ZENworks 2020 Update 1

Riferimento rapido per l'amministrazione

Giugno 2020

Note legali

Sommario

Informazioni sulla Guida

Questo *Riferimento rapido per l'amministrazione di ZENworks* fornisce informazioni utili per acquisire le nozioni di base dell'amministrazione del sistema ZENworks Management. È necessario che il sistema ZENworks sia già installato. In caso contrario, consultare *Installazione del server ZENworks*.

Le informazioni della guida sono organizzate come segue:

- Configurazione del sistema (pagina 9): fornisce informazioni sulla configurazione della zona di gestione ZENworks prima dell'utilizzo dei prodotti ZENworks
- Amministrazione dei prodotti (pagina 57): fornisce istruzioni per l'utilizzo dei prodotti ZENworks (Asset Management, Configuration Management, Endpoint Security Management, Full Disk Encryption e Patch Management).

Destinatari

Questa guida è destinata agli utenti che si occuperanno di configurare e controllare il sistema ZENworks, nonché di eseguire i task di ZENworks correlati alla gestione di dispositivi o utenti.

Feedback

È possibile inviare i propri commenti e suggerimenti relativi a questa guida e agli altri documenti forniti con questo prodotto. Utilizzare il collegamento per *i commenti sull'argomento* nella parte inferiore di 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 (http://www.novell.com/documentation/zenworks-2020).

Configurazione del sistema

Nelle seguenti sezioni vengono fornite informazioni sulla configurazione del sistema ZENworks. I task di configurazione sono applicabili indipendentemente dal prodotto ZENworks in uso (Configuration Management, Patch Management, Asset Management ed Endpoint Security Management).

1 Elenco rapido

Uno o più server ZENworks sono stati installati e possono ora utilizzare tutte le funzionalità di ZENworks che consentono di risparmiare tempo prezioso.

Prima di iniziare a utilizzare i prodotti ZENworks (Configuration Management, Patch Management, Asset Management, Endpoint Security Management e Full Disk Encryption) per i quali si dispone di una licenza completa o di valutazione, è necessario rivedere i concetti e i task descritti nelle sezioni seguenti. Tali sezioni sono ideate per introdurre rapidamente alle nozioni e alle operazioni necessarie per configurare la zona di gestione:

Strumenti di gestione

ZENworks fornisce una console basata sul Web (Centro di controllo ZENworks) e un'utility dalla riga di comando (zman) che è possibile utilizzare per la gestione del sistema ZENworks. È necessario acquisire familiarità almeno con il Centro di controllo ZENworks.

Task		Dettagli
	Avviare il Centro di controllo ZENworks	Per informazioni, vedere "Centro di controllo ZENworks" a pagina 17.
	Come eseguire l'utility zman	L'utility zman è un'interfaccia da riga di comando che consente di eseguire molti dei task eseguibili nel Centro di controllo ZENworks. Per informazioni, vedere "Utility della riga di comando zman" a pagina 19.
	Come eseguire l'utility zac	L'utility zac è un'interfaccia da riga di comando per ZENworks Agent. Per informazioni, vedere "Utility della riga di comando zac" a pagina 20.

Configurazione della zona

Prima di poter usufruire pienamente dei vantaggi delle funzionalità di gestione fornite dai prodotti ZENworks attivati durante l'installazione della zona di gestione, è necessario completare alcuni task per garantire la corretta configurazione della stessa.

Task		Dettagli
	Creare cartelle e gruppi per l'organizzazione dei dispositivi	È possibile organizzare i dispositivi in cartelle e gruppi per ridurre l'overhead implicato nell'applicazione delle impostazioni di configurazione di ZENworks e nell'esecuzione dei task su dispositivi simili. Al posto di effettuare assegnazioni o eseguire task su dispositivi singoli, è possibile gestire cartelle e gruppi in modo che ciascun dispositivo in essi erediti l'assegnazione o il task. Per informazioni, vedere "Organizzazione dei dispositivi: Cartelle e gruppi" a pagina 23.
	Creare regole o chiavi di registrazione	È necessario distribuire l'agente ZENworks Agent a ciascun dispositivo da gestire. Quando si distribuisce ZENworks Agent a un dispositivo, quest'ultimo viene registrato nella Zona di gestione. È possibile utilizzare chiavi e regole di registrazione per assegnare automaticamente i dispositivi alle cartelle e ai gruppi appropriati, in modo che ereditino immediatamente le assegnazioni associate alle cartelle e ai gruppi. Per informazioni, vedere "Creazione di chiavi e regole di registrazione" a pagina 27.
	Aggiungere origini utente	Per fornire origini utente con autorità in ZENworks, è possibile eseguire la connessione a una o più directory LDAP. L'aggiunta di un'origine utente consente di associare account amministratore ZENworks ad account utente LDAP e i dispositivi agli utenti che principalmente li utilizzano. Inoltre, l'aggiunta di utenti consente di abilitare ulteriori funzionalità per i seguenti prodotti ZENworks: ◆ **Gestione della configurazione:** consente di assegnare pacchetti e policy a utenti e dispositivi. Consente di utilizzare rapporti sull'inventario basati sull'utente. ◆ **Gestione risorse:** consente di rendere conto delle licenze software in base all'utente e al dispositivo. ◆ **Endpoint Security Management:** consente di assegnare policy a utenti e a dispositivi. Per informazioni, vedere "Connessione alle origini utente" a pagina 29.

Task		Dettagli
	Creare conti amministratore aggiuntivi	Durante l'installazione viene creato un account amministratore ZENworks di default (denominato Amministratore). Si tratta di un account di tipo Super amministratore. Dispone di diritti amministrativi completi all'interno della zona di gestione. È possibile creare account amministratore aggiuntivi e assegnare a essi diritti di Super amministratore. Oppure è possibile creare account amministratore con diritti limitati per restringere l'ambito dei task, dei dispositivi e degli utenti accessibili all'amministratore. Per informazioni, vedere "Creazione di un account amministratore" a pagina 31.
	Creare account gruppo di amministratori	È possibile scegliere di creare un gruppo di amministratori. Se si assegnano diritti e ruoli a un gruppo di amministratori, i diritti e i ruoli assegnati si applicano a tutti i membri del gruppo. Per informazioni, vedere "Creazione di un account gruppo di amministratori" a pagina 31.
	Modificare impostazioni di configurazione della zona	Le impostazioni della zona di gestione sono predefinite in base alla configurazione più comune. Non è necessario modificarle in questa fase, ma può essere utile visualizzarle per acquisire maggiore familiarità. Per informazioni, vedere "Modifica delle impostazioni di configurazione" a pagina 32.
	Aggiorna software ZENworks	La funzione Aggiornamenti del sistema consente di ottenere regolarmente gli aggiornamenti di ZENworks e quindi di pianificare scaricamenti automatici degli aggiornamenti. Per informazioni, vedere "Aggiornamento del software ZENworks" a pagina 34.
	Crea ubicazioni	Le policy di sicurezza possono essere globali o specifiche di un'ubicazione. Una policy globale è valida per tutte le ubicazioni. Una policy basata sull'ubicazione viene applicata solo quando ZENworks Agent determina che l'ambiente di rete del dispositivo corrisponde a quello definito per l'ubicazione. Per informazioni, vedere "Creazione delle ubicazioni" a pagina 35.

Distribuzione dell'agente

ZENworks Agent comunica con il server ZENworks per eseguire task di gestione su un dispositivo. È necessario distribuire l'agente ZENworks a tutti i dispositivi da gestire. Mediante la distribuzione dell'agente ZENworks si installano i file dell'agente e si effettua la registrazione del dispositivo nella zona di gestione. Per ulteriori informazioni sulla registrazione dei dispositivi mobili alla zona, consultare Registrazione dei dispositivi mobili.

Task		Dettagli
	Abilitare le funzioni di ZENworks Agent	ZENworks Agent include funzioni specifiche per ogni prodotto ZENworks (Asset Management, Configuration Management, Endpoint Security Management, Full Disk Encryption e Patch Management). Per default, le funzioni per i prodotti attivati (con licenza completa o di valutazione) vengono abilitate durante l'installazione della zona di gestione. Tuttavia, è opportuno verificare la configurazione nel Centro di controllo ZENworks. Per informazioni, vedere "Configurazione delle funzioni dell'agente ZENworks" a pagina 39.
	Proteggere l'agente ZENworks	È possibile configurare le impostazioni di auto-protezione e disinstallazione di ZENworks Agent. Per informazioni, vedere "Configurazione della sicurezza dell'agente ZENworks" a pagina 41.
	Installare l'agente ZENworks	Per installare l'agente ZENworks in un dispositivo è possibile avvalersi di diversi metodi: ◆ È possibile utilizzare il Centro di controllo ZENworks per distribuire il Server ZENworks sul dispositivo. ◆ Sul dispositivo, usare un browser Web per scaricare l'agente dal Server ZENworks e installarlo. ◆ Includere l'agente in un'immagine e applicare quest'ultima al dispositivo. Per informazioni, vedere "Installazione di ZENworks Agent" a pagina 42.
	Login e uso di ZENworks Agent	Per ricevere pacchetti e norme assegnati agli utenti su un dispositivo, è necessario accedere alla zona di gestione. Per informazioni, vedere "Utilizzo dell'agente ZENworks" a pagina 46.

Messaggi di sistema

Durante l'esecuzione dei task di gestione nella zona, le informazioni vengono registrate affinché sia possibile visualizzare lo stato della zona e le attività che vengono svolte al suo interno.

Task		Dettagli
	Visualizzare messaggi di sistema	Per controllare attività quali la distribuzione del software e l'applicazione delle norme, dal sistema ZENworks vengono generati messaggi informativi, di avviso e di errore. Per informazioni, vedere “Visualizzazione dei messaggi di sistema” a pagina 49.
	Creare un elenco di controllo	Se si desidera controllare attentamente l'attività di alcuni dispositivi, pacchetti e norme, è possibile aggiungerli all'elenco di controllo. Per informazioni, vedere “Creazione di un elenco di controllo” a pagina 51.

2 Strumenti di gestione

ZENworks fornisce una console basata sul Web (Centro di controllo ZENworks) e un'utility dalla riga di comando (zman) che è possibile utilizzare per la gestione del sistema ZENworks. Le seguenti sezioni spiegano come accedere agli strumenti di gestione e usarli:

Centro di controllo ZENworks

Il Centro di controllo ZENworks viene installato su tutti i server ZENworks nella zona di gestione. Tutti i task di gestione possono essere eseguiti su qualsiasi server ZENworks. Poiché è una console di gestione basata su Web, è possibile accedere al Centro di controllo ZENworks da qualsiasi workstation supportata.

Se si utilizza iManager per amministrare altri prodotti Micro Focus nell'ambiente di rete, è possibile configurare il Centro di controllo ZENworks in modo che venga avviato da iManager. Per ulteriori informazioni, vedere "Accessing Control Center through Novell iManager" in *ZENworks Control Center Reference* (in lingua inglese).

Accesso al Centro di controllo ZENworks

1. Immettere il seguente URL in un browser Web:

   `https://ZENworks_Server_Address:port`

   Sostituire *Indirizzo_Server_ZENworks* con l'indirizzo IP o il nome DNS del server ZENworks. È sufficiente specificare la *porta* se non se ne sta utilizzando una di default (80 o 443). Il Centro di controllo ZENworks richiede una connessione HTTPS poiché le richieste HTTP vengono reindirizzate a HTTPS.

   Viene visualizzata la finestra di dialogo di login.

2. Nel campo **Nome utente**, digitare `Amministratore`.
3. Nel campo **Password**, digitare la password dell'amministratore creata durante l'installazione.

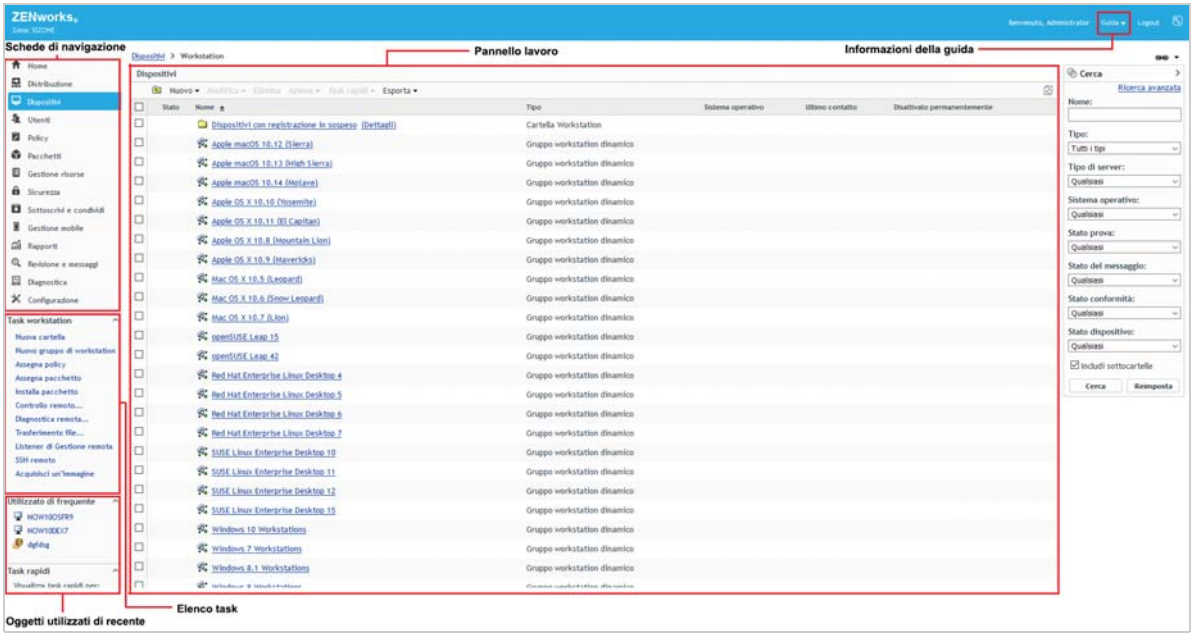
   Per evitare che utenti non autorizzati possano accedere al Centro di controllo ZENworks, l'account amministratore viene disabilitato dopo tre tentativi di login non riusciti ed è necessario attendere 60 secondi prima di poter effettuare un altro tentativo di login. Per modificare tali valori di default, vedere "Changing the Default Login Disable Values" in *ZENworks Control Center Reference* (in lingua inglese).

4 Fare clic su **Login** per visualizzare il Centro di controllo ZENworks.

Per informazioni più dettagliate su come eseguire il login come altro amministratore, vedere "Accessing Control Center" in *ZENworks Control Center Reference* (in lingua inglese).

Esplorazione del Centro di controllo ZENworks

La seguente pagina Workstation rappresenta la vista standard del Centro di controllo ZENworks.



Schede Esplorazione: le schede nel pannello sinistro consentono di passare alle varie aree funzionali di ZENworks. Ad esempio, la pagina Workstation visualizzata sopra consente di gestire i task associati alle workstation.

Elenco dei task: l'elenco dei task nel pannello sinistro consente di accedere rapidamente ai task più usati per la pagina corrente. L'elenco dei task cambia per ciascuna pagina. Ad esempio, l'elenco dei task nella pagina dei dispositivi visualizza i task correlati ai dispositivi e l'elenco dei task nella pagina della configurazione visualizza i task correlati alla configurazione.

Oggetti utilizzati frequentemente: l'elenco Utilizzati frequentemente nel riquadro sinistro visualizza i 10 oggetti più utilizzati, dal più al meno usato. Se si seleziona un oggetto, è possibile passare direttamente alla pagina Dettagli relativa all'oggetto.

Pannello di lavoro: il pannello di lavoro può essere usato per controllare e gestire il sistema ZENworks. I pannelli cambiano a seconda della pagina correntemente visualizzata. Nell'esempio precedente sono illustrati due pannelli di lavoro: **Dispositivi** e **Cerca**. Nel pannello **Dispositivi**, utilizzato per gestire le workstation, sono elencate le workstation e i relativi gruppi, cartelle e gruppi di workstation dinamici creati. Tramite il pannello **Cerca**, è possibile applicare dei filtri al pannello Dispositivi in base a criteri come il nome, il sistema operativo o lo stato della workstation.

Informazioni sulla Guida: il pulsante ? consente di visualizzare gli argomenti della Guida che contengono ulteriori informazioni sulla pagina correntemente visualizzata. I collegamenti del pulsante ? cambiano a seconda della pagina visualizzata.

Utility della riga di comando zman

L'utility zman fornisce un'interfaccia di gestione da riga di comando che consente di eseguire molti dei task disponibili nel Centro di controllo ZENworks. Ad esempio è possibile aggiungere contenuto ai pacchetti, assegnare norme ai dispositivi e registrare i dispositivi. Il vantaggio principale di usare l'utility della riga di comando risiede nella possibilità di creare script per la gestione delle operazioni ripetitive o globali. Come ZCC, l'utility zman viene installata in tutti i server primari, ma è possibile eseguirla solo dalla riga di comando sul server.

Lo scopo principale dell'utility zman è permettere all'utente di eseguire operazioni specifiche tramite uno script. Tuttavia, è possibile anche eseguire le operazioni manualmente tramite la riga di comando.

Ubicazione

L'utility è installata su tutti i server ZENworks nella seguente ubicazione:

`%ZENWORKS_HOME%\bin`

dove `%ZENWORKS_HOME%` è il percorso di installazione di ZENworks. In Windows, il percorso di default è `C:\Program Files (x86)\Novell\Zenworks\bin`. In Linux, il percorso di default è `/opt/novell/zenworks/bin`.

Sintassi

L'utility zman utilizza la seguente sintassi di base:

`zman` *`category-action`* `[`*`opzioni`*`]`

Ad esempio, per assegnare un pacchetto software a un dispositivo, è possibile usare il seguente comando:

```
zman bundle-assign workstation bundle1 wks1
```

dove `bundle-assign` è la categoria-azione e `workstation bundle1 wks1` sono le opzioni. In questo esempio le opzioni sono Tipo di dispositivo (workstation), Nome pacchetto (Pacchetto1) e Dispositivo di destinazione (wks1).

Ad esempio, per avviare una scansione dell'inventario di un dispositivo, si utilizza il seguente comando:

```
zman inventory-scan-now device/servers/server1
```

dove `inventory-scan-now` è la categoria-azione e `device/servers/server1` è un'opzione che specifica il percorso della cartella del dispositivo di cui effettuare la scansione.

Descrizione dei comandi

Per conoscere in modo approfondito il funzionamento dei comandi, consultare la Guida online oppure vedere "zman(1)" nel *Riferimento per le utility da riga di comando di ZENworks*.

Per usare la Guida online:

1 Sul server ZENworks immettere `zman --help` al prompt dei comandi.

Questo comando visualizza l'uso di base (sintassi) e un elenco di tutte le categorie dei comandi disponibili. È possibile anche utilizzare le seguenti opzioni per visualizzare ulteriori informazioni:

Comando	Descrizione
`zman --help | more`	Visualizza un elenco completo dei comandi divisi per categoria.
`zman category --help | more`	Visualizza un elenco completo dei comandi divisi per categoria.
`zman category --help | more`	Visualizza ulteriori informazioni sul comando

Utility della riga di comando zac

L'utility zac offre un'interfaccia di gestione della riga di comando che permette di eseguire i task disponibili in ZENworks Agent.

Ubicazione

L'utility è installata su tutti i server Windows gestiti nella seguente ubicazione:

`%ZENWORKS_HOME%\bin`

dove %ZENWORKS_HOME% è il percorso di installazione di ZENworks. Il percorso di default è `c:\program files\novell\zenworks\bin` in un dispositivo Windows a 32 bit e `c:\program files (x86)\novell\zenworks\bin` in un dispositivo Windows a 64 bit.

Sintassi

L'utility zac utilizza la seguente sintassi di base:

`zac opzioni comando`

Ad esempio, per avviare un pacchetto su un dispositivo, è possibile usare il seguente comando:

```
zac bundle-launch "bundle 1"
```

dove `bundle-launch` è il comando e `bundle 1` è l'opzione del comando. In questo esempio, l'opzione è il nome visualizzato del pacchetto da avviare. L'uso delle virgolette è richiesto solo se il nome visualizzato del pacchetto comprende spazi.

Ad esempio, per avviare una scansione dell'inventario su un dispositivo, si utilizza il seguente comando:

```
zac inv scannow
```

dove`inv` è il comando e `scannow` è l'opzione del comando.

Descrizione dei comandi

Il modo migliore per comprendere il funzionamento dei comandi consiste nell'utilizzare la Guida online oppure vedere “zac for Windows(1)” nel *Riferimento per le utility dalla riga di comando di ZENworks*.

Per usare la Guida online:

1 Sul dispositivo gestito, immettere uno dei seguenti comandi al prompt dei comandi.

Comando	Descrizione
`zac --help`	Visualizza l'elenco completo dei comandi.
`zac` *`comando`* `--help`	Visualizza informazioni dettagliate sul comando.

3 Configurazione della zona di gestione

ZENworks è progettato in modo da consentire la gestione efficiente di un numero elevato di dispositivi e utenti con il minore sforzo possibile. La prima operazione da eseguire per semplificare la gestione consiste nel configurare la zona di gestione in modo che possa utilizzare tutte le funzionalità di ZENworks.

Le seguenti sezioni descrivono i concetti di base che è necessario apprendere per configurare una zona di gestione che supporti i task di gestione in esecuzione. In ciascuna sezione è spiegato un concetto di gestione e sono riportati i passaggi generali per eseguire i task associati al concetto.

Organizzazione dei dispositivi: Cartelle e gruppi

Mediante l'uso del Centro di controllo ZENworks è possibile gestire i dispositivi eseguendo i task direttamente su singoli oggetti del dispositivo. Tuttavia, questo approccio non è molto efficiente a meno che non si debba gestire solo un numero ridotto di dispositivi. Per ottimizzare la gestione di molti dispositivi, ZENworks consente di organizzare i dispositivi in cartelle e gruppi; quindi è possibile eseguire i task su una cartella o un gruppo per gestirne i dispositivi.

È possibile creare cartelle e gruppi in qualsiasi momento. Tuttavia, è consigliato creare cartelle e gruppi prima di registrare i dispositivi nella zona. In tal modo è possibile utilizzare chiavi e regole di registrazione per aggiungere automaticamente i dispositivi nelle cartelle e nei gruppi appropriati al momento della registrazione (vedere "Creazione di chiavi e regole di registrazione" a pagina 27).

Cartelle

Le cartelle costituiscono uno strumento ottimale per organizzare i dispositivi in modo di semplificarne la gestione. È possibile applicare impostazioni di configurazione, assegnare contenuti ed eseguire task su qualsiasi cartella. In tal caso, i dispositivi della cartella ereditano impostazioni, assegnazioni e task.

Per ottenere risultati ottimali si consiglia di inserire nella stessa cartella dispositivi con requisiti di configurazione simili. Se tutti i dispositivi inclusi nella cartella richiedono gli stessi contenuti o task, è altresì possibile assegnare contenuti o task sulla cartella. Tuttavia, è possibile che tutti i dispositivi all'interno della cartella presentino dei requisiti di contenuto e task diversi, quindi è possibile organizzarli in gruppi e assegnare i contenuti e i task appropriati a ciascun gruppo (vedere “Gruppi” a pagina 25 qui di seguito).

Se ad esempio si dispone di workstation in tre siti diversi e Si desidera applicare impostazioni di configurazione differenti, creare tre cartelle (`/Workstations/Site1`, `/Workstations/Site2` e `/Workstations/Site3`) e inserire le workstation appropriate in ciascuna di esse. Una volta stabilito che la maggior parte delle impostazioni di configurazione vengono applicate a tutte le workstation, configurare tali impostazioni nella zona di gestione. Tuttavia, è opportuno eseguire settimanalmente una raccolta del software e l'inventario hardware nel Sito1 e nel Sito2, nonché una raccolta dell'inventario mensile nel Sito3. Configurare una raccolta dell'inventario settimanale nella zona di gestione, quindi ignorare l'impostazione sulla cartella Sito3 per applicare una pianificazione mensile. La raccolta dell'inventario nel Sito1 e nel Sito2 ha luogo ogni settimana, mentre la raccolta dell'inventario nel Sito3 è mensile.

Creazione di una cartella

1. Nel Centro di controllo ZENworks, fare clic sulla scheda **Dispositivi**.
2. Fare clic sulla cartella **Workstation**,**Server**o **Dispositivi mobili**.
3. Fare clic su **Nuovo** > **Cartella** per visualizzare la finestra di dialogo Nuova cartella.
4. Nel campo **Nome**, specificare un nome per la nuova cartella.

   Quando si assegna un nome a un oggetto nel Centro di controllo ZENworks (ad esempio a cartelle, gruppi, pacchetti, norme e così via), è necessario verificare che il nome rispetti le seguenti convenzioni:

   - Il nome deve essere univoco nell'ambito della cartella.
   - A seconda del software utilizzato per il database di ZENworks, è possibile che le lettere maiuscole e minuscole non siano univoche per lo stesso nome. Il database incorporato incluso in ZENworks non distingue tra lettere maiuscole o minuscole, quindi Cartella 1 e CARTELLA 1 sono nomi identici e non è possibile utilizzarli per la stessa cartella. Se si usa un database esterno che applica la distinzione tra maiuscole e minuscole, Cartella 1 e CARTELLA 1 sono dei nomi univoci.
   - Se si utilizzano spazi, è necessario racchiudere il nome tra virgolette quando lo si immette nella riga di comando. Ad esempio, è necessario racchiudere Cartella 1 tra virgolette (“Cartella 1”) quando si immette tale nome nella utility zman.
   - I seguenti caratteri non sono validi e non possono essere usati: / \ * ? : " ' < > | ` % ~
5. Fare clic su **OK** per creare la cartella.

È possibile anche usare i comandi `workstation-folder-create` e `server-folder-create` dell'utility zman per creare cartelle dispositivi. Per ulteriori informazioni, vedere "Comandi per le workstation" e "Comandi per i server" nel *Riferimento per le utility da riga di comando di ZENworks*.

Gruppi

Come con le cartelle, è inoltre possibile assegnare contenuti ed eseguire task su gruppi di dispositivi. In tal caso, i dispositivi del gruppo ereditano tali assegnazioni e task. Diversamente da quanto si verifica con le cartelle, non è possibile applicare impostazioni di configurazione ai gruppi.

I gruppi forniscono uno strato aggiuntivo di flessibilità per l'assegnazione di contenuto e task. In alcuni casi, non è necessario assegnare lo stesso contenuto ed eseguire lo stesso task su tutti i dispositivi all'interno di una cartella. Oppure può essere necessario assegnare lo stesso contenuto ed eseguire task su uno o più dispositivi in cartelle diverse. A tal fine, è possibile aggiungere i dispositivi a un gruppo (indipendentemente dalla cartella in cui sono contenuti i dispositivi), quindi assegnare il contenuto ed eseguire i task in tale gruppo.

Si consideri di nuovo l'esempio delle workstation in tre siti diversi (vedere "Cartelle" a pagina 24). Per alcune workstation di ciascun sito è necessario lo stesso software per la contabilità. Data la possibilità di assegnare il software ai gruppi, è possibile creare un gruppo Contabilità, aggiungervi le workstation di destinazione e assegnare il software per la contabilità appropriato al gruppo. Analogamente, è possibile utilizzare i gruppi per assegnare la configurazione e le policy di sicurezza di Windows.

Il vantaggio nell'assegnazione a un gruppo è costituito dal fatto che tutti i dispositivi contenuti nel gruppo ricevono l'assegnazione, ma è necessario effettuarla una sola volta. Inoltre, un dispositivo può appartenere a un numero qualsiasi di gruppi univoci e le assegnazioni da più gruppi sono additive. Se ad esempio si assegna un dispositivo al gruppo A e B, esso eredita il software assegnato a entrambi i gruppi.

In ZENworks sono disponibili gruppi e gruppi dinamici. Per quanto riguarda le assegnazioni dei contenuti o l'esecuzione dei task, i gruppi e i gruppi dinamici funzionano allo stesso modo. La sola differenze tra i due tipi di gruppo consiste nel modo in cui vengono aggiunti i dispositivi. Con il gruppo è necessario aggiungere i dispositivi manualmente. Con il gruppo dinamico, prima si definiscono i criteri che il dispositivo deve rispettare per far parte del gruppo, quindi vengono aggiunti automaticamente i dispositivi che soddisfano i criteri specificati.

In ZENworks sono inclusi diversi gruppi di server dinamici predefiniti, ad esempio i server Windows 2012, Windows 2003 e SUSE Linux Enterprise Server.

In ZENworks sono inclusi anche gruppi di workstation dinamici, ad esempio le workstation Windows XP, Windows 8, Windows Vista e SUSE Linux Enterprise Desktop. I dispositivi con questi sistemi operativi vengono aggiunti automaticamente al gruppo dinamico appropriato.

Creazione di un gruppo

1. Nel Centro di controllo ZENworks, fare clic sulla scheda **Dispositivi**.
2. Per creare un gruppo di server, fare clic sulla cartella **Server**.

   oppure

   Se si desidera creare un gruppo di workstation, fare clic sulla cartella **Workstation**.

   oppure

Se si desidera creare un gruppo per i dispositivi mobili, fare clic sulla cartella **Dispositivi mobili**.

3. Fare clic su **Nuovo** > **Gruppo di server** (**Nuovo** > **Gruppo di workstation** per le workstation o **Nuovo** > **Gruppo dispositivi mobili** per i dispositivi mobili). per avviare la Procedura guidata per la creazione di un nuovo gruppo.
4. Nella pagina Informazioni di base, digitare un nome per il nuovo gruppo nel campo **Nome gruppo**, quindi fare clic su **Avanti**.

   Il nome del gruppo deve rispettare le convenzioni di denominazione.
5. Nella pagina Riepilogo, fare clic su **Fine** per creare il gruppo senza aggiungere membri.

   oppure

   Per aggiungere membri al gruppo, fare clic su **Avanti**, quindi continuare con il Passo 6.
6. Nella pagina Aggiungi membri del gruppo, fare clic su **Aggiungi** per aggiungere i dispositivi al gruppo, quindi fare clic su **Avanti** dopo aver aggiunto i dispositivi.
7. Nella pagina Riepilogo, fare clic su **Fine** per creare il gruppo.

È possibile anche usare i comandi `workstation-group-create` e `server-group-create` dell'utility zman per creare gruppi dispositivi. Per ulteriori informazioni, vedere "Comandi per le workstation" e "Comandi per i server" nel *Riferimento per le utility da riga di comando di ZENworks*.

Creazione di un gruppo dinamico

1. Nel Centro di controllo ZENworks, fare clic sulla scheda **Dispositivi**.
2. Per creare un gruppo di server, fare clic sulla cartella **Server**.

   oppure

   Se si desidera creare un gruppo di workstation, fare clic sulla cartella **Workstation**.

   oppure

   Se si desidera creare un gruppo per i dispositivi mobili, fare clic sulla cartella **Dispositivi mobili**.
3. Fare clic su **Nuovo** > **Gruppo di server dinamico** (**Nuovo** > **Gruppo workstation dinamico** per le workstation o **Nuovo** > **Gruppo dinamico dispositivi mobili** per i dispositivi mobili) per avviare la Procedura guidata per la creazione di un nuovo gruppo.
4. Nella pagina Informazioni di base, digitare un nome per il nuovo gruppo nel campo **Nome gruppo**, quindi fare clic su **Avanti**.

   Il nome del gruppo deve rispettare le convenzioni di denominazione.
5. Nella pagina Definisci filtro per i membri del gruppo, definire i criteri che il dispositivo deve rispettare per diventare un membro del gruppo, quindi fare clic su **Avanti**.

   Fare clic sul pulsante della **guida** per ottenere informazioni dettagliate sulla creazione dei criteri.
6. Nella pagina Riepilogo, fare clic su **Fine** per creare il gruppo.

Ereditarietà delle assegnazioni per cartelle e gruppi

Quando si assegna un contenuto una cartella, tutti gli oggetti (utenti, dispositivi e sottocartelle) ereditano l'assegnazione eccetto i gruppi ubicati nella cartella. Se, ad esempio, si assegna un PacchettoA e una PolicyB alla CartellaDispositivi1, tutti i dispositivi inclusi nella cartella (compresi tutti i dispositivi presenti nelle sottocartelle) ereditano le due assegnazioni. Tuttavia, le assegnazioni

non vengono ereditate da nessuno dei gruppi di dispositivi ubicati nella CartellaDispositivi1. Sostanzialmente le assegnazioni delle cartelle non vengono passate ai gruppi ubicati nella cartella stessa.

Creazione di chiavi e regole di registrazione

Quando si distribuisce l'agente ZENworks a un dispositivo, quest'ultimo viene registrato nella zona di gestione e diventa un dispositivo gestito. Come parte della registrazione, è possibile specificare il nome ZENworks del dispositivo e la cartella e i gruppi ai quali si desidera aggiungere il dispositivo.

Per default, viene utilizzato un nome host del dispositivo come nome ZENworks, esso viene aggiunto alla cartella `/Server` o `/Workstation` e non gli viene assegnata l'appartenenza in alcun gruppo. È possibile spostare manualmente i dispositivi in altre cartelle e aggiungerli a gruppi. Tuttavia, questa operazione può risultare complessa se il numero di dispositivi è elevato o se si aggiungono frequentemente nuovi dispositivi. Il modo migliore per gestire un numero elevato di dispositivi consiste nell'aggiungerli automaticamente nelle cartelle e nei gruppi corretti durante la registrazione.

Per aggiungere i dispositivi a cartelle e gruppi durante la registrazione, è possibile utilizzare chiavi o regole di registrazione o entrambe. Sia le chiavi sia le regole di registrazione consentono di assegnare a un dispositivo le appartenenze a cartelle o gruppi. Tuttavia, poiché ci sono delle differenze effettive tra le chiavi e le regole, è necessario comprendere bene come funzionano prima di usare un metodo o entrambi i metodi contemporaneamente.

Questa funzione non è applicabile ai dispositivi mobili.

Chiavi di registrazione

Una chiave di registrazione è una stringa alfanumerica definita manualmente o generata casualmente. Durante la distribuzione dell'agente ZENworks a un dispositivo, è necessario disporre della chiave di registrazione. La prima volta che si connette al server ZENworks, il dispositivo viene aggiunto alla cartella e ai gruppi definiti nella chiave.

È possibile creare una o più chiavi di registrazione per garantire che il dispositivo venga collocato nelle cartelle e nei gruppi desiderati. Ad esempio può essere necessario verificare che tutte le workstation del reparto vendite vengano aggiunte alla cartella `/Workstation/Vendite`, ma che vengano divise in tre gruppi diversi (Teamvendite1, Teamvendite2, Teamvendite3) a seconda delle assegnazioni dei team. In questo caso è possibile creare tre diverse chiavi di registrazione e configurare ciascuna di questi in modo che aggiunga le workstation del reparto Vendite alla cartella `/Workstation/Vendite` e al gruppo del team appropriato. Tutte le workstation che utilizzano la chiave di registrazione corretta vengono aggiunte alla cartella e al gruppo appropriati.

Per creare una chiave di registrazione:

1 In Centro di controllo ZENworks, fare clic sulla scheda **Configurazione**, quindi fare clic sulla scheda **Registrazione**.

2 Nel pannello Chiavi di registrazione, fare clic su **Nuovo** > **Chiave di registrazione** per avviare la procedura guidata Crea nuova chiave di registrazione.

3 Seguire le istruzioni visualizzate.

Per informazioni su cosa è necessario fornire a ogni passaggio della procedura guidata, fare clic sul pulsante della **guida**.

