ZENworks 2020

Schnellstart zur Verwaltung

Oktober 2019

Rechtliche Hinweise

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

Inhalt

Allgemeines zu diesem Handbuch

Mit dem vorliegenden *ZENworks: Schnellstart zur Verwaltung* können Sie die Grundlagen der Verwaltung Ihres ZENworks Management-Systems schnell erlernen. Sie sollten das ZENworks-System bereits installiert haben. Andernfalls finden Sie diesbezügliche Informationen im Handbuch *ZENworks-Server-Installation*.

Die Informationen in diesem Handbuch gliedern sich wie folgt:

- Systemkonfiguration (Seite 9): Enthält Anweisungen zum Konfigurieren Ihrer ZENworks-Verwaltungszone vor der Verwendung der ZENworks -Produkte.
- Produktverwaltung (Seite 61): Enthält Anweisungen zur Verwendung von ZENworks -Produkten (Asset Management, Configuration Management, Endpoint Security Management, vollständige Festplattenverschlüsselung und Patch Management).

Zielgruppe

Dieses Handbuch richtet sich an alle Benutzer, die das ZENworks-System konfigurieren oder überwachen bzw. jegliche ZENworks-bezogenen Aufgaben durchführen sollen, die bei der Verwaltung von Geräten bzw. Benutzern anfallen.

Rückmeldungen

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

Weitere Dokumentation

Im Lieferumfang von ZENworks finden Sie weitere Dokumentationen (im PDF- und HTML-Format), die Informationen zum Produkt und zu dessen Implementierung beinhalten. Weiteres Dokumentationsmaterial finden Sie auf der Dokumentations-Website zu ZENworks (http://www.novell.com/documentation/zenworks-2020).

Systemkonfiguration

Die folgenden Abschnitte enthalten Informationen zum Konfigurieren des ZENworks-Systems. Die Konfigurationsaufgaben gelten unabhängig von den verwendeten ZENworks -Produkten (Configuration Management, Patch Management, Asset Management und Endpoint Security Management).

1 Kurzübersicht

Sie haben Ihren ZENworks-Server (oder auch mehrere Server) installiert und möchten alle zeitsparenden Funktionen von ZENworks verwenden.

Bevor Sie eines der ZENworks -Produkte (Configuration Management, Patch Management, Asset Management, Endpoint Security Management und Full Disk Encryption), die Sie testen wollen oder für die Sie eine Lizenz oder Evaluierungslizenz erworben haben, verwenden, sollten Sie sich mit den in den folgenden Abschnitten beschriebenen Konzepten und Aufgaben vertraut machen. Diese Abschnitte bieten eine kurze Einführung in die Informationen und Schritte, die zum Konfigurieren Ihrer Verwaltungszone erforderlich sind.

Management-Tools

ZENworks enthält sowohl eine webbasierte Konsole (ZENworks-Kontrollzentrum) als auch ein Befehlszeilenprogramm (zman) zur Verwaltung Ihres ZENworks-Systems. Machen Sie sich zumindest mit dem ZENworks-Kontrollzentrum vertraut.

Aufgabe		Details
	Starten des ZENworks-Kontrollzentrums	Eine Anleitung dazu finden Sie in „ZENworks-Kontrollzentrum“, auf Seite 17.
	Ausführen des zman-Dienstprogramms	Das zman-Dienstprogramm ist eine Befehlszeilenschnittstelle, mit der Sie viele der Aufgaben des ZENworks-Kontrollzentrums ausführen können. Eine Anleitung dazu finden Sie in „zman-Befehlszeilenprogramm“, auf Seite 19.
	Ausführen des zac-Dienstprogramms	Das zac-Dienstprogramm ist eine Befehlszeilenschnittstelle für den ZENworks Agent. Eine Anleitung dazu finden Sie in „zac-Befehlszeilenprogramm“, auf Seite 20.

Zonenkonfiguration

Bevor Sie die Verwaltungsfunktionen der ZENworks-Produkte, die Sie bei der Installation Ihrer Verwaltungszone aktiviert haben, vollständig nutzen können, müssen Sie zunächst einige Konfigurationsaufgaben ausführen, um die korrekte Konfiguration Ihrer Verwaltungszone sicherzustellen.

Aufgabe		Details
	Erstellen von Ordnern und Gruppen zum Organisieren von Geräten	Organisieren Sie Geräte in Ordnern und Gruppen, um den Overhead beim Anwenden von ZENworks-Konfigurationseinstellungen und beim Ausführen von Aufgaben auf ähnlichen Geräten zu reduzieren. Statt Zuweisungen vorzunehmen oder Aufgaben auf einzelnen Geräten auszuführen können Sie die Ordner und Gruppen verwalten, sodass jedes Gerät in einem Ordner oder einer Gruppe die Zuweisung oder Aufgabe übernimmt. Eine Anleitung dazu finden Sie in „Geräte organisieren: Ordner und Gruppen“, auf Seite 23.
	Erstellen von Registrierungsschlüsseln und -regeln	Der ZENworks-Agent muss auf allen zu verwaltenden Geräten bereitgestellt werden. Wenn Sie den ZENworks Agent auf einem Gerät bereitstellen, wird das Gerät in der Verwaltungszone registriert. Sie können Registrierungsschlüssel oder -regeln dazu verwenden, Geräte automatisch entsprechenden Ordnern und Gruppen zuzuweisen. So werden alle mit den Ordnern und Gruppen verknüpften Zuweisungen direkt an die Geräte vererbt. Eine Anleitung dazu finden Sie in „Erstellen von Registrierungsschlüsseln und -regeln“, auf Seite 27.

Aufgabe		Details
	Hinzufügen von Benutzerquellen	Sie können eine Verbindung zu einem oder mehreren Verzeichnissen herstellen, um autorisierende Benutzerquellen in ZENworks zur Verfügung zu stellen. Durch Hinzufügen einer Benutzerquelle können Sie ZENworks-Administratorkonten mit LDAP-Benutzerkonten verknüpfen und Geräte mit den Benutzern verknüpfen, die sie hauptsächlich verwenden. Darüber hinaus werden durch das Hinzufügen von Benutzern für folgende ZENworks-Produkte zusätzliche Funktionen ermöglicht: ◆ **Konfigurationsmanagement:** Ermöglicht es Ihnen, Bundles und Richtlinien Benutzern und Geräten zuzuweisen. Ermöglicht benutzerbasierte Inventarberichte. ◆ **Bestandsverwaltung:** Ermöglicht es Ihnen, Softwarelizenzen sowohl auf Benutzer- als auch auf Gerätebasis auszuweisen. ◆ **Endpoint Security Management:** Ermöglicht es Ihnen, Richtlinien sowohl Benutzern als auch Geräten zuzuweisen. Eine Anleitung dazu finden Sie in „Verbinden mit Benutzerquellen“, auf Seite 30.
	Erstellen von zusätzlichen Administratorkonten	Während der Installation wird ein standardmäßiges ZENworks-Administratorkonto (mit dem Namen Administrator) erstellt. Hierbei handelt es sich um ein Superadministratorkonto. Dieses Konto verfügt innerhalb der Verwaltungszone über vollständige Verwaltungsrechte. Sie können zusätzliche Administratorkonten erstellen und ihnen Superadministratorrechte erteilen. Oder Sie können Administratorkonten mit eingeschränkten Rechten erstellen, um den Umfang der verfügbaren Aufgaben, Geräte und Benutzer für den Administrator zu beschränken. Eine Anleitung dazu finden Sie in „Erstellen eines Administratorkontos“, auf Seite 31.

Aufgabe		Details
	Erstellen von Administratorgruppenkonten	Sie können Administratorgruppen erstellen. Wenn Sie Rechte und Rollen zu Administratorgruppen hinzufügen, gelten die zugewiesenen Rechte und Rollen für alle Mitglieder in der Gruppe. Eine Anleitung dazu finden Sie in „Erstellen eines Administratorgruppenkontos“, auf Seite 32.
	Modifizieren von Zonenkonfigurations-einstellungen	Die Verwaltungszoneneinstellungen sind bereits auf die am häufigsten verwendete Konfiguration voreingestellt. Sie brauchen an dieser Stelle keine Änderungen der Einstellungen vorzunehmen, können sie jedoch durchgehen, um sich mit ihnen vertraut zu machen. Eine Anleitung dazu finden Sie in „Ändern der Konfigurationseinstellungen“, auf Seite 33.
	Aktualisieren der ZENworks-Software	Mit der Funktion „Systemaktualisierung“ können Sie Aktualisierungen der ZENworks - Software frühzeitig beziehen und auch automatische Downloads der Aktualisierungen zeitlich planen. Eine Anleitung dazu finden Sie in „Aktualisieren der ZENworks-Software“, auf Seite 35.
	Standorte erstellen	Sicherheitsrichtlinien können global sein oder sich auf bestimmte Standorte beziehen. Eine globale Richtlinie wird auf alle Standorte angewendet. Eine standortbasierte Richtlinie wird nur angewendet, wenn der ZENworks Agent feststellt, dass die Netzwerkumgebung des Geräts mit der für den Standort definierten Umgebung übereinstimmt. Eine Anleitung dazu finden Sie in „Erstellen von Standorten“, auf Seite 36.

Agentenbereitstellung

ZENworks Agent kommuniziert mit dem ZENworks-Server, um Verwaltungsaufgaben auf einem Gerät auszuführen. Sie müssen den ZENworks-Agenten für alle zu verwaltenden Geräte bereitstellen. Durch die Bereitstellung des ZENworks-Agenten werden die Agentendateien installiert und das Gerät wird in der Verwaltungszone registriert. Weitere Informationen zum Registrieren von Mobilgeräten in der Zone finden Sie unter Registrieren von Mobilgeräten.

Aufgabe		Details
	Aktivieren der Funktionen des ZENworks Agent	Der ZENworks Agent umfasst Funktionen, die auf jedes der ZENworks -Produkte (Asset Management, Configuration Management, Endpoint Security Management, Full Disk Encryption und Patch Management) zugeschnitten sind. Standardmäßig werden die Funktionen für Ihre aktivierten Produkte (per Lizenz oder Evaluierungslizenz) bei der Installation der Verwaltungszone aktiviert. Sie sollten die Konfiguration jedoch im ZENworks-Kontrollzentrum überprüfen. Eine Anleitung dazu finden Sie in „Konfigurieren der ZENworks-Agent-Funktionen“, auf Seite 41.
	Schützen des ZENworks-Agenten	Sie können die ZENworks Agent-Einstellungen für die Deinstallation und Selbstverteidigung konfigurieren. Eine Anleitung dazu finden Sie in „Konfigurieren der ZENworks-Agent-Sicherheit“, auf Seite 43.
	Installieren des ZENworks-Agenten	Sie können den ZENworks Agent auf verschiedene Art und Weise auf einem Gerät installieren: ◆ Verwenden Sie das ZENworks-Kontrollzentrum, um den Agent von einem ZENworks-Server für das Gerät bereitzustellen. ◆ Verwenden Sie auf dem Gerät einen Webbrowser, um den Agent von einem ZENworks-Server herunterzuladen und ihn zu installieren. ◆ Schließen Sie den Agenten in ein Image ein und wenden Sie das Image auf das Gerät an. Eine Anleitung dazu finden Sie in „Installieren des ZENworks Agent“, auf Seite 44.
	Anmeldung und Verwendung von ZENworks Agent	Um auf einem Gerät benutzerzugewiesene Bundles und Richtlinien zu empfangen, müssen Sie sich bei der Verwaltungszone anmelden. Eine Anleitung dazu finden Sie in „Verwenden des ZENworks-Agenten“, auf Seite 48.

Systemmeldungen

Wenn Sie Verwaltungsaufgaben in Ihrer Zone durchführen, werden Informationen aufgezeichnet, sodass Sie den Status der Zone und die darin stattfindenden Aktivitäten anzeigen können.

Aufgabe		Details
	Systemmeldungen anzeigen	Das ZENworks-System generiert Informations-, Warn- und Fehlermeldungen, um Sie bei der Überwachung von Aktivitäten, wie zum Beispiel die Verteilung von Software und die Anwendung von Richtlinien, zu unterstützen. Eine Anleitung dazu finden Sie in „Anzeigen von Systemmeldungen“, auf Seite 53.
	Überwachungsliste erstellen	Wenn Sie über Geräte, Bundles und Richtlinien verfügen, deren Aktivitäten Sie genau überwachen möchten, können Sie sie der Überwachungsliste hinzufügen. Eine Anleitung dazu finden Sie in „Erstellen einer Überwachungsliste“, auf Seite 55.

2 Management-Tools

ZENworks enthält sowohl eine webbasierte Konsole (ZENworks-Kontrollzentrum) als auch ein Befehlszeilenprogramm (zman) für die Verwaltung des ZENworks-Systems. In diesem Abschnitt wird der Zugriff auf bzw. die Verwendung der Verwaltungstools erläutert.

ZENworks-Kontrollzentrum

ZENworks-Kontrollzentrum ist auf allen ZENworks-Servern in der Verwaltungszone installiert. Sie können alle Verwaltungsaufgaben auf jedem ZENworks-Server durchführen. Da es sich bei dem ZENworks-Kontrollzentrum um eine webbasierte Verwaltungskonsole handelt, kann darauf von jeder unterstützten Arbeitsstation aus zugegriffen werden.

Wenn Sie weitere Micro Focus-Produkte in Ihrer Netzwerkumgebung mit iManager verwalten, können Sie festlegen, dass das ZENworks-Kontrollzentrum in iManager gestartet werden soll. Weitere Informationen finden Sie im Abschnitt „Zugriff auf das ZENworks-Kontrollzentrum über Novell iManager“ im Handbuch *Referenz für das ZENworks-Kontrollzentrum*.

Zugreifen auf das ZENworks-Kontrollzentrum

1 Geben Sie die folgende URL in einen Webbrowser ein:

`https://ZENworks_Server_Address:port`

Ersetzen Sie *ZENworks_Server_Adresse* durch die IP-Adresse oder den DNS-Namen des ZENworks-Servers. Sie brauchen nur den *Port* anzugeben, falls Sie keinen der Standard-Ports (80 oder 443) verwenden. Für das ZENworks-Kontrollzentrum ist eine HTTPS(HyperText Transfer Protocol Secure)-Verbindung erforderlich; HTTP(HyperText Transfer Protocol)- Anforderungen werden an HTTPS umgeleitet.

Das Anmeldedialogfeld wird angezeigt.

