 2017 e la sicurezza endpoint è abilitata, sarà necessario un secondo riavvia per caricare il driver ZESNETAccess.
  - Se in un dispositivo gestito è in esecuzione Windows 10 con l'impostazione Autodifesa client abilitata e si esegue l'upgrade da 11.4.x a ZENworks 2017 o all'Aggiornamento 1 2017, è necessario disabilitare tale impostazione nel Centro di controllo ZENworks, riavviare il dispositivo gestito ed eseguire l'aggiornamento, per il quale è richiesto un secondo riavvio del dispositivo.
  - Se è stata applicata una policy di cifratura disco e si desidera aggiornare l'agente FDE (Full Disk Encryption) all'Aggiornamento 1 di ZENworks 2017, prima è necessario rimuovere la policy e decifrare il dispositivo. Per l'aggiornamento è richiesto il riavvio del dispositivo. Successivamente si aggiorna il dispositivo all'Aggiornamento 1 2017 e si riavvia una seconda volta il dispositivo.

Importante: per i dispositivi gestiti sui quali sono in esecuzione versioni precedenti a 11.x, prima è necessario eseguire l'upgrade a 11.x. Al termine dell'upgrade a 11.x il dispositivo viene riavviato dal sistema, quindi, una volta completata la distribuzione dell'Aggiornamento 1 di ZENworks 2017, ha luogo un secondo riavvio.

Tabella 1 *Aggiornamento dell'agente cumulativo all'Aggiornamento 1 di ZENworks 2017: percorsi supportati*

Tipo di dispositivo gestito	Sistema operativo	Versioni supportate	Versioni non supportate
Server primario	Windows/Linux	Aggiornamento v2017	Tutte le versioni precedenti alla v2017
Server satellite	Windows/Linux/Mac	v11.0 e versioni successive	Tutte le versioni precedenti alla v11.x
Dispositivo gestito	Windows	v11.0 e versioni successive	Tutte le versioni precedenti alla v11.0
	Linux	v11.0 e versioni successive	N/D
	Mac	v11.2 e versioni successive	N/D

- Prima di installare l'aggiornamento di sistema, assicurarsi di avere spazio libero su disco sufficiente nelle seguenti ubicazioni:

Ubicazione	Descrizione	Spazio su disco
Windows: `%zenworks_home%\install\downloads` **Linux:** `opt/novell/zenworks/install/downloads`	Per aggiornare i pacchetti agente.	5 GB
Windows: `%zenworks_home%\work\content-repo` **Linux:** `/var/opt/novell/zenworks/content-repo`	Per importare il file zip nel sistema dei contenuti.	5 GB

Ubicazione	Descrizione	Spazio su disco
Cache agente	Per scaricare il contenuto dell'aggiornamento di sistema applicabile richiesto per aggiornare il server ZENworks.	1.5 GB
Ubicazione in cui viene copiato il file dell'aggiornamento di sistema. si applica solo al server ZENworks utilizzato per importare il file zip dell'aggiornamento di sistema	Memorizzare il file zip dell'aggiornamento di sistema scaricato.	5 GB

3 Download e distribuzione dell'Aggiornamento 1 di ZENworks 2017

Per istruzioni su download e distribuzione dell'Aggiornamento 1 di ZENworks 2017, vedere *ZENworks 2017 Update 1 System Updates Reference* (in lingua inglese).

Se la zona di gestione è costituita da server primari sui quali è installata una versione precedente a ZENworks 2017, è possibile distribuire l'Aggiornamento 1 di ZENworks 2017 a tali server primari solo dopo averli sottoposti tutti all'upgrade a ZENworks 2017. Per istruzioni, vedere *Guida all'upgrade di ZENworks*.

Per i task amministrativi, visitare il sito relativo alla documentazione dell'Aggiornamento 1 di ZENworks 2017.

Importante: Non aggiornare il visualizzatore di Gestione remota prima di avere aggiornato tutti Join Proxy Satellite Server della zona. Per eseguire Gestione remota attraverso Join Proxy, è necessario che la versione del visualizzatore di Gestione remota sia la stessa di quella di Join Proxy.