È possibile anche usare il comando `registration-create-key` nell'utility zman per creare una chiave di registrazione. Per ulteriori informazioni, vedere "Comandi di registrazione" nel *Riferimento per le utility da riga di comando di ZENworks*.

Regole di registrazione

Se non si desidera immettere una chiave di registrazione durante la distribuzione o se si desidera aggiungere automaticamente i dispositivi a cartelle e gruppi diversi in base ai criteri predefiniti (ad esempio in base al tipo di sistema operativo, alla CPU o all'indirizzo IP), è possibile usare le regole di registrazione.

ZENworks fornisce una regola di registrazione di default per i server e un'altra per le workstation. Se un dispositivo si registra senza una chiave e non sono state create regole di registrazione, le assegnazioni delle cartelle vengono applicate sulla base delle regole di registrazione di default. Le due regole di default provocano l'aggiunta di tutti i server alla cartella `/Server` e di tutte le workstation alla cartella `/Workstation`.

Le due regole di default sono state appositamente definite per verificare che la registrazione di tutti i server e di tutte le workstation venga effettuata correttamente. Per questo motivo non è possibile cancellare o modificare queste due regole di default. Tuttavia, è possibile anche definire ulteriori regole per filtrare i dispositivi al momento della registrazione e aggiungerli a cartelle e gruppi diversi. Se, come consigliato nella "Organizzazione dei dispositivi: Cartelle e gruppi" a pagina 23, sono state definite cartelle per i dispositivi con impostazioni di configurazione simili e per gruppi relativi a dispositivi con assegnazioni simili, i nuovi dispositivi registrati ricevono automaticamente le impostazioni di configurazione e le assegnazioni appropriate.

Per creare una regola di registrazione:

1 In Centro di controllo ZENworks, fare clic sulla scheda **Configurazione**, quindi fare clic sulla scheda **Registrazione**.

2 Nel riquadro Regole di registrazione, fare clic su **Nuovo** per avviare la procedura guidata Crea nuova regola di registrazione.

3 Seguire le istruzioni visualizzate per creare la regola.

Per informazioni su cosa è necessario fornire a ogni passaggio della procedura guidata, fare clic sul pulsante della **guida**.

È possibile anche usare il comando `registration-create-key` nell'utility zman per creare una chiave di registrazione. Per ulteriori informazioni, vedere "Comandi per i gruppi di regole" nel *Riferimento per le utility da riga di comando di ZENworks*.

Modello denominazione dispositivo

Il modello di denominazione del dispositivo determina la modalità di assegnazione del nome ai dispositivi al momento della registrazione. Per default viene utilizzato un nome host del dispositivo. È possibile modificare tale nome per utilizzare qualsiasi combinazione delle seguenti variabili del computer: ${HostName}, ${GUID}, ${OS}, ${CPU}, ${DNS}, ${IPAddress} e ${MACAddress}.

1. Nel Centro di controllo ZENworks, fare clic sulla scheda **Configurazione**.
2. Nel pannello Impostazioni zona di gestione, fare clic su **Gestione dispositivi**.
3. Fare clic su **Registrazione** per visualizzare la pagina corrispondente.
4. Nel riquadro Modello denominazione dispositivo fare clic su  , quindi selezionare la variabile di computer desiderata dall'elenco.

   È possibile utilizzare qualsiasi combinazione di una o più variabili; ad esempio:

   `${HostName}${GUID}`
5. Fare clic su **OK** per salvare le modifiche.

Ulteriori informazioni

Per ulteriori informazioni sulla registrazione di dispositivi, vedere il *Riferimento per la rilevazione, la distribuzione e la disattivazione permanente di ZENworks*.

Connessione alle origini utente

Per fornire origini utente con autorità in ZENworks, è possibile eseguire la connessione a una o più directory LDAP.

L'aggiunta di un'origine utente consente di associare account amministratore ZENworks ad account utente LDAP e i dispositivi agli utenti che principalmente li utilizzano. Inoltre, l'aggiunta di utenti consente di abilitare ulteriori funzionalità per i seguenti prodotti ZENworks:

- **Gestione della configurazione:** consente di assegnare pacchetti e policy a utenti e dispositivi. Consente di utilizzare rapporti sull'inventario basati sull'utente.
- **Gestione risorse:** consente di rendere conto delle licenze software in base all'utente e al dispositivo.
- **Endpoint Security Management:** consente di assegnare policy a utenti e a dispositivi.

Quando si definisce una directory LDAP come origine utente, la directory non subisce modifiche; ZENworks richiede solo accesso in lettura alla directory LDAP e memorizza tutte le informazioni sull'assegnazione nel database ZENworks. Per informazioni più dettagliate sui diritti di lettura specifici richiesti per la connessione a un'origine utente, vedere “Creating User Source Connections” in *ZENworks User Source and Authentication Reference* (in lingua inglese).

È possibile connettersi a Novell eDirectory e Microsoft Active Directory come origini utente. I requisiti minimi sono Novell eDirectory 8.7.3 e Microsoft Active Directory in Windows 2000 SP4. Il requisito minimo per LDAP è la versione 3.

Dopo la connessione a una directory LDAP, si definiscono i container nella directory che si desidera che sia visibile. Si supponga ad esempio di avere una struttura di domini Microsoft Active denominata MiaSocietà. Tutti gli utenti risiedono in due container nella struttura MiaSocietà: MyCompany/Users e MyCompany/Temp/Users. È possibile impostare la struttura MiaSocietà come origine e MyCompany/Users e MyCompany/Temp/Users come container utente a sé stanti. Ciò limita l'accesso alla directory solo ai container che comprendono utenti.

Oltre agli utenti che risiedono nei container aggiunti, il Centro di controllo ZENworks visualizza anche tutti i gruppi di utenti ubicati nei container. Ciò consente di gestire sia il singolo utente sia gruppi di utenti.

Per connettersi a un'origine utente:

1. Nel Centro di controllo ZENworks, fare clic sulla scheda **Configurazione**.
2. Nel pannello Origini utente, fare clic su **Nuovo** per avviare la procedura guidata Crea nuova origine utente.
3. Seguire le istruzioni visualizzate per creare un'origine utente.

   Per informazioni su cosa è necessario fornire a ogni passaggio della procedura guidata, fare clic sul pulsante della **guida**.

È possibile anche usare il comando `user-source-create` nell'utility zman per creare una connessione a un'origine utente. Per ulteriori informazioni, vedere "Comandi per l'utente" nel *Riferimento per le utility da riga di comando di ZENworks*.

Per ulteriori informazioni sull'abilitazione di origini utente per la registrazione di dispositivi mobili, vedere Configuring User Sources in ZENworks Mobile Management Reference (in lingua inglese).

Creazione di conti amministratore ZENworks

Durante l'installazione viene creato un account amministratore ZENworks di default (denominato Amministratore). Questo account, denominato Super amministratore, offre diritti amministrativi completi per la zona di gestione.

In genere, è necessario creare account di amministratore per tutti gli utenti che eseguono task amministrativi. È possibile definire tali account come account super amministratore o account amministratore con diritti limitati. Ad esempio, è possibile assegnare a un utente un account amministratore che gli consenta solo di rilevare e registrare dispositivi nella zona di gestione, oppure un account che permetta all'utente solo di assegnare pacchetti ai dispositivi. In alternativa, è possibile limitare l'account all'esecuzione di task di gestione quali la gestione di contratti, licenze e documenti.

In alcuni casi, è possibile disporre di più account di amministratore che richiedono gli stessi diritti amministrativi. Anziché assegnare diritti a ciascun account singolarmente, è possibile creare un ruolo amministratore, assegnare diritti amministrativi al ruolo, quindi aggiungere gli account al ruolo. Ad esempio, è possibile che il ruolo di help desk fornisca i diritti amministrativi richiesti da diversi amministratori.

È possibile scegliere di creare un gruppo di amministratori. Se si assegnano diritti e ruoli a un gruppo di amministratori, i diritti e i ruoli assegnati si applicano a tutti i membri del gruppo.

Creazione di un account amministratore

1. Nel Centro di controllo ZENworks, fare clic sulla scheda **Amministratori**.
2. Nel pannello Amministratori, fare clic su **Nuovo** > Amministratore per visualizzare la finestra di dialogo Aggiungi nuovo amministratore.
3. Immettere le informazioni richieste nei campi.

   La finestra di dialogo Aggiungi nuovo amministratore consente di creare un nuovo conto amministratore specificando un nome o una password. In alternativa, è possibile creare un nuovo amministratore in base a un utente esistente nell'origine utente. A scelta, è possibile fornire all'amministratore gli stessi diritti di cui dispone l'amministratore che ha eseguito il login.

   Crea un nuovo amministratore fornendo nome e password: selezionare questa opzione per creare un nuovo account amministratore specificando manualmente un nome e una password.

   Basato sull'utente o sugli utenti in un'origine utenti: selezionare questa opzione per creare un nuovo conto amministratore in base alle informazioni sull'utente provenienti dall'origine utente. A tal fine, fare clic su **Aggiungi**, quindi cercare e selezionare l'utente desiderato.

   Fornisci a questo amministratore gli stessi miei diritti: selezionare questa opzione per assegnare al nuovo amministratore gli stessi diritti dell'amministratore attualmente connesso. Se si dispone dei diritti di Super amministratore, il nuovo amministratore viene creato come Super amministratore.
4. Fare clic su **OK** per aggiungere il nuovo amministratore nel pannello Amministratori.
5. Se è necessario modificare i diritti o i ruoli del nuovo amministratore, fare clic sull'account dell'amministratore, quindi sulla scheda **Diritti** per visualizzare i dettagli dell'account.
6. Se l'opzione **Super amministratore** è selezionata, deselezionarla.

   Non è possibile modificare i diritti di Super amministratore.
7. Modificare i diritti assegnati dal riquadro Diritti assegnati.
8. Modificare i diritti assegnati utilizzando il riquadro Ruoli assegnati.
9. Fare clic su **Applica** per salvare le modifiche.

Per ulteriori informazioni su come creare account amministratore, diritti di amministratore o ruoli amministratore ZENworks, vedere ZENworks Administrator Accounts and Rights Reference (in lingua inglese).

È possibile anche usare il comando `admin-create` nell'utility zman per creare un conto amministratore ZENworks. Per ulteriori informazioni, vedere "Comandi per l'amministratore" nel *Riferimento per le utility dalla riga di comando di ZENworks*.

Creazione di un account gruppo di amministratori

1. Nel Centro di controllo ZENworks, fare clic sulla scheda **Amministratori**.
2. Nel pannello Amministratori fare clic su **Nuovo** > **Gruppo di amministratori** per visualizzare la finestra di dialogo Aggiungi nuovo gruppo di amministratori.
3. Immettere le informazioni richieste nei campi.

Nella finestra di dialogo Aggiungi nuovo gruppo di amministratori è possibile creare un nuovo account gruppo amministratori specificando un nome per il gruppo e aggiungendovi i membri. In alternativa è possibile anche creare un nuovo gruppo di amministratori utilizzando un gruppo utenti esistente nell'origine utente. Il nome del gruppo di amministratori deve essere univoco.

Crea nuovo gruppo di amministratori specificando un nome e aggiungendo membri:

selezionare questa opzione se si desidera creare un nuovo account gruppo di amministratori specificandone il nome e aggiungervi i membri manualmente. Per aggiungere membri, fare clic su **Aggiungi**, quindi ricercare e selezionare gli amministratori desiderati. È possibile aggiungere un numero qualsiasi di amministratori al gruppo. Non è possibile aggiungere altri gruppi di amministratori al gruppo.

Basato sui gruppi di utenti in un'origine utente: selezionare questa opzione se si desidera creare un nuovo account gruppo di amministratori in base alle informazioni sui gruppi di utenti presenti nell'origine utente. A tal fine, fare clic su **Aggiungi**, quindi ricercare e selezionare il gruppo di utenti desiderato.

Importare i membri utente come amministratori per ogni gruppo utente: selezionare questa opzione per consentire ai membri utente dei gruppi di utenti selezionati di essere aggiunti immediatamente come amministratori.

4. Fare clic su **OK** per aggiungere il nuovo gruppo di amministratori nel pannello Amministratori.
5. Se è necessario modificare i diritti o i ruoli del nuovo gruppo di amministratori, fare clic sull'account gruppo di amministratori, quindi sulla scheda **Diritti** per visualizzare i dettagli dell'account.
6. Modificare i diritti assegnati dal riquadro Diritti assegnati.
7. Modificare i diritti assegnati utilizzando il riquadro Ruoli assegnati.
8. Fare clic su **Applica** per salvare le modifiche.

Per ulteriori informazioni su come creare account gruppi di amministratori, diritti di amministratore o ruoli amministratore ZENworks, vedere *ZENworks Administrator Accounts and Rights Reference* (in lingua inglese).

È possibile anche usare il comando `admin-create` nell'utility zman per creare un conto amministratore ZENworks. Per ulteriori informazioni, vedere “Comandi per l'amministratore” nel *Riferimento per le utility dalla riga di comando di ZENworks*.

Modifica delle impostazioni di configurazione

Le impostazioni di configurazione della zona di gestione consentono di controllare un'ampia gamma di funzionalità che agiscono sulla zona. Le impostazioni della gestione dei dispositivi consentono di controllare la frequenza di accesso dei dispositivi a un server ZENworks per aggiornare le informazioni, la frequenza di aggiornamento dei gruppi dinamici e quali livelli di messaggi (informativi, di avviso o di errore) vengono registrati dall'agente di ZENworks. Sono disponibili impostazioni di eventi e messaggi, rilevazione e distribuzione e molto altro.

Le impostazioni della zona di gestione che si applicano ai dispositivi vengono ereditate da tutti i dispositivi della zona. Come indicato in “Organizzazione dei dispositivi: Cartelle e gruppi” a pagina 23, è possibile ignorare le impostazioni della zona configurandole sulle cartelle o sui dispositivi individuali. In questo modo è possibile stabilire impostazioni di zona che si applicano al numero più elevato di dispositivi e quindi, laddove necessario, ignorare le impostazioni sulle cartelle e sui dispositivi.

Per default le impostazioni della zona sono preconfigurate con valori che forniscono funzionalità comuni. Tuttavia, è possibile modificare le impostazioni per adattarle al meglio al comportamento necessario all'ambiente.

Modifica delle impostazioni di configurazione a livello di zona

1. Nel Centro di controllo ZENworks, fare clic sulla scheda **Configurazione**.
2. Nel pannello Impostazioni zona di gestione, fare clic sulla categoria di impostazioni (ad esempio, **Gestione dispositivo**, **Rilevazione e distribuzione** ed **Evento e messaggi**) di cui si desidera modificare le impostazioni.
3. Fare clic sull'impostazione per visualizzarne la pagina dei dettagli.
4. Modificare le impostazioni secondo necessità.

   Per ulteriori informazioni sulle impostazioni, vedere *ZENworks Management Zone Settings Reference* (in lingua inglese).
5. Fare clic su **OK** o su **Applica**.

   Se si applica l'impostazione di configurazione ai dispositivi, essa viene ereditata da tutti i dispositivi nella zona a meno che l'impostazione non sia ignorata a livello di cartella o di dispositivo.

Modifica delle impostazioni di configurazione su una cartella

1. Nel Centro di controllo ZENworks, fare clic sulla scheda **Dispositivi**.
2. Nel pannello Dispositivi (nella scheda **Gestiti**), cercare la cartella di cui si desidera modificare le impostazioni.
3. Per visualizzare i dettagli, fare clic su **Dettagli** accanto al nome della cartella.
4. Fare clic sulla scheda **Impostazioni**.
5. Nel pannello Impostazioni, fare clic sulla categoria di impostazioni (**Gestione dispositivi**, **Gestione infrastruttura** e così via) delle impostazioni che si desidera modificare.
6. Fare clic sull'impostazione per visualizzare la pagina dei dettagli.
7. Modificare le impostazioni secondo necessità.

   Per ulteriori informazioni sulle impostazioni, vedere *ZENworks Management Zone Settings Reference* (in lingua inglese).
8. Fare clic su **OK** o su **Applica**.

   L'impostazione di configurazione viene ereditata da tutti i dispositivi nella cartella, inclusi tutti i dispositivi contenuti nelle sottocartelle, a meno che l'impostazione non sia ignorata su una sottocartella o su un dispositivo individuale.

Modifica delle impostazioni di configurazione su un dispositivo

1. Nel Centro di controllo ZENworks, fare clic sulla scheda **Dispositivi**.
2. Nel pannello Dispositivi (nella scheda **Gestiti**), cercare il dispositivo di cui si desidera modificare le impostazioni.
3. Individuato il dispositivo, fare clic sul suo nome per visualizzarne i dettagli.
4. Fare clic sulla scheda **Impostazioni**.
5. Nel pannello Impostazioni, fare clic sulla categoria di impostazioni (**Gestione dispositivi**, **Gestione infrastruttura** e così via) di cui si desidera modificare i valori.
6. Fare clic sull'impostazione per visualizzarne la pagina dei dettagli.
7. Apportare le modifiche desiderate alle impostazioni.

   Per informazioni sull'impostazione, fare clic sul pulsante **Guida** nel Centro di controllo ZENworks.
8. Una volta terminato di modificare le impostazioni, fare clic su **OK** (o su **Applica**) per salvare le modifiche apportate.

Condivisione e sottoscrizione delle zone

La funzione Sottoscrizione e condivisione di ZENworks consente di condividere oggetti di contenuto (come pacchetti e policy) che è possibile assegnare in più zone ZENworks:

- **Zona di condivisione:** per la condivisione del contenuto.
- **Zona sottoscrittore:** per la sottoscrizione alla zona di condivisione e la replica del contenuto condiviso nella rispettiva zona.

Nel Centro di controllo ZENworks è possibile utilizzare il collegamento alle impostazioni di condivisione della zona nel pannello Gestione infrastruttura per gestire le attività di condivisione della zona.

Nella zona di condivisione viene identificato un server primario come server di condivisione. Tutte le attività di condivisione del contenuto vengono effettuate mediante tale server. Per eseguire la registrazione della zona sottoscrittore è necessario fornire una chiave sottoscrittore ricavata dalla zona di condivisione. La chiave sottoscrittore non concede al sottoscrittore l'accesso ad alcun contenuto. La chiave sottoscrittore viene utilizzata per la registrazione del sottoscrittore.

Il contenuto richiesto viene quindi condiviso dalla zona di condivisione e viene replicato nella zona sottoscrittore. Se si verificano problemi con la replica, si verrà notificati in modo da poter prendere le dovute misure correttive.

Per ulteriori dettagli, vedere *ZENworks Subscribe and Share Reference* (in lingua inglese).

Aggiornamento del software ZENworks

È possibile aggiornare il software ZENworks su tutti i dispositivi nella zona di gestione in cui è installato. È possibile pianificare gli scaricamenti degli aggiornamenti. Gli aggiornamenti software vengono distribuiti nelle release di Support Pack. È possibile scegliere di applicare ciascuno di essi dopo averne visualizzato il contenuto (le release di Support Pack sono cumulative). È inoltre

possibile scaricare l'ultimo aggiornamento di riconoscimento del prodotto (Product Recognition Update, PRU) per aggiornare la knowledge base in modo da consentire a ZENworks Inventory di riconoscere il software più recente.

Per ulteriori informazioni, vedere *ZENworks System Updates Reference* (in lingua inglese).

Creazione delle ubicazioni

I requisiti di sicurezza di un dispositivo possono variare a seconda dell'ubicazione. Possono ad esempio sussistere restrizioni per firewall personali diverse a seconda che un dispositivo si trovi nel terminal di un aeroporto o in un ufficio protetto da un firewall aziendale.

Affinché i requisiti di sicurezza di un dispositivo siano appropriati per l'ubicazione in cui è installato, ZENworks supporta sia le policy globali sia quelle basate sulle ubicazioni. Una policy globale viene applicata indipendentemente dall'ubicazione del dispositivo. Una policy basata sulle ubicazioni viene applicata solo quando l'ubicazione corrente del dispositivo soddisfa i criteri di un'ubicazione associata alla policy. Ad esempio, se si crea una policy basata sulle ubicazioni per il proprio ufficio aziendale e la si assegna a un computer portatile, la policy viene applicata solo quando l'ubicazione del computer portatile corrisponde all'ufficio aziendale.

Se si desidera utilizzare le policy basate sulle ubicazioni, è necessario definire innanzitutto le ubicazioni appropriate per l'organizzazione. Un'ubicazione è un luogo o un tipo di luogo per il quale si dispone di requisiti di sicurezza specifici. È possibile ad esempio applicare requisiti di sicurezza diversi per un dispositivo utilizzato in ufficio, a casa o in un aeroporto.

Le ubicazioni sono definite in base agli ambienti di rete. Si consideri ad esempio un'organizzazione con un ufficio a New York e uno a Tokyo. Entrambi gli uffici hanno gli stessi requisiti. Verrà creata pertanto un'ubicazione Ufficio, che verrà associata a due ambienti di rete, ovvero Rete ufficio di New York e Rete ufficio di Tokyo. Ciascuno di questi ambienti è definito esplicitamente da un insieme di servizi gateway, server DNS e punti di accesso wireless. Ogniqualvolta ZENworks Agent determina che l'ambiente corrente corrisponde a Rete ufficio di New York o Rete ufficio di Tokyo, l'agente imposta l'ubicazione su Ufficio e applica le policy di sicurezza associate a tale ubicazione.

Nelle sezioni riportate di seguito viene illustrato come creare le ubicazioni:

- “Definizione di un ambiente di rete” a pagina 35
- “Creazione delle ubicazioni” a pagina 36
- “Selezione di ubicazione e ambiente di rete su un dispositivo gestito” a pagina 37

Definizione di un ambiente di rete

Le definizioni degli ambienti di rete costituiscono gli elementi di base delle ubicazioni. Durante la creazione di un'ubicazione è possibile definire gli ambienti di rete. Si consiglia tuttavia di definire prima gli ambienti di rete e di aggiungerli in un secondo momento quando si creano le ubicazioni.

Per creare un ambiente di rete:

1. Nel Centro di controllo ZENworks, fare clic su **Configurazione** > **Ubicazioni**.
2. Nel pannello Ambienti di rete, fare clic su **Nuovo** per avviare la procedura guidata Crea nuovo ambiente di rete.

3 Nella pagina Definisci dettagli, specificare un nome per l'ambiente di rete, quindi fare clic su **Avanti**.

4 Nella pagina dei dettagli dell'ambiente di rete, specificare quanto segue:

Limite al tipo adattatore: per default, i servizi di rete definiti in questa pagina vengono valutati negli adattatori di rete cablati, wireless e di connessione remota di un dispositivo. Se si desidera limitare la valutazione a un tipo di adattatore specifico, selezionare **Cablato**, **Wireless** o **Accesso remoto**.

Corrispondenza minima: specificare il numero minimo di servizi di rete definiti che devono corrispondere per selezionare l'ambiente di rete.

specificare il numero minimo di servizi di rete definiti che devono corrispondere per selezionare l'ambiente di rete.

Se ad esempio si definiscono un indirizzo gateway, tre server DNS e un server DHCP, si avrà un totale di cinque servizi. È quindi possibile specificare che per selezionare l'ambiente di rete è necessario trovare una corrispondenza con almeno tre di questi servizi.

Quando si specifica un numero di corrispondenza minima, verificare che vengano soddisfatti i requisiti seguenti:

- Il numero non può essere inferiore al numero di servizi contrassegnati come Corrispondenza obbligatoria.
- Il numero non deve superare il numero totale di servizi definiti. In caso contrario, la corrispondenza minima non verrà mai raggiunta e non sarà possibile selezionare l'ambiente di rete.

Servizi di rete: consente di definire i servizi di rete valutati dall'agente ZENworks per controllare se l'ambiente di rete corrente corrisponde a quello specificato. Selezionare la scheda relativa al servizio di rete da definire. Fare clic su **Aggiungi**, quindi specificare le informazioni richieste.

5 Fare clic su **Avanti** per visualizzare la pagina Riepilogo, quindi fare clic su **Fine**.

Creazione delle ubicazioni

Quando si crea un'ubicazione, si specifica un nome di ubicazione e quindi si associano a essa gli ambienti di rete richiesti.

1 Nel Centro di controllo ZENworks, fare clic su **Configurazione** > **Ubicazioni**.

2 Nel pannello Ubicazioni, fare clic su **Nuovo** per avviare la procedura guidata Crea nuova ubicazione.

3 Nella pagina Definisci dettagli, specificare un nome per l'ubicazione, quindi fare clic su **Avanti**.

4 Nella pagina Assegna ambienti di rete:

4a Selezionare **Assegnare ambienti di rete esistenti all'ubicazione**.

4b Fare clic su **Aggiungi**, selezionare gli ambienti di rete per cui si desidera definire l'ubicazione, quindi fare clic su **OK** per aggiungerli all'elenco.

4c Dopo aver aggiunto gli ambienti di rete, fare clic su **Avanti**.

5 Nella pagina di riepilogo, fare clic su **Fine** per creare l'ubicazione e aggiungerla all'elenco Ubicazioni.

Quando più ubicazioni includono l'ambiente di rete identificato dall'agente ZENworks, l'ordine dell'elenco determina l'ubicazione che viene utilizzata. Per default viene selezionata la prima ubicazione visualizzata nell'elenco. Per riordinare l'elenco utilizzare le opzioni **Sposta su** and **Sposta giù**.

Inoltre, è possibile utilizzare i comandi `network-environment-create` e `location-create` nell'utility zman per creare un ambiente di rete e le relative ubicazioni utilizzando l'ambiente di rete creato. Per ulteriori informazioni, vedere "Comandi di registrazione" nel *Riferimento per le utility da riga di comando di ZENworks*.

Selezione di ubicazione e ambiente di rete su un dispositivo gestito

Se nel Centro di controllo ZENworks sono disponibili più ambienti di rete e ubicazioni, l'agente ZENworks sul dispositivo gestito ne esegue la scansione, per individuare gli ambienti che hanno corrispondenze. Dopo averli identificati, l'agente ZENworks seleziona gli ambienti di rete con il maggior numero di servizi di rete corrispondenti (ad esempio con lo stesso indirizzo IP client e gli stessi server DNS). L'agente ZENworks esegue quindi la scansione delle ubicazioni elencate e individua la prima che contiene gli ambienti di rete selezionati; seleziona in seguito l'ubicazione e il primo ambiente di rete nell'ubicazione con il maggior numero di corrispondenze.

Ad esempio:

- Le ubicazioni definite nel Cento di controllo ZENworks sono elencate secondo l'ordine seguente: L1 e L2.
- Gli ambienti di rete in L1 vengono elencati nel seguente ordine: NE1, NE2 e NE4.
- Gli ambienti di rete in L2 vengono elencati nel seguente ordine: NE2, NE3 e NE4.
- L'agente ZENworks sul dispositivo gestito rileva che NE2, NE3 e NE4 corrispondono tutti al dispositivo gestito.

Se gli ambienti di rete NE2 e NE4 hanno due servizi di rete corrispondenti a quelli delle ubicazioni, mentre l'ambiente di rete NE3 dispone di un solo servizio corrispondente, l'agente ZENworks selezionerà NE2 e NE4, dato il maggior numero di corrispondenze di servizi individuate. Poiché NE2 p il primo ambiente di rete elencato in L1, L1 e NE2 vengono selezionati come ubicazione e ambiente di rete.

Nota: perché un ambiente di rete sia considerato corrispondente nel dispositivo gestito, è necessario che tutte le limitazioni impostate in tale ambiente siano soddisfatte. Queste includono l'attributo **Corrispondenza minima** specificato per l'ambiente di rete e anche l'attributo **Corrispondenza obbligatoria** specificato per i servizi di rete nell'ambiente di rete.

Dashboard

La funzione Dashboard fornisce un'istantanea completa degli indicatori chiave, in modo da poter valutare rapidamente lo stato e la conformità complessivi dei dispositivi nella zona. Mediante l'uso dei dashboard, è possibile eseguire il drill-down di ulteriori aree di interesse.

I dashboard di ZENworks consentono di visualizzare le informazioni relative allo stato dei dispositivi e delle patch nella zona e di eseguire le azioni richieste.

Per ulteriori informazioni, vedere ZENworks Dashboard Reference (in lingua inglese).

4 Distribuzione dell'agente ZENworks

L'agente ZENworks deve essere installato nei dispositivi che si desidera gestire. Le sezioni seguenti forniscono istruzioni utili per comprendere il processo di installazione dell'agente:

Nota: se un dispositivo non soddisfa i requisiti di installazione dell'agente ZENworks (vedere “Requisiti per i dispositivi gestiti” in *Requisiti di sistema dell'Aggiornamento 1 di ZENworks 2020*), è possibile installarvi l'Inventory Only Module (Modulo solo inventario) per supportare la funzione di creazione di inventari del dispositivo. Per ulteriori informazioni, vedere *ZENworks Discovery, Deployment, and Retirement Reference* (in lingua inglese).

Configurazione delle funzioni dell'agente ZENworks

ZENworks Agent utilizza diversi moduli per eseguire funzioni sui dispositivi. Tali moduli vengono denominati funzioni dell'agente ZENworks. A ciascun prodotto ZENworks sono associate funzioni specifiche, come illustrato nella tabella seguente. I prodotti ZENworks sono elencati nella colonna di sinistra; le altre colonne contengono le funzioni dell'agente ZENworks.

	Gestione risorse	Gestione pacchetti	Sicurezza endpoint	FDE (Full Disk Encryption)	Gestione immagini	Gestione patch	Gestione policy	Gestione remota	Gestione utenti
ZENworks Asset Management	✓								✓
ZENworks Configuration Management		✓			✓		✓	✓	✓
ZENworks Endpoint Security Management			✓						✓
ZENworks Full Disk Encryption				✓					
ZENworks Patch Management						✓			

Per default, quando si attiva un prodotto ZENworks, tutte le funzioni dell'agente ZENworks vengono installate e abilitate. L'unica eccezione è rappresentata da ZENworks Asset Management, che non abilita automaticamente la funzione Gestione utenti.

La funzione Gestione utenti è l'unica supportata dai dispositivi gestiti di Windows in tutti i prodotti ZENworks.

Se non si desidera installare o abilitare una funzione su un dispositivo, è possibile disinstallarla o disabilitarla nella zona di gestione, nella cartella dei dispositivi o nel singolo dispositivo.

Se, ad esempio, si utilizza ZENworks Configuration Management e non si desidera utilizzare Gestione remota con nessun dispositivo, è possibile disabilitare la funzione nella zona di gestione. Oppure, se si dispone di ZENworks Configuration Management e ZENworks Asset Management, ma non si desidera utilizzare Gestione risorse su tutti i dispositivi, è possibile abilitare la funzione Gestione risorse nella zona di gestione, quindi disabilitarla (o disinstallarla) nelle cartelle dei dispositivi o nei singoli dispositivi.

Per personalizzare le funzioni dell'agente ZENworks, prima o dopo la distribuzione dell'agente, vedere le sezioni riportate di seguito:

- "Personalizzazione delle funzioni dell'agente ZENworks" a pagina 40
- "Coesistenza con ZENworks Desktop Management Agent" a pagina 41

Personalizzazione delle funzioni dell'agente ZENworks

Durante la fase iniziale della distribuzione, ZENworks Agent installa e abilita le funzioni selezionate a livello di zona di gestione. Dopo la registrazione, l'agente utilizza le impostazioni definite a livello di cartella dei dispositivi o di dispositivo (se diverse da quelle della zona di gestione).

Nota: non è possibile personalizzare le funzioni dell'agente ZENworks se questo è installato su dispositivi Macintosh.

Nei passaggi seguenti viene descritto come personalizzare le impostazioni al livello della zona di gestione. Per informazioni sulla personalizzazione delle impostazioni in una cartella di dispositivi o in un singolo dispositivo, vedere "Customizing the Agent Features" nel *ZENworks Discovery, Deployment, and Retirement Reference* (in lingua inglese).

1. Nel Centro di controllo ZENworks, fare clic sulla scheda **Configurazione**.
2. Nel pannello Impostazioni zona di gestione fare clic su **Gestione dispositivi** > **Agente ZENworks**.
3. Nel riquadro Funzioni agente:
   - Se non si desidera installare una funzione, deselezionare **Installato** vicino alla funzione. La funzione selezionata non viene installata sul dispositivo. Se si sceglie di deselezionare tutte le funzioni, viene installato solo l'agente core.
   - Se si desidera installare ma disabilitare una funzione, selezionare **Installato** e **Disabilitato** accanto alla funzione. La funzione viene installata su un dispositivo, ma risulta non abilitata.

   Per l'installazione delle funzioni Gestione pacchetti, Gestione remota o Gestione utenti è necessario riavviare il dispositivo. Per l'installazione della funzione Gestione immagini è necessario il riavvio solo con Windows 2008 e Windows Vista. All'utente viene richiesto di riavviare il dispositivo in base all'opzione di riavvio selezionata.
4. Per salvare le modifiche, fare clic su **OK**.

Coesistenza con ZENworks Desktop Management Agent

È possibile distribuire ZENworks Agent su dispositivi sui quali sia già installato ZENworks Desktop Agent.

ZENworks Agent e ZENworks Desktop Agent possono coesistere sullo stesso dispositivo per consentire l'utilizzo di ZENworks Asset Management con ZENworks Desktop Management. In questo caso, quando si distribuisce l'agente ZENworks in un dispositivo sul quale è già installato l'agente desktop ZENworks, è possibile utilizzare solo le funzioni dell'agente ZENworks non associate a ZENworks Configuration Management, mentre non è consentito utilizzare le funzioni Gestione pacchetti, Gestione immagini, Gestione policy, Gestione remota o Gestione utenti. Se si seleziona una di tali funzioni, l'agente desktop ZENworks viene disinstallato prima dell'installazione dell'agente ZENworks.

Per ulteriori informazioni in merito alla coesistenza di ZENworks Agent e ZENworks Desktop Agent, vedere "ZENworks Agent Deployment" in *ZENworks Discovery, Deployment, and Retirement Reference* (in lingua inglese).

Configurazione della sicurezza dell'agente ZENworks

Per proteggere ZENworks Agent sui dispositivi, è possibile configurare sia le impostazioni di disinstallazione che quelle di auto-difesa dell'agente.

1. Nel Centro di controllo ZENworks, fare clic sulla scheda **Configurazione**.
2. Nel riquadro Impostazioni zona di gestione fare clic su **Gestione dispositivo**, quindi selezionare **Agente ZENworks**.
3. Nel pannello Sicurezza agente, configurare le seguenti impostazioni:
   - **Consenti agli utenti di disinstallare ZENworks Agent:** selezionare questa opzione per disinstallare ZENworks Agent.
   - **Richiedi una password di disinstallazione per ZENworks Agent:** selezionare questa opzione per specificare una password obbligatoria per la disinstallazione di ZENworks Agent. Fare clic su **Cambia** per impostare la password.

     Per evitare la distribuzione della password di disinstallazione agli utenti, si consiglia di utilizzare l'utility Generatore chiave password per generare una chiave password. La chiave, basata sulla password di disinstallazione, funziona come tale password, ma può essere collegata a un singolo dispositivo o utente in modo da limitarne l'utilizzo.

     L'utility Generatore chiave password è disponibile nell'elenco Task configurazione nel riquadro di navigazione sinistro.
   - **Abilita una password di sostituzione per ZENworks Agent:** selezionare questa opzione per specificare una password di sostituzione utilizzabile in ZENworks Agent per:
     - Accedere alle informazioni sull'ubicazione corrente del dispositivo e sulla modalità di assegnazione dell'ubicazione.
     - Accedere alle opzioni di amministrazione nell'agente di sicurezza endpoint. Queste opzioni consentono di disabilitare le policy di sicurezza applicate (ad eccezione della policy di cifratura dati), di visualizzare informazioni dettagliate sulle policy e di visualizzare informazioni sullo stato degli agenti.