2 Geben Sie im Feld **Benutzername** `Administrator` ein.

3 Geben Sie im Feld **Passwort** das bei der Installation erstellte Administratorpasswort ein.

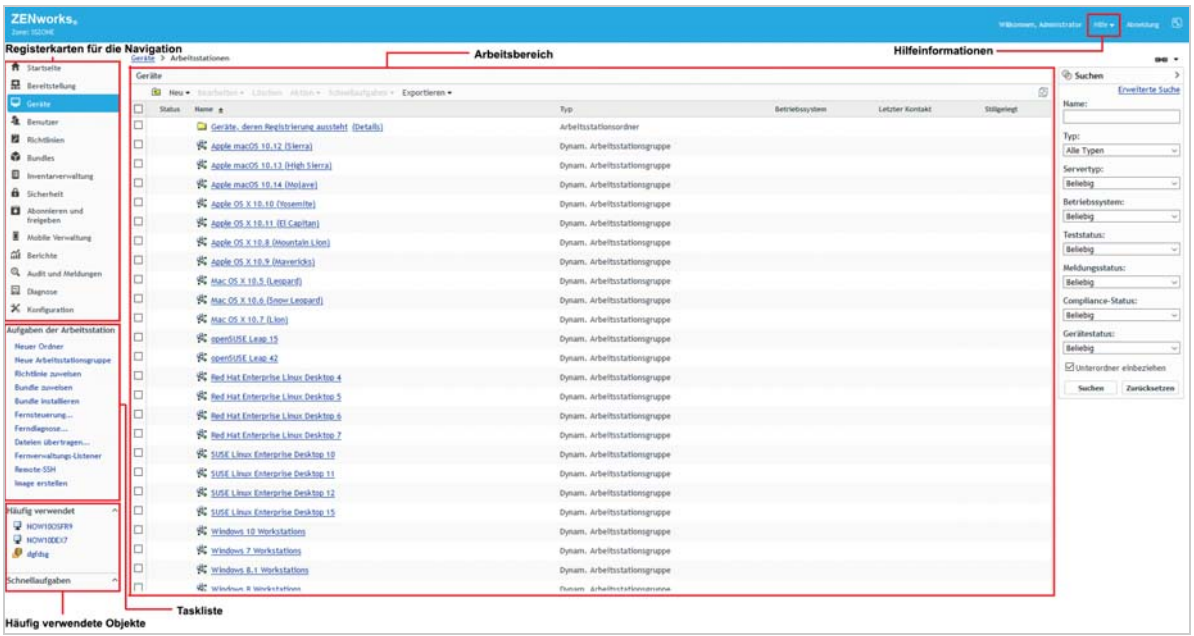
Um den Zugriff nicht berechtigter Benutzer auf das ZENworks-Kontrollzentrum zu verhindern, wird das Administratorkonto nach drei nicht erfolgreichen Anmeldeversuchen deaktiviert. Zusätzlich wird eine Wartezeit von 60 Sekunden vor dem nächsten möglichen Anmeldeversuch erzwungen. Weitere Informationen zum Ändern der Standardwerte finden Sie im Abschnitt „Ändern der Standardwerte zur Deaktivierung der Anmeldung“ im Handbuch *Referenz für das ZENworks-Kontrollzentrum*.

4 Klicken Sie auf **Anmelden**, um das ZENworks-Kontrollzentrum einzublenden.

Detailliertere Informationen zum Anmelden als ein anderer Administrator finden Sie im Abschnitt „Zugreifen auf das ZENworks-Kontrollzentrum“ im Handbuch *Referenz für das ZENworks-Kontrollzentrum*.

Navigation im ZENworks-Kontrollzentrum

Bei der unten dargestellten Seite „Arbeitsstationen“ handelt es sich um eine Standardansicht im ZENworks-Kontrollzentrum.



Registerkarten für die Navigation: Mithilfe der Registerkarte im linken Bereich können Sie in den funktionsbezogenen Bereichen von ZENworks navigieren. Beispielsweise können Sie mit der oben dargestellten Seite „Arbeitsstationen“ die mit Arbeitsstationen verknüpften Aufgaben verwalten.

Aufgabenliste: Über die Aufgabenliste im linken Bereich können Sie schnell auf die am häufigsten durchgeführten Aufgaben für die jeweils aktuelle Seite zugreifen. Die Aufgabenliste ändert sich je nach Seite. In der Aufgabenliste der Seite „Geräte“ werden beispielsweise Aufgaben angezeigt, die sich auf Geräte beziehen, während die Aufgabenliste der Seite „Konfiguration“ Aufgaben enthält, die sich auf die Konfiguration beziehen.

Häufig verwendete Objekte: In der Liste „Häufig verwendet“ im linken Bereich werden die zehn Objekte angezeigt, auf die Sie am häufigsten zugegriffen haben. Dabei stehen die am häufigsten verwendeten Objekte oben in der Liste. Durch Klicken auf ein Objekt gelangen Sie direkt zur zugehörigen Detailseite.

Arbeitsbereich: In den Arbeitsbereichen überwachen und verwalten Sie das ZENworks-System. Die Bereiche ändern sich in Abhängigkeit von der aktuellen Seite. Im obigen Beispiel gibt es zwei Arbeitsbereiche: **Geräte** und **Suchen**. Im Bereich **Geräte** werden die Arbeitsstationen, Arbeitsstationsordner und Arbeitsstationsgruppen aufgelistet sowie die dynamischen Arbeitsstationsgruppen, die erstellt wurden; Sie können diesen Bereich zur Verwaltung der Arbeitsstationen verwenden. Mit dem Bereich **Suchen** können Sie die Anzeige im Bereich „Geräte“ filtern, und zwar nach Kriterien wie dem Namen, Betriebssystem oder Status der Arbeitsstation.

Hilfeinformationen: Die Hilfe-Schaltfläche ist mit Hilfethemen mit Informationen zur aktuellen Seite verknüpft. Mit welchen Themen die Hilfe-Schaltfläche verknüpft ist, ändert sich in Abhängigkeit von der aktuellen Seite.

zman-Befehlszeilenprogramm

Das zman-Dienstprogramm stellt eine Schnittstelle zur Befehlszeilenverwaltung bereit, über die Sie viele der im ZENworks-Kontrollzentrum zur Verfügung stehenden Aufgaben durchführen können. Sie können beispielsweise Inhalt zu Bundles hinzufügen, Geräten Richtlinien zuweisen und Geräte registrieren. Der Hauptvorteil des Befehlszeilendienstprogramms liegt in der Möglichkeit, Skripts für die Behandlung sich wiederholender Vorgänge oder Massenvorgänge zu erstellen. Wie das ZENworks-Kontrollzentrum (ZCC) wird auch das Dienstprogramm zman auf allen Primärservern installiert, kann aber im Gegensatz zu ZCC nur über die Befehlszeile des Servers ausgeführt werden.

Das zman-Dienstprogramm dient vornehmlich dazu, Ihnen das Durchführen von Vorgängen über ein Skript zu ermöglichen. Sie haben jedoch auch die Möglichkeit, Vorgänge manuell an der Befehlszeile durchzuführen.

- „Standort“, auf Seite 19
- „Syntax“, auf Seite 19
- „Hilfe zu Befehlen“, auf Seite 20

Standort

Das Dienstprogramm ist auf allen ZENworks-Server an folgendem Ort installiert:

`%ZENWORKS_HOME%\bin`

Hierbei steht `%ZENWORKS_HOME%` für den ZENworks-Installationspfad. Unter Windows lautet der Standardpfad `C:\Programme (x86)\Novell\Zenworks\bin`. Unter Linux lautet der Standardpfad `opt/novell/zenworks/bin`.

Syntax

Im zman-Dienstprogramm wird folgende grundlegende Syntax verwendet:

`zman` *`kategorieaktion`* `[` *`optionen`*`]`

Zur Zuweisung eines Software-Bundles zu einem Gerät verwenden Sie beispielsweise folgenden Befehl:

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

Hierbei steht `bundle-assign` für die Kategorieaktion und `workstation bundle1 wks1` für die Optionen. In diesem Beispiel geben die Optionen den Gerätetyp (workstation), den Bundle-Namen (bundle1) und das Zielgerät (wks1) an.

Beispielsweise können Sie zur Initiierung einer Inventarabsuche eines Gerätes den folgenden Befehl verwenden:

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

Dabei bezeichnet `inventory-scan-now` die Kategorieaktion und `device/servers/server1` eine Option, die den Ordnerpfad des abzusuchenden Geräts angibt.

Hilfe zu Befehlen

Am besten können Sie sich mit den Befehlen vertraut machen, indem Sie die Online-Hilfe oder den Abschnitt „zman(1)“ im Handbuch*ZENworks: Referenz für Befehlszeilenprogramme zurate ziehen*.

So verwenden Sie die Online-Hilfe:

1 Geben Sie auf dem ZENworks-Server an der Eingabeaufforderung `zman --help` ein.

Mit diesem Befehl werden die grundlegende Verwendung (Syntax) sowie eine Liste der verfügbaren Befehlskategorien angezeigt. Sie können zum Abrufen von Hilfeinformationen auch folgendermaßen vorgehen:

Befehl	Beschreibung
`zman --help | more`	Zeigt eine vollständige, nach Kategorie sortierte Liste mit Befehlen an.
`zman kategorie --help | more`	Zeigt eine vollständige Liste mit Befehlen innerhalb einer Kategorie an.
`zman Befehl --help | more`	Zeigt die Hilfe zu einem Befehl an.

zac-Befehlszeilenprogramm

Das zac-Dienstprogramm stellt eine Schnittstelle für die Befehlszeilenverwaltung bereit, über die Sie im ZENworks Agent verfügbare Aufgaben durchführen können.

- „Standort“, auf Seite 20
- „Syntax“, auf Seite 20
- „Hilfe zu Befehlen“, auf Seite 21

Standort

Das Dienstprogramm ist auf allen verwalteten Windows-Geräten an folgendem Ort installiert:

`%ZENWORKS_HOME%\bin`

Hierbei steht %ZENWORKS_HOME% für den ZENworks-Installationspfad. Der Standardpfad lautet `c:\Programme\novell\zenworks\bin` auf einem 32-Bit-Windows-Gerät und `c:\Programme (x86)\novell\zenworks\bin` auf einem 64-Bit-Windows-Gerät.

Syntax

Im zac-Dienstprogramm wird folgende grundlegende Syntax verwendet:

`zac Befehlsoptionen`

Zum Aufrufen eines Bundles auf einem Gerät verwenden Sie beispielsweise folgenden Befehl:

```
zac bundle-launch „bundle 1"
```

Hierbei ist `bundle-launch` der Befehl und `bundle 1` die Befehlsoption. In diesem Fall handelt es sich bei der Option um den Anzeigenamen des Bundles, das aufgerufen werden soll. Öffnende und schließende Anführungszeichen sind nur erforderlich, wenn der Anzeigename des Bundles Leerschritte enthält.

Sie können zur Initiierung einer Inventarabsuche auf einem Gerät beispielsweise den folgenden Befehl verwenden:

```
zac inv scannow
```

Hierbei ist `inv` der Befehl und `scannow` die Befehlsoption.

Hilfe zu Befehlen

Am besten können Sie sich mit den Befehlen vertraut machen, indem Sie die Online-Hilfe oder den Abschnitt zu „zac für Windows(1)“ im Handbuch *Novell ZENworks: Referenz für Befehlszeilenprogramme* zurate ziehen.

So verwenden Sie die Online-Hilfe:

1 Geben Sie auf dem verwalteten Gerät an einer Eingabeaufforderung einen der folgenden Befehle ein:

Befehl	Beschreibung
`zac --help`	Zeigt eine vollständige Befehlsliste an.
`zac befehl --help`	Zeigt detaillierte Hilfe zu einem Befehl an.

3 Konfiguration der Verwaltungszone

Mit ZENworks können Sie eine große Anzahl Geräte und Benutzer mit möglichst wenig Aufwand effizient verwalten. Der erste Schritt beim Verringern des Verwaltungsaufwands besteht darin, sicherzustellen, dass Sie die Verwaltungszone so konfiguriert haben, dass Sie die ZENworks-Funktionen voll nutzen können.

Die folgenden Abschnitte geben Ihnen eine Einführung in die grundlegenden Konzepte, die Sie benötigen, um eine Verwaltungszone einzurichten, die die laufenden Verwaltungsaufgaben, die Sie durchführen, optimal unterstützt. In jedem Abschnitt wird ein Verwaltungskonzept erläutert, das die allgemeinen Schritte zum Durchführen der zum Konzept gehörenden Aufgaben bereitstellt.

Geräte organisieren: Ordner und Gruppen

Mithilfe des ZENworks-Kontrollzentrums können Sie Geräte verwalten, indem Sie Aufgaben direkt an individuellen Geräteobjekten ausführen. Diese Methode ist jedoch nicht sehr effizient, es sei denn, es müssen nur wenige Geräte verwaltet werden. Zum Optimieren der Verwaltung einer großen Geräteanzahl ermöglicht Ihnen ZENworks, Geräte in Ordner und Gruppen zu gliedern. Sie können dann Aufgaben an einem Ordner oder einer Gruppe ausführen, um die enthaltenen Geräte zu verwalten.

Sie können jederzeit Ordner und Gruppen erstellen. Jedoch ist die beste Vorgehensweise das Anlegen von Ordnern und Gruppen, bevor Sie Geräte in Ihrer Zone registrieren. Auf diese Weise können Sie Registrierungsschlüssel und Regeln verwenden, um Geräte beim Registrieren automatisch den passenden Ordnern und Gruppen hinzuzufügen (siehe „Erstellen von Registrierungsschlüsseln und -regeln“, auf Seite 27).

Ordner

Ordner sind ein großartiges Werkzeug, mit dem Sie Geräte organisieren können, um die Verwaltung dieser Geräte zu vereinfachen. Sie können bei jedem Ordner Konfigurationseinstellungen anwenden, Inhalte zuweisen und Aufgaben ausführen. Zu diesem Zweck übernehmen die Geräte dieses Ordners die entsprechenden Einstellungen, Zuweisungen und Aufgaben.

Für beste Ergebnisse sollten Sie Geräte mit ähnlichen Anforderungen an Konfigurationseinstellungen im selben Ordner ablegen. Wenn für alle Geräte im Ordner dieselben Inhalte und Aufgaben erforderlich sind, können Sie auch Inhalts- oder Aufgabenzuweisungen für den Ordner vornehmen. Möglicherweise gelten jedoch nicht für alle Geräte im Ordner dieselben Inhalts- und Aufgabenanforderungen. Daher können Sie die Geräte in Gruppen strukturieren und jeder Gruppe die geeigneten Inhalte und Aufgaben zuweisen (siehe unten „Gruppen“, auf Seite 25).

Nehmen Sie z. B. an, Sie haben Arbeitsstationen an drei verschiedenen Standorten. Sie möchten auf die Arbeitsstationen an den drei Standorten unterschiedliche Konfigurationseinstellungen anwenden, also erstellen Sie die drei Ordner (`/Arbeitsstationen/Standort1`, `/Arbeitsstationen/Standort2` und `/Arbeitsstationen/Standort3`) und legen die Arbeitsstationen im jeweils entsprechenden Ordner ab. Sie beschließen, dass die meisten Konfigurationseinstellungen für alle Arbeitsstationen gelten, also konfigurieren Sie diese Einstellungen in der Verwaltungszone. Sie möchten jedoch eine wöchentliche Erfassung des Software- und Hardware-Inventars an Standort1 und Standort2 sowie eine monatliche Inventarerfassung an Standort3 ausführen. Sie konfigurieren eine wöchentliche Inventarerfassung in der Verwaltungszone und überschreiben dann die Einstellung des Ordners an Standort3 mit einem monatlichen Zeitplan. Standort1 und Standort2 erfassen das Inventar wöchentlich, und Standort3 erfasst das Inventar monatlich.

Erstellen eines Ordners

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Geräte**.
2. Klicken Sie auf den Ordner **Arbeitsstationen**, **Server** oder **Mobilgeräte**.
3. Klicken Sie auf **Neu** > **Ordner**, um das Dialogfeld „Neuer Ordner“ anzuzeigen.
4. Geben Sie im Feld **Name** einen Namen für den neuen Ordner ein.