Leggere Sezione 2, “Pianificazione della distribuzione dell'Aggiornamento 1 di ZENworks 2017”, a pagina 1 prima di effettuare il download e distribuire l'Aggiornamento 1 di ZENworks 2017.

Non distribuire l'Aggiornamento 1 di ZENworks 2017 prima di avere eseguito l'upgrade a ZENworks 2017 di tutti i server primari della zona.

Per questo aggiornamento è necessario apportare modifiche allo schema nel database. Durante l'installazione iniziale delle patch, i servizi vengono eseguiti solo sul server master o su quello primario dedicato. In tal modo si ha la garanzia che gli altri server primari non tenteranno di accedere alle tabelle che vengono modificate nel database.

Dopo l'aggiornamento del server master o del server primario dedicato, i servizi riprendono sui server restanti e contemporaneamente ha luogo l'aggiornamento.

Nota: durante l'aggiornamento non è necessario interrompere o riavviare manualmente i servizi nei server. I servizi vengono interrotti e riavviati automaticamente.

Quando si posticipa un aggiornamento del sistema e si esegue il logout dal dispositivo gestito, su questo viene applicato l'aggiornamento del sistema.

Per l'elenco delle versioni supportate dei dispositivi gestiti e dei server satellite in una zona di gestione con l'Aggiornamento 1 di ZENworks 2017, vedere Versioni supportate dei dispositivi gestiti e dei server satellite.

4 Problemi risolti nell'Aggiornamento 1 di ZENworks 2017

Alcuni dei problemi identificati nelle release precedenti sono stati risolti. Per un elenco dei problemi risolti, vedere il documento TID 7020155 nella Knowledgebase del supporto tecnico.

5 Problemi che permangono nell'Aggiornamento 1 di ZENworks 2017

Alcuni dei problemi riscontrati nelle versioni precedenti all'Aggiornamento 1 di ZENworks 2017 non sono stati ancora risolti. Per ulteriori informazioni, consultare i seguenti readme:

- Readme di ZENworks 2017

6 Problemi noti

Questa sezione contiene le informazioni relative ai problemi di che possono verificarsi durante l'uso dell'Aggiornamento 1 di ZENworks 2017:

6.1 Configurazione di ZENworks

6.1.1 Nei dispositivi Windows 2012 R2, l'adattatore di rete non è visibile quando i valori di IPv4 e IPv6 vengono modificati con il comando zisedit

Dopo aver installato l'agente su un dispositivo Windows 2012 R2, quando si avvia il dispositivo tramite PXE o da CD di avvio e si esegue il comando zisedit con le seguenti impostazioni, l'adattatore di rete non è visibile nelle connessioni di rete al momento del login al dispositivo:

1. Impostare i valori di DHCP e DHCP6 su Off.
2. Modificare i valori di IPv4 e IPv6.

Soluzione: Configurare separatamente i valori di IPv4 e IPv6.

6.1.2 In un dispositivo SLES 11 potrebbe risultare impossibile rilevare l'ubicazione e l'ambiente di rete con l'indirizzo DHCP

Se una rete è configurata con NetworkManager, è possibile che in un dispositivo SLES 11 il servizio di rete dell'indirizzo IP client non corrisponda all'indirizzo DHCP IPv6. Pertanto, il rilevamento di ubicazione e ambiente di rete risulta impossibile.

Soluzione: Configurare la rete con il metodo `ifup`.

6.1.3 Le applicazioni Java ZENworks potrebbero non funzionare nei dispositivi Windows sui quali non è installata l'interfaccia IPv4

Per le applicazioni Java 8 è necessario configurare lo stack IPv4 in un dispositivo Windows. Pertanto, le applicazioni Java ZENworks come ZCC Helper potrebbero non funzionare se non è installato IPv4.

Soluzione: Configurare lo stack IPv4 oltre allo stack IPv6.