- Accedere alle opzioni di amministrazione nell'agente FDE (Full Disk Encryption). Queste opzioni consentono di visualizzare informazioni dettagliate sulle policy, di visualizzare informazioni sullo stato degli agenti, nonché di eseguire altre funzioni quali ad esempio abilitazione dei volumi di decifratura e acquisizione utente.
- Disinstallare ZENworks Agent.

- **Abilita autodifesa per ZENworks Agent:** selezionare questa opzione per abilitare l'autodifesa. Attualmente la funzionalità di autodifesa protegge solo l'agente di sicurezza endpoint ZENworks. Non protegge invece gli altri moduli di ZENworks Agent.

  L'autodifesa impedisce l'arresto, la disabilitazione o la manomissione dell'agente di sicurezza endpoint. Se l'utente esegue una qualsiasi delle seguenti attività, il dispositivo viene automaticamente riavviato per consentire il ripristino della configurazione di sistema corretta:

  - Utilizzo di Windows Task Manager per interrompere qualsiasi processo dell'agente di sicurezza endpoint.
  - Interruzione o sospensione di qualsiasi servizio dell'agente di sicurezza endpoint.
  - Rimozione di voci di registro e di file critici. Se si apporta una modifica alle chiavi di registro o ai valori associati all'agente di sicurezza endpoint, tali chiavi o valori verranno reimpostati immediatamente.
  - Disabilitazione del binding tra driver filtro NDIS e adattatori.

4 Per salvare le modifiche, fare clic su **OK**.

Installazione di ZENworks Agent

Nelle seguenti sezioni sono fornite le istruzioni per l'installazione manuale di ZENworks Agent nei dispositivi.

- “Installazione manuale su Windows” a pagina 42
- “Installazione manuale su Linux” a pagina 44
- “Installazione manuale su Macintosh” a pagina 45

Nota: oltre a installare manualmente l'agente ZENworks, è possibile automatizzare l'installazione utilizzando il processo di rilevazione e distribuzione dei dispositivi di rete. Il processo di rilevazione e distribuzione supera l'ambito di questo Riferimento rapido. Per scoprire come utilizzare il processo, vedere *ZENworks Discovery, Deployment, and Retirement Reference* (in lingua inglese).

Installazione manuale su Windows

1 Assicurarsi che il dispositivo soddisfi i requisiti necessari (consultare “Requisiti dei dispositivi gestiti)”.

2 Sul dispositivo di destinazione, aprire un browser Web e accedere al seguente indirizzo:

`https://server:port/zenworks-setup`

Sostituire il *server* con il nome DNS o l'indirizzo IP di un server ZENworks e sostituire la *porta* solo se il server ZENworks non utilizza quella di default (80 o 443).

Il browser Web visualizza un elenco di pacchetti di distribuzione per l'agente ZENworks. Per ciascuna architettura (32 bit e 64 bit), sono disponibili i seguenti tipi di pacchetti:

- **Rete (.NET obbligatorio):** il pacchetto di rete (.NET obbligatorio) installa solo il pre-agente nel dispositivo di destinazione; il pre-agente effettua quindi il download di ZENworks Agent dal server ZENworks e lo installa. Il pacchetto di rete (.NET obbligatorio) richiede l'installazione di Microsoft .NET 4.0 o successivo nel dispositivo prima della distribuzione dell'agente.
- **Autonomo (.NET obbligatorio):** il pacchetto autonomo (.NET obbligatorio) richiede l'installazione di Microsoft .NET 4.0 o versione successiva nel dispositivo prima della distribuzione dell'agente. Questo pacchetto include tutti i file eseguibili necessari per l'installazione dell'agente ZENworks, ad eccezione del programma di installazione di Microsoft .NET.
- **Autonoma:** il pacchetto autonomo installa il pre-agente ed estrae tutti i file eseguibili necessari per l'installazione dell'agente ZENworks, incluso il programma di installazione di Microsoft .NET nel dispositivo di destinazione. Il pre-agente installa quindi l'agente ZENworks dal dispositivo locale. Questo pacchetto indipendente è utile se si ha l'esigenza di installare ZENworks Agent in un dispositivo che è attualmente disconnesso dalla rete. È possibile salvare il pacchetto su un supporto rimovibile (CD, unità USB flash e così via) e far eseguire al dispositivo autonomo il pacchetto dal supporto. L'agente ZENworks viene installato sul dispositivo, ma le operazioni di registrazione o gestione vengono effettuate solo nel momento in cui il dispositivo si connette alla rete.
- **Personalizzato:** il nome del pacchetto, Agente di default, si riferisce ai pacchetti di distribuzione predefiniti. I pacchetti di distribuzione personalizzati creati tramite **Distribuzione** > **Modifica pacchetto distribuzione** vengono visualizzati con il nome assegnato al momento della creazione del pacchetto.

3 Fare clic sul nome del pacchetto di distribuzione che si desidera usare, quindi salvare il pacchetto sull'unità locale del dispositivo oppure eseguirlo dal server ZENworks.

4 Se il pacchetto è stato scaricato, avviarlo sul dispositivo.

Per informazioni sulle opzioni che è possibile utilizzare con il pacchetto quando viene avviato da una riga di comando, vedere "Package Options for Windows, Linux, and Macintosh" in *ZENworks Discovery, Deployment, and Retirement Reference* (in lingua inglese).

Importante: se si sceglie di installare un pacchetto completo, l'installazione di Windows Installer o .NET Framework potrebbe richiedere un riavvio del computer dopo l'avvio del pacchetto. Viene visualizzato un messaggio che offre diverse opzioni per il riavvio. Selezionare una delle seguenti opzioni:

- Non fare niente e attendere il riavvio automatico dopo 5 minuti.
- Fare clic su **Annulla**. Successivamente, sarà necessario eseguire il riavvio.
- Fare clic su **OK** per eseguire immediatamente il riavvio.

L'installazione riprende automaticamente al riavvio del dispositivo.

---

5 Una volta completata l'installazione, il dispositivo si riavvia automaticamente se è stato riavviato durante l'installazione di Windows Installer o .NET Framework.

Al momento del riavvio, il dispositivo viene registrato nella zona di gestione e l'icona ZENworks viene inserita nell'area di notifica (barra delle applicazioni).

Nel Centro di controllo ZENworks il dispositivo viene visualizzato nella cartella`\Server` o `\Workstation` della pagina dei dispositivi.

Per informazioni sul login e sull'uso dell'agente ZENworks su un dispositivo, vedere "Utilizzo dell'agente ZENworks" a pagina 46.

Installazione manuale su Linux

Anziché lasciare al server ZENworks il compito di installare l'agente ZENworks in un dispositivo, è possibile effettuare manualmente il download del pacchetto di distribuzione dell'agente ZENworks dal server e installare l'agente.

Importante: è possibile installare l'agente ZENworks su Linux se si dispone delle autorizzazioni root o di amministratore.

---

1. Verificare che il dispositivo soddisfi i requisiti necessari (vedere "Requisiti per i dispositivi gestiti" in *Requisiti di sistema dell'Aggiornamento 1 di ZENworks 2020*).
2. Sul dispositivo di destinazione, aprire un browser Web e accedere al seguente indirizzo:

   `http://server:port/zenworks-setup`

   Sostituire il *server* con il nome DNS o l'indirizzo IP di un server ZENworks e sostituire la *porta* solo se il server ZENworks non utilizza quella di default (80 o 443).

   Nel browser Web viene visualizzato l'elenco di tutti i pacchetti di distribuzione. Per ciascuna architettura (32 bit e 64 bit), sono disponibili i seguenti tipi di pacchetti:

   - **Rete:** questo pacchetto installa solo il pre-agente sul dispositivo di destinazione; il pre-agente effettua quindi il download di ZENworks Agent dal server ZENworks e lo installa.
   - **Autonoma:** il pacchetto autonomo installa il pre-agente ed estrae tutti i file eseguibili necessari per l'installazione dell'agente ZENworks, incluso il programma di installazione di JRE sul dispositivo di destinazione. Il pre-agente installa quindi l'agente ZENworks dal dispositivo locale. Il pacchetto autonomo è utile quando occorre installare ZENworks Agent su un dispositivo momentaneamente disconnesso dalla rete. È possibile salvare il pacchetto su un supporto rimovibile (ad esempio un CD o un'unità USB Flash) e fare eseguire a un dispositivo autonomo il pacchetto dal supporto. L'agente ZENworks viene installato sul dispositivo, ma le operazioni di registrazione o gestione vengono effettuate solo nel momento in cui il dispositivo si connette alla rete.
   - **Personalizzato:** il nome del pacchetto, Agente di default, si riferisce ai pacchetti di distribuzione predefiniti. I pacchetti di distribuzione personalizzati, creati selezionando **Distribuzione** > **Modifica pacchetto distribuzione**, vengono visualizzati con il nome assegnato al momento della creazione del pacchetto.
3. Fare clic sul nome del pacchetto di distribuzione da utilizzare, salvarlo sull'unità locale del dispositivo, quindi assegnare autorizzazioni di esecuzione al file eseguendo il comando `chmod 755 nomefile`.

   Per informazioni sulle opzioni che è possibile utilizzare con il pacchetto quando viene avviato da una riga di comando, vedere "Package Options for Windows, Linux, and Macintosh" in *ZENworks Discovery, Deployment, and Retirement Reference* (in lingua inglese).
4. (Opzionale) Su un dispositivo RHEL, eseguire il seguente comando:

   `chcon -u system_u -t rpm_exec_t nome file`

5 Nella finestra del terminale, accedere alla directory in cui è stato effettuato il download del pacchetto, quindi avviare quest'ultimo sul dispositivo eseguendo il comando `./nomefile`, dove **nomefile** è il nome del pacchetto di cui è stato effettuato il download in Passo 3.

6 (Condizionale) Se si desidera visualizzare l'icona di notifica di ZENworks nell'area di notifica dopo l'installazione dell'agente per il dispositivo Linux, eseguire il logout, quindi il login al dispositivo.

Nel Centro di controllo ZENworks il dispositivo viene visualizzato nella cartella`\Server` o `\Workstation` della pagina Dispositivi.

Installazione manuale su Macintosh

È possibile installare ZENworks Agent su un dispositivo Macintosh scaricando il pacchetto per l'installazione dalla pagina dei download di ZENworks.

Importante

- È possibile installare l'agente ZENworks su un dispositivo Macintosh se si dispone delle autorizzazioni di utente radice o amministratore.

---

1 Sul dispositivo Macintosh di destinazione, aprire il browser Web e immettere il seguente indirizzo:

http://<server>/zenworks-setup

Sostituire *<server>* con il nome DNS o con l'indirizzo IP del server ZENworks.

2 Fare clic sul pacchetto Macintosh appropriato per effettuare il download.

Nota: esistono due tipi di pacchetti:

- **Rete:** per effettuare il download dei file PKG il pacchetto deve disporre dell'accesso di rete al server ZENworks.
- **Autonoma:** per installare l'agente non è necessario disporre di accesso al server ZENworks.

---

3 Dal prompt dei comandi, specificare le autorizzazioni di esecuzione per il file `.bin` scaricato eseguendo il comando `chmod +x<nome_file>`.

Per ulteriori informazioni sulle opzioni che è possibile utilizzare con il pacchetto, vedere "Package Options for Windows, Linux, and Macintosh" in *ZENworks Discovery, Deployment, and Retirement Reference* (in lingua inglese).

4 Dal prompt dei comandi, spostarsi nella directory in cui si è effettuato il download del pacchetto, quindi avviare il pacchetto sul dispositivo eseguendo il comando seguente:

```
sudo./nome file
```

`nomefile` è il nome del pacchetto scaricato in Passo 2 a pagina 45.

5 Dopo aver eseguito l'installazione dell'agente per il dispositivo Macintosh, eseguire il logout e il login nel dispositivo per visualizzare l'icona di notifica di ZENworks nella relativa area.

Nel Centro di controllo ZENworks il dispositivo viene visualizzato nella cartella`\Server` o `\Workstation` della pagina Dispositivi.

Nota: dopo aver installato ZENworks Agent su un dispositivo Macintosh, `/opt/novell/zenworks/bin` non viene aggiunto alla variabile PATH, quindi i comandi contenuti all'interno di quella directory non possono essere utilizzati direttamente. Per eseguire i comandi da `/opt/novell/zenworks/bin` effettuare una delle seguenti operazioni sul dispositivo Macintosh:

- Eseguire nuovamente il login al dispositivo.
- Specificare il percorso completo per accedere al comando.

  Ad esempio: `/opt/novell/zenworks/bin/zac`.

Utilizzo dell'agente ZENworks

Le seguenti sezioni spiegano come accedere a ZENworks Agent e usarlo:

Accesso alla zona di gestione

Quando un dispositivo gestito Windows si avvia tramite il relativo sistema operativo, l'agente ZENworks viene avviato e tutti i pacchetti e le policy assegnati al dispositivo sono disponibili. Per rendere disponibili i pacchetti e le norme assegnati a un utente, è necessario accedere alla zona di gestione.

L'agente di ZENworks si integra con il client di login di Windows o Novell per consentire agli utenti un singolo login. Quando gli utenti immettono le loro credenziali eDirectory o Active Directory sul client Windows o Novell, accedono alla zona di gestione se le credenziali corrispondono a quelle di una delle origini utente ZENworks. In caso contrario, viene visualizzata la schermata di login dell'agente ZENworks con un messaggio che chiede all'utente di immettere le credenziali corrette.

Si supponga, ad esempio, che l'utente abbia dei conti in due alberi eDirectory: Albero1 e Albero2. Diversamente dall'Albero2, l'Albero1 è definito come origine utente nella zona di gestione. Se esegue il login all'Albero1, l'utente viene automaticamente collegato anche alla zona di gestione. Tuttavia, se l'utente esegue il login all'Albero2, viene visualizzata la schermata di login all'agente ZENworks con un messaggio che chiede all'utente di immettere le credenziali dell'Albero1.

Esplorazione delle viste dell'agente ZENworks

L'agente ZENworks fornisce le seguenti viste:

ZENworks Application

ZENworks Application è una finestra autonoma che consente di accedere ai pacchetti. È possibile aprire la finestra dal menu Start (**menu Start** > **Programmi** > **Novell ZENworks** > **ZENworks Application**).

Nel riquadro sinistro di ZENworks Application è visualizzato quanto segue:

- **Cartella [Tutto]:** contiene tutti i pacchetti distribuiti all'utente, indipendentemente dalla cartella in cui sono ubicati.
- **Cartella ZENworks:** contiene tutti i pacchetti che non sono stati assegnati a una cartella diversa. La cartella ZENworks è la cartella di default per i pacchetti. Tuttavia, gli amministratori possono creare ulteriori cartelle in cui organizzare i pacchetti e perfino rinominare la cartella ZENworks.
- **Cartella Favorites (Preferiti):** contiene tutti i pacchetti contrassegnati come preferiti.

Quando si seleziona una cartella nel riquadro a sinistra, i pacchetti contenuti nella cartella vengono visualizzati nel riquadro a destra. È possibile effettuare le seguenti operazioni:

- Installare un pacchetto o avviare un'applicazione già installata.
- Visualizzare le proprietà di un pacchetto. Le proprietà comprendono una descrizione del pacchetto, informazioni su chi contattare per assistenza sul pacchetto, indicazioni su quando il pacchetto è disponibile per l'uso e i requisiti di sistema definiti per il pacchetto.
- Riparare un'applicazione installata.
- Disinstallare un'applicazione. Questa è una funzione gestita dall'amministratore ed è quindi possibile che non sia abilitata.

ZENworks Explorer

ZENworks Explorer è un'estensione di Windows Explorer che consente di visualizzare i pacchetti in Esplora risorse, sul desktop, nel menu di avvio, sulla barra degli strumenti di avvio veloce e nell'area di notifica. La seguente figura mostra i pacchetti visualizzati in Esplora risorse.

La seguente figura mostra i pacchetti visualizzati sul desktop.

È possibile eseguire i task nei pacchetti in ZENworks Window anche in ZENworks Explorer.

ZENworks Icon

L'icona ZENworks  è ubicata nell'area delle notifiche di Windows (barra delle applicazioni). Facendo doppio clic sull'icona, è possibile visualizzare la finestra dell'agente ZENworks.

Per visualizzare le proprietà dell'agente, fare clic con il pulsante destro del mouse sull'icona ZENworks e selezionare Applicazione tecnica. Viene visualizzata la finestra delle proprietà dell'agente ZENworks.

Nel riquadro di spostamento sinistro della finestra delle proprietà sono contenuti i collegamenti relativi allo stato dell'agente ZENworks e le rispettive funzioni:

- **Stato:** visualizza informazioni, ad esempio l'ultima volta che l'agente ha contattato il server ZENworks, e indica se le funzioni dell'agente sono in esecuzione.

- **Policy:** visualizza le policy assegnate al dispositivo e l'utente che ha eseguito il login. Indica anche se la policy è effettiva. È inclusa solo se ZENworks Configuration Management o ZENworks Endpoint Security Management è abilitato.
- **Pacchetti:** visualizza i pacchetti al dispositivo e all'utente collegato. Visualizza anche lo stato di installazione attuale di ciascun pacchetto (disponibile, scaricamento in corso, installazione in corso e così via) e indica se il pacchetto è effettivo (ossia se il dispositivo soddisfa i requisiti per la distribuzione). È inclusa solo se ZENworks Configuration Management o ZENworks Patch Management è abilitato.
- **Inventario:** visualizza le informazioni sull'inventario del dispositivo. È possibile visualizzare informazioni dettagliate sull'hardware come il nome del produttore e il modello dei dischi rigidi, delle unità disco e della scheda video. È possibile anche visualizzare informazioni dettagliate sul software come gli hot fix e le patch di Windows installati e i numeri di versione e le ubicazioni dei prodotti software installati. È inclusa solo se ZENworks Configuration Management o ZENworks Asset Management è abilitato.
- **Sicurezza endpoint:** visualizza informazioni sull'agente di sicurezza endpoint e l'ubicazione utilizzata per determinare quali policy di sicurezza vengono applicate. È inclusa solo se ZENworks Endpoint Security Management è abilitato.
- **Gestione remota:** visualizza informazioni sugli operatori remoti correntemente connessi e le impostazioni della norma Gestione remota applicate al dispositivo. Consente anche di avviare una sessione di gestione e di controllare le impostazioni di sicurezza della sessione. È inclusa solo se ZENworks Configuration Management è abilitato.
- **Satellite:** visualizza le informazioni sul ruolo satellite di un dispositivo utilizzato come server satellite. I ruoli satellite includono Raccolta, Contenuto, Autenticazione, Imaging e Join Proxy.

  Questa funzione è visualizzata solo se l'amministratore ZENworks ha utilizzato il dispositivo come satellite.
- **Registrazione:** visualizza informazioni sul file di log dell'agente ZENworks, come l'ubicazione del file di log, il server ZENworks su cui verrà effettuato l'upload del file di log dell'agente e l'ora dell'upload successivo pianificato. Consente anche di specificare il livello di gravità per i messaggi registrati.
- **Proxy Windows:** visualizza i risultati delle attività di rilevazione e distribuzione eseguite sul dispositivo quando quest'ultimo agisce come proxy Windows per il server primario ZENworks.

Promozione di un dispositivo gestito a satellite

Un satellite è un dispositivo gestito in grado di eseguire determinati ruoli normalmente eseguiti dal server primario ZENworks, inclusi quelli di autenticazione, raccolta delle informazioni, distribuzione del contenuto e imaging. Qualsiasi dispositivo Windows gestito, dispositivo Linux gestito o dispositivo Macintosh gestito può essere un satellite, ma non un server primario. Quando si configura un satellite, è necessario specificare quali ruoli esegue (autenticazione, raccolta, contenuto o imaging). Un satellite può svolgere anche ruoli che possono essere aggiunti da prodotti di terze parti, che costituiscono snap-in al framework di ZENworks

---

Nota: ZENworks non consente più la promozione dei dispositivi a 32 bit al ruolo di server satellite o l'aggiunta di un nuovo ruolo a un server satellite a 32 bit esistente.

Per informazioni dettagliate sui satelliti e su come promuovere un dispositivo gestito a satellite, vedere “Satellites” in *ZENworks Primary Server and Satellite Reference* (in lingua inglese).

5 Messaggi di sistema

ZENworks consente di monitorare l'attività nella zona di gestione tramite messaggi di sistema.

Visualizzazione dei messaggi di sistema

Il sistema ZENworks crea messaggi normali (informativi), di avviso e di errore che possono essere utilizzati per controllare attività come la distribuzione del software e l'applicazione delle norme.

Ciascun server ZENworks e ZENworks Agent crea un log delle attività a esso associate. I messaggi vengono visualizzati in aree diverse del Centro di controllo ZENworks:

- **Log messaggi di sistema:** il log dei messaggi di sistema, cui è possibile accedere selezionando **Dashboard > Messaggi di sistema**, visualizza i messaggi provenienti da tutti i server e gli agenti ZENworks all'interno della zona.
- **Log messaggi del dispositivo:** il log dei messaggi del dispositivo, situato nella pagina di riepilogo di un server o di una workstation, mostra i messaggi generati dal server o dall'agente ZENworks. Ad esempio, il log dei messaggi di Workstation1 comprende tutti i messaggi generati dall'agente ZENworks sulla Workstation1.
- **Log messaggi di contenuto:** il log dei messaggi di contenuto, situato nella pagina Riepilogo di un pacchetto o di una policy, mostra solo i messaggi generati dal server o dall'agente ZENworks associati al pacchetto o alla policy. Ad esempio, il log dei messaggi di Pacchetto1 può contenere messaggi generati da tre diversi server ZENworks e 100 diversi agenti ZENworks.

Visualizzazione di un riepilogo dei messaggi

È possibile visualizzare un riepilogo che mostra il numero di messaggi generati per server, workstation, pacchetti e policy della zona.

1 Nel Centro di controllo ZENworks, fare clic sulla scheda **Home**.

Nel pannello Riepilogo messaggio è visualizzato lo stato di tutti i server, le workstation, le policy e i pacchetti nella zona di gestione. Ad esempio, se due server presentano messaggi critici non riconosciuti (ovvero i messaggi la cui ricezione non è stata ancora confermata dall'utente o da un altro amministratore), viene visualizzato il numero 2 nella colonna . Oppure, se sono presenti tre pacchetti con messaggi di avviso e cinque pacchetti con messaggi normali, viene visualizzato il numero 3 nella colonna e il numero 5 nella colonna . Tramite il riepilogo è possibile effettuare le seguenti operazioni:

- Fare clic su un tipo di oggetto per visualizzare la cartella radice. È ad esempio possibile fare clic su **Server** per visualizzare la cartella radice Server (`/Servers`).

- Per ciascun tipo di oggetto, fare clic sul numero in una delle colonne di stato () per visualizzare un elenco di tutti gli oggetti con lo stato selezionato. Ad esempio, per visualizzare l'elenco dei server con uno stato normale, fare clic sul numero nella colonna .
- Per qualsiasi tipo di oggetto, è possibile fare clic sul numero nella colonna **Totale** per visualizzare tutti gli oggetti che hanno messaggi critici, di avviso o normali. Ad esempio, fare clic sul conteggio **Totale** per i **Server** per visualizzare un elenco di tutti i server con qualsiasi tipo di messaggio.

Riconoscimento dei messaggi

I messaggi rimangono nel log dei messaggi fintanto che non vengono riconosciuti. È possibile riconoscere messaggi individuali o tutti i messaggi inclusi nel log in una volta sola.

1. Nel Centro di controllo ZENworks, fare clic sulla scheda **Dispositivi**.
2. Scorrere la cartella `Server` fino a individuare un server ZENworks.
3. Fare clic sul server per visualizzarne i dettagli.
4. Nella scheda **Riepilogo**, individuare il riquadro Log messaggi.

   Nel riquadro Log messaggi sono elencati tutti i messaggi (informativi, di avviso e di errore) generati dal server ZENworks. Nella seguente tabella vengono spiegati i vari metodi con i quali è possibile riconoscere e cancellare i messaggi.

Task	Passaggi	Dettagli aggiuntivi
Riconoscimento di un messaggio	1. Fare clic sul messaggio per visualizzare la finestra di dialogo Informazioni dettagli messaggi. 2. Fare clic su **Riconosci**.	Se non si desidera confermare il messaggio, fare clic su **Completato** per chiudere la finestra di dialogo. In tal modo, il messaggio rimane nell'elenco **Log messaggi**.
Riconoscimento di tutti i messaggi	1. Nell'elenco **Task** situato nel riquadro di navigazione a sinistra, fare clic su **Riconosci tutti i messaggi**.	
Visualizzare tutti i messaggi riconosciuti e non	1. Fare clic sul pulsante **Avanzate** per visualizzare la pagina Modifica log messaggi.	Oltre a visualizzare tutti i messaggi riconosciuti e non, è possibile anche visualizzare solo i messaggi con uno stato o una data specifici, visualizzare ulteriori dettagli sui messaggi e riconoscere i messaggi. Fare clic sul pulsante **Guida** nella pagina Modifica log messaggi per visualizzare informazioni specifiche sui task che possono essere effettuati nella pagina.
Cancellazione di un messaggio	1. Fare clic su un messaggio per visualizzare la finestra di dialogo Log dettagli messaggio. 2. Fare clic su **Cancella**.	La cancellazione di un messaggio ne provoca la rimozione dal sistema ZENworks.

È possibile anche usare il comando `messages-acknowledge` nell'utility zman per confermare i messaggi associati ai dispositivi, ai pacchetti e alle norme. Per ulteriori informazioni, vedere "Comandi per i messaggi" nel *Riferimento per le utility da riga di comando di ZENworks*.

Ulteriori informazioni

Per informazioni sui messaggi di sistema, vedere "Using Message Logging" in *ZENworks Control Center Reference* (in lingua inglese).

Creazione di un elenco di controllo

Se si desidera controllare attentamente lo stato di alcuni dispositivi, pacchetti o norme, è possibile aggiungerli all'elenco di controllo. L'elenco di controllo fornisce le seguenti informazioni:

- **Agente:** per server e workstation, visualizza se ZENworks Agent del dispositivo è attualmente connesso ( ) o disconnesso ( ).
- : indica se ci sono messaggi critici per l'oggetto.

- **Tipo:** visualizza un'icona che rappresenta l tipo di oggetto. Ad esempio, un pacchetto può presentare l'icona  a indicare che si tratta di un pacchetto Windows. Oppure è possibile che venga visualizzata l'icona  su un dispositivo a indicare che si tratta di un server. È possibile passare il mouse sull'icona per visualizzarne la descrizione.
- **Nome:** visualizza il nome dell'oggetto. È possibile fare clic sul nome per passare al log dei messaggi dell'oggetto.

Per aggiungere un dispositivo, un pacchetto o una norma all'elenco di controllo:

1. Nel Centro di controllo ZENworks, fare clic sulla scheda **Home**.
2. Nel pannello Elenco di controllo, fare clic su **Aggiungi**, quindi selezionare il tipo di oggetto (dispositivo, pacchetto o policy) che si desidera aggiungere all'elenco.
3. Nella finestra di dialogo di selezione, selezionare l'oggetto desiderato, quindi fare clic su **OK** per aggiungerlo all'elenco di controllo.

   Se ad esempio si aggiungono dei server, individuare e selezionarne uno.

Gli oggetti rimangono nell'elenco di controllo fino a che non li si rimuove.

6 Gestione revisione

ZENworks consente di registrare e visualizzare attività che hanno luogo nel sistema ZENworks mediante l'uso della funzione Gestione revisione. Questa funzione permette di catturare vari eventi che si verificano nella zona. I dettagli di un evento catturato possono essere utilizzati ai fini della sicurezza e della conformità, in modo da poter identificare gli utenti e le rispettive azioni su un determinato sistema quando nell'ambiente si verifica un evento importante. Grazie a questa funzione è possibile monitorare centralmente le attività correlate ai server primari, ai server satellite e ai dispositivi gestiti.

Tipi di eventi di revisione

Gli eventi di revisione ZENworks si dividono in due tipi:

- **Eventi modifica:** questi eventi catturano le modifiche della configurazione apportate alla zona dal Centro di controllo ZENworks Control Center o con le utility da riga di comando zman. È possibile catturare varie modifiche, dalle modifiche dei pacchetti a quelle del sistema ZENworks. Ad esempio, è possibile configurare un evento di revisione che registra l'attività di un amministratore che assegna un pacchetto a un dispositivo.
- **Eventi agente:** questi eventi catturano le azioni che si verificano sui dispositivi ZENworks. Sono noti anche come eventi dei dispositivi.

Sia gli eventi modifica sia gli eventi agente possono essere abilitati per tutti i dispositivi nella zona o per singoli dispositivi.

Abilitazione di un evento

Per revisionare un evento, innanzitutto è necessario abilitarlo nel Centro di controllo ZENworks. È possibile abilitare l'evento a livello di zona o di dispositivo. Un evento abilitato a livello di zona viene applicato a tutti i dispositivo nella zona, mentre un evento abilitato a livello di dispositivo viene applicato solo al dispositivo selezionato.

1. Eseguire il login al Centro di controllo ZENworks.
2. (Zona) Per abilitare eventi a livello di zona, fare clic su **Configurazione > Impostazioni zona di gestione > Gestione revisione**.

   oppure

   (Dispositivi) Per abilitare eventi a livello di dispositivo, fare clic su **Dispositivi > Dispositivi gestiti**. Individuare il dispositivo nelle cartelle Server o Workstation, fare clic sull'oggetto dispositivo per visualizzarne le proprietà, quindi fare clic su **Impostazioni > Gestione revisione**.

3 Fare clic su **Configurazione eventi** per visualizzare la pagina della finestra di dialogo corrispondente.

4 Nella scheda **Eventi modifica** o **Eventi agente**, fare clic su **Aggiungi** per visualizzare la finestra di dialogo Aggiungi eventi modifica o Aggiungi eventi agente.

   Per informazioni sulle categorie di eventi modifica e agente, vedere *ZENworks Audit Management Reference* (in lingua inglese).

5 Espandere l'albero **Eventi modifica** o **Eventi agente** e selezionare l'evento richiesto.

6 Specificare le seguenti informazioni per **Impostazioni evento**:

   - **Classificazione evento:** in base all'importanza dell'evento, selezionare **Critico**, **Più importante** o **Informativo**.
   - **Giorni di conservazione:** indicare per quanti giorni deve essere conservato l'evento prima di eliminarlo definitivamente.
   - **Tipi di notifica:** specificare se la notifica deve essere inviata tramite e-mail, trap SNMP, UDP o a un file locale quando si verifica l'evento. Se si seleziona **Registra il messaggio in un file locale**, è necessario configurare le impostazioni del file di log locale.

     è anche possibile selezionare tutti i tipi di notifica. Per ulteriori informazioni, vedere "Using Message Logging".
   - (Eventi agente) Specificare la **frequenza campione** con cui raccogliere i dati per generare eventi di revisione. Questo campo viene visualizzato solo se è selezionato un evento di ZENworks Endpoint Security Management o di ZENworks Agent.

7 Fare clic su **OK** per aggiungere l'evento.

È possibile modificare o cancellare un evento selezionandolo nella pagina Configurazione eventi e facendo clic su **Modifica** o **Cancella** nella barra dei menu. Per selezionare più eventi contemporaneamente, premere **Ctrl** e fare clic per selezionare.

Visualizzazione di un evento generato

Quando si verifica un evento abilitato, viene generato un evento di revisione.

Dopo la generazione di un evento di revisione è possibile accedere ai dettagli dell'evento dalle seguenti ubicazioni:

- **Dashboard:** è possibile visualizzare i dati di revisione dal dashboard del Centro di controllo ZENworks. Il dashboard presenta le seguenti schede:
  - **Dashboard:** da questa scheda è possibile visualizzare un riepilogo degli eventi di revisione che si sono verificati nella zona. È possibile visualizzare gli indicatori chiave degli eventi principali e degli oggetti interessati, inoltre è possibile ottenere una vista del log degli eventi filtrata. Per default, nel dashboard è illustrata una panoramica degli eventi che hanno avuto luogo nelle ultime quattro ore. Per visualizzare ulteriori dati, è possibile modificare il periodo di tempo.
  - **Eventi (log di revisione):** in questa scheda è possibile visualizzare tutti gli eventi che si sono verificati nella zona. Le informazioni vengono visualizzate in un formato simile alla pagina di Configurazione eventi. Viene visualizzato un conteggio a fronte delle categorie per le quali è stato generato un evento. Se ad esempio è stato generato un evento **Gestione**

assegnazione pacchetto, viene visualizzato **1** a fronte della categoria Gestione assegnazione pacchetto nella struttura dell'albero. Quando si fa clic sull'evento, nel riquadro a destra vengono visualizzati i rispettivi dettagli.

- **(Eventi modifica) cartelle oggetti:** la scheda **Revisione** nelle cartelle oggetti (**Dispositivi**, **Pacchetti**, **Policy** e **Utenti**) consente di visualizzare gli eventi di revisione generati per tutti gli oggetti all'interno della cartella selezionata. Ad esempio, è possibile visualizzare gli eventi generati per tutti i pacchetti in una cartella di pacchetti. Pertanto è possibile visualizzare nella cartella Pacchetti tutti gli eventi correlati ai pacchetti. Le informazioni vengono classificate in modo analogo alla pagina **Configurazione eventi**. È possibile scorrere gli eventi che si sono verificati e qualora fossero necessarie ulteriori informazioni, è possibile fare clic sull'evento per visualizzarne i dettagli.
- **(Eventi modifica) oggetti:** è inoltre possibile visualizzare gli eventi di revisione per un oggetto all'interno della cartella oggetti. Se ad esempio si seleziona un determinato pacchetto in una cartella di pacchetti, è possibile visualizzare gli eventi generati per tale pacchetto specifico.
- **(Eventi agente) cartella Dispositivi:** la scheda **Revisione** nella cartella **Dispositivi** consente di visualizzare gli eventi generati per un determinato dispositivo (server o workstation).

Per visualizzare i dettagli degli eventi generati:

1. Eseguire il login al Centro di controllo ZENworks.
2. (Dashboard) Per visualizzare gli eventi nel dashboard, fare clic su **Dashboard** > **Eventi**.

   oppure

   (Cartella oggetti) Per visualizzare gli eventi per tutti gli oggetti in una cartella (ad esempio una cartella dispositivi, pacchetti o policy), fare clic sul collegamento **Dettagli** della cartella, quindi fare clic sulla scheda **Revisione**.

   oppure

   (Oggetto) Per visualizzare gli eventi per un oggetto specifico (ad esempio un dispositivo, pacchetto o policy) fare clic sull'oggetto, quindi fare clic sulla scheda **Revisione**.

   (Cartella Dispositivi) per visualizzare gli eventi nella cartella Dispositivi, nel riquadro a sinistra fare clic su **Dispositivi**. Se l'evento è stato eseguito su un server nella zona, fare clic su **Dettagli** del server o se l'evento è stato eseguito su un dispositivo gestito, fare clic su **Dettagli** della workstation. Quindi fare clic sulla scheda **Revisione** per visualizzare la schermata Eventi.
3. Fare clic sulla scheda **Eventi modifica** o **Eventi agente**.
4. Espandere la struttura dell'albero e individuare la categoria pertinente.

   A seconda del numero di eventi di revisione configurati, a fronte della categoria viene visualizzato il conteggio pertinente.
5. Fare clic sull'evento.

   Nel riquadro a destra vengono visualizzati i dettagli dell'evento generato.

Nota: per visualizzare i dettagli dell'evento in una nuova finestra, fare clic su  .