   Wenn Sie ein Objekt im ZENworks-Kontrollzentrum (Ordner, Gruppen, Bundles, Richtlinien usw.) benennen, stellen Sie sicher, dass der Name die folgenden Konventionen einhält:

   - Der Name muss innerhalb des Ordners eindeutig sein.
   - Je nach der für die ZENworks-Datenbank verwendeten Datenbanksoftware wird durch Klein- und Großbuchstaben keine Einzigartigkeit für denselben Namen erzeugt. Bei der eingebetteten Datenbank, die mit ZENworks verwendet wird, wird nicht zwischen Groß- und Kleinschreibung unterschieden, d. h., „Ordner 1“ und „ORDNER 1“ sind derselbe Name und können nicht im selben Ordner verwendet werden. Wenn Sie eine externe Datenbank verwenden, die Groß-/Kleinschreibung unterscheidet, sind „Ordner 1“ und „ORDNER 1“ eindeutige Namen.
   - Wenn Sie Leerzeichen verwenden, müssen Sie diese bei der Eingabe in die Befehlszeile in Anführungszeichen setzen. Beispielsweise müssen Sie „Ordner 1“ mit Anführungszeichen umgeben, wenn Sie den Namen in das Dienstprogramm zman eingeben.
   - Folgende Zeichen sind unzulässig und dürfen nicht verwendet werden: / \ * ? : „ ' < > | ` % ~
5. Klicken Sie auf **OK**, um den Ordner hinzuzufügen.

Zum Erstellen von Geräteordnern können Sie auch die Befehle `workstation-folder-create` und `server-folder-create` im zman-Dienstprogramm verwenden. Weitere Informationen finden Sie unter „Arbeitsstationsbefehle“ und „Serverbefehle“ im Handbuch *ZENworks: Referenz für Befehlszeilenprogramme*.

Gruppen

Genau wie bei den Ordnern können Sie bei Gerätegruppen Inhalte zuweisen und Aufgaben ausführen. Zu diesem Zweck übernehmen die Geräte der Gruppe die entsprechenden Zuweisungen und Aufgaben. Anders als bei Ordnern können Sie auf Gruppen jedoch keine Konfigurationseinstellungen anwenden.

Gruppen bieten eine weitere Stufe der Flexibilität für Inhaltszuweisung und Aufgaben. In einigen Fällen sollen möglicherweise dieselben Inhalte nicht allen Geräten in einem Ordner zugewiesen oder dieselbe Aufgabe dafür ausgeführt werden. Oder Sie möchten eventuell Geräten in verschiedenen Ordnern dieselben Inhalte zuweisen oder dieselben Aufgaben dafür ausführen. Zu diesem Zweck können Sie die Geräte einer Gruppe hinzufügen (unabhängig davon, in welchen Ordnern sich die Geräte befinden) und die Inhalte dann der Gruppe zuweisen oder die Aufgaben dafür ausführen.

Betrachten wir noch einmal das Beispiel mit den Arbeitsstationen an drei verschiedenen Standorten (siehe „Ordner“, auf Seite 24). Nehmen Sie an, dass einige der Arbeitsstationen an jedem Standort dieselbe Buchhaltungssoftware benötigen. Da Gruppen Software zugewiesen werden kann, können Sie die Gruppe „Buchhaltung“ erstellen, die Zielarbeitsstationen in die Gruppe aufnehmen und dann der Gruppe die passende Buchhaltungssoftware zuweisen. Entsprechend können Sie die Gruppen verwenden, um Windows-Konfigurations- und -Sicherheitsrichtlinien zuzuweisen.

Der Vorteil der Erstellung einer Zuweisung für eine Gruppe besteht darin, dass alle in der entsprechenden Gruppe enthaltenen Geräte die Zuweisung erhalten und Sie die Zuweisung nur ein Mal erstellen müssen. Außerdem kann ein Gerät einer beliebigen Anzahl eindeutiger Gruppen angehören und die Zuweisungen von mehreren Gruppen sind additiv. Wenn Sie beispielsweise der Gruppe A und B ein Gerät zuweisen, erbt dieses die Software, die beiden Gruppen zugewiesen ist.

ZENworks bietet sowohl Gruppen als auch dynamische Gruppen. Aus der Perspektive von Inhaltszuweisungen oder derAusführung von Aufgaben funktionieren Gruppen und dynamische Gruppen exakt gleich. Die einzigen Unterschiede zwischen den beiden Gruppentypen ist die Art, in der Geräte zur Gruppe hinzugefügt werden. Einer Gruppe müssen Sie Geräte manuell hinzufügen. Für eine dynamische Gruppe definieren Sie Kriterien, die erfüllt werden müssen, um Mitglied einer Gruppe zu werden. Die Geräte, die diese Kriterien erfüllen, werden der Gruppe automatisch hinzugefügt.

In ZENworks sind verschiedene dynamische Servergruppen bereits vordefiniert, beispielsweise Windows 2012 Server, Windows 2003 Server und SUSE Linux Enterprise Server.

ZENworks umfasst auch dynamische Arbeitsstationsgruppen, z. B. Windows XP-Arbeitsstation, Windows 8-Arbeitsstation, Windows Vista-Arbeitsstation und SUSE Linux Enterprise Desktop. Alle Geräte mit diesen Betriebssystemen werden automatisch in die entsprechende dynamische Gruppe aufgenommen.

Erstellen von Gruppen

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Geräte**.
2. Wenn Sie eine Gruppe für Server erstellen möchten, klicken Sie auf den Ordner **Server**.

oder

Wenn Sie eine Gruppe für Arbeitsstationen erstellen möchten, klicken Sie auf den Ordner **Arbeitsstationen**.

Alternativ:

Wenn eine Gruppe für Mobilgeräte erstellt werden soll, klicken Sie auf den Ordner **Mobilgeräte**.

3 Klicken Sie auf **Neu** > **Servergruppe** (bzw. auf **Neu** > **Arbeitsstationsgruppe** bei Arbeitsstationenoder **Neu** > **Mobilgerätegruppe** bei Mobilgeräten). Der Assistent „Neue Gruppe erstellen“ wird gestartet.

4 Geben Sie auf der Seite „Grundlegende Informationen“ einen Namen für die neue Gruppe in das Feld **Gruppenname** ein und klicken Sie auf **Weiter**.

Der Gruppenname muss sich nach den Namenskonventionen richten.

5 Klicken Sie in der Zusammenfassungsseite auf **Fertig stellen**, um die Gruppe anzulegen, ohne Mitglieder hinzuzufügen.

oder

Klicken Sie auf **Weiter**, wenn Sie der Gruppe Mitglieder hinzufügen möchten. Fahren Sie dann mit Schritt 6 fort.

6 Klicken Sie auf der Seite „Gruppenmitglieder hinzufügen“ auf **Hinzufügen**, um Geräte zur Gruppe hinzuzufügen. Klicken Sie anschließend auf **Weiter**, wenn Sie alle Geräte hinzugefügt haben.

7 Klicken Sie in der Zusammenfassungsseite auf **Fertigstellen**, um die Gruppe anzulegen.

Zum Erstellen von Gerätegruppen können Sie auch die Befehle `workstation-group-create` und `server-group-create` im zman-Dienstprogramm verwenden. Weitere Informationen finden Sie unter „Arbeitsstationsbefehle“ und „Serverbefehle“ im Handbuch *ZENworks: Referenz für Befehlszeilenprogramme*.

Erstellen einer dynamischen Gruppe

1 Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Geräte**.

2 Wenn Sie eine Gruppe für Server erstellen möchten, klicken Sie auf den Ordner **Server**.

oder

Wenn Sie eine Gruppe für Arbeitsstationen erstellen möchten, klicken Sie auf den Ordner **Arbeitsstationen**.

Alternativ:

Wenn eine Gruppe für Mobilgeräte erstellt werden soll, klicken Sie auf den Ordner **Mobilgeräte**.

3 Klicken Sie auf **Neu** > **Dynamische Servergruppe** (bzw. auf **Neu** > **Dynamische Arbeitsstationsgruppe** bei Arbeitsstationen oder **Neu** > **Dynamische Mobilgerätegruppe** bei Mobilgeräten). Der Assistent „Neue Gruppe erstellen“ wird gestartet.

4 Geben Sie auf der Seite „Grundlegende Informationen“ einen Namen für die neue Gruppe in das Feld **Gruppenname** ein und klicken Sie auf **Weiter**.

Der Gruppenname muss sich nach den Namenskonventionen richten.

5 Definieren Sie auf der Seite Filter für Gruppenmitglieder definieren die Kriterien, denen ein Gerät entsprechen muss, um ein Mitglied der Gruppe zu werden. Klicken Sie dann auf **Weiter**.

Klicken Sie auf die Schaltfläche **Hilfe**, um Details zum Erstellen der Kriterien zu erhalten.

6 Klicken Sie auf der Seite „Zusammenfassung“ auf **Fertig stellen**, um die Gruppe zu erstellen.

Vererbung von Zuweisungen für Ordner und Gruppen

Wenn einem Ordner Inhalte zugewiesen werden, wird die Zuweisung an alle Objekte (Benutzer, Geräte, Unterordner) außer den in diesem Ordner befindlichen Gruppen vererbt. Wenn Sie beispielsweise dem Geräteordner1 ein BundleA und eine RichtlinieB zuweisen, werden die beiden Zuweisungen an alle Geräte im Ordner (einschließlich der Geräte in den Unterordnern) vererbt. Die Zuweisungen werden jedoch keiner der im Geräteordner1 befindlichen Gerätegruppen vererbt. Grundsätzlich finden Ordnerzuweisungen keine Anwendung auf die im Ordner befindlichen Gruppen.

Erstellen von Registrierungsschlüsseln und -regeln

Wenn Sie den ZENworks Agent an ein Gerät verteilen, wird das Gerät in Ihrer Verwaltungszone registriert und wird zu einem verwalteten Gerät. Als Teil der Registrierung können Sie den ZENworks-Namen des Geräts sowie den Ordner und die Gruppen angeben, denen das Gerät hinzugefügt werden soll.

Standardmäßig wird der Hostname eines Geräts als sein ZENworks-Name benutzt, es wird dem Ordner `/Server` oder `/Arbeitsstationen` hinzugefügt und erhält keine Mitgliedschaft in Gruppen. Sie können Geräte manuell in andere Ordner verschieben und zu Gruppen hinzufügen, aber das kann eine ermüdende Aufgabe sein, wenn eine große Anzahl an Geräten vorhanden ist oder Sie ständig neue Geräte hinzufügen. Am besten verwalten Sie eine große Anzahl an Geräten, indem Sie sie beim Registrieren automatisch in die korrekten Ordner und Gruppen aufnehmen lassen.

Um Geräte bei der Registrierung zu Ordnern oder Gruppen hinzuzufügen, können Sie Registrierungsschlüssel und/oder Registrierungsregeln verwenden. Mithilfe von Registrierungsschlüsseln und Registrierungsregeln können Sie einem Gerät Ordner- und Gruppenmitgliedschaften zuweisen. Es gibt jedoch Unterschiede zwischen Schlüsseln und Regeln, deren Sie sich bewusst sein sollten, bevor Sie entscheiden, ob Sie eine oder beide Methoden für die Registrierung verwenden möchten.

Diese Funktion ist für Mobilgeräte nicht verfügbar.

- „Registrierungsschlüssel“, auf Seite 28
- „Registrierungsregeln“, auf Seite 28
- „Vorlage zur Benennung von Geräten“, auf Seite 29
- „Weitere Informationen“, auf Seite 29

Registrierungsschlüssel

Ein Registrierungsschlüssel ist eine alphanumerische Zeichenkette, die manuell festgelegt oder per Zufallsgenerator erstellt wird. Während der Bereitstellung des ZENworks Agent auf einem Gerät muss der Registrierungsschlüssel angegeben werden. Wenn das Gerät das erste Mal eine Verbindung zu einem ZENworks-Server aufbaut, wird es dem Ordner und den Gruppen hinzugefügt, die im Schlüssel definiert sind.

Sie können einen oder mehrere Registrierungsschlüssel anlegen, um sicherzustellen, dass die Geräte in die gewünschten Ordner und Gruppen platziert werden. Sie sollten beispielsweise sicherstellen, dass alle Arbeitsstationen der Vertriebsabteilung dem Ordner `/Arbeitsstationen/Vertrieb` hinzugefügt, aber abhängig von ihren Teamaufgaben in drei verschiedene Gruppen gegliedert werden (Team1, Team2, Team3). Sie könnten in diesem Fall drei verschiedene Registrierungsschlüssel erstellen und jeden dieser Schlüssel so konfigurieren, dass die Arbeitsstationen des Vertriebs zum Ordner `/Arbeitsstationen/Vertrieb` und zur passenden Teamgruppe hinzugefügt werden. Solange jede Arbeitsstation den korrekten Registrierungsschlüssel verwendet, wird sie dem entsprechenden Ordner und der entsprechenden Gruppe hinzugefügt.

So erstellen Sie einen Registrierungsschlüssel:

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Konfiguration** und dann auf die Registerkarte **Registrierung**.
2. Klicken Sie im Bereich „Registrierungsschlüssel“ auf **Neu** > **Registrierungsschlüssel**, um den Assistenten zum Erstellen eines neuen Registrierungsschlüssels zu starten.
3. Folgen Sie zur Erstellung des Schlüssels den Anweisungen.

   Informationen darüber, was Sie in den einzelnen Schritten des Assistenten angeben müssen, erhalten Sie über die Schaltfläche **Hilfe**.

Zum Erstellen eines Registrierungsschlüssels können Sie auch den Befehl `registration-create-key` im zman-Dienstprogramm verwenden. Weitere Informationen finden Sie unter „Registrierungskommandos“ im Handbuch *ZENworks: Referenz für Befehlszeilen-Dienstprogramme*.

Registrierungsregeln

Wenn Sie während der Bereitstellung keinen Registrierungsschlüssel eingeben möchten oder wenn Geräte auf der Grundlage vordefinierter Kriterien (z. B. Betriebssystemtyp, CPU oder IP-Adresse) automatisch in verschiedene Ordner und Gruppen aufgenommen werden sollen, können Sie Registrierungsregeln verwenden.

ZENworks schließt eine Standardregistrierungsregel für Server und eine andere für Arbeitsstationen ein. Wenn sich ein Gerät ohne Schlüssel registriert und Sie keine Registrierungsregeln erstellt haben, werden die standardmäßigen Registrierungsregeln angewendet, um die Ordnerzuweisungen zu ermitteln. Diese beiden Standardregeln bewirken, dass alle Server zum Ordner `/Server` und alle Arbeitsstationen zum Ordner `/Arbeitsstationen` hinzugefügt werden.

Die beiden Standardregeln wurden entworfen, um abzusichern, dass kein Fehler mit der Registrierung eines Servers oder einer Arbeitsstation auftritt. Daher können Sie diese beiden Standardregeln nicht löschen oder ändern. Sie können jedoch zusätzliche Regeln definieren, die es Ihnen ermöglichen, Geräte bei der Registrierung zu filtern und sie verschiedenen Ordnern und Gruppen hinzuzufügen. Wenn Sie, wie im Thema „Geräte organisieren: Ordner und Gruppen“, auf

Seite 23 empfohlen wird, Ordner für Geräte mit ähnlichen Konfigurationseinstellungen und Gruppen für Geräte mit ähnlichen Zuweisungen angelegt haben, erhalten neu registrierte Geräte automatisch die für sie passenden Konfigurationseinstellungen und Zuweisungen.

So erstellen Sie eine Registrierungsregel:

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Konfiguration** und dann auf die Registerkarte **Registrierung**.
2. Klicken Sie im Bereich „Registrierungsregel“ auf **Neu**, um den Assistenten zum Erstellen neuer Registrierungsregeln zu starten.
3. Folgen Sie zur Erstellung der Regel den Anweisungen.