Per ulteriori informazioni, fare riferimenti ai seguenti collegamenti:

- http://www.oracle.com/technetwork/java/javase/8-known-issues-2157115.html
- http://bugs.java.com/bugdatabase/view_bug.do?bug_id=8040229

6.1.4 Durante l'esecuzione di una modifica CA, la convalida di un certificato concatenato risulta impossibile se la catena di certificati è nell'ordine sbagliato

Durante la modifica dell'autorità di certificazione esterna, se nel nuovo file certificato è inclusa la catena di certificati nell'ordine sbagliato, la convalida del certificato risulta impossibile. Ad esempio, al posto di Server > SubCA > RootCA, se l'ordine della catena è il seguente: SubCA > Server > RootCA, il certificato non è considerato valido.

Soluzione: ricreare la catena di certificati server (con i certificati nell'ordine specificato) utilizzando un metodo a scelta. Uno dei modi più semplici per compiere questa operazione è il seguente:

1. Salvare ciascun certificato come file separato nel formato base64.
2. Aprire ciascun certificato con un editor di testo. Il contenuto sarà simile a quello riportato sotto:

   ```
   -----BEGIN CERTIFICATE-----
   <cert data>
   -----END CERTIFICATE-----
   ```

3. Creare un nuovo file e denominarlo `server.cer`.
4. Copiare il testo da ciascun file certificato nel file server.cer in modo che tutti i certificati siano inclusi in un unico file nell'ordine seguente:

```
-----BEGIN CERTIFICATE-----
<Server cert data>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<SubCA cert data>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<RootCA cert data>
-----END CERTIFICATE-----
```

5. Salvare il file `server.cer`.
6. Utilizzare il file `server.cer` come nuovo certificato e completare la procedura per modificare l'autorità di certificazione (CA) esterna.

6.1.5 Impossibile avviare pgadmin3 su un dispositivo SLES

Quando si apre pgadmin3 su un dispositivo SLES, è possibile che venga visualizzato uno dei seguenti errori:

- *pgadmin3: errore durante il caricamento delle librerie condivise: libiconv.so.2: impossibile aprire il file oggetto condiviso: file specificato o directory inesistente*
- *./pgadmin3: errore di ricerca del simbolo: /usr/lib64/libgdk-x11-2.0.so.0: simbolo non definito: pango_font_map_create_context*

Soluzione: eseguire il seguente comando nel terminale prima di aprire pgadmin3:

```
export LD_LIBRARY_PATH="/usr/local/lib64:/usr/local/lib:/lib64:/lib:/usr/lib64:/
usr/lib:/opt/novell/zenworks/share/pgsql/lib:/opt/novell/zenworks/share/pgsql/
pgAdmin3/lib:$LD_LIBRARY_PATH"
```

6.1.6 Le azioni dei pacchetti Installa MSI in rete e Crea directory si concludono con l'errore WNetAddConnection quando questi vengono configurati con la condivisione DFS

I pacchetti configurati con l'azione Installa MSI in rete o Crea directory dalla condivisione DFS generano l'errore WNetAddConnection.

Soluzione: nessuna.

Mentre si configura l'azione Installa MSI in rete, utilizzare il percorso UNC al posto della condivisione DFS.

6.1.7 Nei dispositivi iOS, è possibile che non venga visualizzato il prompt per immettere la password dell'account e-mail

Quando un account e-mail viene configurato in remoto su un dispositivo iOS che utilizza una policy e-mail per dispositivi mobili, è possibile che il prompt per immettere la password dell'account e-mail non venga visualizzato.

Soluzione: specificare manualmente la password dal menu Impostazioni del dispositivo.

6.2 Agente ZENworks

6.2.1 Quando si riavvia l'agente in un dispositivo gestito precedente e il nome host del server primario viene risolto in un indirizzo IPv6, è possibile che il dispositivo gestito non venga registrato nella zona

Quando si svuota la cache di un dispositivo gestito e questo viene riavviato, l'agente legge gli URL del server dal file `initial-web-service`. Se l'URL del server contiene un nome host che viene risolto in un indirizzo IPv6, la verifica del nome host SSL ha esito negativo. Pertanto, è possibile che gli agenti precedenti non vengano registrati.