II Amministrazione dei prodotti

Le seguenti sezioni forniscono informazioni sull'uso dei prodotti ZENworks Prima di consultarle, è necessario completare i task di configurazione in Parte I, “Configurazione del sistema,” a pagina 9.

7 Elenco rapido

Una volta terminata la configurazione della zona di gestione (vedere Parte I, “Configurazione del sistema,” a pagina 9), è necessario rivedere i concetti e i task descritti nelle sezioni seguenti per tutti i prodotti ZENworks concessi in licenza o in fase di valutazione:

Gestione risorse

ZENworks Asset Management consente di controllare la conformità delle licenze software, l'uso del software e la proprietà del software tramite l'allocazione di licenze a dispositivi, siti, reparti e centri di costo.

Task	Dettagli
Attivare Asset Management	Se Asset Management non è stato attivato durante l'installazione della zona di gestione, specificando una chiave di licenza o attivando la licenza di valutazione, è necessario eseguire questa operazione prima di utilizzare il prodotto. Per informazioni, vedere “Attivazione di Asset Management” a pagina 65.
Abilitare ZENworks Agent per eseguire operazioni di gestione risorse	La funzione Gestione risorse dell'agente è abilitata per default all'attivazione di ZENworks Asset Management (licenza completa o di valutazione). È necessario accertarsi che la funzione Gestione risorse dell'agente sia comunque abilitata. Inoltre, se si desidera controllare le licenze software a fronte degli utenti (anziché solo a fronte dei dispositivi), è necessario abilitare la funzione Gestione utenti disabilitata per default. Per informazioni, vedere “Abilitazione di Asset Management in ZENworks Agent” a pagina 65.

Task	Dettagli
Eseguire la scansione dei dispositivi per creare un inventario software e hardware	Eseguire la scansione dei dispositivi per creare inventari software e hardware per i dispositivi stessi. Le informazioni sull'inventario sono di ausilio per prendere decisioni in merito alla distribuzione del software e agli aggiornamenti hardware. È necessario eseguire questo task prima degli altri. Per informazioni, vedere "Raccolta dell'inventario software e hardware" a pagina 66.
Controllare l'utilizzo del software	Task generato per analizzare in che misura e con quale frequenza vengono utilizzati i prodotti software. Per informazioni, vedere "Monitoraggio dell'utilizzo del software" a pagina 67.
Controllare la conformità delle licenze software	Verificare se il numero di licenze dei prodotti software installati è corretto, insufficiente o eccessivo. Per informazioni, vedere "Verifica della conformità delle licenze" a pagina 68.
Allocare le licenze	Allocare le licenze all'interno dell'organizzazione per tenere traccia della proprietà e della distribuzione delle licenze stesse. Non è possibile allocare le licenze a dispositivi o dati demografici (siti, reparti e centri di costo). Per informazioni, vedere "Allocazione delle licenze" a pagina 75.

Gestione della configurazione

ZENworks Configuration Management consente di gestire la configurazione di un dispositivo, incluse la distribuzione del software nel dispositivo, l'applicazione delle policy di configurazione di Windows, l'imaging e l'applicazione di immagini. Inoltre, è possibile raccogliere dati dell'inventario hardware e software a supporto delle decisioni relative a upgrade e acquisti e accedere da remoto ai dispositivi per individuare e risolvere problemi.

È possibile eseguire i task elencati di seguito a seconda delle necessità e in qualsiasi ordine.

Task	Dettagli
Attivare Configuration Management	Se Configuration Management non è stato attivato durante l'installazione della zona di gestione, specificando una chiave di licenza o attivando una licenza di valutazione, è necessario eseguire questa operazione prima di utilizzare il prodotto. Per informazioni, vedere "Attivazione di Configuration Management" a pagina 77.

Task	Dettagli
Abilitare ZENworks Agent per l'esecuzione di operazioni di gestione della configurazione	Affinché ZENworks Agent esegua operazioni di gestione della configurazione su un dispositivo, è necessario abilitare le funzioni dell'agente appropriate. Tali funzioni (Gestione pacchetti, Gestione delle immagini, Gestione policy, Gestione remota e Gestione utenti) sono abilitate per default quando viene attivato ZENworks Configuration Management (licenza completa o di valutazione). È necessario accertarsi che le funzioni siano abilitate. Oppure, se non si desidera utilizzare determinate funzioni, è possibile disabilitarle. Per informazioni, vedere “Abilitazione di Configuration Management in ZENworks Agent” a pagina 78.
Registrare dispositivi mobili	Per abilitare le operazioni di gestione della configurazione nei dispositivi mobili, come la distribuzione di pacchetti, l'applicazione di policy di sicurezza e varie operazioni di gestione del dispositivo, è necessario registrare i dispositivi mobili nella zona di gestione ZENworks. Per ulteriori informazioni, vedere ZENworks Mobile Management Reference (in lingua inglese).
Distribuire il software	Distribuire il software nei pacchetti. Nei pacchetti sono inclusi i file software e le istruzioni per l'installazione, l'avvio e la disinstallazione (se necessaria) del software. È possibile creare i pacchetti per distribuire applicazioni di Windows Installer (MSI e MSP), applicazioni non appartenenti a Windows Installer, collegamenti Web e applicazioni thin client, applicazioni Linux e applicazioni Macintosh. Per informazioni, vedere “Distribuzione del software” a pagina 78.
Applicare norme	Controllare il comportamento del dispositivo tramite l'applicazione delle policy. ZENworks consente di creare e applicare policy di gruppo Windows, policy del profilo comune, policy dei segnalibri del browser, policy della stampante e altre ancora. Per informazioni, vedere “Applicazione delle policy” a pagina 80.
Prendere immagini e applicare immagini ai dispositivi	Creare immagini dei dispositivi, applicare le immagini ai dispositivi ed eseguire script di imaging sui dispositivi. ZENworks Configuration Management utilizza la rispettiva funzionalità Servizi di preavvio per eseguire i task di imaging sui dispositivi al momento dell'avvio. Per informazioni, vedere “Dispositivi di imaging” a pagina 83.
Eseguire la scansione dei dispositivi per creare un inventario software e hardware	Eseguire la scansione dei dispositivi per creare inventari software e hardware per i dispositivi stessi. Le informazioni sull'inventario sono di ausilio per prendere decisioni in merito alla distribuzione del software e agli aggiornamenti hardware. Per informazioni, vedere “Raccolta dell'inventario software e hardware” a pagina 100.

Endpoint Security Management

ZENworks Endpoint Security Management consente di proteggere i dispositivi applicando le impostazioni di sicurezza tramite le policy. È possibile controllare l'accesso di un dispositivo a dispositivi di memorizzazione rimovibili, reti wireless e applicazioni. Inoltre, è possibile proteggere i dati mediante cifratura e la comunicazione in rete tramite l'applicazione di firewall (porte, protocolli ed elenchi di controlli dell'accesso). nonché modificare la sicurezza di un dispositivo endpoint in base alla relativa ubicazione.

È necessario eseguire i task seguenti nell'ordine in cui sono elencati.

Task	Dettagli
Attivare Endpoint Security Management	Se Endpoint Security Management non è stato attivato durante l'installazione della zona di gestione, specificando una chiave di licenza o attivando la licenza di valutazione, è necessario attivarlo prima di utilizzare il prodotto. Per informazioni, vedere “Attivazione di Endpoint Security Management” a pagina 113.
Abilitare l'agente Endpoint Security	L'agente Endpoint Security applica policy di sicurezza ai dispositivi. Deve essere installato e abilitato su tutti i dispositivi nei quali si intende distribuire le policy di sicurezza. Per informazioni, vedere “Abilitazione dell'agente di sicurezza endpoint” a pagina 114.
Crea ubicazioni	Le policy di sicurezza possono essere globali o specifiche di un'ubicazione. Una policy globale è valida per tutte le ubicazioni. Una policy basata sull'ubicazione viene applicata solo quando Endpoint Security Agent determina che l'ambiente di rete del dispositivo corrisponde a quello definito per l'ubicazione. Se si desidera utilizzare policy basate sull'ubicazione, è necessario creare delle ubicazioni. Per informazioni, vedere “Creazione delle ubicazioni” a pagina 114.
Creare policy di sicurezza	Le impostazioni di sicurezza di un dispositivo vengono configurate mediante le policy di sicurezza. È possibile creare 11 tipi di policy di sicurezza. Per informazioni, vedere “Creazione di una policy di sicurezza” a pagina 115.
Assegnare policy a utenti e dispositivi	È possibile assegnare le policy a utenti o a dispositivi. Per informazioni, vedere “Assegnazione di una policy agli utenti e ai dispositivi” a pagina 117.

Task	Dettagli
Assegnare policy alle zone	Per garantire che un dispositivo sia sempre protetto, è possibile definire policy di sicurezza di default per ciascun tipo di policy assegnando le policy alla zona. Una policy assegnata a una zona viene applicata quando un dispositivo non è coperto da una policy assegnata all'utente o al dispositivo. Per informazioni, vedere “Assegnazione di una policy alla zona” a pagina 118.

FDE (Full Disk Encryption)

ZENworks Full Disk Encryption protegge i dati di un dispositivo da tentativi di accesso non autorizzati quando il dispositivo è spento o in modalità ibernazione. Per garantire la protezione dei dati viene eseguita la cifratura dell'intero disco o dell'intera partizione, inclusi i file temporanei, i file di scambio e il sistema operativo. Non è possibile accedere ai dati fino a quando un utente autorizzato non esegue il login e non è possibile accedere mai avviando il dispositivo da supporti come CD/DVD, dischi floppy o unità USB. Per un utente autorizzato, l'accesso ai dati sul disco cifrato non è diverso da quello ai dati sul disco non cifrato.

È necessario eseguire i task seguenti nell'ordine in cui sono elencati.

Task	Dettagli
Attivare Full Disk Encryption	Se Full Disk Encryption non è stato attivato durante l'installazione della zona di gestione, specificando una chiave di licenza o attivando la licenza di valutazione, è necessario attivarlo prima di utilizzare il prodotto. Per informazioni, vedere “Attivazione di Full Disk Encryption” a pagina 121.
Abilitare l'agente Full Disk Encryption	L'agente Full Disk Encryption esegue la cifratura del disco. È necessario installarlo e attivarlo su ogni dispositivo di cui si desidera cifrare i dischi. Per informazioni, vedere “Abilitazione dell'agente FDE (Full Disk Encryption)” a pagina 122.
Creare una policy di cifratura del disco	Le informazioni necessarie alla cifratura dei dischi di un dispositivo sono passate all'agente Full Disk Encryption mediante una policy Disk Encryption. È necessario creare almeno una policy. Per informazioni, vedere “Creazione di una policy di cifratura del disco” a pagina 122.
Assegnare la policy ai dispositivi	È possibile assegnare le policy di cifratura dei dischi solo a dispositivi, gruppi di dispositivi o cartelle dispositivo. Per informazioni, vedere “Assegnazione della policy ai dispositivi” a pagina 123.

Gestione delle patch

ZENworks Patch Management consente di automatizzare il processo di valutazione delle vulnerabilità del software e applicazione di patch per eliminarle.

È necessario eseguire i task seguenti nell'ordine in cui sono elencati.

Task	Dettagli
Attivare Patch Management	Se Patch Management non è stato attivato durante l'installazione della zona di gestione, specificando una licenza di sottoscrizione o attivando la licenza di valutazione, è necessario attivare il prodotto. Per informazioni, vedere “Attivazione di Gestione patch” a pagina 130.
Abilitare ZENworks Agent per l'esecuzione di operazioni di gestione patch	Affinché ZENworks Agent esegua operazioni di gestione patch su un dispositivo, è necessario abilitare la funzione Gestione patch. La funzione Gestione patch è abilitata per default quando ZENworks Patch Management è attivato (licenza completa o di valutazione). È necessario verificare che la funzione Gestione patch dell'agente sia abilitata. Per informazioni, vedere “Abilitazione di Patch Management in ZENworks Agent” a pagina 130.
Avviare il servizio di sottoscrizione	È necessario avviare il servizio di sottoscrizione su un server ZENworks. Questo server effettua il download delle patch e le replica su altri server ZENworks (se sono disponibili più server). Per informazioni, vedere “Avvio del servizio di sottoscrizione patch” a pagina 131.
Creare policy patch	Una volta che il servizio di sottoscrizione ha eseguito il download delle patch, applicare quelle desiderate. Per informazioni, vedere “Creazione di policy patch” a pagina 131.

8 Gestione delle risorse

Le sezioni seguenti forniscono spiegazioni e istruzioni su come utilizzare ZENworks Asset Management per raccogliere dati di inventario software e hardware dai dispositivi, monitorare l'uso del software nei dispositivi e controllare la conformità delle licenze software.

Attivazione di Asset Management

Se Asset Management non è stato attivato durante l'installazione della zona di gestione, specificando una chiave di licenza o attivando la licenza di valutazione, effettuare le seguenti operazioni:

1. Nel Centro di controllo ZENworks, fare clic su **Configurazione**.
2. Nel pannello Licenze fare clic su **ZENworks 2020 Asset Management**.
3. Selezionare Valuta/attiva prodotto, quindi completare i seguenti campi:

   Utilizza valutazione: selezionare questa opzione per abilitare un periodo di valutazione di 60 giorni. Dopo il periodo di 60 giorni, è necessario applicare una chiave di licenza per continuare a utilizzare il prodotto.

   Chiave di licenza del prodotto: specificare la chiave di licenza acquistata per Asset Management. Per acquistare una licenza del prodotto, visitare il sito dei prodotti ZENworks Asset Management (http://www.novell.com/products/zenworks/assetmanagement).
4. Fare clic su **OK**.

Abilitazione di Asset Management in ZENworks Agent

Affinché ZENworks Agent esegua operazioni di gestione risorse su un dispositivo, è necessario abilitare la funzione Gestione risorse. La funzione Gestione risorse viene abilitata per default al momento dell'attivazione di ZENworks Asset Management (licenza completa o di valutazione).

È necessario accertarsi che la funzione Gestione risorse dell'agente sia abilitata. Inoltre, se si desidera controllare le licenze software a fronte degli utenti (anziché solo a fronte dei dispositivi), è necessario abilitare la funzione Gestione utenti disabilitata per default. Per informazioni, vedere “Configurazione delle funzioni dell'agente ZENworks” a pagina 39.

Nota: dopo aver abilitato il modulo ZENworks Asset Management, assicurarsi di effettuare una scansione completa su tutti i dispositivi eseguendo il comando `zac inv -f scannow`. Fino a quando non si esegue la scansione, il rapporto di gestione risorse non sarà preciso.

Raccolta dell'inventario software e hardware

Durante l'inventario di un dispositivo, ZENworks Asset Management raccoglie dal dispositivo sia le informazioni sul software che sull'hardware. Dal Centro di controllo ZENworks è possibile visualizzare l'inventario di un singolo dispositivo oppure è possibile generarlo per più dispositivi in base a criteri specifici.

È possibile utilizzare l'inventario software per vari scopi, come per controllare l'utilizzo di applicazioni specifiche e verificare che le licenze a disposizione siano sufficienti per tutte le copie dell'applicazione in uso. Ad esempio, si supponga che una società disponga di 50 licenze di un software di elaborazione di testo. Poiché dall'inventario software risulta che il software è installato su 60 dispositivi, non è rispettata la conformità al contratto di licenza. Tuttavia, dopo aver visualizzato l'utilizzo del software negli ultimi 6 mesi, è possibile constatare che l'utilizzo effettivo del software riguarda solo 45 dispositivi. Per conformarsi al contratto di licenza, disinstallare il software dai 15 dispositivi che non lo utilizzano.

Anche l'inventario hardware viene utilizzato per molteplici scopi, come per verificare che l'hardware in uso soddisfi i requisiti necessari per l'esecuzione di determinati software. Ad esempio, si supponga che il reparto contabilità desideri eseguire il roll-out di una nuova versione del software per la contabilità. Il nuovo software presenta maggiori requisiti per il processore, la memoria e lo spazio su disco. Mediante l'inventario hardware raccolto dai dispositivi, è possibile creare due rapporti: in uno vengono elencati i dispositivi che soddisfano i requisiti e nell'altro quelli che non lo fanno. In base ai rapporti, si distribuisce il software ai dispositivi compatibili e si crea un piano di aggiornamento per i dispositivi che non lo sono.

Per default, i dispositivi vengono sottoposti a scansione alle ore 01.00, il primo giorno del mese. È possibile modificare la pianificazione e altre impostazioni di configurazione di **Inventario** nella scheda **Configurazione** del Centro di controllo ZENworks.

Le seguenti sezioni forniscono le istruzioni per avviare la scansione di un dispositivo e utilizzare l'inventario raccolto.

- “Avvio di una scansione del dispositivo” a pagina 66
- “Visualizzazione dell'inventario dei dispositivi” a pagina 67
- “Generazione di un rapporto sull'inventario” a pagina 67
- “Ulteriori informazioni” a pagina 67

Avvio di una scansione del dispositivo

È possibile avviare la scansione di un dispositivo in qualsiasi momento.

1. Nel Centro di controllo ZENworks, fare clic sulla scheda **Dispositivi**.
2. Scorrere la cartella `Server` o `Workstation` fino a individuare il dispositivo da sottoporre a scansione.
3. Fare clic sul dispositivo per visualizzarne i dettagli.

4 Nell'elenco dei task situato nel pannello di navigazione a sinistra, fare clic su **Scansione inventario server** o **Scansione inventario workstation** per avviare la scansione.

   Nella finestra di dialogo Stato task rapidi viene visualizzato lo stato del task. Al completamento del task, è possibile fare clic sulla scheda **Inventario** per visualizzare i risultati della scansione.

Per eseguire contemporaneamente la scansione di più dispositivi, è possibile aprire la cartella in cui si trovano i dispositivi, selezionare le caselle di controllo accanto ai dispositivi e quindi fare clic su **Task rapidi** > **Scansione inventario**.

È possibile anche usare il comando `inventory-scan-now` nell'utility zman per eseguire la scansione di un dispositivo. Per ulteriori informazioni, vedere "Comandi per l'inventario" nel *Riferimento per le utility da riga di comando di ZENworks*.

Visualizzazione dell'inventario dei dispositivi

1 Nel Centro di controllo ZENworks, fare clic sulla scheda **Dispositivi**.

2 Passare alla cartella `Server` o `Workstation` e individuare il dispositivo di cui si desidera visualizzare l'inventario.

3 Fare clic sul dispositivo per visualizzarne i dettagli.

4 Fare clic sulla scheda **Inventario**.

   Nella pagina Inventario è disponibile un riepilogo dell'inventario hardware. Per visualizzare le informazioni dettagliate sull'inventario, fare clic su **Inventario software/hardware dettagliato**.

Generazione di un rapporto sull'inventario

ZENworks Asset Management include diversi rapporti standard. È inoltre possibile creare dei rapporti personalizzati per fornire viste diverse delle informazioni sull'inventario.

1 Nel Centro di controllo ZENworks, fare clic sulla scheda **Rapporti**.

2 Nel pannello Rapporti standard inventario, fare clic su **Applicazioni software**.

3 Fare clic sul rapporto **Sistema operativo** per generare il rapporto.

   Utilizzando le opzioni riportate in fondo al rapporto è possibile salvare il rapporto generato come foglio di calcolo Microsoft Excel, file CSV (con valori separati da virgole), file PDF o file grafico PDF.

Ulteriori informazioni

Per ulteriori informazioni sull'inventario, vedere *ZENworks Asset Inventory Reference* (Riferimento per ZENworks Asset Inventory).

Monitoraggio dell'utilizzo del software

Una volta effettuato l'inventario dei dispositivi, è possibile eseguire i rapporti per visualizzare in quale misura vengono utilizzate le applicazioni dei dispositivi. ZENworks Asset Management include rapporti standard relativi all'utilizzo delle applicazioni suddivisi per prodotto, utente e dispositivo. È

altresì possibile personalizzare i rapporti per fornire informazioni più dettagliate o circoscritte. Ad esempio, in Gestione risorse è disponibile un rapporto personalizzato predefinito che mostra che l'applicazione non è stata utilizzata negli ultimi 90 giorni.

Per eseguire un rapporto che illustri in quale misura viene utilizzata un'applicazione specifica:

1. Nel Centro di controllo ZENworks fare clic sulla scheda **Gestione risorse**, quindi fare clic sulla scheda **Utilizzo software**.
2. Nel pannello Rapporti standard sull'uso del software, fare clic su **Utilizzo applicazione** per visualizzare l'elenco di rapporti sull'utilizzo delle applicazioni.
3. Nel pannello fare clic su **Utilizzo locale applicazione per prodotto**.

   Il rapporto mostra tutti i prodotti, raggruppati per produttore, installati sui dispositivi.
4. Individuare il produttore di cui si desidera visualizzare i prodotti, quindi fare clic sul numero nella colonna Installazioni per visualizzare i prodotti installati.

   Nel rapporto che ne risulta, è riportato il numero attuale di installazioni per ciascun prodotto, il numero di installazioni utilizzate, la data dell'ultimo utilizzo e altre informazioni correlate.
5. Per modificare l'intervallo del rapporto e l'elenco dei prodotti visualizzati (tutti i prodotti, i prodotti utilizzati o quelli non utilizzati), fare clic su **Modifica intervallo/filtri** in fondo al rapporto.

Sono disponibili molti altri rapporti personalizzati standard e predefiniti da utilizzare a piacere. Per ulteriori informazioni sull'utilizzo dell'applicazione, vedere “Reports” in *ZENworks Asset Management Reference* (in lingua inglese).

Verifica della conformità delle licenze

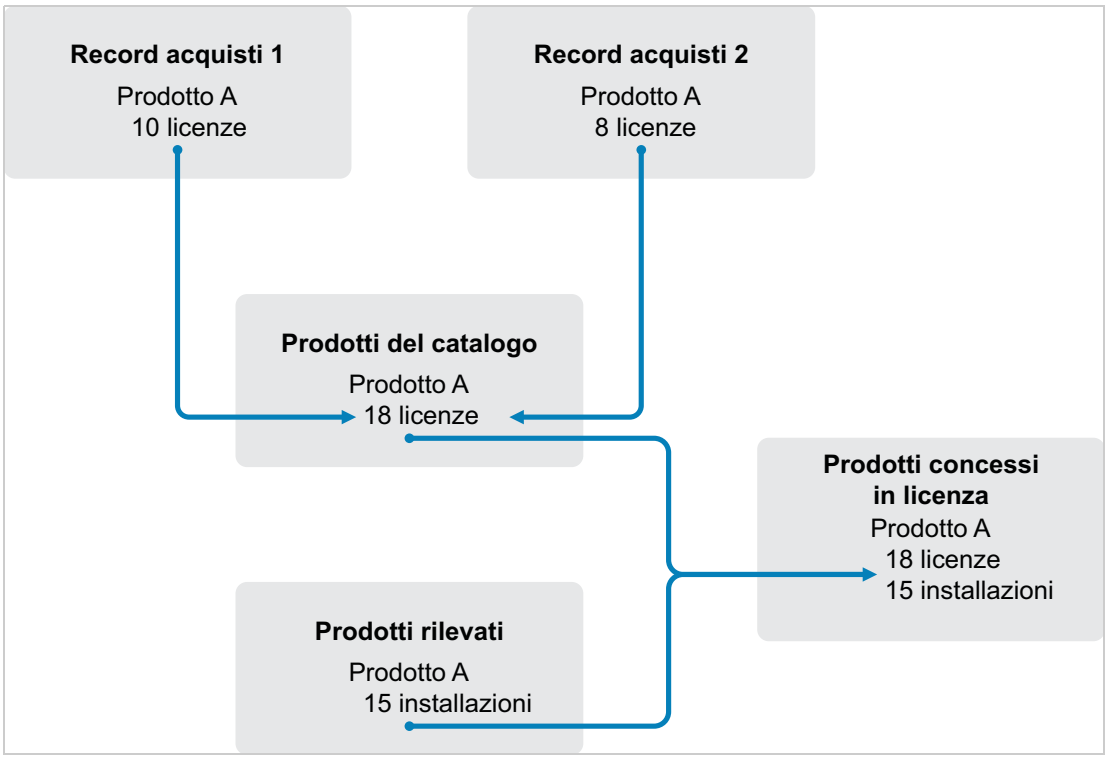
ZENworks Asset Management consente di controllare la conformità dell'organizzazione ai contratti di licenza software confrontando le licenze software acquistate con le attuali installazioni software rilevate durante le scansioni dell'inventario.

La conformità licenze di Gestione risorse rappresenta uno strumento avanzato e flessibile. Di conseguenza, quando si configura la conformità licenze sono disponibili più approcci e metodi. Nelle sezioni seguenti vengono fornite istruzioni di base con spiegazioni minime per consentire all'utente di configurare rapidamente un singolo prodotto per il controllo della conformità licenze. Al termine di questo scenario di base, vedere “Conformità licenze” nel *Riferimento per ZENworks Asset Management* per informazioni e istruzioni più dettagliate.

Componenti della conformità delle licenze

Prima di iniziare a implementare la verifica della conformità, è necessario conoscere i componenti coinvolti e come funzionano insieme, come spiegato nell'illustrazione seguente e nel testo successivo.

Figura 8-1 *Componenti della conformità delle licenze*



- Eseguire la scansione della zona di gestione per raccogliere l'elenco dei prodotti software installati, denominati *prodotti rilevati*. Nell'illustrazione riportata sopra, la scansione dell'inventario ha rilevato che il prodotto A è installato su 15 dispositivi.
- Creare i *prodotti del catalogo* per rappresentare i prodotti software acquistati dall'organizzazione. Di norma, ciascun prodotto del catalogo corrisponde a un numero parte di un produttore specifico. Nell'illustrazione riportata sopra, il prodotto A è l'unico prodotto del catalogo. Tuttavia, è possibile disporre di prodotti del catalogo per il prodotto A, per l'upgrade del prodotto A e per il prodotto B.
- Creare i *record acquisti* per rappresentare le fatture o gli ordini di acquisto relativi ai prodotti software. Ciascun elemento di riga nel record acquisti elenca un prodotto catalogo insieme alla quantità di acquisto delle licenze. Se un prodotto del catalogo è elencato in più record acquisti, il totale delle licenze del prodotto del catalogo equivale alla quantità di acquisto relativa a entrambi i record. Nell'illustrazione riportata sopra, un record acquisti comprende 10 licenze del prodotto A e un altro record ne comprende 8. Il numero totale di licenze del prodotto A è 18.
- Creare i *prodotti concessi in licenza* e associarvi i prodotti rilevati e i prodotti del catalogo corrispondenti. In tal modo si ottiene un unico prodotto concesso in licenza che include il numero di licenze e installazioni del prodotto. È quindi possibile visualizzare rapidamente se

l'utilizzo del prodotto è conforme o no al contratto di licenza. Nell'illustrazione riportata sopra, il prodotto A dispone di 18 licenze ed è installato su 15 dispositivi, quindi è conforme al contratto di licenza.

Rilevamento dei prodotti installati

Se non è ancora stata eseguita la scansione dei dispositivi nella zona di gestione per raccogliere informazioni sui prodotti installati (indicati come **prodotti rilevati**), completare i passaggi descritti nella "Raccolta dell'inventario software e hardware" a pagina 66.

Dopo aver rilevato i prodotti, scegliere quello di cui si desidera controllare la conformità.

1. Nel Centro di controllo ZENworks fare clic sulla scheda **Gestione risorse**, quindi fare clic sulla scheda **Gestione licenze**.
2. Nel pannello Gestione licenze fare clic su **Prodotti rilevati** per visualizzare l'elenco corrispondente.
3. Sfogliare l'elenco per scegliere il prodotto rilevato da utilizzare.

   Il prodotto deve avere almeno un'installazione elencata nella colonna **Quantità installata**. Se possibile, scegliere un prodotto il cui ordine di acquisto o la cui fattura è a portata di mano. In questo modo, è possibile completare lo scenario utilizzando informazioni reali. In alternativa, è possibile inventare le informazioni di acquisto mentre si procede. Annotare il prodotto scelto, in modo da poterlo utilizzare in seguito.
4. Proseguire con la sezione successiva, "Creazione di un prodotto catalogo e di un record acquisti" a pagina 70.

Creazione di un prodotto catalogo e di un record acquisti

I prodotti rilevati forniscono le informazioni di installazione per i prodotti. Per fornire informazioni sugli acquisti di prodotti, creare prodotti catalogo e record acquisti.

Un prodotto catalogo rappresenta un prodotto software. Un record acquisti popola il prodotto catalogo con il numero delle licenze di prodotto acquistate.

Di seguito viene spiegato come creare un prodotto catalogo e un record acquisti per il prodotto rilevato scelto nella "Rilevamento dei prodotti installati" a pagina 70.

1. Nel Centro di controllo ZENworks fare clic sulla scheda **Gestione risorse**, quindi fare clic sulla scheda **Gestione licenze**.
2. Creare il prodotto catalogo:
   - **2a** Nel riquadro Gestione licenze, fare clic su **Prodotti catalogo**.
   - **2b** Fare clic su **Nuovo** > **Prodotto catalogo** per avviare la Creazione guidata del nuovo prodotto catalogo.
   - **2c** Immettere le informazioni nei campi:

     Produttore: selezionare il produttore software dall'elenco. Se il produttore corretto non è elencato, digitare il nome del produttore (ad esempio, Novell, Symantec o Microsoft).

Prodotto: digitare il nome del prodotto, Il prodotto dovrebbe rappresentare il pacchetto del prodotto software (SKU, Software Product Package) acquistato. Ad esempio, il pacchetto acquistato potrebbe essere la singola licenza del prodotto A o il pacchetto 10 del prodotto A. Se si dispone di un record fatture che include il prodotto per il quale si desidera creare il prodotto catalogo, utilizzare il nome del prodotto riportato sulla fattura.

Licenze per pacchetto: specificare il numero di licenze incluse nel pacchetto del prodotto.

Tipo di prodotto - Note: questi campi sono opzionali. È possibile utilizzarli per identificare ulteriormente il prodotto.

Escluso: non selezionare questa casella di controllo.

2d Fare clic su **Avanti** per visualizzare la pagina Riepilogo, quindi fare clic su **Fine** per aggiungere il prodotto all'elenco Prodotti catalogo.

2e Fare clic su **Gestione licenze** (nel percorso nella parte superiore della pagina) per tornare alla pagina Gestione licenze.

3 Creare il record acquisti:

3a Nel pannello Gestione licenze, fare clic su **Record di acquisto**.

3b Fare clic su **Nuovo** > **Record acquisti** per avviare la Creazione guidata del nuovo record acquisti.

3c Immettere le informazioni nei campi.

Numero di ordine: specificare il numero dell'ordine di acquisto o della fattura associato al prodotto software acquistato. Se non si dispone dell'ordine di acquisto o della fattura del prodotto, utilizzare un numero qualsiasi.

Data ordine: selezionare la data di acquisto del software.

Destinatario - Rivenditore: questi campi sono opzionali. È possibile utilizzarli per identificare ulteriormente il record acquisti.

3d Fare clic su Avanti per visualizzare la pagina Riepilogo.

3e Selezionare la casella **Definisci proprietà aggiuntive**, quindi fare clic su **Fine** per creare il record acquisti e visualizzare la rispettiva pagina Dettagli acquisto.

3f Fare clic su **Aggiungi** per visualizzare la finestra di dialogo Aggiungi dettaglio acquisto, quindi compilare i seguenti campi:

Prodotto: fare clic su  per selezionare il prodotto catalogo creato nel Passo 2.

Quantità: specificare la quantità di prodotto acquistata. Ad esempio, se il prodotto del catalogo selezionato è Prodotto A da 10 pacchetti e nell'ordine di acquisto era visualizzato 5 Prodotto A da 10 pacchetti, specificare 5.

Prezzo unitario consigliato - Prezzo ampliato: questi campi sono obbligatori. Specificare il prezzo al dettaglio consigliato dal produttore, il prezzo pagato per unità e il prezzo massimo. Se si lascia vuoto il campo **Prezzo massimo**, la procedura guidata lo popolerà moltiplicando **Quantità acquisto** e**Prezzo unitario**.

N. fattura - Commenti: questi campi sono opzionali. È possibile utilizzarli per identificare ulteriormente l'acquisto.

3g Fare clic su **OK**.

4 Proseguire con la sezione successiva, “Creazione di un prodotto concesso in licenza”.

In Gestione risorse le informazioni di acquisto possono essere importate anche da file elettronici. Durante il processo, vengono creati il record acquisti e tutti i prodotti catalogo per i prodotti software inclusi nel record acquisti. Per ulteriori informazioni, vedere "Conformità licenze" nel *Riferimento per ZENworks Asset Management*.

Creazione di un prodotto concesso in licenza

Il passaggio finale del processo di configurazione della conformità per il prodotto software consiste nel creare un prodotto concesso in licenza e nell'associarlo al prodotto rilevato e al prodotto catalogo. In questo modo, il prodotto concesso in licenza viene popolato con le informazioni su installazione e licenze necessarie per determinare il relativo stato di conformità licenze.

Nei passaggi seguenti viene spiegato come utilizzare la procedura guidata Sincronizzazione automatica per creare il prodotto concesso in licenza e associarlo al prodotto rilevato e al prodotto catalogo.

1. Nel Centro di controllo ZENworks fare clic sulla scheda **Gestione risorse**, quindi fare clic sulla scheda **Gestione licenze**.
2. Nel pannello Gestione licenze, fare clic su **Prodotti con licenza**.
3. Nel pannello Prodotti con licenza, fare clic su **Azione > Riconciliazione automatica: crea prodotti con licenza** per avviare la procedura guidata Riconciliazione automatica. Completare la procedura guidata compilando i campi con le informazioni incluse nella seguente tabella.

Pagina della procedura guidata	Dettagli
Filtro prodotti rilevati	Con la procedura guidata Sincronizzazione automatica vengono creati prodotti concessi in licenza a partire dai prodotti rilevati esistenti. Per trovare il prodotto rilevato: 1. Fare clic sull'opzione **Prodotti specificati sotto**. 2. Nell'elenco **Seleziona** selezionare il produttore del prodotto rilevato. 3. Nel campo **Prodotto** immettere il nome del prodotto rilevato.
Seleziona prodotti concessi in licenza da creare	In base alle informazioni specificate nella pagina Filtro prodotti rilevati, in questa pagina dovrebbero essere visualizzati il prodotto rilevato e il prodotto concesso in licenza che verrà creato per esso. La procedura guidata tenta di abbinare i prodotti catalogo al prodotto rilevato confrontando i campi relativi a produttore e prodotto. Se la procedura guidata è in grado di abbinare il prodotto catalogo creato al prodotto rilevato, anche il prodotto catalogo comparirà nell'elenco. Selezionare il prodotto catalogo per associarlo al prodotto concesso in licenza. Se la procedura guidata non è in grado di abbinare il prodotto catalogo al prodotto rilevato, sarà necessario assegnare manualmente il prodotto catalogo al termine della procedura guidata.

Pagina della procedura guidata	Dettagli
Cartella di destinazione	Selezionare la cartella in cui posizionare il nuovo prodotto concesso in licenza. Per default, il campo viene impostato sulla cartella corrente (ovvero la cartella da cui è stata avviata la procedura guidata Sincronizzazione automatica). Per specificare un'altra cartella, fare clic su , individuare la cartella e selezionarla. La cartella deve esistere già perché non è possibile utilizzare la finestra di dialogo per creare una nuova cartella.
Autorizzazioni licenze	Ogni prodotto concesso in licenza deve disporre di almeno un modello di autorizzazione e licenza. Un'autorizzazione in genere rappresenta un contratto di licenza. In molti casi, un prodotto concesso in licenza potrebbe disporre di un'unica autorizzazione. Tuttavia, concedendo più autorizzazioni è possibile determinare la conformità per un prodotto concesso in licenza con più contratti di licenza. Ad esempio, è possibile disporre di un contratto di licenza completo e di un contratto di licenza di upgrade per lo stesso prodotto. Anziché creare due prodotti concessi in licenza per lo stesso prodotto, si creerà un unico prodotto concesso in licenza con due autorizzazioni diverse. Il modello di licenza determina il modo in cui vengono conteggiate le licenze. Le licenze possono essere conteggiate per installazione, utente o dispositivo. Per questo scenario, specificare **Per installazione** come descrizione e selezionare **Per installazione** come modello di licenza. Con queste impostazioni, ogni installazione del prodotto utilizzerà una licenza.
Riepilogo creazione sincronizzazione automatica	Rivedere i dati.