   Informationen darüber, was Sie in den einzelnen Schritten des Assistenten angeben müssen, erhalten Sie über die Schaltfläche **Hilfe**.

Zum Erstellen einer Registrierungsregel können Sie auch den Befehl `ruleset-create` im zman-Dienstprogramm verwenden. Weitere Informationen finden Sie unter „Regelsatzkommandos“ im Handbuch *ZENworks: Referenz für Befehlszeilen-Dienstprogramme*.

Vorlage zur Benennung von Geräten

Die Vorlage zur Benennung von Geräten bestimmt, wie Geräte beim Registrieren benannt werden. Standardmäßig wird der Hostname eines Geräts verwendet. Sie können diesen durch eine beliebige Kombination der folgenden Computervariablen ändern: ${HostName}, ${GUID}, ${OS}, ${CPU}, ${DNS}, ${IPAddress} und ${MACAddress}.

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Konfiguration**.
2. Klicken Sie im Bereich „Verwaltungszoneneinstellungen“ auf **Geräteverwaltung**.
3. Klicken Sie auf **Registrierung**, um die Registrierungsseite anzuzeigen.
4. Klicken Sie im Bereich „Vorlage zur Benennung von Geräten“ auf  und wählen Sie die gewünschte Computervariable aus der Liste aus.

   Sie können eine beliebige Kombination aus einer oder mehreren Variablen verwenden, z. B.

   `${HostName}${GUID}`
5. Klicken Sie zum Speichern der Änderungen auf **OK**.

Weitere Informationen

Weitere Informationen zum Registrieren von Geräten finden Sie im Handbuch *ZENworks Discovery, Deployment, and Retirement Reference* (Referenz für die Ermittlung, Bereitstellung und Stilllegung).

Verbinden mit Benutzerquellen

Sie können eine Verbindung zu einem oder mehreren Verzeichnissen herstellen, um autorisierende Benutzerquellen in ZENworks zur Verfügung zu stellen.

Durch Hinzufügen einer Benutzerquelle können Sie ZENworks-Administratorkonten mit LDAP-Benutzerkonten verknüpfen und Geräte mit den Benutzern verknüpfen, die sie hauptsächlich verwenden. Darüber hinaus werden durch das Hinzufügen von Benutzern für folgende ZENworks-Produkte zusätzliche Funktionen ermöglicht:

- **Konfigurationsmanagement:** Ermöglicht es Ihnen, Bundles und Richtlinien Benutzern und Geräten zuzuweisen. Ermöglicht benutzerbasierte Inventarberichte.
- **Bestandsverwaltung:** Ermöglicht es Ihnen, Softwarelizenzen sowohl auf Benutzer- als auch auf Gerätebasis auszuweisen.
- **Endpoint Security Management:** Ermöglicht es Ihnen, Richtlinien sowohl Benutzern als auch Geräten zuzuweisen.

Wenn Sie ein LDAP-Verzeichnis als Benutzerquelle definieren, ist das Verzeichnis nicht betroffen. ZENworks erfordert lediglich Lesezugriff auf das LDAP-Verzeichnis und speichert alle Zuweisungsinformationen in der ZENworks-Datenbank. Ausführlichere Informationen zu den spezifischen Leseberechtigungen, die beim Verbindungsaufbau mit einer Benutzerquelle erforderlich sind, finden Sie unter „Erstellen von Benutzerquellenverbindungen“ im Handbuch *ZENworks: Referenz für Benutzerquellen und Authentifizierung*.

Sie können eine Verbindung zu Novell eDirectory und Microsoft Active Directory herstellen und diese als Benutzerquellen verwenden. Es gelten folgende Mindestanforderungen: Novell eDirectory 8.7.3 und Microsoft Active Directory unter Windows 2000 SP4. Von LDAP ist mindestens Version 3 erforderlich.

Nach der Verbindung zu einem LDAP-Verzeichnis definieren Sie die Container im Verzeichnis, die bekannt gemacht werden sollen. Angenommen, Sie verfügen über einen Microsoft Active Directory-Domänenbaum namens MeineFirma. Sämtliche Benutzer befinden sich in zwei Containern des MeineFirma-Baums: MeineFirma/Benutzer und MeineFirma/Temp/Benutzer. Sie können den MeineFirma-Baum als Quelle und MeineFirma/Benutzer und MeineFirma/Temp/Benutzer als separate Benutzercontainer referenzieren. Hiermit wird der Zugriff innerhalb des Verzeichnisses auf die Container beschränkt, die Benutzer enthalten.

Neben den Benutzern in den von Ihnen hinzugefügten Containern werden im ZENworks-Kontrollzentrum zudem sämtliche in den Containern enthaltenen Benutzergruppen angezeigt. Dadurch wird die Verwaltung von einzelne Benutzern als auch von Bentuzergruppen ermöglicht.

So bauen Sie eine Verbindung zu einer Benutzerquelle auf:

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Konfiguration**.
2. Klicken Sie in der Kontrollleiste „Benutzerquellen“ auf **Neu**, um den Assistenten für die Erstellung neuer Benutzerquellen zu starten.
3. Reagieren Sie zur Erstellung der Benutzerquelle auf die Eingabeaufforderungen.

   Informationen darüber, was Sie in den einzelnen Schritten des Assistenten angeben müssen, erhalten Sie über die Schaltfläche **Hilfe**.

Sie können auch über den Befehl `user-source-create` im zman-Dienstprogramm verwenden, um eine Verbindung mit einer Benutzerquelle herzustellen. Weitere Informationen finden Sie unter „Benutzerkommandos“ im Handbuch *ZENworks: Referenz für Befehlszeilen-Dienstprogramme*.

Weitere Informationen zum Aktivieren von Benutzerquellen zur Registrierung von Mobilgeräten finden Sie unter Configuring User Sources (Konfigurieren von Benutzerquellen) im Handbuch ZENworks Mobile Management Reference (Referenz zu Mobile Management).

Erstellen von ZENworks-Administratorkonten

Während der Installation wird ein standardmäßiges ZENworks-Administratorkonto (mit dem Namen Administrator) erstellt. Dieses Konto, das Super-Administratorkonto genannt wird, bietet volle Verwaltungsrechte für die Verwaltungszone.

Typischerweise sollten Sie Administratorkonten für alle Personen erstellen, die Verwaltungsaufgaben ausführen. Sie können diese Konten als Superadministratorkonten definieren oder als Administratorkonten mit eingeschränkten Rechten. Sie können für einen Benutzer ein Administratorkonto erstellen, mit dem dieser lediglich Geräte in der Verwaltungszone ermitteln und registrieren kann. Oder das Konto ermöglicht es dem Benutzer nur, Geräten Bundles zuzuweisen. Das Konto könnte auch auf die Ausführung von Inventarverwaltungsaufgaben wie die Vertrags-, Lizenz- und Dokumentenverwaltung beschränkt sein.

In einigen Fällen haben Sie möglicherweise mehrere Administratorkonten, für die dieselben Verwaltungsrechte erforderlich sind. Sie brauchen dann die Rechte nicht jedem Konto einzeln zuzuweisen, sondern können eine Administratorrolle erstellen, die Verwaltungsrechte der Rolle zuweisen und anschließend die Konten der Rolle hinzufügen. Sie haben beispielsweise eventuell eine Helpdesk-Rolle, die Verwaltungsrechte bietet, die von mehreren Administratoren benötigt werden.

Sie können Administratorgruppen erstellen. Wenn Sie Rechte und Rollen zu Administratorgruppen hinzufügen, gelten die zugewiesenen Rechte und Rollen für alle Mitglieder in der Gruppe.

Erstellen eines Administratorkontos

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Administratoren**.
2. Klicken Sie in der Kontrollleiste „Administratoren“ auf **Neu** > „Administrator“, um das Dialogfeld „Neuen Administrator hinzufügen“ anzuzeigen.
3. Füllen Sie die Felder aus.

   Mit dem Dialogfeld „Neuen Administrator hinzufügen“ können Sie ein neues Administratorkonto erstellen, indem Sie einen Namen und ein Passwort angeben, oder Sie können einen neuen Administrator basierend auf einem in der Benutzerquelle vorhandenen Benutzer erstellen. Sie können dem neuen Administrator dieselben Rechte geben, über die auch der angemeldete Administrator verfügt.

   Neuen Administrator durch Angabe von Namen und Passwort erstellen: Wählen Sie diese Option, wenn Sie ein neues Administratorkonto anlegen möchten, indem Sie manuell einen Namen und ein Passwort angeben.

Auf Grundlage eines oder mehrerer Benutzer in einer Benutzerquelle: Wählen Sie diese Option, wenn Sie ein neues Administratorkonto auf der Basis von Benutzerinformationen aus Ihrer Benutzerquelle anlegen möchten. Klicken Sie dazu auf **Hinzufügen** und navigieren Sie zu den gewünschten Benutzern und wählen Sie sie aus.

Dieser Administrator erhält dieselben Rechte wie ich: Wählen Sie diese Option aus, um dem neuen Administrator dieselben Rechte wie Ihnen (als aktuell angemeldeter Administrator) zuzuweisen. Wenn Sie über Superadministratorrechte verfügen, wird der neue Administrator als Superadministrator erstellt.

4. Klicken Sie auf **OK**. Der neue Administrator wird in die Kontrollleiste „Administratoren“ aufgenommen.
5. Wenn Sie die Rechte oder Rollen des neuen Administrators ändern müssen, klicken Sie auf das Administratorkonto und dann auf die Registerkarte **Rechte**, um die Kontodetails anzuzeigen.
6. Wenn die Option **Super-Administrator** aktiviert ist, deaktivieren Sie diese Option.

   Superadministratorrechte können nicht geändert werden.
7. Modifizieren Sie die zugewiesenen Rechte mithilfe des Bereichs „Zugewiesene Rechte“.
8. Ändern Sie die zugewiesenen Funktionen im Bereich „Zugewiesene Funktionen“.
9. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

Weitere Informationen zum Erstellen von ZENworks-Administratorkonten, -Administratorrechten oder -Administratorrollen finden Sie im Handbuch ZENworks: Referenz für Administratorkonten und -rechte.

Zum Erstellen eines ZENworks-Administratorkontos können Sie auch den Befehl `admin-create` im zman-Dienstprogramm verwenden. Weitere Informationen finden Sie unter „Administratorbefehle“ im Handbuch *ZENworks: Referenz für Befehlszeilenprogramme*.

Erstellen eines Administratorgruppenkontos

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Administratoren**.
2. Klicken Sie in der Kontrollleiste „Administratoren“ auf **Neu** > **Administratorgruppe**. Das Dialogfeld „Neue Administratorgruppe hinzufügen“ wird geöffnet.
3. Füllen Sie die Felder aus.

   Im Dialogfeld „Neue Administratorgruppe hinzufügen“ können Sie ein neues Administratorgruppenkonto erstellen, indem Sie einen Gruppennamen angeben und der Gruppe Mitglieder hinzufügen, oder Sie können eine neue Administratorgruppe basierend auf einer in der Benutzerquelle vorhandenen Benutzergruppe erstellen. Jeder Administratorgruppenname muss eindeutig sein.

   Neue Administratorgruppe durch Angabe eines Namens und durch Hinzufügen von Mitgliedern erstellen: Wählen Sie diese Option aus, wenn Sie ein neues Administratorgruppenkonto durch manuelle Angabe des Namens und manuelles Hinzufügen der Mitglieder erstellen möchten. Klicken Sie zum Hinzufügen von Mitgliedern auf **Hinzufügen**, suchen Sie nach den gewünschten Administratoren und wählen Sie sie aus. Sie können der Gruppe eine beliebige Zahl von Administratoren hinzufügen. Andere Administratorgruppen können der Gruppe jedoch nicht hinzugefügt werden.

Basierend auf Benutzergruppen in einer Benutzerquelle: Wählen Sie diese Option aus, wenn Sie ein neues Administratorgruppenkonto basierend auf Benutzergruppeninformationen aus der Benutzerquelle erstellen möchten. Klicken Sie hierzu auf **Hinzufügen**, suchen Sie nach der gewünschten Benutzergruppe und wählen Sie diese aus.

Importieren Sie umgehend die Benutzermitglieder der jeweiligen Benutzergruppe als Administratoren: Wählen Sie diese Option aus, damit die Benutzermitglieder der ausgewählten Benutzergruppen direkt als Administratoren hinzugefügt werden können.

4. Klicken Sie auf **OK**. Die neue Administratorgruppe wird in die Kontrollleiste „Administratoren“ aufgenommen.
5. Wenn Sie die Rechte oder Rollen der neuen Administratorgruppe ändern müssen, klicken Sie auf das Administratorgruppenkonto und dann auf die Registerkarte **Rechte**, um die Kontodetails anzuzeigen.
6. Modifizieren Sie die zugewiesenen Rechte mithilfe des Bereichs „Zugewiesene Rechte“.
7. Ändern Sie die zugewiesenen Funktionen im Bereich „Zugewiesene Funktionen“.
8. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

Weitere Informationen zum Erstellen von ZENworks-Administratorgruppenkonten, -Administratorrechten oder -Administratorrollen finden Sie im Handbuch *ZENworks: Referenz für Administratorkonten und -rechte*.

Zum Erstellen eines ZENworks-Administratorkontos können Sie auch den Befehl `admin-create` im zman-Dienstprogramm verwenden. Weitere Informationen finden Sie unter „Administratorbefehle“ im Handbuch *ZENworks: Referenz für Befehlszeilenprogramme*.

Ändern der Konfigurationseinstellungen

Mit den Konfigurationseinstellungen der Verwaltungszone können Sie verschiedene Funktionen für Ihre Zone steuern. Es gibt Einstellungen zur Geräteverwaltung, mit denen Sie steuern können, wie oft Geräte für aktualisierte Daten auf einen ZENworks-Server zugreifen, wie häufig dynamische Gruppen aktualisiert werden und welche Meldungsstufen (Information, Warnung oder Fehler) des ZENworks Agent protokolliert werden. Es gibt Ereignis- und Messaging-Einstellungen, Ermittlungs- und Bereitstellungseinstellungen usw.

Verwaltungszoneneinstellungen, die für Geräte gelten, werden von allen Geräten in der Zone geerbt (übernommen). Wie schon in „Geräte organisieren: Ordner und Gruppen“, auf Seite 23 erläutert, können Sie Zoneneinstellungen außer Kraft setzen, indem Sie sie für Geräteordner oder einzelne Geräte konfigurieren. Auf diese Weise können Sie Zoneneinstellungen festlegen, die für die meisten Geräte gelten, und dann die Einstellungen je nach Bedarf für einzelne Ordner und Geräte überschreiben.

Die Zoneneinstellungen sind standardmäßig mit Werten vorkonfiguriert, mit denen häufig verwendete Funktionen bereitgestellt werden. Sie können diese Einstellungen allerdings ändern und so optimal auf das in Ihrer Umgebung erforderliche Verhalten abstimmen.

- „Ändern von Konfigurationseinstellungen in der Zone“, auf Seite 34
- „Bearbeiten von Konfigurationseinstellungen für einen Ordner“, auf Seite 34
- „Ändern von Konfigurationseinstellungen an einem Gerät“, auf Seite 34

Ändern von Konfigurationseinstellungen in der Zone

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Konfiguration**.
2. Klicken Sie in der Kontrollleiste „Verwaltungszoneneinstellungen“ auf die Einstellungskategorie (z. B. **Geräteverwaltung**, **Ermittlung und Bereitstellung** und **Ereignis und Messaging**), deren Einstellungen geändert werden sollen.
3. Klicken Sie auf die Einstellung, um die Detailseite anzuzeigen.
4. Bearbeiten Sie die Einstellung nach Bedarf.