Soluzione: aggiungere manualmente l'URL basato su IPv4 al file initial-web-service, quindi aggiornare l'agente precedente.

6.2.2 Gli agenti installati su ZENworks 2017 o versioni precedenti sono in grado di registrarsi a un server dell'Aggiornamento 1 di ZENworks 2017 con un indirizzo IPv6

La registrazione di un agente precedente che utilizza un indirizzo IPv6 del server ZENworks può riuscire, tuttavia, alcune funzioni dell'agente potrebbero non funzionare come previsto.

Soluzione: annullare la registrazione dell'agente, quindi registrarlo utilizzando un indirizzo IPv4 del server ZENworks. Evitare di registrare agenti precedenti con un indirizzo IPv6.

6.3 ZENworks Application

6.3.1 ZAPP si avvia automaticamente dopo un riavvio

Se si crea una policy ZECP per nascondere l'icona della barra delle applicazioni ZENworks e si assegna la policy a un dispositivo, quando si riavvia il dispositivo, ZAPP si avvia automaticamente.

Soluzione: cancellare la chiave di registro `ZAPP`:

1. Aprire l'editor di registro.
2. Andare a
   - Per 32 bit: `HKLM\Software\Microsoft\Windows\CurrentVersion\Run`
   - Per 64 bit: `HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run`
3. Cancellare la chiave di registro `ZAPP`.

6.4 Gestione remota

6.4.1 I visualizzatori VNC open source non sono supportati quando si controlla in remoto un dispositivo gestito Windows con un indirizzo IPV6

In un dispositivo Windows, l'agente ZENworks non è in grado di connettersi con i visualizzatori open source come RealVNC, TightVNC e UltraVNC utilizzando un indirizzo IPv6.

Soluzione: per gestire i dispositivi Windows con indirizzi IPv6, utilizzare visualizzatori VNC open source compatibili con IPv6. È possibile utilizzare i visualizzatori VNC open source per comunicare con i dispositivi gestiti utilizzando indirizzi IPv4.

6.5 Imaging di ZENworks

6.5.1 Il dispositivo RHEL 7 si avvia in modalità manutenzione dopo il ripristino dell'immagine

Quando si acquisisce un'immagine di un dispositivo RHEL 7 con SELinux abilitato, il dispositivo si avvia in modalità manutenzione dopo il ripristino dell'immagine.

Soluzione: prima di acquisire un'immagine, disabilitare SELINUX:

1. Andare alla cartella `/etc/selinux`.
2. Nel file `config`, impostare il valore di SELINUX come `disabilitato`.
3. Riavviare il dispositivo.

6.5.2 L'assegnazione del pacchetto di distribuzione MDT per reinstallare il sistema operativo in un dispositivo in cui è già installato un sistema operativo dà come risultato un ciclo infinito.

Quando si assegna il pacchetto di distribuzione MDT per reinstallare il sistema operativo in un dispositivo in cui è già installato un sistema operativo, si ottiene come risultato un ciclo infinito. All'avvio PXE, il dispositivo seleziona sempre lo stesso pacchetto MDT. Questo problema si verifica perché il pacchetto Microsoft Deployment Toolkit (MDT) elimina i dati immagine sicuri ZENworks (ZISD, Image Safe Data) quando prepara il disco per reinstallare il sistema operativo nel dispositivo. Pertanto il server di imaging non conosce lo stato del lavoro di imaging assegnato al dispositivo e non viene mai cancellato.

Soluzione: eseguire uno dei metodi descritti di seguito.