4 Se non è ancora stata eseguita questa operazione, fare clic su **Fine** per creare il prodotto concesso in licenza e aggiungerlo all'elenco Prodotti concessi in licenza.

5 Se la procedura guidata Sincronizzazione automatica non è in grado di associare il prodotto catalogo al prodotto concesso in licenza:

5a Fare clic sul prodotto concesso in licenza.

5b Fare clic sulla scheda **Autorizzazioni licenze**.

5c Nel pannello Autorizzazioni fare clic sull'autorizzazione.

5d Fare clic sulla scheda **Prova di proprietà**.

5e Nel riquadro Prodotti catalogo, fare clic su **Aggiungi**.

5f Selezionare il prodotto catalogo, quindi fare clic su **OK** per aggiungerlo al pannello Prodotti catalogo.

Nel pannello Prodotti catalogo vengono visualizzate la Quantità acquisto del prodotto catalogo, ovvero il numero di unità del prodotto catalogo acquistate (in base al record acquisti), nonché la quantità licenze, ovvero il numero totale di licenze incluse nelle unità acquistate.

6 Passare alla sezione successiva Visualizza dati di conformità, per informazioni sulla verifica della conformità.

Visualizza dati di conformità

Per verificare lo stato di conformità dei prodotti concessi in licenza sono disponibili due viste. Nella pagina Prodotti concessi in licenza è possibile visualizzare il riepilogo dello stato di conformità di tutti i prodotti oppure è possibile generare il Rapporto di conformità del software per ottenere informazioni più dettagliate.

- "Visualizzazione del riepilogo dello stato di conformità" a pagina 74
- "Generazione del Rapporto di conformità del software" a pagina 74

Visualizzazione del riepilogo dello stato di conformità

1 Nel Centro di controllo ZENworks fare clic sulla scheda **Gestione risorse**, quindi fare clic sulla scheda **Gestione licenze**.

2 Nel pannello Gestione licenze, fare clic su **Prodotti concessi in licenza** per visualizzare la pagina corrispondente.

Nell'elenco Prodotti concessi in licenza sono visualizzati tutti i prodotti concessi in licenza e il rispettivo stato di conformità attuale:

- Il numero di licenze del prodotto software è corretto. Il numero delle licenze acquistate equivale al numero di installazioni.
- Il numero di licenze del prodotto software è eccessivo. Il numero di licenze acquistate è maggiore del numero di installazioni.
- Il numero di licenze del prodotto software è insufficiente. Il numero di licenze acquistate è inferiore al numero di installazioni.

Generazione del Rapporto di conformità del software

1 Nel Centro di controllo ZENworks fare clic sulla scheda **Gestione risorse**, quindi fare clic sulla scheda **Gestione licenze**.

2 Nel pannello Gestione licenze, fare clic su **Gestione licenze**.

3 Nel pannello Rapporti standard di Gestione licenze, fare clic su **Conformità del software**.

4 Nel pannello fare clic su **Rapporto di conformità**.

Viene visualizzato un report che visualizza i dati di conformità per licenza. È possibile filtrare i dati per stato di conformità, costruttore e valore, oppure per criteri demografici. Esaminare **Quantità licenze** per verificare i dati di conformità per un determinato prodotto. Per ulteriori informazioni vedere *ZENworks Asset Management Reference* (in lingua inglese).

Ulteriori informazioni

Lo scenario descritto nelle sezioni precedenti mostra solo una piccola parte delle funzionalità di conformità licenze disponibili in ZENworks Asset Management. Per ulteriori informazioni, vedere "Conformità licenze" nel *Riferimento per ZENworks Asset Management*.

Allocazione delle licenze

ZENworks Asset Management consente di allocare le licenze all'interno dell'organizzazione per tenere traccia della proprietà e della distribuzione delle licenze stesse. Non è possibile allocare le licenze a dispositivi o dati demografici (siti, reparti e centri di costo).

Per *allocazione dispositivo* si intende l'allocazione di una licenza a un dispositivo specifico. Il prodotto può essere installato o meno sul dispositivo. Ad esempio, si sono acquistate 10 licenze di ProdottoA. È possibile allocare le licenze ai dispositivi di destinazione prima che ProdottoA sia installato sui dispositivi.

Un'*allocazione demografica* è l'associazione di una o più licenze a un sito, reparto o centro di costo. Qualsiasi dispositivo assegnato a dati demografici e dove sia installato un prodotto viene visualizzato come un'installazione associata all'allocazione. Ad esempio, si sono acquistate 15 licenze di ProdottoA che vengono allocate al RepartoQ. Vi sono 20 dispositivi assegnati al RepartoQ. Su 12 di questi 20 dispositivi è installato ProdottoA. Di conseguenza, l'allocazione del Reparto Q mostrerà 15 licenze allocate con 12 installazioni.

Nei passaggi seguenti viene spiegato come allocare le licenze ai dispositivi. Per informazioni sull'allocazione delle licenze ai dati demografici, vedere "Allocazione delle licenze" nel *Riferimento ZENworks Asset Management*.

1. Nel Centro di controllo ZENworks, fare clic sulla scheda **Gestione risorse**.
2. Nella pagina Gestione licenze, fare clic su **Prodotti concessi in licenza**.
3. Nell'elenco Prodotti con licenza, fare clic sul prodotto concesso in licenza per il quale si desidera allocare una licenza.
4. Per default, solo l'allocazione dei dispositivi è abilitata per tenere traccia della proprietà per le licenze dei prodotti. Per allocare licenze ai dati demografici, è necessario che un utente abiliti l'allocazione demografica per il prodotto effettuando le operazioni seguenti:
   - **4a** Selezionare la scheda **Generale**.
   - **4b** Nel pannello Impostazioni allocazioni licenze, compilare i seguenti campi:

     Abilita allocazioni demografiche: selezionare questa opzione.

     Tipo di allocazione demografica: tutte le allocazioni demografiche per un prodotto con licenza individuale devono essere dello stesso tipo. Selezionare il tipo (**Sito**, **Reparto**, **Centro di costo**) che si desidera utilizzare per questo prodotto.

     Aggiorna allocazioni licenze con dati demografici provenienti dalle importazioni di record di acquisti futuri: selezionare questa opzione se, quando si importano record acquisti futuri per il prodotto, si desidera aggiornare automaticamente il numero di licenze allocate in base ai dati demografici del record acquisti.

     Ad esempio, si supponga che il prodotto utilizzi allocazioni Reparto. Si importa un record acquisti che include licenze assegnate al RepartoQ. Le licenze sono aggiunte all'allocazione demografica del RepartoQ.

Inoltre, crea nuove allocazioni, se necessario. Ad esempio, se un record acquisti comprende licenze di ProdottoA che non sono assegnate a RepartoZ (un nuovo reparto non elencato nell'allocazione di ProdottoA), viene creata una nuova allocazione per RepartoZ.

Quantità allocata: visualizza il numero totale di licenze allocate ai dispositivi o ai dati demografici.

4c Fare clic su **Applica** per salvare le modifiche.

5 Fare clic sulla scheda **Allocazioni licenze**.

6 (Opzionale) Per visualizzare quali dispositivi dispongono di un prodotto installato ma non dispongono di licenza allocata, fare clic sul valore **Installazioni senza allocazioni** nel pannello Allocazioni dispositivo.

7 Fare clic su **Aggiungi** > **Dispositivi con prodotto installato** se il dispositivo al quale si desidera allocare una licenza dispone del prodotto installato.

oppure

Fare clic su **Aggiungi** > **Qualsiasi dispositivo** se il dispositivo al quale si desidera allocare una licenza non dispone del prodotto installato.

Viene visualizzata la finestra di dialogo Ricerca dispositivo.

8 Nel campo **Tipo di dispositivo**, selezionare se si desidera cercare **Dispositivi gestiti**, **Dispositivi inventariati**, **Dispositivi gestiti o Inventariati**, **Dispositivi ZAM migrati** o **Tutti**.

Se non si è sicuri del tipo di dispositivo, selezionare **Tutti**.

9 Per circoscrivere la ricerca, utilizzare filtri per creare criteri di ricerca.

Se non si creano filtri, tutti i dispositivi (o tutti i dispositivi con il prodotto installato) sono visualizzati, fino al numero di visualizzazione massimo.

10 Specificare il numero massimo di dispositivi da visualizzare nella ricerca.

11 Selezionare la colonna o le colonne che si desidera visualizzare nella finestra di dialogo di ricerca risultante. Per selezionare più campi, fare clic con il mouse e tenere premuto il tasto Ctrl.

12 Fare clic su **Cerca** per visualizzare la finestra di dialogo Seleziona dispositivo, in cui sono elencati i risultati della ricerca.

13 Selezionare i dispositivi ai quali si desidera allocare licenze, quindi fare clic su **OK**.

Vengono visualizzate le seguenti informazioni per ciascuna allocazione:

- **Nome computer, Nome di login e Indirizzo IP:** informazioni standard sul dispositivo, compreso nome di login dell'utente che aveva eseguito il login quando il dispositivo è stato inventariato.
- **Sito, Reparto, Centro di costo:** dati demografici sul dispositivo. Se uno o più campi sono vuoti, i dati inventario del dispositivo non contengono informazioni.
- **Quantità installata:** numero di installazioni del prodotto concesso in licenza sul dispositivo. In genere il valore è 1.
- **Allocazione duplicata:** include un segno di spunta se l'installazione del dispositivo è anche inclusa in un'allocazione demografica.
- **Installazioni senza allocazioni:** visualizza il numero di installazioni alle quali non sono allocate licenze sia tramite allocazione demografica, sia allocazione di dispositivo. Fare clic sul numero per visualizzare l'elenco di installazioni.

9 Gestione della configurazione

Le sezioni seguenti forniscono spiegazioni e istruzioni relative ai task che è possibile eseguire con ZENworks Configuration Management. A seconda dell'ambiente e della funzionalità di che si intende usare, potrebbe non essere necessario sapere come eseguire tutti i task. È possibile rivedere i task di proprio interesse in qualsiasi ordine.

Attivazione di Configuration Management

Se Configuration Management non è stato attivato durante l'installazione della zona di gestione, specificando una chiave di licenza o attivando la licenza di valutazione, completare la procedura seguente:

1. Nel Centro di controllo ZENworks, fare clic su **Configurazione**.
2. Nel pannello Licenze, fare clic su **ZENworks 2020 Configuration Management**.
3. Selezionare Valuta/attiva prodotto, quindi completare i seguenti campi:

   Utilizza valutazione: selezionare questa opzione per abilitare un periodo di valutazione di 60 giorni. Dopo il periodo di 60 giorni, è necessario applicare una chiave di licenza per continuare a utilizzare il prodotto.

   Chiave di licenza del prodotto: specificare la chiave di licenza acquistata per Configuration Management. Per acquistare una licenza del prodotto, visitare il sito dei prodotti Novell ZENworks Configuration Management (http://www.novell.com/products/zenworks/configurationmanagement).
4. Fare clic su **OK**.

Abilitazione di Configuration Management in ZENworks Agent

Affinché ZENworks Agent esegua operazioni di gestione della configurazione su un dispositivo, è necessario abilitare le funzioni dell'agente appropriate. Tali funzioni (Gestione pacchetti, Gestione delle immagini, Gestione policy, Gestione remota e Gestione utenti) sono abilitate per default quando viene attivato ZENworks Configuration Management (licenza completa o di valutazione).

È necessario accertarsi che le funzioni siano abilitate. Oppure, se non si desidera utilizzare determinate funzioni, è possibile disabilitarle. Per informazioni, vedere "Configurazione delle funzioni dell'agente ZENworks" a pagina 39.

Distribuzione del software

ZENworks Configuration Management è estremamente flessibile nella distribuzione del software. È possibile distribuire applicazioni e singoli file; apportare semplicemente modifiche ai file esistenti su un dispositivo; installare, rimuovere ed eseguire il rollback delle applicazioni sui dispositivi.

Il software viene distribuito mediante l'uso di pacchetti. Un pacchetto comprende tutti i file, le impostazioni di configurazione, le istruzioni di installazione, ecc., richiesti per distribuire e gestire l'applicazione o i file su un dispositivo. Quando si assegna un pacchetto a un dispositivo, è possibile installarlo o avviarlo sul dispositivo in base alle pianificazioni (di distribuzione, avvio e disponibilità) definite.

Dal dashboard Pacchetti è inoltre possibile visualizzare il riepilogo dello stato di assegnazione, distribuzione, installazione e avvio del pacchetto. Per ulteriori informazioni, consultare il Riferimento per la distribuzione del software ZENworks.

È possibile creare quattro tipi di pacchetti:

- **Pacchetto aziendale:** consente di configurare e gestire le risorse aziendali sui dispositivi mobili.
- **Pacchetto iOS/iPadOS:** consente di distribuire applicazioni e profili di installazione sui dispositivi iOS e iPadOS. palmari.
- **Pacchetto Linux:** consente di configurare e gestire le applicazioni sui dispositivi Linux.
- **Pacchetto dipendenze Linux:** consente di disporre dei pacchetti software nei dispositivi Linux per la risoluzione delle dipendenze dei pacchetti.
- **Pacchetto Macintosh:** consente di configurare e gestire le applicazioni sui dispositivi Macintosh.
- **Pacchetto di preavvio:** consente di eseguire una serie di task su un dispositivo gestito o non gestito prima dell'avvio del sistema operativo del dispositivo.
- **Pacchetto Windows:** consente di configurare e gestire le applicazioni sui dispositivi Windows.

I pacchetti Android (app di lavoro associate ad Android nell'azienda) e i pacchetti Apple VPP vengono creati automaticamente non appena ZENworks si sincronizza con i rispettivi server Google e Apple. Tuttavia, è possibile creare pacchetti Android o Apple VPP aggiuntivi. Per ulteriori informazioni, consultare Provisioning Applications(in lingua inglese).

Viene effettuato l'upload del software incluso in un pacchetto nell'archivio del server ZENworks. In tal modo si consente al server ZENworks di distribuire il software senza dover accedere ad altre ubicazioni della rete.

Sono disponibili i seguenti video per apprendere le procedure di distribuzione software a dispositivi Windows, Linux e Macintosh:

- Distribuzione del software Windows con ZENworks
- Distribuzione del software Linux con ZENworks
- Gestione Mac con ZENworks: Distribuzione dell'agente
- Gestione Mac con ZENworks: Distribuzione delle applicazioni standardizzata

Creazione di un pacchetto

Per creare un pacchetto software si utilizza la Creazione guidata nuovo pacchetto. Oltre a costituire una guida per la creazione del pacchetto, la procedura guidata consente di assegnare il pacchetto a dispositivi e utenti, nonché di creare pianificazioni per la distribuzione, l'avvio e la disponibilità dello stesso.

1. Nel Centro di controllo ZENworks, fare clic sulla scheda **Pacchetti**.
2. Nel pannello Pacchetti, fare clic su **Nuovo** > **Pacchetto** per avviare la Creazione guidata nuovo pacchetto.
3. Seguire i prompt visualizzati per creare il pacchetto.

   Fare clic sul pulsante della **guida** su ciascuna pagina della procedura guidata per informazioni dettagliate sulla pagina.

   Al termine della procedura guidata, il pacchetto viene aggiunto nel riquadro Pacchetti. È possibile fare clic sul pacchetto per visualizzarne e modificarne i dettagli.
4. Proseguire con la sezione successiva, "Assegnazione di un pacchetto".

È possibile anche usare il comando `bundle-create` nell'utility zman per creare un pacchetto software. Per ulteriori informazioni, vedere "Comandi per i pacchetti" nel *Riferimento per le utility da riga di comando di ZENworks*.

Assegnazione di un pacchetto

Una volta creato il pacchetto, è necessario assegnarlo ai dispositivi nei quali si intende installarlo. È possibile effettuare assegnazioni a dispositivi e utenti.

1. Nel pannello Pacchetti, selezionare il pacchetto da assegnare facendo clic nella casella di controllo corrispondente.
2. Fare clic su **Azione** > **Assegna a dispositivo**.

   oppure

   Fare clic su **Azione** > **Assegna a utente.**
3. Seguire i prompt visualizzati per assegnare il pacchetto.

   Fare clic sul pulsante della **guida** su ciascuna pagina della procedura guidata per informazioni dettagliate sulla pagina.

   Al termine della procedura guidata, i dispositivi o gli utenti a cui è stato assegnato il pacchetto vengono aggiunti alla pagina Relazioni del pacchetto. È possibile fare clic sul pacchetto per visualizzare le assegnazioni.

Inoltre, è possibile utilizzare il comando `bundle-assign` nell'utility zman per assegnare un pacchetto. Per ulteriori informazioni, vedere "Comandi per i pacchetti" nel *Riferimento per le utility da riga di comando di ZENworks*.

Ulteriori informazioni

Per ulteriori informazioni sulla distribuzione del software, consultare la documentazione di riferimento relativa alla *distribuzione del software in ZENworks*.

Per ulteriori informazioni sulla distribuzione delle app ai dispositivi mobili, vedere *ZENworks Mobile Management Reference* (in lingua inglese).

Applicazione delle policy

ZENworks Configuration Management consente di usare criteri per creare un set di configurazioni che possono essere assegnate a un numero qualsiasi di dispositivi gestiti. Ciò è utile per configurare in modo uniforme i dispositivi ed elimina la necessità di configurare singolarmente ciascun dispositivo.

Le policy di ZENworks Configuration Management consentono di gestire i servizi esterni, le impostazioni relative alle policy Puppet, i preferiti di Internet Explorer, le policy di gruppo Windows, i diritti dei file locali, le impostazioni di gestione del risparmio energia C/A, le stampanti, le impostazioni dei servizi SNMP, i profili mobili, configurare gli account degli utenti locali dinamici e gestirli sui dispositivi gestiti. È inoltre possibile configurare il comportamento o l'esecuzione di una sessione di gestione remota sul dispositivo gestito e amministrare e gestire centralmente il comportamento e le funzioni di ZENworks Explorer.

La sezione seguente include l'elenco delle policy di configurazione di Windows che è possibile creare e assegnare a un utente o a un dispositivo gestito.

- **Policy segnalibri browser:** consente di configurare i preferiti di Internet Explorer per i dispositivi e gli utenti di Windows.
- **Policy utente locale dinamiche:** consente di configurare gli utenti creati sulle workstation Windows XP, Windows Vista, Windows 7, e sui terminal server Windows 2003, Windows 2008, Windows 2008 R2 dopo che tali utenti sono stati autenticati in Novell eDirectory.
- **Policy diritti file locali:** consente di configurare i diritti per i file o le cartelle che risiedono nei file system NTFS.

  È possibile utilizzare la policy per configurare le autorizzazioni di base e avanzate per gli utenti e i gruppi locali e di dominio. Con questa funzione un amministratore può creare gruppi personalizzati sui dispositivi gestiti.
- **Policy risparmio energia:** consente di configurare le impostazioni di Risparmio energia sui dispositivi gestiti.

   Video sulla procedura di configurazione di una policy di risparmio energia.
- **Policy stampante:** consente di configurare stampanti locali, SMB, HTTP, TCP/IP, CUPS e iPrint per utenti e dispositivi Windows.

- **Norme di gestione remota:** consente di configurare il comportamento o l'esecuzione di una sessione di gestione remota sul dispositivo gestito. La norma include proprietà quali le operazioni di gestione remota, sicurezza e così via. È possibile assegnare una norma di gestione remota sia a utenti sia a dispositivi gestiti.
- **Norme profilo comune:** consente all'utente di configurare il percorso in cui memorizzare il proprio profilo.

  Un profilo utente contiene informazioni sulle impostazioni desktop e le preferenze personali dell'utente, che vengono mantenute da sessione a sessione.

  Tutti i profili utente archiviati in un percorso di rete vengono chiamati profili comuni. Ogni volta che l'utente esegue il login a un computer, il relativo profilo viene caricato dal percorso di rete. In questo modo l'utente può utilizzare diversi computer mantenendo le impostazioni personali.
- **Policy SNMP:** consente di configurare i parametri SNMP sui dispositivi gestiti.
- **Policy di gruppo Windows:** consente di configurare le norme di gruppo per i dispositivi e gli utenti Windows.
- **Norme di configurazione di ZENworks Explorer:** consente di amministrare e gestire centralmente il comportamento e le funzioni di ZENworks Explorer.

La sezione seguente include l'elenco delle policy di configurazione di Linux che è possibile creare e assegnare a un utente o a un dispositivo gestito.

- **Policy Servizi esterni:** consente di configurare i servizi esterni su un dispositivo Linux gestito per l'archivio YUM, ZYPP o MOUNT. Consente all'amministratore di effettuare il download di pacchetti o aggiornamenti software da tali archivi e installarli sui dispositivi gestiti.
- **Policy Puppet:** specifica come eseguire manifesti e moduli puppet su un dispositivo gestito, come effettuare l'upload dei file degli script e, se è necessario, effettuare un'esecuzione di prova degli script sul dispositivo.

Nella seguente sezione sono elencate le policy applicabili per i dispositivi mobili registrati nella zona.

- **Policy di controllo dispositivo mobile:** consente di concedere o limitare agli utenti l'accesso a varie funzioni di un dispositivo mobile.
- **Policy e-mail per dispositivi mobili:** consente di gestire l'account e-mail aziendale sui dispositivi mobili.
- **Policy di registrazione dispositivo mobile:** indica quali utenti possono registrare i propri dispositivi mobili, quali dispositivi mobili possono registrare gli utenti, la modalità da utilizzare per la registrazione dei dispositivi mobili, nonché l'ubicazione e la denominazione del dispositivo.
- **Policy di sicurezza dispositivo mobile:** configura le restrizioni della password, le impostazioni di cifratura e le impostazioni dell'inattività sui dispositivi.
- **Policy di conformità per dispositivi mobili:** assicura che i dispositivi siano conformi con le regole applicate su di essi.
- **Policy di registrazione di Android per le aziende:** consente agli utenti di registrare i rispettivi dispositivi Android nella modalità profilo di lavoro o nella modalità dispositivo gestito per il lavoro come parte del programma Android per le aziende.
- **Policy di protezione app Intune:** applica restrizioni sulle app Microsoft Intune limitando, ad esempio, le azioni di taglia, copia e incolla e imponendo l'uso di un PIN per l'accesso. È applicabile per i dispositivi iOS, iPadOS e Android.

Creazione di una policy

Per creare una policy è necessario usare la procedura guidata Crea nuove policy. Oltre a costituire una guida per la creazione della policy, la procedura guidata consente di assegnare la policy a dispositivi e utenti, nonché di decidere se applicare la policy immediatamente o attendere che il dispositivo aggiorni le informazioni.

1. Nel Centro di controllo ZENworks, fare clic sulla scheda **Policy**.
2. Nell pannello Policy, fare clic su **Nuovo** > **Policy** per visualizzare la pagina Seleziona piattaforma.
3. Selezionare la categoria di policy, quindi fare clic su **Avanti** per visualizzare la pagina Seleziona categoria di policy.
4. Selezionare la categoria della policy da creare, quindi fare clic su **Avanti**.
5. Selezionare un tipo di policy dall'elenco di policy disponibile. Seguire i prompt visualizzati per creare la policy.

   Fare clic sul pulsante della **guida** su ciascuna pagina della procedura guidata per informazioni dettagliate sulla pagina.

   Al termine della procedura guidata, la norma viene aggiunta nel riquadro Norme. È possibile fare clic sulla norma per visualizzare i dettagli della norma e modificare le assegnazioni.

È possibile anche usare il comando `policy-create` nell'utility zman per creare una norma. Per ulteriori informazioni, vedere "Comandi per le norme" nel *Riferimento per le utility da riga di comando di ZENworks*.

Assegnazione di una policy

Al termine della creazione della policy, è necessario assegnarla ai dispositivi ai quali si desidera applicarla. È possibile effettuare assegnazioni a dispositivi e utenti.

1. Nel pannello Policy, selezionare la policy che si desidera assegnare selezionando la casella di controllo corrispondente.
2. Fare clic su **Azione** > **Assegna a dispositivo**.

   oppure

   Fare clic su **Azione** > **Assegna a utente.**
3. Seguire le istruzioni visualizzate per assegnare la policy.

   Fare clic sul pulsante della **guida** su ciascuna pagina della procedura guidata per informazioni dettagliate sulla pagina.

   Al termine della procedura guidata, i dispositivi o gli utenti a cui è stata assegnata la policy vengono aggiunti nella pagina Relazioni della policy. Fare clic sulla policy per visualizzare le assegnazioni.

È anche possibile utilizzare il comando `policy-assign` nell'utility zman per assegnare una policy. Per ulteriori informazioni, vedere "Comandi per le norme" nel *Riferimento per le utility da riga di comando di ZENworks*.

Ulteriori informazioni

Per ulteriori informazioni sull'applicazione delle policy, vedere *ZENworks Configuration Policies Reference* (in lingua inglese).

Per ulteriori informazioni sull'applicazione delle policy ai dispositivi mobili, vedere *ZENworks Mobile Management Reference* (in lingua inglese).

Dispositivi di imaging

ZENworks Configuration Management comprende un servizio di preavvio che permette di eseguire task sui dispositivi prima dell'avvio del loro sistema operativo. I servizi di preavvio consentono di eseguire automaticamente o manualmente le seguenti operazioni prima dell'avvio di un dispositivo:

- Eseguire gli script di ZENworks Imaging che contengono i comandi da generare al prompt della shell bash
- Creare un'immagine del disco rigido del dispositivo e degli altri dispositivi di memorizzazione
- Ripristinare un'immagine su un dispositivo
- Partecipare a una sessione in cui l'immagine esistente viene applicata a più dispositivi tramite multidiffusione
- Acquisire o ripristinare un'immagine WIM tramite ImageX
- Acquisire o ripristinare un'immagine Ghost mediante Symantec Ghost

Per eseguire automaticamente i seguenti task, è sufficiente abilitare pxe (Preboot Execution Environment) sui dispositivi, quindi configurare i task di preavvio nel Centro di controllo Zenworks e assegnarli ai dispositivi. A questo punto i dispositivi possono eseguire automaticamente i task all'avvio.

Per implementare manualmente i task, è possibile configurare i dispositivi in modo che richiedano l'intervento dell'utente durante l'avvio.

Nel Centro di controllo ZENworks, è inoltre possibile replicare le modifiche della directory `tftp` da un server primario ad altri server di imaging (dispositivo server primario o satellite con ruolo di imaging).

- “Configurazione dei Servizi di preavvio” a pagina 83
- “Acquisizione di un'immagine” a pagina 87
- “Applicazione di un'immagine” a pagina 88
- “Ulteriori informazioni” a pagina 91

Configurazione dei Servizi di preavvio

Per utilizzare i Servizi di preavvio, è necessario completare i task descritti nelle seguenti sezioni:

- “Abilitazione di PXE su un dispositivo” a pagina 84
- “Configurazione di un server di imaging” a pagina 84
- “Configurazione delle impostazioni per l'imaging di terze parti” a pagina 84
- “Configurazione delle impostazioni del driver NTFS di terze parti” a pagina 86

Abilitazione di PXE su un dispositivo

I servizi di preavvio richiedono l'abilitazione di PXE (Preboot Execution Environment) sui dispositivi gestiti in cui si desidera acquisire o applicare un'immagine.

Per verificare se PXE sia abilitato su un dispositivo, riavviare il dispositivo e selezionare l'opzione di avvio (F12 sulla maggior parte dei dispositivi). PXE è abilitato se è presente un'opzione di avvio di rete.

Se PXE non è abilitato su un dispositivo, modificarne il BIOS per abilitarlo. Per fare in modo che l'ambiente PXE sia disponibile a ogni avvio del dispositivo, è anche possibile modificare l'ordine di avvio cosicché l'opzione NIC (Network Interface Card) sia elencata prima delle altre opzioni di avvio.

Configurazione di un server di imaging

Il server di imaging è il server PXE a cui si connette il motore PXE di un dispositivo. Per fare in modo che un server ZENworks funzioni come server di imaging, è sufficiente avviare il servizio Novell Proxy DHCP sul server ZENworks. Quando si avvia il servizio, è necessario anche modificare il tipo di avvio da Manuale ad Automatico in modo che venga avviato ad ogni riavvio del server.

Configurazione delle impostazioni per l'imaging di terze parti

Per poter usare soluzioni di imaging di terze parti, è necessario configurare Impostazioni imaging di terze parti nel Centro di controllo ZENworks. ZENworks supporta i seguenti strumenti di imaging di terzi:

- Microsoft ImageX che utilizza il formato di file immagine WIM e WINPE come distribuzione
- Symantec Ghost che utilizza il formato di file immagine Ghost e WINPE come distribuzione

La funzione di imaging di terze parti di ZENworks consente di utilizzare come meccanismo di avvio solo PXE.

Per configurare le impostazioni di imaging di terze parti:

1. Installare ZENworks Configuration Management sul server di imaging.

   Per ulteriori informazioni sull'installazione di ZENworks 2020, consultare “Installazione di un server primario ZENworks in Windows” in *Installazione del server ZENworks*.

2. Configurare le impostazioni dell'imaging di terze parti nel Centro di controllo ZENworks.

   2a Verificare che Microsoft Windows Automated Installation Kit (WAIK) o Windows Assessment and Deployment Kit (WADK) sia installato sul dispositivo sul quale viene eseguito il Centro di controllo ZENworks.

   2b Nel Centro di controllo ZENworks fare clic sulla scheda **Configurazione**.

   2c Nel riquadro **Impostazioni zona di gestione** fare clic su **Gestione dispositivi** > **Servizi di preavvio** > riquadro **Impostazioni imaging di terze parti**.

   2d Per **Impostazioni upload a 32 bit**:

   Upload della distribuzione di base WinPE (richiede Windows AIK /Windows ADK): fare clic sull'icona per effettuare l'upload del file di imaging WIM. Nella finestra di dialogo Carica file di imaging WIM eseguire le seguenti operazioni:

   1. Per caricare un file `winpe.wim` a 32 bit:

Da WAIK: passare alla cartella `Windows AIK\Tools\PETools\x86` nella directory di installazione, quindi selezionare il file `winpe.wim`.

Da WADK: Passare alla cartella `Windows Kits\<versione>\Assessment and Deployment Kit\Windows Preinstallation Environment\x86\en-us` nella directory di installazione, quindi selezionare il file `winpe.wim`.

Dove *<versione>* è una versione del sistema operativo Windows.

Nota: se si effettua di nuovo l'upload del file `winpe.wim`, viene sovrascritta l'istanza precedente del file sul server.

---

2. Fare clic su **OK**.

   In questo modo si effettua il download dei file di imaging dal server nel dispositivo da cui si accede al Centro di controllo ZENworks e viene ricreato `winpe.wim` con i file di imaging, quindi viene effettuato l'upload dei file dal dispositivo al server. L'avanzamento del download e dell'upload dei file viene mostrato nel campo **Stato**.

Caricamento di file ImageX per supportare l'imaging WIM (ImageX.exe):

1. fare clic sull'icona per individuare e selezionare il motore di imaging Microsoft (`imagex.exe`) nel dispositivo da cui è possibile accedere al Centro di controllo ZENworks.
2. Dopo aver configurato le impostazioni di imaging di terze parti, fare clic su **Applica**.
3. Fare clic su **Stato** per visualizzare lo stato della replica di contenuto su tutti i server primari e satellite con il ruolo Imaging nella zona di gestione. Avviare l'operazione di imaging solo quando lo stato è Disponibile.

Nota: se si effettua l'upload di file ImageX sia a 32 bit sia a 64 bit, assicurarsi di farlo in istanze diverse.

Upload del file Ghost 11.5. o versioni successive per supportare l'imaging Ghost (Ghost32.exe):

1. Fare clic sull'icona per individuare e selezionare il motore Symantec GHOST (`ghost32.exe`) nel dispositivo da cui è possibile accedere al Centro di controllo ZENworks.
2. Dopo aver configurato le impostazioni di imaging di terze parti, fare clic su **Applica**.
3. Fare clic su **Stato** per visualizzare lo stato della replica di contenuto su tutti i server primari e satellite con il ruolo Imaging nella zona di gestione. Avviare l'operazione di imaging solo quando lo stato è Disponibile.

2e Per **Impostazioni upload a 64 bit**:

Upload della distribuzione di base WinPE (richiede Windows AIK /Windows ADK): fare clic sull'icona per effettuare l'upload del file di imaging WIM. Nella finestra di dialogo Carica file di imaging WIM eseguire le seguenti operazioni:

1. Per effettuare l'upload di un file `winpe.wim` a 64 bit da WADK, passare alla cartella `Windows Kits\<versione>\Assessment and Deployment Kit\Windows Preinstallation environment\amd64\en-us` nella directory di installazione, quindi selezionare il file `winpe.wim`. .

   Dove *<versione>* è una versione del sistema operativo Windows.

2. Fare clic su **OK**.

   In questo modo si effettua il download dei file di imaging dal server nel dispositivo da cui si accede al Centro di controllo ZENworks e viene ricreato `winpe.wim` con i file di imaging, quindi viene effettuato l'upload dei file dal dispositivo al server. L'avanzamento del download e dell'upload dei file viene mostrato nel campo **Stato**.

Caricamento di file ImageX per supportare l'imaging WIM (ImageX.exe):

1. fare clic sull'icona per individuare e selezionare il motore di imaging Microsoft (`imagex.exe`) nel dispositivo da cui è possibile accedere al Centro di controllo ZENworks.
2. Dopo aver configurato le impostazioni di imaging di terze parti, fare clic su **Applica**.
3. Fare clic su **Stato** per visualizzare lo stato della replica di contenuto su tutti i server primari e satellite con il ruolo Imaging nella zona di gestione. Avviare l'operazione di imaging solo quando lo stato è Disponibile.

Nota: se si effettua l'upload di file ImageX sia a 32 bit sia a 64 bit, assicurarsi di farlo in istanze diverse.

Upload del file Ghost 11.5. o versioni successive per supportare l'imaging Ghost (Ghost64.exe):

1. fare clic sull'icona per individuare e selezionare il motore Symantec GHOST (`ghost64.exe`) nel dispositivo da cui è possibile accedere al Centro di controllo ZENworks.
2. Dopo aver configurato le impostazioni di imaging di terze parti, fare clic su **Applica**.
3. Fare clic su **Stato** per visualizzare lo stato della replica di contenuto su tutti i server primari e satellite con il ruolo Imaging nella zona di gestione. Avviare l'operazione di imaging solo quando lo stato è Disponibile.

3 Abilitare PXE sul dispositivo.

4 Verificare di avere a disposizione un server DHCP standard sul server di imaging o su un altro server di rete.

Configurazione delle impostazioni del driver NTFS di terze parti

È possibile effettuare il download del driver NTFS ad elevate prestazioni più recente e salvarlo sul sistema. È possibile visualizzare lo stato della replica del contenuto sul server primario e sui satelliti utilizzando il ruolo di imaging nella zona di gestione. È possibile avviare Imaging utilizzando il driver NTFS di terze parti quando lo stato indica che è disponibile.