   Weitere Informationen zu dieser Einstellung finden Sie im Handbuch *Referenz zu den ZENworks - Verwaltungszoneneinstellungen*.
5. Klicken Sie auf **OK** oder **Anwenden**.

   Wenn die Konfigurationseinstellung für Geräte gilt, wird die Einstellung an alle Geräte in der Zone vererbt, falls sie nicht auf Ordner- oder Geräteebene außer Kraft gesetzt wird.

Bearbeiten von Konfigurationseinstellungen für einen Ordner

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Geräte**.
2. Navigieren Sie im Bereich „Geräte“ (auf der Registerkarte **Verwaltet**) zu dem Ordner, dessen Einstellungen Sie ändern möchten.
3. Zum Anzeigen der Details klicken Sie neben dem Ordnernamen auf **Details**.
4. Klicken Sie auf die Registerkarte **Einstellungen**.
5. Klicken Sie in der Kontrollleiste „Einstellungen“ auf die Einstellungskategorie (z. B. **Geräteverwaltung** oder **Infrastrukturverwaltung**), deren Einstellungen geändert werden sollen.
6. Klicken Sie auf die Einstellung. Die zugehörige Detailseite wird geöffnet.
7. Bearbeiten Sie die Einstellung nach Bedarf.

   Weitere Informationen zu dieser Einstellung finden Sie im Handbuch *Referenz zu den ZENworks - Verwaltungszoneneinstellungen*.
8. Klicken Sie auf **OK** oder **Anwenden**.

   Die Konfigurationseinstellung wird an alle Geräte im Ordner vererbt, einschließlich etwaiger Geräte in Unterordnern, es sei denn, die Einstellung wird für einen Unterordner oder individuelle Geräte überschrieben.

Ändern von Konfigurationseinstellungen an einem Gerät

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Geräte**.
2. Navigieren Sie im Bereich „Geräte“ (auf der Registerkarte **Verwaltet**) zu dem Gerät, dessen Einstellungen Sie ändern möchten.
3. Wenn Sie das Gerät gefunden haben, klicken Sie auf seinen Namen, um die Details anzuzeigen.
4. Klicken Sie auf die Registerkarte **Einstellungen**.
5. Klicken Sie in der Kontrollleiste „Einstellungen“ auf die Einstellungskategorie (**Geräteverwaltung**, **Infrastrukturverwaltung** usw.), deren Einstellungen Sie ändern möchten.
6. Klicken Sie auf die Einstellung, um die Detailseite anzuzeigen.

7 Ändern Sie die Einstellung wie gewünscht.

   Weitere Informationen zur Einstellung erhalten Sie mit der Schaltfläche **Hilfe** im ZENworks Control Center.

8 Wenn Sie die Einstellung wie gewünscht festgelegt haben, klicken Sie auf **OK** (oder **Anwenden**), um Ihre Änderungen zu speichern.

Zonenfreigabe und Zonenabonnement

Die Funktion zum Abonnieren und Freigeben in ZENworks bietet die Möglichkeit, Inhaltsobjekte wie Bundles und Richtlinien über mehrere ZENworks-Zonen hinweg freizugeben:

- **Freigabezone:** Gibt Inhalte frei.
- **Abonnentenzone:** Abonniert die Freigabezone und reproduziert den freigegebenen Inhalt in der eigenen Zone.

Im ZENworks-Kontrollzentrum verwalten Sie die Freigabeaktionen der Zone über den Link „Zonenfreigabeeinstellungen“ im Bereich für die Infrastrukturverwaltung.

In der Freigabezone wird ein Primärserver als Freigabeserver bezeichnet. Die gesamte Freigabe von Inhalten läuft über diesen Server ab. Zum Registrieren der Abonnentenzone wird ein Abonnentenschlüssel aus der Freigabezone übermittelt. Der Abonnentenschlüssel gibt den Abonnenten keine Rechte auf bestimmte Inhalte. Der Abonnentenschlüssel ist für die Abonnentenregistrierung vorgesehen.

Der erforderliche Inhalt wird dann von der Freigabezone freigegeben und in der Abonnentenzone reproduziert. Falls Probleme bei der Reproduktion auftreten, erhalten Sie eine Benachrichtigung und Sie können die entsprechenden Gegenmaßnahmen ergreifen.

Weitere Informationen finden Sie im Handbuch *ZENworks: Referenz für Abonnieren und Freigeben*.

Aktualisieren der ZENworks-Software

Die ZENworks -Software kann auf allen Geräten in der Verwaltungszone aktualisiert werden, auf denen die Software installiert ist. Das Herunterladen von Updates kann zeitlich geplant werden. Software-Aktualisierungen werden auf Ebene der Support Pack-Versionen zur Verfügung gestellt. Sie können dabei wählen, ob Sie die jeweilige Aktualisierung nach Prüfung des Inhalts anwenden möchten (Support Pack-Versionen sind kumulativ). Sie können zur Aktualisierung Ihrer Wissensdatenbank auch die jüngste Aktualisierung zur Produkterkennung (PRU=Product Recognition Update) verwenden, womit das ZENworks-Inventar jüngere Software erkennt.

Weitere Informationen finden Sie im Handbuch *ZENworks Referenz für Systemaktualisierungen*.

Erstellen von Standorten

Die Sicherheitsanforderungen für ein Gerät können sich von Standort zu Standort unterscheiden. Zum Beispiel kann die persönliche Firewall bei einem Gerät in einem Flughafen-Terminal andere Einschränkungen haben als ein Gerät in einem Büro innerhalb der Firewall in Ihrem Unternehmen.

Damit die Sicherheitsanforderungen eines Geräts in jedem Fall für den jeweiligen Standort geeignet sind, unterstützt ZENworks sowohl globale als auch standortbasierte Richtlinien. Globale Richtlinien werden unabhängig vom Standort des Geräts angewendet. Standortbasierte Richtlinien werden nur angewendet, wenn der aktuelle Standort des Geräts die Kriterien für einen mit der Richtlinie verknüpften Standort erfüllt. Wenn Sie beispielsweise eine standortbasierte Richtlinie für Ihr Firmenbüro erstellen und diese einem Notebook zuweisen, gilt die Richtlinie nur, wenn es sich bei dem Standort des Notebooks um das Firmenbüro handelt.

Wenn standortbasierte Richtlinien verwendet werden sollen, müssen Sie zunächst die Standorte definieren, die für Ihre Organisation sinnvoll sind. Ein Standort stellt einen Ort oder einen Ortstyp dar, für den spezifische Sicherheitsanforderungen gelten. So können beispielsweise unterschiedliche Anforderungen für ein Gerät gelten, je nachdem, ob es im Büro, zu Hause oder in einem Flughafen verwendet wird.

Standorte sind durch Netzwerkumgebungen definiert. Angenommen, Sie haben ein Büro in New York und ein Büro in Tokio. Für beide Büros gelten dieselben Sicherheitsanforderungen. Daher erstellen Sie einen Standort vom Typ „Büro“ und verknüpfen ihn mit zwei Netzwerkumgebungen: „Netzwerk von Büro New York“ und „Netzwerk von Büro Tokio“. Jede dieser Umgebungen ist explizit durch eine Menge von Services für Gateways, DNS-Server und drahtlose Zugriffspunkte definiert. Wenn der ZENworks Agent feststellt, dass seine aktuelle Umgebung mit dem Netzwerk von Büro New York oder dem Netzwerk von Büro Tokio übereinstimmt, legt er seinen Standort als Standort vom Typ „Büro“ fest und wendet die Sicherheitsrichtlinien an, die mit dem Standort vom Typ „Büro“ verknüpft sind.

In den folgenden Abschnitten wird erläutert, wie Standorte erstellt werden:

- „Definieren einer Netzwerkumgebung“, auf Seite 36
- „Erstellen von Standorten“, auf Seite 37
- „Auswahl eines Standorts und einer Netzwerkumgebung auf einem verwalteten Gerät“, auf Seite 38

Definieren einer Netzwerkumgebung

Netzwerkumgebungsdefinitionen sind die Bausteine für Standorte. Netzwerkumgebungen können beim Erstellen eines Standorts definiert werden. Es wird jedoch empfohlen, zunächst die Netzwerkumgebungen zu definieren und sie dann beim Erstellen von Standorten hinzuzufügen.

So erstellen Sie eine Netzwerkumgebung:

1. Klicken Sie im ZENworks-Kontrollzentrum auf **Konfiguration** > **Standorte**.
2. Klicken Sie in der Kontrollleiste „Netzwerkumgebungen“ auf **Neu**. Der Assistent zum Erstellen einer neuen Netzwerkumgebung wird gestartet.
3. Geben Sie auf der Seite „Details definieren“ einen Namen für die Netzwerkumgebung an und klicken Sie anschließend auf **Weiter**.
4. Geben Sie auf der Seite „Details der Netzwerkumgebung“ Folgendes an:

Auf Adaptertyp beschränken: Standardmäßig werden die auf dieser Seite definierten Netzwerkdienste hinsichtlich der kabelgebundenen, kabellosen und Dialup-Netzwerkadapter evaluiert. Wenn die Evaluierung auf einen bestimmten Adaptertyp eingeschränkt werden soll, wählen Sie **Kabelgebunden**, **Kabellos** oder **Dialup** aus.

Mindestübereinstimmung: Geben Sie die minimale Anzahl an definierten Netzwerkdiensten an, die übereinstimmen müssen, damit diese Netzwerkumgebung ausgewählt werden kann.

Geben Sie die minimale Anzahl an definierten Netzwerkdiensten an, die übereinstimmen müssen, damit diese Netzwerkumgebung ausgewählt werden kann.

Wenn Sie beispielsweise eine Gateway-Adresse, drei DNS-Server und einen DHCP-Server definieren, haben Sie insgesamt fünf Services. Sie können angeben, dass mindestens drei dieser Services übereinstimmen müssen, damit diese Netzwerkumgebung ausgewählt wird.

Bei der Angabe eines Werts für die Mindestübereinstimmung beachten Sie Folgendes:

- Die Zahl darf nicht kleiner sein als die Anzahl der Dienste, die als „Muss übereinstimmen“ gekennzeichnet sind.
- Die Anzahl sollte die Gesamtzahl der definierten Services nicht übersteigen. Anderenfalls würde die Mindestübereinstimmung nie erreicht und die Netzwerkumgebung wird nie ausgewählt.

Netzwerk-Services: Hier können Sie die Netzwerkdienste definieren, mit denen der ZENworks-Agent ermittelt, ob seine derzeitige Netzwerkumgebung mit dieser Netzwerkumgebung übereinstimmt. Wählen Sie die Registerkarte für den zu definierenden Netzwerkdienst. Klicken Sie auf **Hinzufügen** und geben Sie dann die erforderlichen Informationen an.

5 Klicken Sie auf **Weiter**. Die Seite „Zusammenfassung“ wird angezeigt. Klicken Sie dort auf **Fertig stellen**.

Erstellen von Standorten

Beim Erstellen eines Standorts geben Sie einen Standortnamen an; anschließend verknüpfen Sie die erforderlichen Netzwerkumgebungen mit dem Standort.

1 Klicken Sie im ZENworks-Kontrollzentrum auf **Konfiguration** > **Standorte**.

2 Klicken Sie in der Kontrollleiste „Standorte“ auf **Neu**. Der Assistent zum Erstellen neuer Standorte wird gestartet.

3 Geben Sie auf der Seite „Details definieren“ einen Namen für den Standort an und klicken Sie anschließend auf **Weiter**.

4 Auf der Seite „Netzwerkumgebungen zuweisen“:

4a Wählen Sie die Option **Vorhandene Netzwerkumgebungen dem Standort zuweisen** aus.

4b Klicken Sie auf **Hinzufügen**, wählen Sie die Netzwerkumgebungen aus, für die der Standort definiert werden soll, und klicken Sie auf **OK**. Die Umgebungen werden in die Liste aufgenommen.

4c Klicken Sie auf **Weiter**, nachdem Sie die Netzwerkumgebungen hinzugefügt haben.

5 Klicken Sie auf der Seite „Zusammenfassung“ auf **Fertig stellen**, um den Standort zu erstellen und ihn der Liste „Standorte“ hinzuzufügen.

Wenn mehrere Standorte die Netzwerkumgebung umfassen, die der ZENworks-Agent ermittelt hat, bestimmt die Reihenfolge der Liste den zu verwendenden Standort. Standardmäßig wird der erste Standort in der Liste ausgewählt. Sie können die Reihenfolge in der Liste mit **Nach oben** und **Nach unten** ändern.

Sie können auch die Befehle `network-environment-create` und `location-create` im zman-Dienstprogramm verwenden, um eine Netzwerkumgebung und mit der erstellten Netzwerkumgebung den entsprechenden Standort zu erstellen. Weitere Informationen finden Sie unter „Registrierungskommandos“ im Handbuch *ZENworks: Referenz für Befehlszeilen-Dienstprogramme*.

Auswahl eines Standorts und einer Netzwerkumgebung auf einem verwalteten Gerät

Wenn Sie mehrere Standorte und Netzwerkumgebungen im ZENworks-Kontrollzentrum definiert haben, sucht der ZENworks-Agent auf dem verwalteten Gerät alle definierten Netzwerkumgebungen ab, um übereinstimmende Umgebungen zu erkennen. Aus den erkannten Umgebungen wählt der ZENworks-Agent die Netzwerkumgebungen mit der größten Anzahl von übereinstimmenden Netzwerkdiensten aus (wie zum Beispiel die Client-IP-Adresse oder die DNS-Server). Der ZENworks-Agent sucht anschließend die geordnete Liste der Standorte ab, erkennt den ersten Standort, der einen oder mehrere der ausgewählten Netzwerkumgebungen enthält, und wählt den Standort und die erste übereinstimmende Netzwerkumgebung an diesem Standort aus.

Beispiel:

- Die im ZENworks-Kontrollzentrum definierten Standorte sind in der folgenden Reihenfolge aufgeführt: S1 und S2.
- Die Netzwerkumgebungen in L1 werden in der folgenden Reihenfolge aufgeführt: NE1, NE2 und NE4.
- Die Netzwerkumgebungen in L2 werden in der folgenden Reihenfolge aufgeführt: NE2, NE3 und NE4.
- Der ZENworks-Agent auf dem verwalteten Gerät erkennt, dass NE2, NE3 und NE4 auf dem verwalteten Gerät übereinstimmen.

Wenn NU2 und NU4 jeweils zwei Netzwerkdienstübereinstimmungen aufweisen und NU3 nur eine aufweist, wählt der ZENworks-Agent NU2 und NU4, weil sie die meisten Netzwerkdienstübereinstimmungen aufweisen. Da NU2 die zuerst in S1 aufgeführte Netzwerkumgebung ist, werden S1 und NU2 als Standort und Netzwerkumgebung ausgewählt.

HINWEIS: Damit eine Netzwerkumgebung auf dem verwalteten Gerät als übereinstimmend erkannt wird, müssen alle in der Netzwerkumgebung festgelegten Beschränkungen erfüllt werden. Hierzu zählen das für die Netzwerkumgebung angegebene Attribut **Mindestübereinstimmung** sowie das für die Netzwerkdienste in der Netzwerkumgebung angegebene Attribut **Muss übereinstimmen**.

Dashboard

Die Dashboard-Funktion umfasst einen umfassenden Snapshot der Schlüsselindikatoren, sodass Sie schnell den Zustand insgesamt sowie die Compliance der Geräte in Ihrer Zone einschätzen können. Dashboards ermöglichen es Ihnen, zu weiteren Interessensbereichen zu gelangen.