Metodo 1

1. Personalizzare la condivisione di distribuzione MDT corrispondente caricata dal file WIM di MDT nei contatti del pacchetto all'avvio. Utilizzare il file `ISDTool.exe` per cancellare il record MBR:
   - **1a** Scaricare il file `ISDTool.exe` a 32 bit dalla pagina di download di ZENworks (`https://indirizzo_IP_server_zenworks:porta/zenworks-setup`) in Strumenti di imaging. Inserirlo nella condivisione di distribuzione MDT nella cartella `/Tools/x86`.
   - **1b** Scaricare il file `ISDTool.exe` a 64 bit dalla pagina di download di ZENworks (`https://indirizzo_IP_server_zenworks:porta/zenworks-setup`) in Strumenti di imaging. Inserirlo nella condivisione di distribuzione MDT nella cartella `/Tools/x64`.
   - **1c** Aprire il file script `ZTIDiskpart.wsf` presente nella condivisione di distribuzione MDT nella cartella `Script` e inserire le seguenti righe al di sopra della riga `Open an instance for diskpart.exe, and dynamically pipe the commands to the program`:

     ```
     Dim sampCmd Dim aScriptDir Dim aArchitecture aScriptDir =
     oFSO.GetParentFolderName(WScript.ScriptFullName) aArchitecture =
     oEnvironment.Item("Architecture") sampCmd = aScriptDir & "\..\tools\" &
     aArchitecture & "\ISDTool.exe mdt cleandisk " & iDiskIndex
     oShell.Exec(sampCmd)
     ```

Quando il dispositivo avvia il file WIM di MDT e contatta la condivisione di distribuzione MDT personalizzata sopra indicata, lo script impedisce che MDT cancelli i dati ZISD.

Metodo 2

1. Cancellare il record MBR utilizzando un pacchetto di preavvio di script di imaging prima di applicare il pacchetto di distribuzione MDT sul dispositivo:
   - **1a** Creare un pacchetto di preavvio di script di imaging in ZENworks. Aggiungere il seguente comando come **Testo dello script**:

     ```
     dd if=/dev/zero of=/dev/sdX count=1 bs=512
     ```

     Dove `/dev/sdX` è il disco; X può essere un valore come a, b o c.
   - **1b** Applicare il pacchetto di preavvio dello script di imaging sul dispositivo.
   - **1c** Applicare il pacchetto di distribuzione MDT richiesto sul dispositivo.

Importante: prestare estrema attenzione quando si usa questa opzione. Il comando `dd` riportato sopra cancella il record MBR. Dopo avere eseguito questo comando, il sistema operativo non verrà avviato. Pertanto il comando deve essere eseguito solo prima della reinstallazione del sistema operativo nel dispositivo.

6.6 L'avvio di un dispositivo Windows con aggiornamenti Windows 10 potrebbe risultare impossibile

Quando si ripristina un'immagine di un dispositivo Windows dotato di Windows 10 Creators Update che utilizza il driver NTFS esistente, è possibile che l'avvio del sistema operativo del dispositivo ripristinato risulti impossibile.

Soluzione: eseguire una delle operazioni indicate:

- Acquisire e ripristinare un'immagine di un dispositivo che utilizza il driver Tuxera.
- Acquisire e ripristinare un'immagine di un dispositivo in formato .zmg utilizzando WinPE.

6.7 ZENworks Appliance

6.7.1 Nel browser Internet Explorer 11 viene visualizzata una pagina vuota quando si apre il riquadro Terminale e File Explorer utilizzando un indirizzo IPv6

Quando si apre il riquadro Terminale e File Explorer in ZENworks Appliance utilizzando un indirizzo IPv6, nel browser Internet Explorer 11 viene visualizzata una pagina vuota.

Soluzione: Aprire ZENworks Appliance utilizzando indirizzi IPv6 con valori letterali nei nomi di percorso UNC.

Ad esempio, *2001:db8::ff00:42:8329* può essere scritto come *2001:db8::ff00:42:8329.ipv6-literal.net*

7 Documentazione aggiuntiva

Nel presente file di Readme sono elencati i problemi specifici dell'Aggiornamento 1 di ZENworks 2017. Per il resto della documentazione ZENworks 2017, consultare il *sito Web della documentazione di ZENworks 2017*.

8 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/.