Per configurare queste impostazioni, fare clic su **Configurazione** nel riquadro a sinistra e visualizzare la scheda **Configurazione**. Se la sezione non è espansa, fare clic su **Impostazioni zona di gestione**, quindi fare clic su **Gestione dispositivi** > **Servizi di preavvio** per visualizzare la pagina Servizi di preavvio.

Acquisizione di un'immagine

È possibile acquisire e ripristinare immagini ZENworks su un dispositivo utilizzando ZENworks Imaging e immagini di terze parti mediante l'utility ZENworks Imaging di terze parti. Questa utility consente di acquisire un'immagine e ripristinarla in un dispositivo o server locale utilizzando il formato Windows Imaging (WIM) o l'imaging Ghost.

1. Nel Centro di controllo ZENworks, fare clic sulla scheda **Dispositivi**.
2. Scorrere la cartella `Server` o `Workstation` fino a individuare il dispositivo di cui si desidera prendere l'immagine.
3. Fare clic sul dispositivo per visualizzarne i dettagli.
4. Nell'elenco dei task situato nel pannello di navigazione a sinistra, fare clic su **Prendi un'immagine** per avviare l'Acquisizione guidata immagine.
5. Nella pagina Informazioni sui file, compilare i campi seguenti, quindi fare clic su **Avanti**.

   Per ZENworks Imaging, specificare quanto segue:

   Formato immagine: selezionare il formato dell'immagine del dispositivo

   Percorso di file e server: fare clic sull'icona per visualizzare la finestra di dialogo Informazioni su server e percorso. Configurare le seguenti opzioni.

   - **Oggetto server/IP/DNS:** fare clic sull'icona per ricercare e selezionare l'oggetto, l'indirizzo IP o il nome DNS del server primario o del dispositivo promosso a server di imaging.
   - **Percorso file su server:** fare clic sull'icona per ricercare e selezionare un file di immagine Il file di immagine deve presentare l'estensione `.zmg` a indicare che si tratta di un file di immagine ZENworks valido.

     Nota: non è possibile passare al file system specificato se sono stati configurati più domini di ricerca con DHCP per Linux e il server è in Windows.

   Per l'imaging di terze parti, specificare quanto segue:

   Percorso rete condiviso per file di immagine: specificare il percorso di rete condiviso in cui salvare i file `.wim` o `.gho`. La directory deve essere una condivisione Windows, Linux SMB o CIFS.

   se l'estensione Novell File Upload non è installata nel dispositivo in uso, è necessario installarla prima di individuare e caricare le directory da installare.

   Nome file immagine: specificare il nome del file per salvare il file `.wim` o `.gho`. Questa opzione viene visualizzata solo per il formato immagine Windows (`.wim`) e il formato immagine Ghost (`.gho`).

   Credenziale di rete: fare clic su per ricercare e selezionare le credenziali di rete da utilizzare per accedere al dispositivo con i file `.wim`. L'opzione è visualizzata solo per il formato immagine Windows (`.wim`) e per il formato immagine Ghost (`.gho`).

   Usa compressione: la compressione è obbligatoria. Scegliere una delle seguenti opzioni:

   - **Bilanciato:** bilancia automaticamente la compressione tra una media della velocità di reimaging e lo spazio disponibile su disco per il file di immagine. L'opzione è visualizzata solo per il formato immagine ZENworks.
   - **Nessuno:** questa opzione viene visualizzata solo per i formati immagine Windows e Ghost.

- **Ottimizza per velocità:** ottimizza la compressione per rendere più veloce il reimaging. Utilizzare questa opzione se la velocità della CPU è un problema.
- **Ottimizza per spazio:** ottimizza la compressione per ridurre le dimensioni del file immagine e preservare spazio su disco. In questo caso il reimaging può richiedere più tempo.

Bilanciatoè l'opzione di default per il formato immagine ZENworks e **Ottimizza per velocità** è l'opzione di default per il formato immagine Windows e il formato immagine Ghost.

Creazione un pacchetto di immagini: lasciare il campo deselezionato.

6 Rivedere le informazioni nella pagina Riepilogo file immagine, fare clic su **Completato**, quindi su **OK**.

Poiché i task di imaging vengono completati dai Servizi di preavvio, l'immagine del dispositivo viene presa all'avvio successivo del dispositivo. Nel riquadro Lavoro di imaging, situato nella pagina Riepilogo del dispositivo è visualizzata la pianificazione del dispositivo. Quando il lavoro è completato, il task viene rimosso dal pannello.

7 Per riavviare immediatamente il dispositivo e iniziare il lavoro di imaging, fare clic su **Riavvia/Chiudi workstation** (o **Riavvia/Chiudi server**) nel pannello di navigazione a sinistra.

Il tempo richiesto per prendere l'immagine dipende dalle dimensioni delle unità del dispositivo.

Applicazione di un'immagine

Per applicare un'immagine a un dispositivo, si utilizza la Creazione guidata nuovo pacchetto per creare un pacchetto di imaging. Il pacchetto contiene l'immagine da applicare. Oltre a costituire una guida per la creazione del pacchetto, la procedura guidata consente di assegnare il pacchetto ai dispositivi. Dopo aver creato il pacchetto di imaging, si avvia il lavoro di imaging.

- “Creazione di un pacchetto immagine ZENworks” a pagina 88
- “Creazione di un pacchetto immagine di terze parti” a pagina 89
- “Avvio del lavoro di imaging” a pagina 90

Video per apprendere le procedure di distribuzione di immagini Windows 7 e Linux nei dispositivi:

- Distribuzione di immagini Windows 7 con ZENworks
- Distribuzione di Linux con ZENworks

Creazione di un pacchetto immagine ZENworks

Per ripristinare le immagini ZENworks su un dispositivo, è necessario creare il pacchetto immagine ZENworks.

1 Nel Centro di controllo ZENworks, fare clic sulla scheda **Pacchetti**.

2 Nel pannello Pacchetti, fare clic su **Nuovo** > **Pacchetto** per avviare la Creazione guidata nuovo pacchetto.

3 Nella pagina Seleziona tipo pacchetto, selezionare **Pacchetto di preavvio**, quindi fare clic su **Avanti**.

4 Nella pagina Seleziona categoria pacchetto selezionare **Immagine ZENworks**, quindi fare clic su **Avanti**.

5 Completare la procedura guidata compilando i campi con le informazioni incluse nella seguente tabella.

Pagina della procedura guidata	Dettagli
Pagina Definisci dettagli	Assegnare un nome al task. Il nome non può contenere i seguenti caratteri non validi: / \ * ? : " ' < > | ` % ~
Pagina Seleziona file immagine ZENworks	Per selezionare un file di immagine: 1. Fare clic sull'icona per visualizzare la finestra di dialogo Informazioni su server e percorso. 2. Immettere le informazioni nei campi. **Oggetto Dispositivo, IP o DNS:** selezionare il server ZENworks in cui si è memorizzata l'immagine. **Percorso file su server:** individuare e selezionare il file di immagine da inserire. La directory di memorizzazione standard per i file di immagine è `\Novell\ZENworks\lavoro\archivio-contenuti\immagini`. 3. Fare clic su **OK**.
Pagina Riepilogo	Fare clic su **Avanti** per continuare con la procedura guidata e assegnare il pacchetto al dispositivo di destinazione.
Pagina Gruppi di pacchetti	Non si deve assegnare il pacchetto di immagini ai gruppi. Fare clic su **Avanti** per ignorare la pagina.
Pagina Aggiungi assegnazioni	Selezionare il dispositivo in cui applicare l'immagine.
Pagina Pianificazioni	Non si deve assegnare una pianificazione al pacchetto di immagini. Fare clic su **Avanti** per ignorare la pagina.
Pagina Fine	Fare clic su **Fine** per creare il pacchetto e assegnarlo al dispositivo selezionato.

Creazione di un pacchetto immagine di terze parti

Per ripristinare immagini di terze parti, è necessario creare un pacchetto immagine di terze parti.

1 Nel Centro di controllo ZENworks, fare clic sulla scheda **Pacchetti**.

2 Nel pannello Pacchetti, fare clic su **Nuovo** > **Pacchetto** per avviare la Creazione guidata nuovo pacchetto.

3 Nella pagina Seleziona tipo pacchetto, selezionare **Pacchetto di preavvio**, quindi fare clic su **Avanti**.

4 Nella pagina Seleziona categoria pacchetto selezionare **Immagine di terze parti**, quindi fare clic su **Avanti**.

5 Completare la procedura guidata compilando i campi con le informazioni incluse nella seguente tabella.

Pagina della procedura guidata	Dettagli
Pagina Definisci dettagli	Assegnare un nome al task. Il nome non può contenere i seguenti caratteri non validi: / \ * ? : " ' < > | ` % ~
Selezionare una pagina con file immagine di terze parti	Per selezionare un file immagine di terze parti: 1. Selezionare il tipo di immagine da usare nel pacchetto. In ZENworks Configuration Management sono disponibili solo il formato immagine Windows (`.wim`) e il formato immagine GHOST (`.gho`). 2. Specificare la directory di rete condivisa contenente i file `.wim` o `.gho`. La directory deve essere una condivisione Windows, Linux SMB o CIFS. 3. Fare clic su per individuare e selezionare le credenziali di rete da utilizzare per accedere al dispositivo contenente i file `.wim` o `.gho`. 4. Per usare il pacchetto WIM come immagine aggiuntiva, selezionare **Ripristina WIM come prodotto aggiuntivo** e configurare le seguenti opzioni: **Numero immagine (solo WIM):** selezionare il numero di indice dell'immagine da ripristinare. **Percorso per il ripristino dell'immagine aggiuntiva:** specificare l'ubicazione sul dispositivo in cui ripristinare l'immagine aggiuntiva. 5. Fare clic su **OK**.
Pagina Riepilogo	Fare clic su **Avanti** per continuare con la procedura guidata e assegnare il pacchetto al dispositivo di destinazione.
Pagina Gruppi di pacchetti	Non si deve assegnare il pacchetto di immagini ai gruppi. Fare clic su **Avanti** per ignorare la pagina.
Pagina Aggiungi assegnazioni	Selezionare il dispositivo in cui applicare l'immagine.
Pagina Pianificazioni	Non si deve assegnare una pianificazione al pacchetto di immagini. Fare clic su **Avanti** per ignorare la pagina.
Pagina Fine	Fare clic su **Fine** per creare il pacchetto e assegnarlo al dispositivo selezionato.

Avvio del lavoro di imaging

1 Nel Centro di controllo ZENworks, fare clic sulla scheda **Dispositivi**.

2 Scorrere la cartella `Server` o `Workstation` fino a individuare il dispositivo in cui applicare l'immagine.

3 Fare clic sul dispositivo per visualizzarne i dettagli.

4 Nell'elenco dei task situato nel riquadro di navigazione a sinistra, fare clic su **Applica pacchetto di imaging assegnato** per pianificare il lavoro.

   Poiché i task di imaging vengono completati dai servizi di preavvio, l'immagine viene applicata al dispositivo all'avvio successivo del dispositivo. Nel riquadro Lavoro di imaging, situato nella pagina Riepilogo del dispositivo è visualizzata la pianificazione del dispositivo. Quando il lavoro è completato, il task viene rimosso dal pannello.

5 Per riavviare immediatamente il dispositivo e iniziare il lavoro di imaging, fare clic su **Riavvia/Chiudi workstation** (o **Riavvia/Chiudi server**) nel pannello di navigazione a sinistra.

Ulteriori informazioni

Per ulteriori informazioni sull'imaging e i servizi di preavvio, vedere *ZENworks Preboot Services and Imaging Reference* (Riferimento per l'imaging e i servizi di preavvio di ZENworks).

Gestione dei dispositivi in modalità remota

ZENworks Configuration Management fornisce la funzione di gestione remota con la quale è possibile gestire i dispositivi in modalità remota. Gestione remota supporta le seguenti operazioni

Operazione remota	Descrizione	Dettagli aggiuntivi
Controllo remoto	Consente di controllare un dispositivo gestito tramite la console di gestione in modo da poter fornire assistenza agli utenti e aiutarli a risolvere i problemi. È possibile eseguire tutte le operazioni generalmente effettuate dall'utente sul dispositivo. Per ulteriori informazioni sul controllo remoto di un dispositivo Windows, vedere "Esecuzione di operazioni di controllo remoto, visualizzazione ed esecuzione remote su un dispositivo Windows" a pagina 94. Per ulteriori informazioni sul controllo remoto di un dispositivo Linux, vedere "Esecuzione delle operazioni di controllo remoto, visualizzazione remota e login remoto su un dispositivo Linux" a pagina 99.	

Operazione remota	Descrizione	Dettagli aggiuntivi
Visualizzazione remota	Consente di connettersi con un dispositivo gestito in modo da poterlo visualizzare anziché controllare. E risolvere i problemi riscontrati dall'utente. Ad esempio, è possibile osservare come l'utente di un dispositivo gestito esegue alcuni task per assicurarsi che esegua la procedura corretta. Per ulteriori informazioni sulla visualizzazione remota di un dispositivo Windows, vedere "Esecuzione di operazioni di controllo remoto, visualizzazione ed esecuzione remote su un dispositivo Windows" a pagina 94. Per ulteriori informazioni sulla visualizzazione remota di un dispositivo Linux, vedere "Esecuzione delle operazioni di controllo remoto, visualizzazione remota e login remoto su un dispositivo Linux" a pagina 99.	
Esecuzione remota	Consente di eseguire qualsiasi file eseguibile su un dispositivo gestito tramite la console di gestione. Per eseguire remotamente un'applicazione, è necessario specificare il nome del file eseguibile nella finestra di dialogo Esecuzione remota. Se l'applicazione non si trova nel percorso di sistema sul dispositivo gestito, fornire il percorso completo dell'applicazione. Ad esempio, è possibile eseguire il comando `regedit` per aprire l'Editor del registro sul dispositivo gestito. La finestra di dialogo Esecuzione remota mostra lo stato dell'esecuzione remota. Per ulteriori informazioni sull'esecuzione remota di un dispositivo Windows, vedere "Esecuzione di operazioni di controllo remoto, visualizzazione ed esecuzione remote su un dispositivo Windows" a pagina 94.	Questa operazione è supportata solo in un dispositivo gestito Windows.
Diagnostica remota	Permette di diagnosticare e analizzare i problemi su un dispositivo gestito. Questo consente di ridurre i tempi di risoluzione dei problemi e assistere gli utenti evitando l'intervento in sede di un tecnico. Aumenta inoltre la produttività dell'utente, il cui desktop rimane attivo e in esecuzione. Per ulteriori informazioni sulla diagnostica remota di un dispositivo, vedere "Esecuzione di un'operazione di diagnostica remota" a pagina 96.	Questa operazione è supportata solo in un dispositivo gestito Windows.
Trasferimento file	Permette di trasferire file fra console di gestione e dispositivo gestito. Per ulteriori informazioni sull'operazione del trasferimento file, vedere "Esecuzione di un'operazione di trasferimento file" a pagina 98.	Questa operazione è supportata solo in un dispositivo gestito Windows.

Operazione remota	Descrizione	Dettagli aggiuntivi
Accesso remoto	Consente di eseguire il login dalla console di gestione a un dispositivo gestito e di avviare una nuova sessione grafica senza interrompere nel dispositivo gestito l'utente, che tuttavia non può visualizzare la sessione di login remoto. Per ulteriori informazioni sull'esecuzione del login remoto a un dispositivo Linux, vedere "Esecuzione delle operazioni di controllo remoto, visualizzazione remota e login remoto su un dispositivo Linux" a pagina 99.	Questa operazione è supportata solo in un dispositivo gestito Linux. È necessario eseguire il login al dispositivo con credenziali utente non-`root`.
SSH remoto	Consente di stabilire una connessione sicura al dispositivo Linux remoto e di eseguire comandi su tale dispositivo. Per ulteriori informazioni sull'esecuzione del login remoto a un dispositivo Linux, vedere "Esecuzione di un'operazione di SSH remoto su un dispositivo Linux" a pagina 100	Questa operazione è supportata solo in un dispositivo gestito Linux.

Le seguenti sezioni spiegano come configurare la gestione remota ed eseguire le seguenti operazioni:


Video sulla gestione remota dei dispositivi.

Creazione di una norma di gestione remota

Per default, norme di Gestione remota sicure vengono create sui dispositivi gestiti quando l'agente di ZENworks viene distribuito con il componente Gestione remota sul dispositivo. È possibile usare le norme di default per gestire un dispositivo in remoto. Le norme di default consentono di eseguire tutte le operazioni di gestione remota su un dispositivo. Per ignorare le norme di default, è possibile creare esplicitamente delle norme di gestione remota per il dispositivo.

Una norma Gestione remota può essere assegnata sia ai dispositivi che agli utenti.

Per creare una norma Gestione remota:

1. Nel Centro di controllo ZENworks, fare clic sulla scheda **Norme**.
2. Nel riquadro Norme, fare clic su **Nuovo** > **Norma** per avviare la Creazione guidata nuova norma.
3. Selezionare **Policy di configurazione Windows**, quindi fare clic su **Avanti**.
4. Seguire i prompt visualizzati per creare la policy di gestione remota.

   Fare clic sul pulsante della **guida** su ciascuna pagina della procedura guidata per informazioni dettagliate sulla pagina. Al termine della procedura guidata, la norma viene aggiunta nel riquadro Norme. È possibile fare clic sulla policy per visualizzarne i dettagli e modificare le assegnazioni, le pianificazioni e così via.
5. Assegnare la policy di gestione remota a utenti e dispositivi:
   - **5a** Nel pannello Policy selezionare la casella di controllo accanto alla policy.
   - **5b** Fare clic su **Azione** > **Assegna a dispositivo**.

     oppure

     Fare clic su **Azione** > **Assegna a utente.**
   - **5c** Seguire le istruzioni visualizzate per assegnare la policy.

     Fare clic sul pulsante della **guida** su ciascuna pagina della procedura guidata per informazioni dettagliate sulla pagina.

     Al termine della procedura guidata, i dispositivi o gli utenti a cui è stata assegnata la policy vengono aggiunti nella pagina Relazioni della policy. Fare clic sulla policy per visualizzare le assegnazioni.

Configurazione delle impostazioni per la gestione remota

Le impostazioni di configurazione della gestione remota visualizzate nella pagina Configurazione consentono di specificare impostazioni quali la porta per la gestione remota, le prestazioni delle sessioni e le applicazioni diagnostiche disponibili.

Le impostazioni sono predefinite per la configurazione più comune. Per modificare le impostazioni:

1. Nel Centro di controllo ZENworks, fare clic sulla scheda **Configurazione**.
2. Nel riquadro Impostazioni zona di gestione, fare clic su **Gestione dispositivo** > **Gestione remota**.
3. Apportare le modifiche desiderate alle impostazioni.

   Fare clic sul pulsante **Guida** per visualizzare informazioni dettagliate sulla pagina.
4. Dopo aver modificato le impostazioni, fare clic su **Applica** o su **OK** per salvare le modifiche.

Esecuzione di operazioni di controllo remoto, visualizzazione ed esecuzione remote su un dispositivo Windows

1. Nel Centro di controllo ZENworks, fare clic sulla scheda **Dispositivi**.
2. Scorrere la cartella `Server` o `Workstation` fino a individuare il dispositivo da gestire.
3. Selezionare il dispositivo facendo clic sulla casella di controllo situata davanti al dispositivo.

4 Nell'elenco dei task situato nel pannello di navigazione a sinistra, fare clic su **Workstation controllo remoto** o **Server controllo remoto** per visualizzare la finestra di dialogo Gestione remota.

5 Nella finestra di dialogo Gestione remota, compilare i seguenti campi:

Dispositivo: specificare il nome o l'indirizzo IP del dispositivo che si desidera gestire in remoto.

Imposta sempre come default indirizzo IP per tutti i dispositivi: selezionare questo campo se si desidera che nel sistema venga visualizzato l'indirizzo IP del dispositivo invece del nome DNS.

I valori forniti per accedere a un dispositivo durante le operazioni di controllo remoto vengono salvati nel sistema, quando si fa clic su **OK**. Alcuni di questi valori vengono selezionati automaticamente durante le operazioni di controllo remoto successive, a seconda del dispositivo e dell'operatore remoto.

Funzionamento: selezionare il tipo di operazione remota (controllo remoto, visualizzazione remota o esecuzione remota) che si desidera eseguire sul dispositivo gestito:

Autenticazione: selezionare la modalità che si desidera utilizzare per autenticare il dispositivo gestito. Le due opzioni disponibili sono:

- **Password:** fornisce l'autenticazione basata su password per eseguire un'operazione di controllo remoto. È necessario immettere la password corretta così come impostata dall'utente sul dispositivo gestito o come configurata dall'amministratore nelle impostazioni di sicurezza della norma Gestione remota. La password impostata dall'utente è prioritaria rispetto a quella configurata dall'amministratore.
- **Diritti:** questa opzione è disponibile solo quando si seleziona il dispositivo gestito in cui si desidera eseguire l'operazione remota. Se un amministratore ha già assegnato all'utente i diritti di gestione remota per eseguire l'operazione remota desiderata sul dispositivo gestito selezionato, l'utente ottiene automaticamente l'accesso all'avvio della sessione.

Port: specificare il numero di porta di ascolto per l'agente di gestione remota. Il numero di porta di default è 5950.

Modalità di sessione: selezionare una delle seguenti modalità per la sessione.

- **Collabora:** consente di avviare una sessione di controllo remoto e di visualizzazione remota in modalità collaborazione. Tuttavia, non è possibile avviare per prima una sessione di visualizzazione remota sul dispositivo gestito. Quando sia avvia una sessione di controllo remoto sul dispositivo gestito, si ottengono tutti i privilegi dell'operatore remoto master che comprendono:
  - Possibilità di invitare altri operatori remoti a partecipare alla sessione remota.
  - Possibilità di delegare i diritti di controllo remoto a un operatore remoto.
  - Possibilità di riottenere il controllo dall'operatore remoto.
  - Possibilità di interrompere una sessione remota.

  Se la sessione di controllo remoto sul dispositivo gestito è stata stabilita in modalità di collaborazione, tutte le altre sessioni remote sul dispositivo gestito diventano sessioni di visualizzazione remota.
- **Condivisa:** consente a più operatori remoti di controllare contemporaneamente il dispositivo gestito.
- **Esclusivo:** consente di disporre di una sessione remota esclusiva sul dispositivo gestito. Dopo l'avvio di una sessione in modalità esclusiva, non è possibile avviare altre sessioni remote.

Cifratura sessione: verifica che la sessione remota sia protetta con la cifratura SSL (protocollo TLSv1).

Abilita cache: abilita la memorizzazione nella cache dei dati della sessione di Gestione remota per migliorare le prestazioni. Questa opzione può essere usata solo per l'operazione di controllo remoto. Questa opzione è attualmente supportata solo su Windows.

Attiva l'ottimizzazione della larghezza di banda dinamica: abilita la rilevazione della larghezza di banda di rete disponibile e regola di conseguenza le impostazioni della sessione per migliorare le prestazioni. Questa opzione può essere usata solo per l'operazione di controllo remoto.

Abilita registrazione: registra le informazioni sulla sessione e di debug nel file `novell-zenworks-vncviewer.txt`. Per default il file viene salvato sul desktop se si avvia il Centro di controllo ZENworks tramite Internet Explorer e nella directory installata in Mozilla se lo si avvia tramite Mozilla FireFox.

Routing tramite proxy: consente il routing dell'operazione di gestione remota del dispositivo gestito tramite un server proxy. Se il dispositivo gestito è ubicato in una rete privata o sull'altro lato di un firewall o su un router che utilizza NAT (Network Address Translation), è possibile instradare l'operazione di gestione remota del dispositivo tramite un server proxy. Immettere le informazioni nei campi:

- **Proxy:** specificare il nome DNS o l'indirizzo IP del server proxy. Per default, in questo campo viene popolato il server proxy configurato nel pannello Impostazioni proxy per l'esecuzione dell'operazione remota sul dispositivo. È possibile specificare un server proxy diverso.
- **Porta proxy:** specificare il numero di porta di ascolto del server proxy. Il numero di porta di default è 5750.

Utilizza la seguente coppia di chiavi per l'identificazione: se si distribuisce un'autorità di certificazione (CA) interna, le seguenti opzioni non vengono visualizzate. Se si distribuisce un'autorità di certificazione (CA) esterna, compilare i seguenti campi:

- **Chiave privata:** fare clic su **Sfoglia** per individuare e selezionare la chiave privata dell'operatore remoto.
- **Certificato:** fare clic su **Sfoglia** per individuare e selezionare il certificato corrispondente alla chiave privata. Il certificato deve essere concatenato all'autorità di certificazione configurata per la zona.

  I formati supportati per la chiave e il certificato sono DER e PEM.

Installa Visualizzatore gestione remota: fare clic sul collegamento **Installa Visualizzatore gestione remota** per installare il Visualizzatore gestione remota. Questo collegamento viene visualizzato solo quando si esegue la sessione di gestione remota sul dispositivo gestito o se il Visualizzatore gestione remota non è installato sul dispositivo gestito.

6 Fare clic su **OK** per avviare la sessione.

Esecuzione di un'operazione di diagnostica remota

1 Nel Centro di controllo ZENworks, fare clic sulla scheda **Dispositivi**.

2 Scorrere la cartella `Server` o `Workstation` fino a individuare il dispositivo da gestire.

3 Selezionare il dispositivo facendo clic sulla casella di controllo situata davanti al dispositivo.

4 Nell'elenco dei task visualizzato nel pannello di navigazione sinistro, fare clic su **Diagnostica remota** per visualizzare la finestra di dialogo corrispondente.

5 Nella finestra di dialogo Diagnostica remota, immettere le informazioni richieste nei seguenti campi:

Dispositivo: specificare il nome o l'indirizzo IP del dispositivo di cui si desidera eseguire la diagnosi in remoto.

Imposta sempre come default indirizzo IP per tutti i dispositivi: selezionare questo campo se si desidera che nel sistema venga visualizzato l'indirizzo IP del dispositivo invece del nome DNS.

I valori forniti per accedere un dispositivo durante l'esecuzione di un'operazione di controllo remoto vengono salvati nel sistema quando si fa clic su **OK**. Alcuni di questi valori vengono selezionati automaticamente durante le operazioni di controllo remoto successive, a seconda del dispositivo e dell'operatore remoto.

Utente: selezionare l'applicazione che si desidera avviare sul dispositivo per la diagnosi remota.

Autenticazione: selezionare la modalità che si desidera utilizzare per autenticare il dispositivo gestito. Le due opzioni disponibili sono:

- **Password:** fornisce un'autenticazione basata su password per l'esecuzione dell'operazione di diagnostica remota. È necessario immettere la password corretta così come impostata dall'utente sul dispositivo gestito o come configurata dall'amministratore nelle impostazioni di sicurezza della norma Gestione remota. La password impostata dall'utente è prioritaria rispetto a quella configurata dall'amministratore.
- **Diritti:** questa opzione è disponibile solo quando si seleziona il dispositivo gestito in cui si desidera eseguire l'operazione remota. Se un amministratore ha già assegnato all'utente i diritti di gestione remota per eseguire l'operazione remota desiderata sul dispositivo gestito selezionato, l'utente ottiene automaticamente l'accesso all'avvio della sessione.

Port: specificare il numero di porta di ascolto per l'agente di gestione remota. Il numero di porta di default è 5950.

Modalità di sessione: non si applica all'operazione di diagnostica remota.

Cifratura sessione: verifica che la sessione remota sia protetta con la cifratura SSL (protocollo TLSv1).

Abilita cache: abilita la memorizzazione nella cache dei dati della sessione di Gestione remota per migliorare le prestazioni. Questa opzione è attualmente supportata solo su Windows.

Attiva l'ottimizzazione della larghezza di banda dinamica: abilita il rilevamento della larghezza di banda di rete disponibile e regola di conseguenza le impostazioni della sessione per migliorare le prestazioni.

Abilita registrazione: registra le informazioni sulla sessione e di debug nel file `novell-zenworks-vncviewer.txt`. Per default il file viene salvato sul desktop se si avvia il Centro di controllo ZENworks tramite Internet Explorer e nella directory installata in Mozilla se lo si avvia tramite Mozilla FireFox.

Routing tramite proxy: consente il routing dell'operazione di gestione remota del dispositivo gestito tramite un server proxy. Se il dispositivo gestito è ubicato in una rete privata o sull'altro lato di un firewall o su un router che utilizza NAT (Network Address Translation), è possibile instradare l'operazione di gestione remota del dispositivo tramite un server proxy. Immettere le informazioni nei campi:

- **Proxy:** specificare il nome DNS o l'indirizzo IP del server proxy. Per default, in questo campo viene popolato il server proxy configurato nel pannello Impostazioni proxy per l'esecuzione dell'operazione remota sul dispositivo. È possibile specificare un server proxy diverso.

- **Porta proxy:** specificare il numero di porta di ascolto del server proxy. Il numero di porta di default è 5750.

6 Fare clic su **OK** per avviare la sessione.

Esecuzione di un'operazione di trasferimento file

1 Nel Centro di controllo ZENworks, fare clic sulla scheda **Dispositivi**.

2 Scorrere la cartella `Server` o `Workstation` fino a individuare il dispositivo da gestire.

3 Selezionare il dispositivo facendo clic sulla casella di controllo situata davanti al dispositivo.

4 Nell'elenco dei task visualizzato nel pannello di navigazione sinistro, fare clic su **Trasferisci file** per visualizzare la finestra di dialogo Trasferimento file.

5 Nella finestra di dialogo Trasferimento file, immettere le informazioni richieste nei seguenti campi:

Dispositivo: specificare il nome o l'indirizzo IP del dispositivo a cui si desidera accedere.

Imposta sempre come default indirizzo IP per tutti i dispositivi: selezionare questo campo se si desidera che nel sistema venga visualizzato l'indirizzo IP del dispositivo invece del nome DNS. I valori forniti per accedere un dispositivo durante l'esecuzione di un'operazione di controllo remoto vengono salvati nel sistema quando si fa clic su **OK**. Alcuni di questi valori vengono selezionati automaticamente durante le operazioni di controllo remoto successive, a seconda del dispositivo e dell'operatore remoto.

Autenticazione: selezionare la modalità che si desidera utilizzare per autenticare il dispositivo gestito. Le due opzioni disponibili sono:

- **Password:** fornisce un'autenticazione basata su password per l'esecuzione di un'operazione. È necessario immettere la password corretta così come impostata dall'utente sul dispositivo gestito o come configurata dall'amministratore nelle impostazioni di sicurezza della norma Gestione remota. La password impostata dall'utente è prioritaria rispetto a quella configurata dall'amministratore.
- **Diritti:** questa opzione è disponibile solo quando si seleziona il dispositivo gestito in cui si desidera eseguire l'operazione remota. Se un amministratore ha già assegnato all'utente i diritti di gestione remota per eseguire l'operazione remota desiderata sul dispositivo gestito selezionato, l'utente ottiene automaticamente l'accesso all'avvio della sessione.

Port: specificare il numero di porta di ascolto per l'agente di gestione remota. Il numero di porta di default è 5950.

Modalità di sessione: non si applica all'operazione di trasferimento file.

Cifratura sessione: verifica che la sessione remota sia protetta con la cifratura SSL (protocollo TLSv1).

Abilita registrazione: registra le informazioni sulla sessione e di debug nel file `novell-zenworks-vncviewer.tx`. Per default il file viene salvato sul desktop se si avvia il Centro di controllo ZENworks tramite Internet Explorer e nella directory installata in Mozilla se lo si avvia tramite Mozilla FireFox. In una console di gestione Linux il file viene salvato nella home directory dell'utente connesso.

Routing tramite proxy: consente il routing dell'operazione di gestione remota del dispositivo gestito tramite un server proxy. Se il dispositivo gestito è ubicato in una rete privata o sull'altro lato di un firewall o su un router che utilizza NAT (Network Address Translation), è possibile instradare l'operazione di gestione remota del dispositivo tramite un server proxy. Immettere le informazioni nei campi:

- **Proxy:** specificare il nome DNS o l'indirizzo IP del server proxy. Per default, in questo campo viene popolato il server proxy configurato nel pannello Impostazioni proxy per l'esecuzione dell'operazione remota sul dispositivo. È possibile specificare un server proxy diverso.
- **Porta proxy:** specificare il numero di porta di ascolto del server proxy. Il numero di porta di default è 5750.

6 Fare clic su **OK** per avviare la sessione

Esecuzione delle operazioni di controllo remoto, visualizzazione remota e login remoto su un dispositivo Linux

1 Nel Centro di controllo ZENworks, fare clic sulla scheda **Dispositivi**.

2 Scorrere la cartella `Server` o `Workstation` fino a individuare il dispositivo da gestire.

3 Selezionare un dispositivo Linux facendo clic sulla casella di controllo accanto al dispositivo.

4 Fare clic su **Azione** > **Controllo remoto**per visualizzare la finestra di dialogo Gestione remota.

5 Nella finestra di dialogo Gestione remota, compilare i seguenti campi:

Dispositivo: specificare il nome o l'indirizzo IP del dispositivo che si desidera gestire in remoto.

Imposta sempre come default indirizzo IP per tutti i dispositivi: selezionare questo campo se si desidera che nel sistema venga visualizzato l'indirizzo IP del dispositivo invece del nome DNS.

I valori forniti per accedere un dispositivo durante l'esecuzione di un'operazione di controllo remoto vengono salvati nel sistema quando si fa clic su **OK**. Alcuni di questi valori vengono selezionati automaticamente durante le operazioni di controllo remoto successive, a seconda del dispositivo e dell'operatore remoto.

Funzionamento: selezionare il tipo di operazione remota (Controllo remoto, Visualizzazione remota o Login remoto) che si desidera eseguire sul dispositivo gestito:

Port: specificare il numero di porta di ascolto per l'agente di gestione remota. Per default, il numero di porta è 5950 per le operazioni di controllo remoto e visualizzazione remota, e 5951 per l'operazione di login remoto.

Abilita registrazione: registra le informazioni sulla sessione e di debug nel file `novell-zenworks-vncviewer.tx`. Per default il file viene salvato sul desktop se si avvia il Centro di controllo ZENworks tramite Internet Explorer e nella directory installata in Mozilla se lo si avvia tramite Mozilla FireFox. In una console di gestione Linux il file viene salvato nella home directory dell'utente connesso.

Routing tramite proxy: consente il routing dell'operazione di gestione remota del dispositivo gestito tramite un server proxy. Se il dispositivo gestito è ubicato in una rete privata o sull'altro lato di un firewall o su un router che utilizza NAT (Network Address Translation), è possibile instradare l'operazione di gestione remota del dispositivo tramite un server proxy. Immettere le informazioni nei campi:

- **Proxy:** specificare il nome DNS o l'indirizzo IP del server proxy. Per default, in questo campo viene popolato il server proxy configurato nel pannello Impostazioni proxy per l'esecuzione dell'operazione remota sul dispositivo. È possibile specificare un server proxy diverso.

- **Porta proxy:** specificare il numero di porta di ascolto del server proxy. Il numero di porta di default è 5750.

Installa Visualizzatore gestione remota: fare clic sul collegamento **Installa Visualizzatore gestione remota** per installare il Visualizzatore gestione remota. Questo collegamento viene visualizzato solo quando si esegue la sessione di gestione remota sul dispositivo gestito o se il Visualizzatore gestione remota non è installato sul dispositivo gestito.