Die ZENworks-Dashboards zeigen Informationen zum Status von Geräten und Patches in der Zone, und Sie können dort die nötigen Aktionen einleiten.

Weitere Informationen finden Sie im Handbuch ZENworks Dashboard Reference (Referenz zu Dashboards).

4 Bereitstellung des ZENworks-Agenten

Der ZENworks Agent muss auf den zu verwaltenden Geräten bereitgestellt werden. Die folgenden Abschnitte enthalten Anweisungen, mit denen der Prozess zur Bereitstellung des Agenten erläutert wird:

HINWEIS: Wenn ein Gerät die Anforderungen für die Installation von ZENworks Agent nicht erfüllt (siehe „Anforderungen an verwaltete Geräte“ in den *ZENworks 2020 System Requirements* (Systemanforderungen)) , können Sie auf diesem Gerät unter Umständen das Modul „Nur Inventar“ installieren und so die Inventarisierung des Geräts unterstützen. Weitere Informationen finden Sie im Handbuch *ZENworks: Referenz für die Ermittlung, Bereitstellung und Stilllegung*.

Konfigurieren der ZENworks-Agent-Funktionen

Der ZENworks Agent verwendet verschiedene Module zur Ausführung von Funktionen auf einem Gerät. Diese Module werden als ZENworks-Agent-Funktionen bezeichnet. Jedes ZENworks -Produkt verfügt über spezifische Funktionen, wie in der folgenden Tabelle dargestellt. Die ZENworks-Produkte sind in der linken Spalte aufgeführt. Die anderen Spalten stellen die ZENworks-Agent-Funktionen dar.

	Inventarverwaltung	Bundle-Verwaltung	Endpoint Security	Full Disk Encryption	Image-Verwaltung	Patchverwaltung	Richtlinienverwaltung	Fernverwaltung	Benutzerverwaltung
ZENworks Asset Management	✓								✓
ZENworks-Konfigurationsverwaltung		✓			✓		✓	✓	✓
ZENworks Endpoint Security Management			✓						✓
ZENworks Full Disk Encryption				✓					
ZENworks Patch Management						✓			

Standardmäßig werden beim Aktivieren eines ZENworks-Produkts alle zugehörigen ZENworks-Agent-Funktionen installiert und aktiviert. Eine Ausnahme bildet ZENworks Asset Management, das die Benutzerverwaltungsfunktion nicht automatisch aktiviert.

Die Benutzerverwaltungsfunktion wird in allen ZENworks-Produkten nur auf verwalteten Windows-Geräten unterstützt.

Wenn eine Funktion auf einem Gerät nicht installiert oder aktiviert werden soll, können Sie es in der Verwaltungszone, im Geräteordner oder auf dem jeweiligen Gerät deinstallieren oder deaktivieren.

Wenn Sie beispielsweise ZENworks Configuration Management verwenden und die Fernverwaltung auf keinem Gerät verwenden möchten, können Sie sie in der Verwaltungszone deaktivieren. Oder wenn Sie ZENworks Configuration Management und ZENworks Asset Management verwenden, die Inventarverwaltung jedoch nicht auf allen Geräten nutzen möchten, können Sie die Inventarverwaltungsfunktion in der Verwaltungszone aktivieren und sie dann in Geräteordnern oder einzelnen Geräten deaktivieren (oder deinstallieren).

Weitere Informationen zum Anpassen der ZENworks-Agent-Funktionen (vor oder nach dem Bereitstellen des Agenten) finden Sie in den folgenden Abschnitten:

- „Anpassen der ZENworks-Agent-Funktionen“, auf Seite 42
- „Koexistenz mit ZENworks Desktop Management Agent“, auf Seite 43

Anpassen der ZENworks-Agent-Funktionen

Bei der ersten Bereitstellung werden die auf Verwaltungszonenebene ausgewählten Funktionen von ZENworks Agent installiert und aktiviert. Nach der Registrierung des Agenten werden die auf Geräteordner- oder Geräteebene definierten Einstellungen verwendet (sofern sie von den Zoneneinstellungen abweichen).

HINWEIS: Die Anpassung von ZENworks-Agent-Funktionen gilt nicht für Macintosh-Geräte.

In den folgenden Schritten wird die Anpassung der Einstellungen auf Verwaltungszonenebene erläutert. Informationen zum Anpassen der Einstellungen in einem Geräteordner oder auf einem einzelnen Gerät finden Sie im Abschnitt „Anpassen der Agentenfunktionen“ im Handbuch *ZENworks: Referenz für die Ermittlung, Bereitstellung und Stilllegung*.

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Konfiguration**.
2. Klicken Sie im Bereich „Verwaltungszoneneinstellungen“ auf **Geräteverwaltung** > **ZENworks-Agent**.
3. In der Kontrollleiste „Agentenfunktionen“:
   - Wenn Sie eine Funktion nicht installieren möchten, heben Sie die Auswahl für **Installiert** neben der betreffenden Funktion auf. Die ausgewählte Funktion wird auf dem Gerät nicht installiert. Wenn Sie die Auswahl für alle Funktionen aufheben, wird nur der Kernagent installiert.
   - Wenn Sie eine Funktion zwar installieren, jedoch deaktivieren möchten, wählen Sie **Installiert** und **Deaktiviert** neben der gewünschten Funktion aus. Die Funktion ist zwar auf dem Gerät installiert, wird aber nicht ausgeführt.

Zur Installation der Funktionen „Bundle-Verwaltung“, „Fernverwaltung“ bzw. „Benutzerverwaltung“ ist ein Neustart des Geräts erforderlich. Zur Installation der Funktion „Image-Verwaltung“ ist ein Neustart nur unter Windows 2008 und Windows Vista erforderlich. Sie werden aufgefordert, das Gerät basierend auf der ausgewählten Neustartoption neu zu starten.

4 Klicken Sie zum Speichern der Änderungen auf **OK**.

Koexistenz mit ZENworks Desktop Management Agent

Sie können ZENworks Agent auf Geräten bereitstellen, auf denen der ZENworks Desktop Agent installiert ist.

Der ZENworks Agent und der ZENworks Desktop Agent können auf demselben Gerät gleichzeitig installiert sein, jedoch nur zur Unterstützung der gemeinsamen Verwendung von ZENworks Asset Management und ZENworks Desktop Management. Wenn Sie den ZENworks-Agenten auf einem Gerät bereitstellen, auf dem der ZENworks-Desktop-Agent installiert ist, sollten Sie nur die ZENworks-Agent-Funktionen verwenden, die nicht mit ZENworks Configuration Management verknüpft sind. Die Funktionen zur Bundle-Verwaltung, Image-Verwaltung, Richtlinienverwaltung, Fernverwaltung und Benutzerverwaltung sollten in diesem Fall nicht verwendet werden. Bei Auswahl einer dieser Funktionen wird vor der Installation von ZENworks-Agent der ZENworks-Desktop-Agent deinstalliert.

Weitere Informationen zur Koexistenz von ZENworks Agent und dem ZENworks Desktop Agent finden Sie im Abschnitt „Bereitstellung des ZENworks Agent“ im Handbuch *ZENworks: Referenz für die Ermittlung, Bereitstellung und Stilllegung*.

Konfigurieren der ZENworks-Agent-Sicherheit

Um den ZENworks Agent auf Geräten zu sichern, können Sie sowohl dessen Einstellungen für die Deinstallation als auch für die Selbstverteidigung konfigurieren.

1 Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Konfiguration**.

2 Klicken Sie im Bereich „Verwaltungszoneneinstellungen“ auf **Geräteverwaltung** und dann auf **ZENworks-Agent**.

3 Konfigurieren Sie im Bereich „Agentensicherheit“ folgende Einstellungen:

- **Benutzern die Deinstallation vom ZENworks Agent erlauben:** Mit dieser Option deinstallieren Sie den ZENworks Agent.
- **Deinstallationspasswort für ZENworks Agent erforderlich:** Mit dieser Option geben Sie ein Passwort an, das für die Deinstallation des ZENworks Agent erforderlich ist. Klicken Sie auf **Ändern**, um das Passwort festzulegen.

  Um die Verteilung des Deinstallationspassworts an die Benutzer zu vermeiden, empfehlen wir, mit dem Dienstprogramm „Password Key Generator“ (Programm zur Erstellung des Passwortschlüssels) einen Passwortschlüssel zu generieren. Der Schlüssel, der auf dem Deinstallationspasswort beruht, funktioniert ebenso wie das Deinstallationspasswort, kann jedoch an ein einzelnes Gerät oder einen einzelnen Benutzer gebunden werden, sodass sein Gebrauch eingeschränkt wird.

  Das Dienstprogramm „Password Key Generator“ kann über die Liste Konfigurationsaufgaben im linken Navigationsbereich aufgerufen werden.

- **Überschreibungspasswort für den ZENworks Agent aktivieren:** Mit dieser Option geben Sie ein Überschreibungspasswort an, das im ZENworks Agent wie folgt verwendet werden kann:
  - Zugriff auf Informationen zum aktuellen Standort des Geräts und dazu, wie dieser Standort zugewiesen wurde.
  - Zugriff auf die Verwaltungsoptionen in Endpoint Security Agent. Mit diesen Optionen können Sie die aktuell angewandten Sicherheitsrichtlinien (mit Ausnahme der Datenverschlüsselungsrichtlinie) deaktivieren und detaillierte Richtlinieninformationen sowie Informationen zum Agentenstatus anzeigen.
  - Zugriff auf die Verwaltungsoptionen im Full Disk Encryption Agent. Mit diesen Optionen können Sie detaillierte Richtlinieninformationen festlegen, Informationen zum Agentenstatus anzeigen und Funktionen ausführen, wie beispielsweise das Aktivieren der Benutzererfassung als auch das Entschlüsseln von Volumes.
  - Deinstallation des ZENworks Agent.
- **Selbstverteidigung für ZENworks Agent aktivieren:** Mit dieser Option aktivieren Sie die Selbstverteidigung. Derzeit schützt die Selbstverteidigungsfunktion nur den ZENworks Endpoint Security Agent. Die anderen ZENworks Agent-Module werden nicht geschützt.

  Die Selbstverteidigung („Self Defense“) schützt den Endpoint Security Agent, sodass er nicht heruntergefahren, deaktiviert oder auf irgendeine Weise manipuliert werden kann. Wenn ein Benutzer eine der folgenden Aktivitäten durchführt, wird das Gerät automatisch neu gebootet, um die korrekte Systemkonfiguration wiederherzustellen:
  - Beenden eines Prozesses des Endpoint Security Agent über den Windows-Task-Manager.
  - Stoppen oder vorübergehendes Anhalten eines Endpoint Security Agent-Diensts.
  - Entfernen wichtiger Dateien und Registrierungseinträge. Wenn eine Änderung an einem Registrierungsschlüssel oder Wert vorgenommen wird, der mit dem Endpoint Security Agent verknüpft ist, wird der Registrierungsschlüssel oder Wert sofort zurückgesetzt.
  - Deaktivierung der Bindung der NDIS-Filtertreiber an Adapter.

4 Klicken Sie zum Speichern der Änderungen auf **OK**.

Installieren des ZENworks Agent

In den nachfolgenden Abschnitten finden Sie Anweisungen für die manuelle Installation des ZENworks Agent auf Geräten.

- „Manuelle Installation unter Windows“, auf Seite 45
- „Manuelle Installation unter Linux“, auf Seite 46
- „Manuelle Installation auf einem Macintosh-Gerät“, auf Seite 47

HINWEIS: Alternativ zur manuellen Installation können Sie die Netzwerkgeräte ermitteln und bereitstellen lassen und so die Installation des ZENworks-Agenten automatisieren. Die Ermittlung und Bereitstellung ist für diesen Schnellstart zu umfangreich. Weitere Informationen zu diesem Verfahren finden Sie im Handbuch *ZENworks -Referenz für die Ermittlung, Bereitstellung und Stilllegung*.

Manuelle Installation unter Windows

1 Stellen Sie sicher, dass das Gerät den Anforderungen entspricht (siehe „Managed Device Requirements (Anforderungen an verwaltete Geräte).“

2 Öffnen Sie auf dem Zielgerät einen Webbrowser und navigieren Sie zur folgenden Adresse:

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

Ersetzen Sie *server* durch den DNS-Namen oder die IP-Adresse eines ZENworks-Servers und ersetzen Sie *port* nur dann, wenn der ZENworks-Server nicht den Standardport (80 oder 443) verwendet.

Im Webbrowser wird eine Liste mit Bereitstellungspaketen für den ZENworks-Agenten angezeigt. Für jede Architektur (32-Bit und 64-Bit) gibt es die folgenden Pakettypen:

- **Netzwerk (.NET erforderlich):** Mit dem Netzwerkpaket (.NET erforderlich) wird lediglich der PreAgent auf dem Zielgerät installiert; im Anschluss nimmt der PreAgent das Herunterladen und Installieren von ZENworks Agent vom ZENworks-Server vor. Für das Netzwerkpaket (.NET erforderlich) muss Microsoft .NET 4.0 oder höher auf dem Gerät installiert werden, bevor der Agent auf dem Gerät bereitgestellt wird.
- **Einzelserver (.NET erforderlich):** Für das Einzelserverpaket (.NET erforderlich) muss Microsoft .NET 4.0 oder höher auf dem Gerät installiert werden, bevor der Agent auf dem Gerät bereitgestellt wird. Dieses Paket enthält alle für die Installation des ZENworks-Agenten erforderlichen ausführbaren Dateien mit Ausnahme des Microsoft .NET-Installationsprogramms.
- **Einzelserver:** Mit dem eigenständigen Paket wird der PreAgent installiert und alle für die Installation des ZENworks-Agenten erforderlichen ausführbaren Dateien (auch das Microsoft .NET-Installationsprogramm) werden auf dem Zielgerät extrahiert. Anschließend installiert der PreAgent den ZENworks-Agenten vom lokalen Gerät aus. Dieses Paket ist hilfreich, wenn Sie ZENworks Agent auf einem Gerät installieren müssen, das zurzeit nicht mit dem Netzwerk verbunden ist. Sie können das Paket auf einem Wechselmedium (CD, USB-Flash-Laufwerk usw.) speichern und angeben, dass das Einzelplatzgerät das Paket vom Medium aus ausführt. Der ZENworks-Agent wird auf dem Gerät installiert, es erfolgt jedoch keinerlei Registrierung oder Verwaltung, bis das Gerät eine Verbindung mit dem Netzwerk herstellt.
- **Benutzerdefiniert:** Die vordefinierten Bereitstellungspakete haben den Paketnamen „Standardagent“. Für benutzerdefinierte Bereitstellungspakete, die über **Bereitstellung** > **Bereitstellungspaket bearbeiten** erstellt wurden, werden die Namen angezeigt, die ihnen während ihrer Erstellung zugewiesen wurden.

3 Klicken Sie auf den Namen des zu verwendenden Bereitstellungspakets. Speichern Sie das Paket auf dem lokalen Laufwerk des Geräts oder führen Sie es vom ZENworks-Server aus aus.

4 Wenn Sie das Paket heruntergeladen haben, starten Sie das Paket auf dem Gerät.

Weitere Informationen zu den Optionen für das Paket, wenn der Aufruf von einer Befehlszeile aus erfolgt, finden Sie unter „Paketoptionen für Windows, Linux und Macintosh“ im Handbuch *ZENworks: Referenz für die Ermittlung, Bereitstellung und Stilllegung*.