6 Fare clic su **OK** per avviare la sessione.

Esecuzione di un'operazione di SSH remoto su un dispositivo Linux

1 Nel Centro di controllo ZENworks, fare clic sulla scheda **Dispositivi**.

2 Scorrere la cartella `Server` o `Workstation` fino a individuare il dispositivo da gestire.

3 Selezionare un dispositivo Linux facendo clic sulla casella di controllo accanto al dispositivo.

4 Fare clic su **Azione** > **SSH remoto**per visualizzare la finestra di dialogo SSH remoto.

5 Nella finestra di dialogo SSH remoto, compilare i seguenti campi:

Dispositivo: consente di specificare il nome o l'indirizzo IP del dispositivo a cui si desidera effettuare la connessione in remoto. Se il dispositivo non si trova nella stessa rete, è necessario specificare il relativo indirizzo IP.

Nome utente: consente di specificare il nome utente utilizzato per eseguire il login al dispositivo remoto. Per default è `radice`.

Port: consente di specificare il numero di porta del servizio SSH remoto. Il numero di porta di default è 22.

Facendo clic su **OK** viene chiesto di avviare Java Web Start Launcher per SSH remoto. Fare clic su Sì per accettare il certificato, quindi su **Esegui**. Per mantenere la connessione al dispositivo, fare clic su **Sì**. Viene chiesto di immettere la password per la connessione al dispositivo gestito.

6 Fare clic su **OK** per avviare la sessione.

Ulteriori informazioni

Per ulteriori informazioni sui dispositivi gestiti in remoto, vedere il *Riferimento per la gestione remota di Novell ZENworks*.

Raccolta dell'inventario software e hardware

ZENworks Configuration Management consente di raccogliere informazioni sul software e hardware dai dispositivi. È possibile visualizzare l'inventario dei singoli dispositivi e generare l'inventario in base a criteri specifici.

Si supponga ad esempio di voler distribuire un'applicazione software con specifici requisiti riguardo a processore, memoria e spazio su disco. Si creeranno due rapporti: uno che elenca tutti i dispositivi che soddisfano i requisiti e un altro che elenca i dispositivi che invece non li soddisfano. In base ai rapporti, si distribuisce il software ai dispositivi compatibili e si crea un piano di aggiornamento per i dispositivi che non lo sono.

Per default, i dispositivi vengono sottoposti a scansione alle ore 01.00, il primo giorno del mese. È possibile modificare la pianificazione, nonché numerose altre impostazioni di configurazione dell'**Inventario** nella scheda **Configurazione** del Centro di controllo ZENworks.

Avvio di una scansione del dispositivo

È possibile avviare la scansione di un dispositivo in qualsiasi momento.

1. Nel Centro di controllo ZENworks, fare clic sulla scheda **Dispositivi**.
2. Scorrere la cartella `Server` o `Workstation` fino a individuare il dispositivo da sottoporre a scansione.
3. Fare clic sul dispositivo per visualizzarne i dettagli.
4. Nell'elenco dei task situato nel pannello di navigazione a sinistra, fare clic su **Scansione inventario server** o **Scansione inventario workstation** per avviare la scansione.

   Nella finestra di dialogo Stato task rapidi viene visualizzato lo stato del task. Al completamento del task, è possibile fare clic sulla scheda **Inventario** per visualizzare i risultati della scansione.

È possibile anche usare il comando `inventory-scan-now` nell'utility zman per eseguire la scansione di un dispositivo. Per ulteriori informazioni, vedere "Comandi per l'inventario" nel *Riferimento per le utility da riga di comando di ZENworks*.

Visualizzazione dell'inventario dei dispositivi

1. Nel Centro di controllo ZENworks, fare clic sulla scheda **Dispositivi**.
2. Scorrere la cartella `Server` o `Workstation` fino a individuare il dispositivo da sottoporre a scansione.
3. Fare clic sul dispositivo per visualizzarne i dettagli.
4. Fare clic sulla scheda **Inventario**.

Generazione di un rapporto sull'inventario

ZENworks Configuration Management comprende diversi rapporti standard. È anche possibile creare rapporti personalizzati per esaminare i dati dell'inventario da diverse angolazioni.

1. Nel Centro di controllo ZENworks, fare clic sulla scheda .
2. Nel pannello Rapporti standard inventario, fare clic su **Applicazioni software**.
3. Fare clic sul rapporto **Sistema operativo** per generare il rapporto.

   Utilizzando le opzioni riportate in fondo al rapporto è possibile salvare il rapporto generato come foglio di calcolo Microsoft Excel, file CSV (con valori separati da virgole), file PDF o file grafico PDF.

Ulteriori informazioni

Per ulteriori informazioni sull'inventario, vedere *ZENworks Asset Inventory Reference* (Riferimento per ZENworks Asset Inventory).

Linux Management

Linux Management semplifica l'adozione e l'implementazione di Linux nell'ambiente utilizzato. Utilizza l'automazione basata su policy per la distribuzione, la gestione e la manutenzione delle risorse Linux. Le policy automatiche e intelligenti permettono di gestire in modo centralizzato il ciclo di vita dei sistemi Linux a livello di blocco del desktop, imaging, gestione remota, gestione dell'inventario e gestione del software. Questa applicazione è una soluzione completa di gestione per Linux che elimina la complessità delle attività informatiche riducendo l'overhead richiesto per gestire i sistemi Linux.

È possibile applicare patch ai dispositivi Linux utilizzando uno degli strumenti seguenti:

- Gestione delle patch
- Gestione pacchetti Linux

Gestione delle patch

Gestione patch è una funzione di ZENworks completamente integrata che fornisce una soluzione di gestione delle patch basate su agente, delle patch per la vulnerabilità e della conformità.

Gestione patch offre le seguenti funzionalità:

- Utilizza le firme per individuare le patch necessarie e consente di tenerne traccia nei rapporti per semplicità di gestione.
- Implementa linee di base obbligatorie affinché determinate patch siano sempre disponibili nel dispositivo.
- Applica patch solo alle distribuzioni SLES e RHEL.

Per ulteriori informazioni, vedere Capitolo 12, “Gestione patch”, a pagina 127.

Gestione pacchetti Linux

La gestione pacchetti Linux fornisce la funzionalità di gestione dei pacchetti di ZENworks Configuration Management per i dispositivi Linux (server e desktop)

e offre le seguenti funzionalità:

- Fornisce un singolo punto di gestione per l'applicazione di patch, l'installazione e l'aggiornamento dei pacchetti per un elevato numero di dispositivi Linux a livello aziendale.
- Esegue la copia speculare di aggiornamenti e pacchetti dagli archivi NU, RHN, RCE e YUM per patch e pacchetti come quelli ZENworks. È possibile assegnare tali pacchetti a dispositivi gestiti Linux per la gestione.
- Supporta il download di RPM delta sui dispositivi gestiti ogniqualvolta sono disponibili e applicabili, riducendo così la larghezza di banda necessaria durante l'applicazione delle patch.

- Consente di scegliere i cataloghi e i pacchetti dei quali si desidera eseguire una copia speculare.
- Consente di applicare patch ai server OES.

Gestione dei dispositivi mobili

Nel Centro di controllo ZENworks è inclusa la pagina **Introduzione alla gestione mobile** che contiene le spiegazioni dei task da eseguire per registrare e gestire i dispositivi mobili nella propria zona.

Per accedere alla pagina **Introduzione alla gestione mobile**:

1. Nel Centro di controllo ZENworks, fare clic su **Gestione mobile** (nel pannello di navigazione sinistro).

   Ciascun task di configurazione all'interno della pagina contiene un'icona contrassegnata con ⛔ o ✅ che ne indica lo stato di completamento, inoltre sono presenti uno o più collegamenti alla pagina in cui si deve completare il task.

   È inoltre possibile fare clic sull'icona ⓘ visualizzata in corrispondenza di ciascun task o sul collegamento alla **Guida** situato nell'angolo in alto a destra di ciascuna pagina per ottenere informazioni sul task.
2. Completare i task di **Configurazione** necessari per la registrazione dei dispositivi nella zona. Successivamente è possibile completare i task elencati nella sezione **Passaggi successivi** per gestire i dispositivi.

   Per ulteriori informazioni su ciascuno di questi task, vedere ZENworks Mobile Management Reference (in lingua inglese).

Registrazione dei dispositivi mobili

Registrazione di un dispositivo DEP iOS/iPadOS

La registrazione di un dispositivo DEP per un utente finale è facile: è possibile fare in modo che l'utente ignori la maggior parte dei prompt di attivazione del dispositivo modificando il profilo DEP. Prima di registrare un dispositivo DEP, assicurarsi che i seguenti prerequisiti vengano soddisfatti:

Prerequisiti

- Aggiungere un server DEP Server in ZCC che colleghi il server MDM ZENworks e il server MDM virtuale nel portale Apple.
- Assegnare i dispositivi al server MDM virtuale nel portale Apple. Questi dispositivi vengono quindi rilevati da ZENworks e compilati in ZCC.
- (Opzionale) Assegnare gli utenti al dispositivo, se si desidera che solo l'utente specificato sia associato al dispositivo durante la registrazione a DEP.
- (Opzionale) Modificare le impostazioni del profilo DEP per migliorare il processo di registrazione.
- (Condizionale) Se si modifica il profilo DEP, assicurarsi che questo venga assegnato correttamente al portale Apple.

Inoltre:

- Assegnare una policy di registrazione per i dispositivi mobili.
- (Condizionale) se si registra di nuovo un dispositivo che è stato disattivato permanentemente da un altro utente, assicurarsi che l'oggetto Dispositivo precedente venga cancellato in ZCC.
- (Opzionale) Assegnare una policy e-mail per dispositivi mobili per configurare l'account e-mail sul dispositivo.

Per ulteriori informazioni su ciascuno di questi task, vedere ZENworks Mobile Management Reference (in lingua inglese).

Procedura

Per registrare il dispositivo, seguire i prompt di configurazione. Dopo che l'utente ha configurato le impostazioni per il Wi-Fi, eseguire il login al dispositivo con le credenziali dell'utente. Se il dispositivo è assegnato a un utente specifico, specificare solo le credenziali di tale utente altrimenti la registrazione avrà esito negativo.

Una volta effettuata la registrazione del dispositivo, è possibile visualizzare lo **Stato distribuzione** del dispositivo in ZCC, che da **Rilevato** dovrebbe diventare **Gestito**. È possibile visualizzare tale stato nella pagina di riepilogo del dispositivo.

Registrazione di un dispositivo iOS/iPadOS tramite Apple Configurator

Apple Configurator è uno strumento Mac OS X utilizzato dagli amministratori per la distribuzione di dispositivi iOS e iPadOS in ambienti aziendali o formativi. Apple Configurator rende rapida e semplice la riassegnazione dei dispositivi, consentendo all'utente successivo di disporre di contenuti del tutto nuovi.

Prerequisiti

- Assegnare una policy di registrazione per i dispositivi mobili.
- Copiare l'URL di registrazione Apple in cui è specificato il server MDM nel quale verrà registrato il dispositivo. Per ottenere tale URL, in ZCC individuare **Configurazione** > **Gestione infrastruttura** > **Server MDM**. Selezionare un server MDM e fare clic su **URL di registrazione Apple**.
- (Opzionale) Assegnare una policy e-mail per dispositivi mobili per configurare l'account e-mail sul dispositivo.

Per ulteriori informazioni su ciascuno di questi task, vedere ZENworks Mobile Management Reference (in lingua inglese).

Procedura

1. Eseguire la connessione del dispositivo al Mac tramite la porta USB.
2. Fare clic con il pulsante destro del mouse e selezionare **Prepara** o selezionare **Prepara** nella barra dei menu superiore in Apple Configurator.
3. Selezionare **Manuale** nel menu a discesa **Configurazione**. Fare clic su **Avanti**.

4 Selezionare il server MDM in cui si desidera registrare il dispositivo. Se nel menu a discesa non è salvato alcun server MDM, selezionare **Nuovo server**.

5 Specificare un nome per il nuovo server e incollarlo nell'URL di registrazione Apple copiato da ZCC. Per ottenere tale URL, in ZCC individuare **Configurazione** > **Gestione infrastruttura** > **Server MDM**. Selezionare un server MDM e fare clic su **URL di registrazione Apple**. Copiare l'URL e incollarlo nella pagina Definisci un server MDM di Apple Configurator. Tale server MDM viene salvato per un uso futuro.

6 Selezionare **Supervisiona dispositivi** se si desidera impostare il dispositivo come supervisionato. La casella di controllo **Consenti ai dispositivi di associarsi ad altri computer** viene abilitata automaticamente.

7 Selezionare l'organizzazione che si occuperà della supervisione dei dispositivi specificati.

8 Nel menu a discesa **Impostazione Assistita** selezionare l'opzione appropriata se si desidera ignorare alcuni passaggi della procedura di registrazione del dispositivo. Verificare gli elementi di configurazione che si dovrebbero presentare durante la registrazione del dispositivo.

9 Fare clic su **Prepara** per preparare il dispositivo connesso.

Dopo la fase di preparazione, vengono ripristinate le impostazioni predefinite del dispositivo iOS/iPadOS. Dopo il ripristino del dispositivo, seguire le richieste visualizzate sul dispositivo iOS/iPadOS così come configurato nella pagina **Configura Impostazione Assistita di iOS** in Apple Configurator. Dopo aver immesso la password per il Wi-Fi, all'utente verranno richieste le credenziali.

Registrazione di un dispositivo iOS/iPadOS tramite il portale utente ZENworks

Questo scenario mostra come registrare un dispositivo iOS e iPadOS come dispositivo completamente gestito nella zona di gestione ZENworks. Questo tipo di registrazione consente di creare un profilo MDM sul dispositivo tramite cui è possibile applicare restrizioni e distribuire le app sul dispositivo.

Prerequisiti

- ZENworks supporta dispositivi che eseguono iOS versione 8 e successive.
- Per la registrazione dei dispositivi mobili è configurata e abilitata un'origine utente.
- Una policy di registrazione viene creata e assegnata all'utente.
- È assegnato un ruolo MDM a un server primario.
- Notifiche push per dispositivi iOS.
- Per abilitare ZENworks alla sincronizzazione di e-mail per gli account Exchange ActiveSync, è necessario configurare un server ActiveSync. Inoltre, si deve creare e assegnare una policy e-mail per dispositivi mobili e il server ZENworks deve essere configurato come server proxy per il server ActiveSync. In tal modo si consentirà a ZENworks di gestire le e-mail aziendali inviate e ricevute sul dispositivo.
- La registrazione dei dispositivi iOS tramite il browser Safari eseguito in modalità privata è supportata solo su iOS versioni 11 o successive.

Procedura

1. Nel browser Safari sul dispositivo, immettere *ZENworks_server_address*/zenworks-eup, dove *ZENworks_server_address* è il nome DNS o l'indirizzo IP del server MDM ZENworks.

   Viene visualizzata la schermata di login al portale utente ZENworks.

2. Immettere il nome utente e la password dell'utente. Se l'opzione **Consenti registrazione semplice** è selezionata per l'origine utente cui appartiene l'utente, non è necessario specificare il dominio di registrazione o altrimenti specificarlo.

   Tutti i dispositivi associati all'utente vengono visualizzati nel portale utente ZENworks.

3. Toccare **Registra** nell'angolo in alto a destra per visualizzare le opzioni di registrazione per il dispositivo.

4. Toccare **Solo dispositivo gestito** per visualizzare la schermata **Registra opzioni dispositivo**. Se si è configurata la policy di registrazione dispositivo mobile per consentire all'utente di specificare la proprietà del dispositivo (aziendale o personale), viene richiesto di specificare tali informazioni. Selezionare l'opzione di proprietà del dispositivo e fare clic su **OK**.

5. Toccare **Effettua il download del certificato** per visualizzare la schermata **Installa profilo**.

   Nota: se si sta registrando un dispositivo iOS 12.1.2 o meno recente, si verrà reindirizzati alla schermata Installa profilo quando si fa clic su Effettua il download del certificato. Fare clic su Installa e seguire i prompt per installare il profilo.

   5a Consentire al sito Web di effettuare il download del profilo di configurazione.

   5b Verrà effettuato il download del profilo di configurazione. Adesso, è possibile andare al menu Impostazioni per effettuare il download del profilo.

   5c Andare al menu Impostazioni e cliccare su **Generale** > **Profiles (Profili)**.

   5d Toccare **Profilo di attendibilità ZENworks**.

   5e Installare il profilo.

6. (Condizionale) Abilitare il certificato di registrazione sul dispositivo. Questo passaggio viene visualizzato nei dispositivi sui quali è in esecuzione iOS 10.3 o versioni successive. Per abilitare il certificato:

   6a Nel menu del dispositivo individuare **Impostazioni** e fare clic su **Generali**.

   6b Fare clic su **Info**.

   6c Fare clic su **Attendibilità certificati**.

   6d Abilitare il certificato radice visualizzato sullo schermo. Ritornare alla pagina EUP.

7. Nella schermata Registra come dispositivo gestito, toccare **Effettua il download del profilo** per visualizzare la schermata di installazione del profilo.

   Nota: se si sta registrando un dispositivo iOS 12.1.2 o meno recente, si verrà reindirizzati alla schermata Installa profilo quando si fa clic su **Effettua il download del profilo**. Toccare **Installa** e seguire le istruzioni per installare il profilo.

   7a Consentire al sito Web di effettuare il download del profilo.

   7b Verrà effettuato il download del profilo di configurazione. Adesso, è possibile andare al menu Impostazioni per effettuare il download del profilo.

7c Andare al menu **Impostazioni** sul dispositivo per installare il profilo e toccare **Generali** > **Profiles (Profili)**.

7d Toccare **ZENworks Device Enrollment Program Profile (Profilo del programma di registrazione del dispositivo ZENworks)**. In questa sezione è riportato il profilo MDM richiesto per la gestione del dispositivo da parte di ZENworks.

7e Toccare **Installa** e seguire le istruzioni per installare il profilo.

8 Ritornare alla pagina EUP. Il dispositivo viene visualizzato nell'elenco Dispositivi personali con lo stato **Registrazione in corso**. È necessario aggiornare il browser per cambiare lo stato in Dispositivo attivo.

A questo punto, in ZCC è possibile visualizzare la modalità di registrazione nella pagina Informazioni sul dispositivo. Per visualizzare le informazioni sul dispositivo, dal pannello di navigazione sinistro di ZCC, fare clic su **Dispositivi** > **Dispositivi mobili** (o individuare la cartella come configurato nella policy di registrazione dispositivo mobile), quindi selezionare il dispositivo appropriato. La registrazione viene visualizzata come **iOS MDM**.

9 A seconda della policy e-mail per dispositivi mobili assegnata all'utente o al dispositivo, viene configurato automaticamente un account e-mail sul dispositivo.

Registrazione dei dispositivi Android nella modalità profilo di lavoro

La modalità profilo di lavoro consente di creare container dedicati sui dispositivi per app e dati aziendali; in questo modo l'organizzazione è in grado di gestire solo i dati di sua pertinenza. Questa modalità è intesa per lo scenario BYOD, dove l'utente utilizza i propri dispositivi sul luogo di lavoro.

Prerequisiti

Impostazioni obbligatorie

- Creare una sottoscrizione ad Android Enterprise.
- Creare e assegnare una policy di registrazione per i dispositivi mobili.
- Creare e assegnare una policy di registrazione del profilo Android.
- Verificare che la versione di Android sia la 5.0 o successiva (per la modalità profilo di lavoro) o la 6.0 o successiva (per la modalità dispositivo gestito per il lavoro).

Impostazioni opzionali

- Invitare gli utenti a registrare i propri dispositivi.

Per ulteriori informazioni su ciascuno di questi task, vedere ZENworks Mobile Management Reference (in lingua inglese).

Procedura

Lo scenario elaborato in questa sezione è previsto per gli utenti che registrano i loro dispositivi su ZENworks per la prima volta. Per gli utenti che hanno già registrato i dispositivi nella modalità di base (solo app Android) e desiderano registrarsi nella modalità profilo di lavoro, vedere Registrazione del profilo di lavoro per gli utenti esistenti.

Procedura

1. Installare ZENworks Agent App da Google Play Store. In alternativa, l'utente può seguire la procedura indicata nella lettera di invito a scaricare ZENworks Agent App.
2. Fare clic su **Apri**, dopo l'installazione. Verrà visualizzata una breve descrizione di ZENworks Agent. Fare quindi clic su **Continua**.
3. Fare clic su **Attiva amministratore dispositivo** per consentire la gestione del dispositivo tramite l'app.
4. Accedere all'app specificando:

   Nome utente, Password, Dominio, URL server: specificare nome utente, password e dominio di registrazione (se **Consenti registrazione semplice** è disattivato per l'utente) insieme all'URL del server MDM ZENworks. L'utente può ottenere queste informazioni dalla lettera di invito.
5. Specificare la proprietà del dispositivo (aziendale o personale) se è stata configurata la policy di registrazione mobile in modo da consentire all'utente di specificare la proprietà. Toccare **OK**.
6. Seguire le richieste visualizzate nelle schermate rimanenti; il dispositivo configura automaticamente un profilo di lavoro e si registra in ZENworks. Viene visualizzata la schermata iniziale di ZENworks Agent App che mostra il dispositivo registrato e attivo.
7. Visualizzare le informazioni sul dispositivo in ZCC. Fare clic su **Dispositivi** > **Dispositivi mobili** (o selezionare la cartella in base alla configurazione nella policy di registrazione mobile) dal riquadro di navigazione sinistro in ZCC. Fare clic sul dispositivo appropriato e visualizzarne i dettagli nella pagina **Riepilogo**. La modalità di registrazione viene visualizzata come **App Android** ed è inoltre abilitata la **Modalità profilo di lavoro**.

Dopo la registrazione del dispositivo, l'icona di un badge associata all'icona di ZENworks Agent App e di altre app di sistema permetterà di distinguere le app di lavoro da quelle personali.

Registrazione del profilo di lavoro per gli utenti esistenti

Per gli utenti già registrati in ZENworks tramite la modalità di base di registrazione (solo App Android) e che ora desiderano essere registrati nella modalità profilo di lavoro, assegnare loro la policy di registrazione profilo Android.

Dopo aver assegnato la policy di registrazione mobile, gli utenti ricevono una notifica sui loro dispositivi per configurare un profilo di lavoro quando aprono ZENworks Agent App.

Fare clic su **Configura** e seguire le indicazioni per configurare il profilo di lavoro. Il dispositivo configura automaticamente il profilo di lavoro.

Registrazione di un dispositivo Android in modalità dispositivo gestito per il lavoro

La modalità dispositivo gestito per il lavoro consente agli amministratori di gestire l'intero dispositivo, che in questo modo viene utilizzato solo in ambito aziendale. Questa modalità è prevista soprattutto per i dispositivi di proprietà aziendale.

Prerequisiti

Impostazioni obbligatorie

- Creare una sottoscrizione ad Android Enterprise.
- Creare e assegnare una policy di registrazione per i dispositivi mobili.
- Creare e assegnare una policy di registrazione del profilo Android.
- Verificare che la versione di Android sia la 5.0 o successiva (per la modalità profilo di lavoro) o la 6.0 o successiva (per la modalità dispositivo gestito per il lavoro).

Procedura

1. Seguire le schermate di configurazione iniziale, come quelle per configurazione della lingua e della rete Wi-Fi.
2. Specificare l'identificatore AFW (afw#zenworks) nella schermata di configurazione in cui viene visualizzato il campo ID e-mail.
3. Fare clic su **Avanti** nella pagina Android Enterprise per procedere con l'installazione di ZENworks App.

   ZENworks Agent App viene scaricata automaticamente sul dispositivo.
4. Fare clic su **Installa** per installare l'app sul dispositivo e seguire tutte le richieste per completare la configurazione del dispositivo.
5. Rispondere alle richieste visualizzate sulle schermate rimanenti per configurare un dispositivo gestito per il lavoro. Il dispositivo è ora configurato ma deve ancora essere registrato come dispositivo gestito per il lavoro.
6. Accedere all'app con i dettagli seguenti:

   Nome utente, Password, Dominio, URL server: specificare nome utente, password e dominio di registrazione (se **Consenti registrazione semplice** è disattivato per l'utente) insieme con l'URL del server del server MDM ZENworks.

   Il dispositivo gestito per il lavoro viene configurato automaticamente sul dispositivo.

Visualizzare le informazioni sul dispositivo in ZCC. Fare clic su **Dispositivi** > **Dispositivi mobili** (o selezionare la cartella in base alla configurazione nella policy di registrazione mobile) dal riquadro di navigazione sinistro in ZCC. Fare clic sul dispositivo appropriato e visualizzarne i dettagli nella pagina **Riepilogo**. La modalità di registrazione viene visualizzata come **App Android** ed è inoltre abilitata la **Modalità dispositivo gestito per il lavoro**.

Registrazione come dispositivo solo ActiveSync

Prerequisiti

Prima di registrare un dispositivo mobile come dispositivo completamente gestito o dispositivo Solo e-mail, è necessario assicurarsi che i seguenti prerequisiti siano soddisfatti:

- ZENworks supporta i dispositivi con ActiveSync 12.1 e versioni più recenti.
- Per la registrazione dei dispositivi mobili è configurata e abilitata un'origine utente.

- Una policy di registrazione viene creata e assegnata all'utente.
- È assegnato un ruolo MDM a un server primario.
- Notifiche push per un dispositivo Android.
- Per abilitare ZENworks alla sincronizzazione di e-mail per gli account Exchange ActiveSync, è necessario configurare un server ActiveSync. Inoltre, si deve creare e assegnare una policy e-mail per dispositivi mobili e il server ZENworks deve essere configurato come server proxy per il server ActiveSync.

Procedura

Questo scenario mostra come registrare un dispositivo come dispositivo Solo e-mail nella zona di gestione ZENworks. In questo scenario è riportata la procedura dettagliata per registrare un dispositivo iOS come dispositivo Solo e-mail.

1. Immettere *`Indirizzo_server_ZENworks`*`/zenworks-eup`, dove *`Indirizzo_server_ZENworks`* è il nome DNS o l'indirizzo IP del server MDM ZENworks, in un browser del dispositivo.

   Viene visualizzata la schermata di login al portale utente ZENworks.

2. Immettere nome utente e password dell'utente nel portale utente ZENworks. Se l'opzione **Consenti registrazione semplice** è selezionata per l'origine utente cui appartiene l'utente, non è necessario specificare il dominio di registrazione o altrimenti specificarlo.

3. Toccare **Registra** nell'angolo in alto a destra per visualizzare le opzioni di registrazione per il dispositivo.

4. Toccare **Solo e-mail** per visualizzare la schermata **Registra solo come e-mail**. Usare le informazioni visualizzate per creare un account e-mail per l'utente.

   Dopo che l'utente ha configurato l'account e-mail, riceve un'e-mail in cui gli viene comunicato che il processo di registrazione deve essere completato. È possibile modificare i contenuti di tale e-mail in ZCC selezionando **Configurazione** > **Impostazioni zona di gestione** > **Evento e messaggi** > **Notifiche e-mail**. Fare clic sull'e-mail pertinente e modificare i rispettivi contenuti.

5. Fare clic sul collegamento al portale per l'utente finale ZENworks fornito nell'e-mail o visitare il portale per l'utente finale ZENworks come descritto in Passo 1.

   Nel portale utente ZENworks, il dispositivo è visualizzato nell'elenco Dispositivi personali. A questo punto il dispositivo è stato aggiunto nella zona di gestione ZENworks, ma la sua registrazione è in sospeso.

6. Toccare **Completa registrazione**.

   Se si è configurata la policy di registrazione dispositivo mobile per consentire all'utente di specificare la proprietà del dispositivo (aziendale o personale), viene richiesto di specificare tali informazioni. Fornire sul dispositivo le informazioni richieste per la registrazione, quindi toccare **OK**.

   L'elenco Dispositivi personali viene aggiornato per mostrare che il dispositivo è registrato e attivo.

7 Verificare che il dispositivo riceva e-mail inviando un'e-mail all'utente da un altro account.

Una volta registrato il dispositivo nella zona di gestione ZENworks, la modalità di registrazione del dispositivo viene visualizzata come **ActiveSync** nella pagina Informazioni sul dispositivo di ZCC. Per visualizzare le informazioni sul dispositivo, dal pannello di navigazione sinistro di ZCC, fare clic su **Dispositivi** > **Dispositivi mobili** (o individuare la cartella come configurato nella policy di registrazione dispositivo mobile), quindi selezionare il dispositivo appropriato.

10 Endpoint Security Management

ZENworks Endpoint Security Management semplifica la sicurezza degli endpoint grazie alla gestione centralizzata delle policy di sicurezza per i dispositivi gestiti. È possibile controllare l'accesso di un dispositivo a dispositivi di memorizzazione rimovibili, reti wireless e applicazioni. Inoltre, è possibile proteggere i dati mediante cifratura e la comunicazione in rete tramite l'applicazione di firewall (porte, protocolli ed elenchi di controlli dell'accesso). nonché modificare la sicurezza di un dispositivo endpoint in base alla relativa ubicazione.

Le sezioni seguenti descrivono come utilizzare Endpoint Security Management per proteggere i dispositivi in ufficio, a casa o nel terminal di un aeroporto:

Attivazione di Endpoint Security Management

Se Endpoint Security Management non è stato attivato durante l'installazione della zona di gestione fornendo una chiave di licenza o attivando la valutazione, completare i seguenti passaggi:

1. Nel Centro di controllo ZENworks, fare clic su **Configurazione**.
2. Nel pannello Licenze, fare clic su **ZENworks 2020 Endpoint Security Management**.
3. Selezionare **Valuta/attiva prodotto**, quindi completare i seguenti campi:

   Utilizza valutazione: selezionare questa opzione per abilitare un periodo di valutazione di 60 giorni. Dopo il periodo di 60 giorni, è necessario applicare una chiave di licenza per continuare a utilizzare il prodotto.

   Chiave di licenza del prodotto: specificare la chiave di licenza acquistata per Endpoint Security Management. Per acquistare una licenza del prodotto, visitare il sito dei prodotti ZENworks Endpoint Security Management (http://www.novell.com/products/zenworks/endpointsecuritymanagement).
4. Fare clic su **OK**.

Abilitazione dell'agente di sicurezza endpoint

L'agente ZENworks è responsabile della registrazione dei dispositivi, della distribuzione del contenuto e degli aggiornamenti software di un dispositivo.

Nei dispositivi in cui è attivato ZENworks Endpoint Security Management (licenza completa o copia di valutazione), oltre all'agente ZENworks viene installato l'agente di sicurezza endpoint. L'agente di sicurezza endpoint è responsabile dell'applicazione delle impostazioni delle policy di sicurezza nel dispositivo.

Verificare che l'agente di sicurezza endpoint sia abilitato. Per informazioni, vedere “Configurazione delle funzioni dell'agente ZENworks” a pagina 39.

Creazione delle ubicazioni

I requisiti di sicurezza di un dispositivo possono variare a seconda dell'ubicazione. Possono ad esempio sussistere restrizioni per firewall personali diverse a seconda che un dispositivo si trovi nel terminal di un aeroporto o in un ufficio protetto da un firewall aziendale.

Affinché i requisiti di sicurezza di un dispositivo siano appropriati per l'ubicazione utilizzata, Endpoint Security Management supporta sia le policy globali che le policy basate sulle ubicazioni. Una policy globale viene applicata indipendentemente dall'ubicazione del dispositivo. Una policy basata sulle ubicazioni viene applicata solo quando l'ubicazione corrente del dispositivo soddisfa i criteri di un'ubicazione associata alla policy. Ad esempio, se si crea una policy basata sulle ubicazioni per il proprio ufficio aziendale e la si assegna a un computer portatile, tale policy verrà applicata solo quando l'ubicazione del computer corrisponde all'ufficio aziendale.

Se si desidera utilizzare le policy basate sulle ubicazioni, è necessario definire innanzitutto le ubicazioni appropriate per l'organizzazione. Un'ubicazione è un luogo o un tipo di luogo per il quale si dispone di requisiti di sicurezza specifici. È possibile ad esempio applicare requisiti di sicurezza diversi per un dispositivo utilizzato in ufficio, a casa o in un aeroporto.

Le ubicazioni sono definite in base agli ambienti di rete. Si consideri ad esempio un'organizzazione con un ufficio a New York e uno a Tokyo. Entrambi gli uffici hanno gli stessi requisiti. Verrà creata pertanto un'ubicazione Ufficio, che verrà associata a due ambienti di rete, ovvero Rete ufficio di New York e Rete ufficio di Tokyo. Ciascuno di questi ambienti è definito esplicitamente da un insieme di servizi gateway, server DNS e punti di accesso wireless. Ogni volta che determina che l'ambiente corrente corrisponde a Rete ufficio di New York o Rete ufficio di Tokyo, l'agente di sicurezza endpoint imposta l'ubicazione su Ufficio e applica le policy di sicurezza associate a tale ubicazione.

Per informazioni dettagliate su come creare ubicazioni, vedere “Creazione delle ubicazioni” a pagina 35.

Creazione di una policy di sicurezza

Esistono 12 diverse policy di sicurezza:

Le impostazioni di sicurezza di un dispositivo sono definite mediante policy di sicurezza applicate dall'agente di sicurezza endpoint. Otto policy di sicurezza definiscono una gamma di funzionalità correlate alla sicurezza. È possibile utilizzare tutte o solo alcune delle policy in base alle esigenze dell'organizzazione.

Policy	Scopo
Controllo delle applicazioni	Blocca l'esecuzione delle applicazioni o impedisce alle applicazioni di accedere a Internet. È possibile specificare quali applicazioni bloccare e a cui negare l'accesso a Internet.
Hardware di comunicazione	Disabilita il seguente hardware di comunicazione: 1394-Firewire, IrDA-Infrarossi, Bluetooth, seriale/parallele, connessione remota, connessione cablata e wireless. Ciascun hardware di comunicazione viene configurato a parte. Quindi, è possibile disabilitare alcuni tipi di hardware (come Blueetooth e la connessione remota) e lasciare gli altri abilitati.
Cifratura dei dati	Abilita la cifratura dati dei file sui dispositivi di archiviazione rimovibili.
Firewall	Controlla la connettività di rete, disabilitando le porte, i protocolli e gli indirizzi di rete (IP e MAC).
Cifratura dei dati di Microsoft	Gestisce la cifratura delle unità dati rimovibili e delle cartelle su disco fisso utilizzando rispettivamente Microsoft BitLocker e Microsoft Encrypting File System (EFS).
Script	esegue uno script (JScript o VBScript) su un dispositivo. È possibile specificare i trigger che determinano l'esecuzione dello script. I trigger possono essere basati su azioni dell'agente di sicurezza endpoint, modifiche all'ubicazione o intervalli di tempo.
Controllo periferiche di memorizzazione	Controlla l'accesso alle unità CD/DVD, alle unità disco floppy e alle unità di memorizzazione riscrivibili. Ciascuno tipo di dispositivo di memorizzazione viene configurato a parte. Quindi, è possibile disabilitare alcuni dispositivi e abilitarne altri.
Connettività USB	Controlla l'accesso ai dispositivi USB, come i dispositivi di memorizzazione riscrivibili, le stampanti e i dispositivi di input (tastiere, mouse, ecc.). È possibile specificare singoli dispositivi o gruppi di dispositivi. È possibile ad esempio disabilitare l'accesso a una stampante specifica e abilitare l'accesso a tutti i dispositivi USB Sandisk.
Applicazione VPN	Applica una connessione VPN basata sull'ubicazione del dispositivo. Ad esempio, se l'ubicazione del dispositivo è sconosciuta, è possibile applicare una connessione VPN per l'instradamento di tutto il traffico Internet.
Wi-Fi	Disabilita gli adattatori wireless, blocca le connessioni wireless, controlla le connessioni ai punti di accesso wireless e così via.

Oltre alle policy di sicurezza sopra descritte, le seguenti policy di sicurezza consentono di proteggere e configurare l'agente di sicurezza endpoint. A causa della natura di queste due policy, è consigliabile crearle e assegnarle per prime.

Policy	Scopo
Impostazioni di sicurezza	Protegge l'agente di sicurezza endpoint dalle manomissioni e dai tentativi di disinstallazione. Per informazioni in merito alla configurazione delle impostazioni ZENworks Agent Security, vedere "Configurazione della sicurezza dell'agente ZENworks" a pagina 41.
Assegnazione ubicazione	Fornisce l'elenco di ubicazioni consentite per un dispositivo o un utente. L'agente di sicurezza endpoint valuta l'ambiente di rete corrente per controllare se corrisponde a una delle ubicazioni consentite. Se viene trovata una corrispondenza, l'ubicazione diventa l'ubicazione di sicurezza e l'agente applica le policy di sicurezza associate a tale ubicazione. Se invece non viene trovata alcuna corrispondenza con le ubicazioni riportate nell'elenco, vengono applicate le policy di sicurezza associate all'ubicazione di tipo Sconosciuto. Se si prevede di utilizzare policy basate sulle ubicazioni, verificare che a ogni utente o dispositivo sia assegnata una policy Assegnazione ubicazione. In caso contrario, l'agente di sicurezza endpoint non potrà applicare al dispositivo alcuna policy basata sulle ubicazioni.

Per creare una policy di sicurezza:

1. Nel Centro di controllo ZENworks fare clic su **Policy** per visualizzare la pagina delle policy.
2. Nel pannello Policy fare clic su **Nuovo** > **Policy** per avviare la Creazione guidata nuova policy.
3. Nella pagina Seleziona piattaforma, selezionare **Windows**, quindi fare clic su **Successivo**.
4. Nella pagina Seleziona categoria di policy, selezionare **Policy di sicurezza endpoint Windows**, quindi fare clic su **Avanti**.
5. Nella pagina Selezionare il tipo di policy, selezionare il tipo di policy che si desidera creare, quindi fare clic su **Avanti**.

   Se sono state create ubicazioni e si prevede di utilizzare policy basate sulle ubicazioni, è necessario creare almeno una policy Assegnazione ubicazione e assegnarla ai dispositivi o agli utenti dei dispositivi. In caso contrario, per i dispositivi non sarà disponibile alcuna delle ubicazioni create e pertanto non potrà essere applicata alcuna delle policy basate sulle ubicazioni.
6. Nella pagina Definisci dettagli, immettere un nome per la policy e selezionare la cartella in cui posizionare la policy.

   Il nome deve essere univoco rispetto a tutte le altre policy contenute nella cartella selezionata.
7. (Condizionale) Se viene visualizzata la pagina Configura Eredità e Assegnazione ubicazione, configurare le seguenti impostazioni, quindi fare clic su **Avanti**.
   - **Eredità:** lasciare l'impostazione **Eredita da gerarchia policy** selezionata se si desidera abilitare questa policy per ereditare le impostazioni da policy dello stesso tipo assegnate a un livello superiore nella gerarchia delle policy. Se ad esempio si assegna questa policy a un dispositivo e un'altra policy (dello stesso tipo) alla cartella del dispositivo, abilitando questa

opzione la policy potrà ereditare le impostazioni dalla policy assegnata alla cartella del dispositivo. Deselezionare l'impostazione **Eredita da gerarchia policy** se non si desidera che la policy erediti le impostazioni.

- **Assegnazione ubicazione:** le policy possono essere globali o basate sulle ubicazioni. Una policy globale viene applicata indipendentemente dall'ubicazione. Una policy basata sulle ubicazioni invece viene applicata solo quando il dispositivo rileva come ubicazione corrente una delle ubicazioni assegnate alla policy.

  Specificare se la policy è globale o basata sulle ubicazioni. Se si specifica che la policy è basata sulle ubicazioni, fare clic su **Aggiungi**, selezionare le ubicazioni a cui si desidera assegnare la policy, quindi fare clic su **OK** per aggiungerle all'elenco.

8 Configurare le impostazioni specifiche della policy, quindi fare clic su **Avanti** finché non viene visualizzata la pagina Riepilogo.

  Per informazioni sulle impostazioni di una policy, fare clic su **Guida** > **Pagina attuale** nel Centro di controllo ZENworks.

9 Nella pagina Riepilogo, esaminare le informazioni per accertarsi che siano corrette. In caso di errori, fare clic sul pulsante **Indietro** per visualizzare nuovamente la pagina appropriata della procedura guidata e apportare le modifiche necessarie. Se invece le informazioni sono corrette, selezionare (se lo si desidera) una delle seguenti opzioni, quindi fare clic su **Fine**.

- **Crea come sandbox:** selezionare questa opzione per creare la policy come versione sandbox. La versione sandbox è isolata dagli utenti e dai dispositivi finché non viene pubblicata. È ad esempio possibile assegnarla a utenti e dispositivi, ma solo dopo la pubblicazione.
- **Definisci proprietà aggiuntive:** selezionare questa opzione per visualizzare le pagine delle proprietà della policy. Queste pagine consentono di modificare le impostazioni di una policy e di assegnare la policy agli utenti e ai dispositivi.

Assegnazione di una policy agli utenti e ai dispositivi

Dopo aver creato una policy, è necessario applicarla ai dispositivi assegnandola ai dispositivi o agli utenti dei dispositivi.

1 Nel pannello Policy, selezionare la casella di controllo accanto alla policy che si desidera assegnare.

2 Fare clic su **Azione** > **Assegna a dispositivo**.

  oppure

  Fare clic su **Azione** > **Assegna a utente.**

3 Seguire le istruzioni visualizzate per assegnare la policy.

  Fare clic sul pulsante della **guida** su ciascuna pagina della procedura guidata per informazioni dettagliate sulla pagina.

  Al termine della procedura guidata, i dispositivi o gli utenti a cui è stata assegnata la policy vengono aggiunti nella pagina Relazioni della policy. Fare clic sulla policy per visualizzare le assegnazioni.

Assegnazione di una policy alla zona

È possibile assegnare policy di sicurezza alla zona di gestione. Al momento della determinazione delle policy effettive da applicare a un dispositivo, le policy Zona vengono valutate dopo tutte le policy assegnate agli utenti e ai dispositivi. Si considerino le seguenti situazioni:

- Se non sono assegnate policy Firewall a un dispositivo o al relativo utente (direttamente o tramite un gruppo o una cartella), la policy Firewall zona diventa la policy effettiva e viene applicata al dispositivo.
- Se sono assegnate policy Firewall a un dispositivo o al relativo utente, entrambe le policy vengono valutate e unite per determinare la policy Firewall effettiva da applicare al dispositivo. Dopo aver determinato la policy effettiva in base alle policy assegnate all'utente e a quelle assegnate al dispositivo, viene utilizzata la policy Firewall zona per fornire gli eventuali valori 1) non impostati nella policy Firewall effettiva e 2) aggiuntivi (ad esempio le tabelle multivalore Regole porte/protocolli).

Le policy Zona possono essere definite a tre livelli. In questo modo è possibile assegnare policy Zona diverse a dispositivi diversi nell'ambito della zona di gestione.

- **Zona di gestione:** le policy assegnate alla zona di gestione diventano le policy Zona di tutti i dispositivi, a meno che non si specifichino policy Zona diverse a livello di cartella dispositivo o a livello di dispositivo.
- **Cartella dispositivo:** le policy definite a livello di cartella dispositivo sostituiscono la zona di gestione (e le eventuali cartelle dispositivo superiori) e diventano le policy Zona di tutti i dispositivi contenuti nella struttura di cartelle, a meno che non si specifichino policy Zona diverse per una sottocartella o per un singolo dispositivo.
- **Dispositivo:** le policy definite per un singolo dispositivo sostituiscono la zona di gestione e la cartella dispositivo e diventano le policy Zona del dispositivo.

Nei passaggi riportati di seguito vengono fornite istruzioni per l'assegnazione delle policy alla zona di gestione.

1. Nel Centro di controllo ZENworks, fare clic su **Configurazione** per visualizzare la pagina di configurazione.
2. Nel pannello Impostazioni zona di gestione, fare clic su **Gestione sicurezza endpoint**.
3. Fare clic su **Impostazioni policy di zona** per visualizzare la pagina Impostazioni policy di zona.
4. Fare clic su **Aggiungi**, ricercare e selezionare le policy che si desidera assegnare alla zona, quindi fare clic su **OK** per aggiungerle all'elenco.
5. Dopo aver aggiunto le policy desiderate, fare clic su **OK**.

Ulteriori informazioni

Per ulteriori informazioni su ZENworks Endpoint Security Management, vedere i seguenti documenti:

- *ZENworks Endpoint Security Policies Reference* (in lingua inglese)
- *ZENworks Endpoint Security Agent Reference* (in lingua inglese)

- *ZENworks Endpoint Security Utilities Reference* (in lingua inglese)
- *ZENworks Endpoint Security Scripting Reference* (in lingua inglese)

11 FDE (Full Disk Encryption)

ZENworks Full Disk Encryption protegge i dati di un dispositivo da tentativi di accesso non autorizzati quando il dispositivo è spento o in modalità ibernazione. Per eseguire questa operazione, viene utilizzata una combinazione di funzionalità di cifratura del disco e autenticazione di preavvio.

FDE (Full Disk Encryption) fornisce la cifratura basata su software in dischi rigidi standard, a stato solido e con cifratura automatica. Viene eseguita la cifratura di tutti i volumi dei dischi (o di alcuni volumi selezionati), inclusi i file temporanei, i file di scambio e quelli del sistema operativo in esecuzione sui volumi. Non è possibile accedere ai dati del volume fino a quando un utente valido non esegue correttamente il login e non è possibile accedere mai ai dati avviando il dispositivo da supporti come CD/DVD, dischi floppy o unità USB. Per un utente autenticato, l'accesso ai dati sul disco cifrato non è diverso da quello ai dati sul disco non cifrato.

FDE (Full Disk Encryption) fornisce l'autenticazione di preavvio opzionale per dischi rigidi. Il componente ZENworks Pre-Boot Authentication (PBA) viene installato come piccola partizione di Linux sul disco rigido. Il login viene eseguito tramite il componente ZENworks PBA, che è protetto da eventuali modifiche grazie ai checksum MD5 e dall'estrazione delle password grazie alla cifratura avanzata delle chiavi.

Il componente ZENworks PBA supporta la funzionalità Single Sign On con il client di Windows, consentendo così agli utenti di eseguire il login contemporaneamente a ZENworks PBA e a Windows immettendo un solo set di credenziali (utente/password o smart card).

Attivazione di Full Disk Encryption

Se Full Disk Encryption non è stato attivato durante l'installazione della zona di gestione, specificando una chiave di licenza o attivando la licenza di valutazione, è necessario farlo adesso.

Per attivare Full Disk Encryption:

1. Nel Centro di controllo ZENworks fare clic su **Configurazione**.
2. Nel pannello Licenze fare clic su **ZENworks 2020 Full Disk Encryption**.
3. Selezionare **Valuta/attiva prodotto**, quindi completare i seguenti campi:

   Utilizza valutazione: selezionare questa opzione per abilitare un periodo di valutazione di 60 giorni. Dopo il periodo di 60 giorni, è necessario applicare una chiave di licenza per continuare a utilizzare il prodotto.

Chiave di licenza del prodotto: specificare la chiave di licenza acquistata per ZENworks Full Disk Encryption. Per acquistare una licenza del prodotto, visitare il sito del prodotto ZENworks Full Disk Encryption (http://www.novell.com/products/zenworks/full-disk-encryption).

4 Fare clic su **OK**.

Abilitazione dell'agente FDE (Full Disk Encryption)

L'agente ZENworks è responsabile della registrazione dei dispositivi, della distribuzione del contenuto e degli aggiornamenti software di un dispositivo.

Nei dispositivi in cui è attivato ZENworks Full Disk Encryption (licenza completa o copia di valutazione), oltre all'agente ZENworks viene installato l'agente FDE (Full Disk Encryption). L'agente FDE è responsabile della cifratura e decifratura dei dischi in base alla policy di cifratura del disco applicata a un dispositivo.

È necessario verificare che tale agente sia abilitato. Per informazioni, vedere Configurazione delle funzioni dell'agente ZENworks.

Importante: in ZENworks Full Disk Encryption non è supportato l'Avvio protetto di Windows, pertanto è necessario disabilitare questa funzione prima di installare l'agente FDE (Full Disk Encryption) nei dispositivi. Per ulteriori informazioni sui requisiti di sistema, vedere "System Requirements" in *ZENworks Full Disk Encryption Agent Reference* (in lingua inglese).

Creazione di una policy di cifratura del disco

La cifratura dei dischi di un dispositivo e l'uso del componente ZENworks Pre-boot Authentication (facoltativo) sono entrambi controllati dalla policy di cifratura del disco.

Per creare una policy di cifratura del disco:

1 Nel Centro di controllo ZENworks fare clic su **Policy** per visualizzare la pagina delle policy.

2 Nel pannello Policy fare clic su **Nuovo** > **Policy** per avviare la Creazione guidata nuova policy.

3 Nella pagina Seleziona piattaforma, selezionare **Windows**, quindi fare clic su **Successivo**.

4 Nella pagina Seleziona categoria di policy, selezionare **Policy Full Disk Encryption Windows**, quindi fare clic su **Successivo**.

5 Nella pagina Selezionare il tipo di policy, selezionare **Policy di cifratura disco**, quindi fare clic su **Avanti**.

6 Nella pagina Definisci dettagli, immettere un nome per la policy e selezionare la cartella in cui posizionare la policy.

Il nome deve essere univoco rispetto a tutte le altre policy contenute nella cartella selezionata.

7 Configurare le impostazioni specifiche della policy, quindi fare clic su **Avanti** finché non viene visualizzata la pagina Riepilogo.

Per informazioni sulle impostazioni di una policy, fare clic su **Guida** > **Pagina attuale** nel Centro di controllo ZENworks.

8 Nella pagina Riepilogo, esaminare le informazioni per accertarsi che siano corrette. In caso di errori, fare clic sul pulsante **Indietro** per visualizzare nuovamente la pagina appropriata della procedura guidata e apportare le modifiche necessarie. Se invece le informazioni sono corrette, selezionare (se lo si desidera) una delle seguenti opzioni, quindi fare clic su **Fine**.

- **Crea come sandbox:** selezionare questa opzione per creare la policy come versione sandbox. La versione sandbox è isolata dagli utenti e dai dispositivi finché non viene pubblicata. È ad esempio possibile assegnarla a utenti e dispositivi, ma solo dopo la pubblicazione.
- **Definisci proprietà aggiuntive:** selezionare questa opzione per visualizzare le pagine delle proprietà della policy. Queste pagine consentono di modificare le impostazioni di una policy e di assegnare la policy agli utenti e ai dispositivi.

Assegnazione della policy ai dispositivi

Dopo aver creato una policy di cifratura del disco, è necessario assegnarla ai dispositivi.

La policy di cifratura del disco è specifica dei dispositivi Può essere assegnata a dispositivi e a cartelle dispositivo, mentre non può essere assegnata a gruppi dispositivo, utenti, gruppi utente o cartelle utente.

Viene inoltre applicata solo la policy più vicina al dispositivo. Nel caso ad esempio in cui a un dispositivo e alla relativa cartella vengano assegnate più policy, viene applicata quella assegnata direttamente al dispositivo.

Importante: la policy di cifratura disco non è supportata nei dispositivi Windows che utilizzano BIOS UEFI. Se si assegna una policy di cifratura disco a un dispositivo Windows UEFI, la policy non viene applicata al dispositivo.

---

1 Nel pannello Policy, selezionare la casella di controllo accanto alla policy di cifratura del disco che si desidera assegnare.

2 Fare clic su **Azione** > **Assegna a dispositivo**.

3 Seguire le istruzioni visualizzate per assegnare la policy.

Fare clic sul pulsante della **guida** su ciascuna pagina della procedura guidata per informazioni dettagliate sulla pagina.

Al termine della procedura guidata, i dispositivi a cui è stata assegnata la policy vengono aggiunti alla pagina Relazioni della policy. Fare clic sulla policy per visualizzare le assegnazioni.

Comprendere cosa accade dopo che una policy viene assegnata a un dispositivo

Dopo aver assegnato una policy a un dispositivo, il workflow di applicazione della policy e di cifratura del disco varia leggermente se si utilizza un'autenticazione di preavvio. Di seguito sono riportati i concetti per la cifratura disco e l'autenticazione di preavvio necessari per capire quando applicare una policy di cifratura disco a un dispositivo.

Cifratura disco

ZENworks Full Disk Encryption fornisce la cifratura basata su software in dischi rigidi standard, a stato solido e con cifratura automatica.

Full Disk Encryption fornisce la cifratura basata su settori dell'intero disco o di volumi selezionati (partizioni). Vengono cifrati tutti i file di un volume, inclusi eventuali file temporanei, file swap o file del sistema operativo. Dal momento che tutti i file sono cifrati, non è possibile accedere ai dati quando si avvia il computer da supporti esterni come un CD-ROM, un disco floppy o un'unità USB.

I dischi rigidi compatibili sono quelli da 3,5 o 2,5 pollici dotati di interfaccia standard IDE, SATA o PATA.

È possibile scegliere l'algoritmo di cifratura standard del settore (AES, Blowfish, DES o DESX) e la lunghezza della chiave che soddisfano meglio i requisiti della propria organizzazione. Se il firmware del dispositivo è configurato per UEFI, vengono utilizzati automaticamente l'algoritmo AES e la lunghezza chiave 256.

Nota: il modulo di cifratura utilizzato in ZENworks Full Disk Encryption per cifrare i dischi rigidi standard *non* è certificato FIPS (Federal Information Processing Standard) 140-2. Nel modulo di cifratura sono tuttavia implementati standard coerenti con la certificazione FIPS 140-2 di Livello 1.

Autenticazione di preavvio

ZENworks Full Disk Encryption protegge i dati di un dispositivo quando questo è spento o è in modalità di ibernazione. Non appena qualcuno esegue il login al sistema operativo Windows, i volumi cifrati non sono più protetti e i dati possono essere accessibili da chiunque. Per rendere più sicuro il login, è possibile utilizzare ZENworks Pre-Boot Authentication (PBA).

ZENworks PBA è un componente basato su Linux. Quando si applica la policy di cifratura disco a un dispositivo, sul disco rigido viene creata una partizione di 500 MB contenente un kernel Linux e ZENworks PBA.

Durante il funzionamento normale il dispositivo si avvia sulla partizione Linux e carica ZENworks PBA. Non appena l'utente fornisce le credenziali (ID utente/password o smart card), il software PBA viene terminato e viene eseguito l'avvio del sistema operativo Windows. In questo modo è possibile accedere ai dati cifrati sulle unità Windows precedentemente nascoste e inaccessibili.

Alla partizione Linux viene applicata la protezione avanzata per aumentare la sicurezza e ZENworks PBA non può essere modificato grazie all'utilizzo di checksum MD5 e della cifratura avanzata per le chiavi di autenticazione.

ZENworks Pre-Boot Authentication è vivamente consigliato. Se non si utilizza ZENworks PBA, i dati cifrati vengono protetti solo tramite l'autenticazione di Windows.

Per ulteriori informazioni su ZENworks Pre-Boot Authentication, vedere *ZENworks Full Disk Encryption PBA Reference* (in lingua inglese)

Ulteriori informazioni

Per ulteriori informazioni su ZENworks Full Disk Encryption, vedere la documentazione seguente:

- *ZENworks Full Disk Encryption Policy Reference* (in lingua inglese)
- *ZENworks Full Disk Encryption Agent Reference* (in lingua inglese)
- *ZENworks Full Disk Encryption PBA Reference* (in lingua inglese)
- *ZENworks Full Disk Encryption Emergency Recovery Reference* (in lingua inglese)

12 Gestione patch

Gestione patch consente di applicare automaticamente e coerentemente le patch del software per ridurre al minimo vulnerabilità e problemi.

Gestione patch rimane aggiornato con le patch e le correzioni più recenti tramite una regolare comunicazione Internet con il servizio di sottoscrizione delle patch di ZENworks. Dopo il periodo di valutazione iniziale di 60 giorni, Gestione patch richiede una sottoscrizione a pagamento per continuare a scaricare quotidianamente le informazioni sulla vulnerabilità e sulle patch più recenti.

Quando il servizio di sottoscrizione rende disponibile una nuova patch, un server ZENworks scarica le relative informazioni. È possibile sia distribuire la patch ai dispositivi, sia ignorarla.

Dopo aver effettuato il download delle patch sul server ZENworks ed eseguito una scansione delle patch, è possibile individuare i dispositivi vulnerabili presenti nella zona tramite Gestione patch. Tuttavia, non è possibile individuare con facilità la vulnerabilità evidenziata dalla patch. Per farlo, occorre aprire la finestra Dettagli patch o conoscere l'ID CVE in base al quale effettuare una ricerca. Adesso, come parte della funzione di sicurezza, in ZENworks è disponibile una nuova vista che semplifica la configurazione e il controllo della sicurezza nella propria zona. La vista basata sulle vulnerabilità e l'approccio alle soluzioni consentono di comprendere con immediatezza il comportamento di sicurezza dei dispositivi. È possibile individuare le patch in base alle informazioni CVE e procedere alla correzione dei dispositivi vulnerabili applicando il pacchetto o la policy per la soluzione patch pertinente. ZENworks individua queste vulnerabilità in base al seguente processo:

1. L'amministratore crea ed esegue una sottoscrizione CVE per importare i dati dall'archivio NVD.
2. L'amministratore crea ed esegue una sottoscrizione patch per importare i dati dall'archivio dei contenuti delle patch.

   In seguito all'esecuzione delle sottoscrizioni CVE e patch, i CVE e le patch vengono importati nel server ZENworks configurato.
3. ZENworks mappa le patch ai CVE in base all'ID CVE associato alla firma della patch.

   Con la scansione delle patch, prevista dal processo di aggiornamento del dispositivo, vengono individuati i dispositivi vulnerabili. Gli utenti possono inoltre configurare una pianificazione di scansione delle patch o eseguire manualmente il task rapido di avvio della scansione delle patch in base alle necessità.
4. Le patch applicabili vengono quindi distribuite ai dispositivi vulnerabili tramite le policy di patch o i pacchetti di soluzione.

In seguito all'installazione delle patch dei CVE sul dispositivo, quest'ultimo non è più vulnerabile.

Nelle sezioni seguenti viene illustrato come utilizzare le funzioni di gestione patch e CVE per individuare le vulnerabilità e i problemi che possono verificarsi con un software aggiornato o senza patch.

- “Creazione e configurazione della sottoscrizione CVE” a pagina 128
- “Attivazione di Gestione patch” a pagina 130
- “Abilitazione di Patch Management in ZENworks Agent” a pagina 130

Creazione e configurazione della sottoscrizione CVE

Per consentire a ZENworks di importare i dati CVE dal National Vulnerability Database (NVD), occorre innanzitutto creare ed eseguire la sottoscrizione CVE.

Creazione della sottoscrizione CVE

Per creare la sottoscrizione CVE:

1. Eseguire il login al Centro di controllo ZENworks e fare clic su **Sottoscrivi e condividi**.
2. Nell'elenco Sottoscrizioni, fare clic su **Nuovo** > **Sottoscrizione**.
3. Nella pagina Seleziona tipo di sottoscrizione, selezionare la sottoscrizione CVE e fare clic su **Avanti**.
4. Nella pagina Definisci dettagli, specificare quanto segue:
   - **Nome sottoscrizione:** un nome univoco per la sottoscrizione.
   - **Cartella:** digitare il nome della cartella o andare alla cartella in cui verrà creata la sottoscrizione. Per default, la sottoscrizione verrà creata nella cartella /Sottoscrizioni.
   - **Descrizione:** una descrizione breve della sottoscrizione. Questa descrizione è visualizzata nella pagina del riepilogo della sottoscrizione.
5. Fare clic su **Next** (Avanti).
6. Nella pagina Select CVE Subscription Server (Seleziona server sottoscrizioni CVE), selezionare il server primario su cui verrà eseguito il servizio della sottoscrizione CVE. Su questo server verrà effettuato il download dei dati CVE provenienti dall'archivio NVD.
7. Selezionare la frequenza con cui si desidera che venga effettuato il download dei dati CVE dall'archivio NVD. Per default, i dati CVE vengono scaricati ogni giorno alle 23:00.

   La sottoscrizione CVE deve essere eseguita prima della sottoscrizione patch per consentire la mappatura CVE-Patch. Se la sottoscrizione CVE viene eseguita dopo la sottoscrizione patch, la mappatura non verrà effettuata fino alla successiva sottoscrizione patch, che potrebbe essere il giorno seguente.
8. Fare clic su **Avanti** per visualizzare la pagina Riepilogo.
9. Rivedere le informazioni e apportare le eventuali modifiche necessarie con il pulsante **Indietro**.
10. (Condizionale) Selezionare la casella di controllo **Definisci proprietà aggiuntive** per visualizzare la pagina di riepilogo della sottoscrizione al termine della procedura guidata.

    È possibile utilizzare le diverse schede della pagina di riepilogo per modificare le informazioni sulla sottoscrizione.

11 (Condizionale) Selezionare la casella di controllo **Esegui sottoscrizione ora** per eseguire il servizio di sottoscrizione subito dopo la sua creazione. È inoltre possibile eseguire la sottoscrizione in un secondo momento andando alla pagina **Sottoscrivi e condividi** e facendo clic sulla sottoscrizione CVE.

12 Fare clic su **Fine** per creare la sottoscrizione.

Configurazione della sottoscrizione CVE

Se durante la creazione della sottoscrizione CVE non è stata selezionata l'opzione per l'avvio del servizio della sottoscrizione CVE al termine dell'operazione, è possibile avviare la sottoscrizione e apportare modifiche selezionando l'oggetto della sottoscrizione CVE.

1 In ZCC, fare clic su **Sottoscrivi e condividi** nel pannello di sinistra.

2 Nella pagina Sottoscrizioni, fare clic sull'oggetto della sottoscrizione CVE. Vengono visualizzati i dettagli della sottoscrizione CVE:

   Sul pannello Generale vengono visualizzate le informazioni seguenti:

   - Nome: visualizza il nome della sottoscrizione.
   - Tipo: visualizza il tipo di sottoscrizione.
   - Creato da: visualizza il nome dell'utente che ha creato la sottoscrizione.
   - GUID: visualizza il GUID (Global Unique Identifier), una stringa generata casualmente che fornisce un identificatore univoco per la sottoscrizione.
   - Descrizione: visualizza una descrizione della sottoscrizione, se ne è stata inserita una al momento della creazione di quest'ultima. La descrizione viene visualizzata solo nel Centro di controllo ZENworks. Fare clic su Modifica per modificare la descrizione.
   - Abilitato: visualizza se la sottoscrizione è abilitata o meno.
   - Log sottoscrizione: visualizza i messaggi associati all'ultima esecuzione della sottoscrizione. Fare clic sul collegamento Visualizza log per visualizzare i log della sottoscrizione.

   Nel pannello Sottoscrizione è fornito un riepilogo della sottoscrizione CVE. È possibile visualizzare i seguenti dettagli:

   - URL feed NVD CVE: l'URL dell'archivio NVD dal quale vengono importati i feed CVE. Per modificare l'URL, è possibile fare clic sul collegamento Modifica.

     Importante: NON modificare l'URL, a meno che non si venga istruiti dal Servizio clienti Micro Focus.

   - Server sottoscrizioni CVE: il server che esegue la sincronizzazione con l'archivio NVD, effettua il download dei dati CVE e li archivia nel database ZENworks.

- Ultima replica: il giorno e l'ora dell'ultima sincronizzazione del server sottoscrizioni con l'archivio NVD. È possibile selezionare le opzioni pertinenti per eseguire le seguenti operazioni:
  - Esegui ora: esegue immediatamente la sincronizzazione senza attendere la pianificazione. Al temine della prima sincronizzazione, viene effettuata un'esecuzione completa per effettuare il download di tutti i dati CVE. Se tuttavia l'ultima esecuzione è stata effettuata meno di 8 giorni fa, verrà effettuato il download solo delle modifiche apportate dall'ultima esecuzione.
  - Importa manualmente: effettua il download dei dati dall'archivio NVD nel formato di file JSON, quindi effettua l'upload del file zip JSON nel server. Non è necessario effettuare questo passaggio, a meno che non si sia verificato un problema con il servizio di sottoscrizione. Per effettuare l'upload manuale del file, andare a https://nvd.nist.gov/vuln/data-feeds e selezionare il file .zip dell'anno per il quale si desidera effettuare il download dei dati. Per effettuare il download dei dati CVE appena modificati, è possibile anche selezionare il file .zip relativo al nome di feed **CVE-Modified**.
- Esecuzione completa: se non viene effettuato il download dei dati CVE, o se l'ultima esecuzione è stata effettuata più di 8 giorni fa, utilizzare questa funzione per effettuare il download di tutti i dati dell'archivio NVD.
- Stato: indica lo stato dell'ultima sincronizzazione con l'archivio NVD.
- Intervallo pianificazione: l'intervallo in base al quale viene effettuata la sincronizzazione con il server NVD. È possibile eseguire la sincronizzazione a una determinata ora, ogni giorno oppure ogni ora.

Attivazione di Gestione patch

1. Nel Centro di controllo ZENworks fare clic su **Configurazione**.
2. Nel pannello Licenze, fare clic su **ZENworks 2020 Patch Management**.
3. Selezionare **Attiva prodotto**, quindi compilare i campi:

   Numero di serie sottoscrizione prodotto: il numero di serie fornito all'utente al momento dell'acquisto della licenza di sottoscrizione. Se non si è acquistata la licenza per l'abbonamento, è possibile immettere il codice di valutazione di prova. Dopo il periodo di valutazione di 60 giorni, è necessario acquistare una licenza per permettere a Gestione patch di continuare a ricevere le patch del servizio di sottoscrizione. Per acquistare una licenza, visitare il sito dei prodotti ZENworks Patch Management (http://www.novell.com/products/zenworks/patchmanagement).
4. Fare clic su **Apply** (Applica).

Abilitazione di Patch Management in ZENworks Agent

Affinché ZENworks Agent esegua operazioni di gestione patch su un dispositivo, è necessario abilitare la funzione Gestione patch. La funzione Gestione patch è abilitata per default quando ZENworks Patch Management è attivato (licenza completa o di valutazione).

È necessario verificare che la funzione Gestione patch dell'agente sia abilitata. Per informazioni, vedere “Configurazione delle funzioni dell'agente ZENworks” a pagina 39.

Avvio del servizio di sottoscrizione patch

Prima di poter iniziare a ricevere patch, è necessario avviare il servizio di sottoscrizione su uno dei server ZENworks e impostare la pianificazione quotidiana per il download delle patch.

Quando è disponibile una nuova patch dal servizio di sottoscrizione, il server ZENworks ne effettua il download automaticamente. Nella pagina Patch (nella scheda **Sicurezza**) viene visualizzata la nuova patch insieme alla descrizione e all'impatto aziendale. È possibile sia distribuire la patch ai dispositivi, sia ignorarla.

Gestione patch rimane aggiornato con le patch e le correzioni più recenti tramite una regolare comunicazione Internet con il servizio di sottoscrizione delle patch di ZENworks. Dopo il periodo di valutazione iniziale di 60 giorni, Gestione patch richiede una sottoscrizione a pagamento per continuare a scaricare quotidianamente le informazioni sulla vulnerabilità e sulle patch più recenti.

Se sono presenti più server ZENworks nella zona di gestione, è possibile selezionarne uno come server di gestione patch. Il server selezionato per la gestione patch deve assicurare connettività ottimale a Internet in quando effettua giornalmente il download di nuove patch e aggiornamenti.

Per avviare il servizio di sottoscrizione:

1. Nel Centro di controllo ZENworks, fare clic sulla scheda **Configurazione**.
2. Nel pannello Impostazioni zona di gestione, cliccare su **Sicurezza**, quindi su **Patch Subscription Service Information (Informazioni servizio di sottoscrizione patch)**.
3. Nell'elenco **Avvia servizio di sottoscrizione**, selezionare il server ZENworks su cui eseguire il servizio di sottoscrizione, quindi fare clic su **Avvia servizio**.

   Dopo l'avvio del servizio di sottoscrizione, l'etichetta del pulsante **Avvia servizio** diventa **Servizio in esecuzione**.
4. Nell'elenco **Intervallo di comunicazione della sottoscrizione (ogni giorno alle)**, selezionare l'intervallo di tempo in cui, ogni giorno, si desidera vengano scaricate le patch.
5. Fare clic su **OK**.

Creazione di policy patch

Prima di iniziare a installare le patch sui dispositivi, ZENworks Agent deve eseguire il task DAU (Discover Applicable Updates o rilevamento degli aggiornamenti applicabili). Il task DAU consente a ZENworks Agent di rilevare lo stato (Con applicazione di patch, Senza applicazione di patch o Non valido) di ciascuna patch, in base ai dispositivi presenti nella rete.

Il ciclo di rilevazione delle patch si verifica ogni giorno sul server ZENworks in cui è pianificato un task DAU per tutti i dispositivi gestiti (server e workstation.) È anche possibile avviare un task DAU da un agente singolo. È possibile visualizzare i risultati della scansione di rilevamento patch nella scheda **Sicurezza** o **Dispositivi** della sezione Patch del server ZENworks. I risultati sono disponibili anche se una workstation è scollegata dalla rete.

Per distribuire patch, è possibile creare policy patch o utilizzare Soluzione per la distribuzione. Le policy patch automatizzano il processo di distribuzione e sono preferibili alla Soluzione per la distribuzione. È possibile definire regole nelle policy patch per limitare la memorizzazione nella cache e la distribuzione solo alle patch necessarie per i dispositivi.

Nell'esempio riportato nei seguenti passaggi sono disponibili più patch dal servizio di sottoscrizione.

1. Nel Centro di controllo ZENworks, andare a **Sicurezza** > **Policy patch**.
2. Nella pagina Policy patch, fare clic su **Nuovo**.
3. Seguire i prompt visualizzati per creare una policy patch.

   Fare clic sul pulsante della **guida** su ciascuna pagina per informazioni dettagliate sulla pagina.
4. Dopo averla creata, fare clic sulla policy e selezionare la pagina **Relazioni**.
5. Cliccare su **Aggiungi** nel pannello Assegnazioni dispositivo e assegnare uno o più dispositivi alla policy.
6. Fare clic su **Pubblicazione** per distribuire e applicare le patch applicabili ai dispositivi secondo la configurazione della policy patch.

Importante: si consiglia di applicare inizialmente le patch a un dispositivo di prova prima di applicarle ai dispositivi in tutta la zona. In tutti i dispositivi configurati come “di prova” verranno applicate automaticamente le patch a tutti i dispositivi di prova assegnati tramite Sandbox, senza eseguire il Passaggio 6 (pubblicazione della policy).

Quando inizialmente si crea una policy patch, è possibile anche configurare la policy per **l'approvazione automatica delle patch dopo le applicazioni di prova andate a buon fine**. Selezionando questa opzione nella configurazione della policy, quest'ultima verrà pubblicata automaticamente a tutti i dispositivi a essa assegnati dopo il passaggio totale dei dispositivi di prova (senza dover pubblicare (Passaggio 6 sopra).

Ulteriori informazioni

Per ulteriori informazioni su come monitorare le vulnerabilità software sui dispositivi tramite i dati CVE e su come reagire a tali vulnerabilità attraverso l'applicazione delle patch pertinenti, consultare la *documentazione di riferimento relativa ai CVE ZENworks*.

Per ulteriori informazioni sulla configurazione di Patch Management, l'automazione della distribuzione delle patch nella zona di gestione mediante le policy patch e l'uso di Soluzione per la distribuzione, vedere *ZENworks Patch Management Reference* (in lingua inglese).