WICHTIG: Beim Installieren eines Komplettpakets ist für die Installation des Windows-Installationsprogramms oder .NET Framework unter Umständen ein Neustart nach dem Start des Pakets erforderlich. In einer Meldung werden die verschiedenen Optionen beim Neustart angezeigt. Wählen Sie eine der folgenden Optionen aus:

- Unternehmen Sie nichts, und nach fünf Minuten erfolgt ein automatischer Neutstart.
- Klicken Sie auf **Abbrechen**. Sie müssen den Neustart zu einem späteren Zeitpunkt ausführen.
- Klicken Sie auf **OK**, um sofort einen Neustart auszuführen.

Beim Neustart des Geräts wird die Installation automatisch fortgesetzt.

5 Nach Abschluss der Installation wird das Gerät automatisch neu gestartet, wenn Sie beim Installieren des Windows-Installationsprogramms oder .NET-Framework einen Neustart des Geräts durchgeführt haben.

Wenn das Gerät neu startet, wird es in der Verwaltungszone registriert und das ZENworks-Symbol wird in den Benachrichtigungsbereich (die Taskleiste) platziert.

Im ZENworks-Kontrollzentrum wird das Gerät auf der Geräteseite im Ordner `\Server` oder `\Arbeitsstation` angezeigt.

Unter „Verwenden des ZENworks-Agenten“, auf Seite 48 finden Sie Informationen zur Anmeldung und zur Verwendung des ZENworks-Agenten auf einem Gerät.

Manuelle Installation unter Linux

Statt den ZENworks-Agenten von einem ZENworks-Server an ein Gerät liefern zu lassen, können Sie das Bereitstellungspaket des ZENworks-Agenten manuell vom Server herunterladen und den Agenten installieren.

WICHTIG: Sie können den ZENworks-Agenten unter Linux installieren, wenn Sie Root- oder Administratorberechtigungen besitzen.

1 Stellen Sie sicher, dass das Gerät den Anforderungen entspricht (siehe „Anforderungen an verwaltete Geräte“ in den *ZENworks 2020 System Requirements* (Systemanforderungen)).

2 Öffnen Sie auf dem Zielgerät einen Webbrowser und navigieren Sie zur folgenden Adresse:

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

Ersetzen Sie *server* durch den DNS-Namen oder die IP-Adresse eines ZENworks-Servers und ersetzen Sie *port* nur, wenn der ZENworks-Server nicht den Standardport (80 oder 443) verwendet.

Im Webbrowser wird eine Liste mit Bereitstellungspaketen angezeigt. Für jede Architektur (32-Bit und 64-Bit) gibt es die folgenden Pakettypen:

- **Netzwerk:** Mit diesem Paket wird lediglich der PreAgent auf dem Zielgerät installiert; im Anschluss nimmt der PreAgent das Herunterladen und Installieren von ZENworks Agent vom ZENworks-Server vor.
- **Einzelserver:** Mit dem eigenständigen Paket wird der PreAgent installiert und alle für die Installation des ZENworks-Agenten erforderlichen ausführbaren Dateien (auch das JRE-Installationsprogramm) werden auf dem Zielgerät extrahiert. Anschließend installiert der PreAgent den ZENworks-Agenten vom lokalen Gerät aus. Das Einzelserverpaket ist

hilfreich, wenn Sie ZENworks Agent auf einem Gerät installieren müssen, das zurzeit nicht mit dem Netzwerk verbunden ist. Sie können das Paket auf einem Wechselmedium (z. B. CD oder USB-Flash-Laufwerk) speichern und angeben, dass das Einzelplatzgerät das Paket vom Medium aus ausführen soll. Der ZENworks-Agent wird auf dem Gerät installiert, es erfolgt jedoch keinerlei Registrierung oder Verwaltung, bis das Gerät eine Verbindung mit dem Netzwerk herstellt.

- **Benutzerdefiniert:** Die vordefinierten Bereitstellungspakete haben den Paketnamen „Standardagent“. Für benutzerdefinierte Bereitstellungspakete, die über **Bereitstellung** > **Bereitstellungspaket bearbeiten** erstellt wurden, werden die Namen angezeigt, die ihnen während ihrer Erstellung zugewiesen wurden.

3 Klicken Sie auf den Namen des zu verwendenden Bereitstellungspakets, speichern Sie das Paket auf der lokalen Festplatte des Geräts und erteilen Sie der Datei mit dem Befehl `chmod 755 Dateiname` die Rechte zur Ausführung.

Weitere Informationen zu den Optionen für das Paket, wenn der Aufruf von einer Befehlszeile aus erfolgt, finden Sie unter „Paketoptionen für Windows, Linux und Macintosh“ im Handbuch *ZENworks: Referenz für die Ermittlung, Bereitstellung und Stilllegung*.

4 (Optional) Führen Sie auf RHEL-Geräten den folgenden Befehl aus:

```
chcon -u system_u -t rpm_exec_t dateiname
```

5 Wechseln Sie im Terminalfenster zu dem Verzeichnis, in das Sie das Paket heruntergeladen haben und starten Sie anschließend das Paket auf dem Gerät mit dem Befehl `./Dateiname`, wobei **Dateiname** den Namen des in Schritt 3 heruntergeladenen Pakets bezeichnet.

6 (Bedingt) Wenn nach der Installation des Agenten für das Linux-Gerät das ZENworks-Benachrichtigungssymbol im Benachrichtigungsbereich angezeigt werden soll, melden Sie sich vom Gerät ab und wieder an.

Im ZENworks-Kontrollzentrum wird das Gerät auf der Geräteseite im Ordner `\Server` oder `\Arbeitsstation` angezeigt.

Manuelle Installation auf einem Macintosh-Gerät

Sie können den ZENworks Agent auf einem Macintosh-Gerät bereitstellen, indem Sie das Bereitstellungspaket von der ZENworks-Download-Seite herunterladen.

WICHTIG

- Sie können den ZENworks-Agenten auf einem Macintosh-Gerät installieren, wenn Sie Root- oder Administratorberechtigungen besitzen.

---

1 Öffnen Sie auf dem Macintosh-Zielgerät einen Webbrowser und geben Sie die folgende Adresse ein:

http://<server>/zenworks-setup

Ersetzen Sie *<server>* durch den DNS-Namen oder die IP-Adresse eines ZENworks-Servers.

2 Klicken Sie auf das herunterzuladende Macintosh-Paket.

HINWEIS: Es gibt zwei Pakettypen:

- **Netzwerk:** Bei diesem Paket ist Netzwerkzugriff auf den ZENworks-Server erforderlich, um die benötigten PKG-Dateien herunterzuladen.

- **Einzelserver:** Zugriff auf den ZENworks-Server ist für die Installation des Agenten nicht erforderlich.

3 Geben Sie an der Eingabeaufforderung die ausführbaren Berechtigungen für die heruntergeladene `.bin`-Datei an, indem Sie den Befehl `chmod +x <Dateiname>` ausführen.

Weitere Informationen zu den Optionen, die Sie mit diesem Paket verwenden können, finden Sie im Abschnitt „Paketoptionen für Windows, Linux und Macintosh“ im Handbuch *ZENworks: Referenz für die Ermittlung, Bereitstellung und Stilllegung*.

4 Navigieren Sie nach der Eingabeaufforderung in das Verzeichnis, in das Sie das Paket heruntergeladen haben, und starten Sie anschließend das Paket auf dem Gerät, indem Sie folgenden Befehl ausführen:

```
sudo ./dateiname
```

Der `Dateiname` ist der Name des in Schritt 2 auf Seite 47 heruntergeladenen Pakets.

5 Melden Sie sich am Gerät ab und wieder an, damit nach der Agenteninstallation für das Macintosh-Gerät das Benachrichtigungssymbol von ZENworks im Benachrichtigungsbereich angezeigt wird.

Im ZENworks-Kontrollzentrum wird das Gerät auf der Geräteseite im Ordner `\Server` oder `\Arbeitsstation` angezeigt.

HINWEIS: Nach der Bereitstellung des ZENworks Agent auf dem Macintosh-Gerät wird `/opt/novell/zenworks/bin` nicht zur PATH-Variablen hinzugefügt. Die Befehle in diesem Verzeichnis können daher nicht direkt ausgeführt werden. Führen Sie auf dem Macintosh-Gerät einen der folgenden Schritte aus, damit Sie die Befehle aus `/opt/novell/zenworks/bin` ausführen können:

- Melden Sie sich erneut beim Gerät an.
- Geben Sie zur Ausführung dieser Befehle den vollständigen Befehlspfad an.

  Zum Beispiel: `/opt/novell/zenworks/bin/zac`.

Verwenden des ZENworks-Agenten

In folgenden Abschnitten finden Sie Informationen zum Anmelden sowie zur Verwendung von ZENworks Agent:

Anmelden in der Verwaltungszone

Wenn ein verwaltetes Windows-Gerät sein Betriebssystem bootet, wird der ZENworks-Agent gestartet und alle Bundles und Richtlinien, die dem Gerät zugewiesen sind, stehen zur Verfügung. Damit die einem Benutzer zugewiesenen Bundles und Richtlinien zur Verfügung stehen, muss sich der Benutzer in der Verwaltungszone anmelden.

ZENworks Agent wird in den Client für die Windows- bzw. Novell-Anmeldung integriert, damit sich die Benutzer nur einmal anmelden müssen. Wenn Benutzer ihren eDirectory- bzw. Active Directory-Berechtigungsnachweis auf dem Windows- bzw. Novell-Client eingeben, werden sie in der Verwaltungszone angemeldet, wenn der Berechtigungsnachweis mit dem in einer ZENworks-Benutzerquelle übereinstimmt. Anderenfalls wird der Benutzer in einem separaten ZENworks-Agent-Anmeldebildschirm aufgefordert, den korrekten Berechtigungsnachweis einzugeben.

Angenommen, ein Benutzer verfügt über Konten in zwei eDirectory-Bäumen: Tree1 und Tree2. Tree1 ist in der Verwaltungszone als Benutzerquelle definiert, Tree2 hingegen nicht. Wenn sich der Benutzer bei Tree1 anmeldet, wird er automatisch in der Verwaltungszone angemeldet. Wenn sich der Benutzer jedoch bei Tree2 anmeldet, wird der ZENworks-Agent-Anmeldebildschirm angezeigt und der Benutzer wird zur Eingabe des Berechtigungsnachweises für Tree1 aufgefordert.

Navigieren in den ZENworks-Agent-Ansichten

Der ZENworks-Agent bietet die folgenden Ansichten:

- „ZENworks-Anwendung“, auf Seite 49
- „ZENworks-Explorer“, auf Seite 50
- „ZENworks-Symbol“, auf Seite 50

ZENworks-Anwendung

Die ZENworks-Anwendung ist ein eigenständiges Fenster, in dem Sie auf Bundles zugreifen. Das Fenster wird über das Startmenü aufgerufen (**Menü „Start“** > **Programme** > **Novell ZENworks** > **ZENworks Application**).

Der linke Bereich der ZENworks-Anwendung enthält Folgendes:

- **Ordner [Alle]:** Enthält alle Bundles, die an Sie verteilt wurden, unabhängig von dem Ordner, in dem sie sich befinden.
- **ZENworks-Ordner:** Enthält alle Bundles, die keinem anderen Ordner zugewiesen wurden. Der ZENworks-Ordner ist der Standardordner für Bundles. Administratoren können jedoch zusätzliche Ordner anlegen, in denen Bundles organisiert werden, und sogar den ZENworks-Ordner umbenennen.
- **Der Ordner „Favoriten“:** Enthält alle Bundles, die als Favoriten markiert sind.

Wenn Sie einen Ordner im linken Fensterbereich auswählen, zeigt der rechte Bereich die Bundles, die sich in dem Ordner befinden. Sie haben folgende Möglichkeiten:

- Ein Bundle installieren oder eine bereits installierte Anwendung aufrufen.

- Die Eigenschaften eines Bundles anzeigen. Die Eigenschaften umfassen eine Beschreibung der Anwendung, Informationen über Kontaktpersonen, bei denen Sie Hilfe zur Anwendung anfordern können, die Zeiten, zu denen die Anwendung eingesetzt werden kann, und die Systemvoraussetzungen für das Bundle.
- Eine installierte Anwendung reparieren.
- Eine Anwendung deinstallieren. Dies ist eine vom Administrator gesteuerte Rolle, die eventuell nicht aktiviert ist.

ZENworks-Explorer

ZENworks Explorer ist eine Erweiterung für Windows Explorer, mit deren Hilfe Bundles in Windows Explorer, auf dem Desktop, im Startmenü oder in der Schnellstartleiste sowie im Benachrichtigungsbereich (Taskleiste) angezeigt werden können. Die folgende Grafik zeigt Bundles in Windows Explorer.

Die folgende Grafik zeigt Bundles auf dem Desktop.

Die Aufgaben, die Sie auf die Bundles im ZENworks-Fenster anwenden, können auch im ZENworks Explorer ausgeführt werden.

ZENworks-Symbol

Das ZENworks-Symbol befindet sich im Benachrichtigungsbereich von Windows (Taskleiste). Wenn Sie auf das Symbol klicken, wird das ZENworks-Agent-Fenster geöffnet.

Zum Anzeigen der Agent-Eigenschaften klicken Sie mit der rechten Maustaste auf das ZENworks-Symbol und wählen Sie „Technikeranwendung“. Das Fenster „Eigenschaften des ZENworks-Agenten“ wird geöffnet.

Der linke Navigationsbereich des Eigenschaftenfensters enthält Links zum Status des ZENworks-Agenten und der zugehörigen Funktionen:

- **Status:** Zeigt unter anderem den letzten Zeitpunkt an, zu dem der Agent mit einem ZENworks-Server kommuniziert hat, und gibt an, ob die Agentenfunktionen ausgeführt werden.
- **Richtlinien:** Zeigt die Richtlinien an, die dem Gerät und dem angemeldeten Benutzer zugewiesen wird, und gibt an, ob die Richtlinie in Kraft ist. Nur vorhanden, wenn ZENworks Configuration Management oder ZENworks Endpoint Security Management aktiviert ist.
- **Bundles:** Zeigt die Bundles an, die dem Gerät und angemeldeten Benutzer zugewiesen sind. Außerdem wird hier der aktuelle Installationsstatus der einzelnen Bundles (verfügbar, Downloaden, Installationsvorgang usw.) angezeigt und hier ist ersichtlich, ob das Bundle in Kraft ist (also ob das Gerät die Anforderungen für die Verteilung erfüllt). Nur vorhanden, wenn ZENworks Configuration Management oder ZENworks Patch Management aktiviert ist.
- **Inventar:** Zeigt Inventarinformationen zum Gerät an. Sie können Hardwaredetails anzeigen, z. B. Hersteller und Modell Ihrer Festplatten, Plattenlaufwerke und Videokarte. Sie können auch Softwaredetails anzeigen, z. B. installierte Hotfixes und Patches von Windows sowie Versionsnummern und Speicherorte von installierten Softwareprodukten. Nur vorhanden, wenn ZENworks Configuration Management oder ZENworks Asset Management aktiviert ist.
- **Endpoint Security:** Zeigt Informationen zum Endpoint Security Agent sowie den verwendeten Standort an, um zu bestimmen, welche Sicherheitsrichtlinien Anwendung finden. Nur vorhanden, wenn ZENworks Endpoint Security Management aktiviert ist.

- **Fernverwaltung:** Zeigt Informationen zu den zurzeit verbundenen Fernoperatoren sowie die Fernverwaltungs-Richtlinieneinstellungen an, die für das Gerät gelten. Mit dieser Funktion können Sie zudem eine Verwaltungssitzung initiieren und Sicherheitseinstellungen für die Sitzung steuern. Nur vorhanden, wenn ZENworks Configuration Management aktiviert ist.
- **Satellit:** Zeigt die Informationen zur Satellitenfunktion eines Geräts an, das als Satellitenserver fungiert. Zu den Satellitenrollen gehören Erfassung, Inhalt, Authentifizierung, Imaging und Beitritts-Proxy.

  Diese Funktion wird nur dann angezeigt, wenn der ZENworks-Administrator Ihr Gerät als Satellit verwendet hat.
- **Protokollierung:** Zeigt Informationen zur ZENworks-Agent-Protokolldatei, beispielsweise den Speicherort der Protokolldatei, den ZENworks-Server, auf den die Protokolldatei des Agenten heraufgeladen wird, und den nächsten geplanten Zeitpunkt für das Heraufladen des Protokolls. Hier können Sie außerdem den Schweregrad für protokollierte Meldungen bestimmen.
- **Windows-Proxy:** Zeigt die Ergebnisse der auf dem Gerät ausgeführten Ermittlungs- und Bereitstellungsaktivitäten an, wenn es als Windows-Proxy für den ZENworks-Primärserver fungiert.

Hochstufen eines verwalteten Geräts zu einem Satelliten

Ein Satellit ist ein verwaltetes Gerät, das einige der normalerweise vom ZENworks-Primärserver ausgeführten Rollen übernehmen kann. Hierzu gehören die Authentifizierung, die Informationserfassung, die Inhaltsverteilung und das Imaging. Ein Satellit kann jedes verwaltete Windows-, Linux- oder Macintosh-Gerät mit Ausnahme eines Primärservers sein. Bei der Konfiguration eines Satelliten geben Sie die Rollen an, die das Gerät ausüben soll (Authentifizierung, Erfassung, Inhalt oder Imaging). Darüber hinaus kann ein Satellit auch Rollen übernehmen, die durch Produkte von Drittanbietern in Form von Snapins zu ZENworks Framework hinzugefügt wurden.

HINWEIS: Mit ZENworks ist es nicht mehr möglich, ein 32-Bit-Gerät zu einer Satellitenserverrolle hochzustufen oder einem vorhandenen 32-Bit-Satellitenserver eine neue Rolle hinzuzufügen.

Detaillierte Informationen zu Satelliten und zum Hochstufen eines verwalteten Geräts zu einem Satelliten finden Sie im Abschnitt „Satelliten“ im Handbuch *ZENworks: Referenz für Primärserver und Satelliten*.

5 Systemmeldungen

Mit ZENworks können Sie die Aktivitäten in Ihrer Verwaltungszone anhand von Systemmeldungen überwachen.

Anzeigen von Systemmeldungen

Das ZENworks-System generiert normale (der Information dienende), Warn- und Fehlermeldungen, um Sie bei der Überwachung von Aktivitäten, wie der Verteilung von Software und der Anwendung von Richtlinien, zu unterstützen.

Jeder ZENworks-Server und jeder ZENworks Agent erstellt ein Protokoll der zugehörigen Aktivitäten. Diese Meldungen werden im ZENworks-Kontrollzentrum in verschiedenen Bereichen angezeigt:

- **Systemmeldungsprotokoll:** Das Systemmeldungsprotokoll, das über **Dashboard > Systemmeldungen** aufgerufen wird, zeigt Meldungen von allen ZENworks-Servern und ZENworks-Agenten in der Zone.
- **Gerätemeldungsprotokoll:** Ein Gerätemeldungsprotokoll auf der Seite „Zusammenfassung“ für einen Server oder eine Arbeitsstation zeigt Meldungen, die vom ZENworks-Server oder vom ZENworks-Agenten erzeugt wurden. Das Meldungsprotokoll für Arbeitsstation1 umfasst beispielsweise alle Meldungen, die der ZENworks-Agent auf Arbeitsstation1 erzeugt hat.
- **Inhaltsmeldungsprotokoll:** Ein Inhaltsmeldungsprotokoll auf der Seite „Zusammenfassung“ für ein Bundle oder eine Richtlinie zeigt nur die ZENworks-Server- oder ZENworks-Agent-Meldungen, die sich auf ein Bundle oder eine Richtlinie beziehen. Das Meldungsprotokoll für Bundle1 kann beispielsweise Meldungen enthalten, die von drei verschiedenen ZENworks-Servern und 100 verschiedenen ZENworks-Agenten erzeugt wurden.

Anzeigen einer Zusammenfassung der Meldungen

Sie können eine Zusammenfassung mit der Anzahl der Meldungen abrufen, die für Server, Arbeitsstationen, Bundles und Richtlinien in der Zone erzeugt wurden.

1 Befehlszeilenprogramm **Basis**.

Das Fenster „Meldungszusammenfassung“ zeigt den Status aller Server, Arbeitsstationen, Richtlinien und Bundles in der Verwaltungszone an. Wenn es beispielsweise für zwei Server nicht bestätigte kritische Meldungen gibt (Meldungen, die Sie oder ein anderer Administrator noch nicht bestätigt haben), wird in Spalte  die Zahl 2 angezeigt. Wenn Sie hingegen drei

Bundles mit Warnmeldungen und fünf Bundles mit ausschließlich normalen Meldungen haben, wird in Spalte die Zahl 3 und in Spalte die Zahl 5 angezeigt. Diese Zusammenfassung können Sie wie folgt verwenden:

- Klicken Sie auf einen Objekttyp, um dessen Root-Ordner anzuzeigen. Klicken Sie beispielsweise auf **Server**, um den Server-Root-Ordner (`/Server`) anzuzeigen.
- Klicken Sie für einen beliebigen Objekttyp auf die Zahl in einer der zugehörigen Statusspalten ( ), um eine Liste aller Objekte anzuzeigen, die zurzeit diesen Status aufweisen. Um beispielsweise die Liste der Server mit einem normalen Status zu sehen, klicken Sie auf die Zahl in der Spalte .
- Klicken Sie für einen beliebigen Objekttyp auf die Zahl in der Spalte **Gesamt**. Dadurch werden alle Objekte mit kritischen Meldungen, Warnmeldungen oder normalen Meldungen angezeigt. Klicken Sie beispielsweise auf die Zahl **Gesamt** für **Server**, um eine Liste aller Server anzuzeigen, die Meldungen aufweisen.

Bestätigen von Meldungen

Eine Meldung verbleibt so lange im Meldungsprotokoll, bis Sie sie bestätigen. Sie können die Meldungen im Meldungsprotokoll einzeln oder alle gleichzeitig bestätigen.

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Geräte**.
2. Durchsuchen Sie den Ordner `Servers`, bis Sie einen ZENworks-Server finden.
3. Klicken Sie auf den Server, um seine Details anzuzeigen.
4. Suchen Sie auf dem Karteireiter **Zusammenfassung** den Meldungsprotokollbereich.

   Im Meldungsprotokollbereich werden alle Meldungen (Informations-, Warn- und Fehlermeldungen) aufgelistet, die vom ZENworks-Server generiert werden. In der folgenden Tabelle werden die verschiedenen Methoden zum Bestätigen und Löschen von Meldungen erläutert.

Aufgabe	Vorgehensweise	Zusätzliche Details
Eine Meldung bestätigen	1. Klicken Sie auf die Meldung, um das Dialogfeld „Meldung – Detailinformationen“ anzuzeigen. 2. Klicken Sie auf **Bestätigen**.	Wenn Sie die Meldung nicht bestätigen möchten, klicken Sie auf **Fertig**; das Dialogeld wird geschlossen. Dadurch bleibt die Meldung weiterhin in der Liste **Meldungsprotokoll**.
Alle Meldungen bestätigen	1. Klicken Sie in der Liste **Aufgaben** im linken Navigationsbereich auf **Alle Meldungen bestätigen**.	
Alle bestätigten oder unbestätigten Meldungen anzeigen	1. Klicken Sie auf die Schaltfläche **Erweitert**, um die Seite „Meldungsprotokoll bearbeiten“ anzuzeigen.	Sie können jedoch nicht nur alle bestätigten oder unbestätigten Meldungen anzeigen, sondern auch Meldungen mit einem bestimmten Status oder Datum sowie weitere Details zu Meldungen anzeigen und Meldungen bestätigen. Klicken Sie auf der Seite „Meldungsprotokoll bearbeiten“ auf die Schaltfläche **Hilfe**, um spezielle Informationen zur Ausführung einer Aufgabe auf dieser Seite zu erhalten.
Eine Meldung löschen	1. Klicken Sie auf die Meldung, um das Dialogfeld „Meldung - Detailinformationen“ anzuzeigen. 2. Klicken Sie auf **Löschen**.	Wenn Sie eine Meldung vollständig löschen, wird die Meldung aus Ihrem ZENworks-System entfernt.

Zum Bestätigen von Meldungen in Bezug auf Geräte, Bundles und Richtlinien können Sie auch das Kommando `messages-acknowledge` im zman-Dienstprogramm verwenden. Weitere Informationen finden Sie unter „Meldungskommandos“ im Handbuch *ZENworks: Referenz für Befehlszeilen-Dienstprogramme*.

Weitere Informationen

Weitere Informationen zu Systemmeldungen finden Sie unter „Verwenden der Meldungsprotokollierung“ im Handbuch *Referenz für das ZENworks -Kontrollzentrum*.

Erstellen einer Überwachungsliste

Wenn Sie über Geräte, Bundles oder Richtlinien verfügen, deren Status Sie genau überwachen möchten, können Sie sie der Überwachungsliste hinzufügen. In der Überwachungsliste werden folgende Informationen bereitgestellt:

- **Agent:** Zeigt für Server und Arbeitsstationen an, ob der ZENworks Agent des Geräts zurzeit verbunden ( ) oder nicht verbunden ( ) ist.

- : Zeigt an, ob für das Objekt kritische Meldungen vorhanden sind.
- **Typ:** Zeigt ein Symbol an, das den Objekttyp darstellt. Ein Bundle könnte beispielsweise mit dem Symbol zeigen, dass es sich um ein Windows-Bundle handelt. Oder ein Gerät könnte mit dem Symbol darauf hinweisen, dass es ein Server ist. Sie können mit der Maus auf das Symbol zeigen, um eine Beschreibung einzublenden.
- **Name:** Zeigt den Namen des Objekts an. Sie können auf den Namen klicken, um das Meldungsprotokoll des Objekts anzuzeigen.

So fügen Sie der Überwachungsliste ein Gerät, Bundle oder eine Richtlinie hinzu:

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Home**.
2. Klicken Sie in der Kontrollleiste „Überwachungsliste“ auf **Hinzufügen**und wählen Sie den Objekttyp aus (Gerät, Bundle oder Richtlinie), der in die Liste aufgenommen werden soll.
3. Wählen Sie im Auswahldialogfeld das gewünschte Objekt aus und klicken Sie anschließend auf **OK**, um es der Überwachungsliste hinzuzufügen.

   Wenn Sie beispielsweise Server hinzufügen, suchen Sie nach einem Server und wählen Sie ihn aus.

Objekte bleiben in der Überwachungsliste, bis Sie sie entfernen.

6 Audit-Verwaltung

Mit ZENworks können Sie die Aktivitäten im ZENworks-System über die Funktion „Audit-Verwaltung“ aufzeichnen und anzeigen. Die Funktion „Audit-Verwaltung“ erfasst verschiedene Ereignisse, die in der Zone eintreten. Die Details zu einem erfassten Ereignis lassen sich zu Sicherheits- und Konformitätszwecken heranziehen, sodass Sie bei wichtigen Ereignissen im System feststellen können, welcher Benutzer was wann auf welchem System getan hat. Mithilfe dieser Funktion können Sie die Aktivitäten der Primärserver, Satellitenserver und verwalteten Geräte zentral überwachen.

Arten von Audit-Ereignissen

Es gibt zwei Arten von ZENworks-Audit-Ereignissen:

- **Änderungsereignisse:** Bei diesen Ereignissen werden Konfigurationsänderungen an der Zone erfasst, die durch das ZENworks-Kontrollzentrum oder über die Befehlszeilenprogramme zman vorgenommen wurden. Sie können verschiedene Änderungen erfassen, von Bundle-Änderungen bis hin zu Änderungen am ZENworks-System. Konfigurieren Sie beispielsweise ein Audit-Ereignis, in dem die Aktivität eines Administrators festgehalten ist, der ein Bundle einem Gerät zugewiesen hat.
- **Agentenereignisse:** In diesen Ereignissen werden alle Aktionen erfasst, die auf den verwalteten ZENworks-Geräten ausgeführt werden. Diese Ereignisse werden auch als Geräte-Ereignisse bezeichnet.

Sowohl Änderungsereignisse als auch Agentenereignisse können wahlweise für alle Geräte in der Zone oder auch nur für einzelne Geräte aktiviert werden.

Aktivieren von Ereignissen

Zum Auditieren eines Ereignisses müssen Sie das Ereignis zunächst im ZENworks-Kontrollzentrum aktivieren. Sie können das Ereignis auf Zonen- oder Geräteebene aktivieren. Ein Ereignis, das auf Zonenebene aktiviert ist, gilt für alle Geräte in der Zone, ein Ereignis, das auf Geräteebene aktiviert ist, dagegen nur für das ausgewählte Gerät.

1. Melden Sie sich beim ZENworks-Kontrollzentrum an.
2. (Zone) Zum Aktivieren von Ereignissen in der Zone klicken Sie auf **Konfiguration > Verwaltungszone > Audit-Verwaltung**.

   Alternativ:

(Geräte) Zum Aktivieren von Ereignissen auf einem Gerät klicken Sie auf **Geräte > Verwaltete Geräte**. Suchen Sie das Gerät im Ordner „Server“ oder „Arbeitsstationen“, und klicken Sie auf das Geräteobjekt. Die Eigenschaften des Geräts werden angezeigt. Klicken Sie dann auf **Einstellungen > Audit-Verwaltung**.

3 Klicken Sie zum Anzeigen der Seite „Ereigniskonfiguration“ auf **Ereigniskonfiguration**.

4 Klicken Sie auf der Registerkarte **Änderungsereignisse** oder **Agentenereignisse** auf **Hinzufügen**. Das Dialogfeld „Änderungsereignisse hinzufügen“ oder „Agentenereignisse hinzufügen“ wird geöffnet.

   Weitere Informationen zu den Kategorien der Änderungs- und Agentenereignisse finden Sie im Handbuch *ZENworks: Referenz für die Audit-Verwaltung*.

5 Erweitern Sie die Baumstruktur **Änderungsereignisse** oder **Agentenereignisse** und wählen Sie das gewünschte Ereignis aus.

6 Geben Sie Folgendes für die **Ereigniseinstellungen** ein:

   - **Ereignisklassifizierung:** Wählen Sie je nach Schweregrad des Ereignisses die Option **Kritisch**, **Wichtig** oder **Information**.
   - **Speicherdauer:** Geben Sie den Zeitraum (in Tagen) an, über den das Ereignis aufbewahrt werden soll, bevor es bereinigt wird.
   - **Benachrichtigungstypen:** Geben Sie an, ob die Benachrichtigung beim Eintreten eines Ereignisses per Email, SNMP-Trap oder UDP oder an eine lokale Datei gesendet werden soll. Wenn Sie die Option **Nachricht in einer lokalen Datei protokollieren** wählen, müssen Sie die Einstellungen für die lokale Datei konfigurieren.

     Sie können auch alle Benachrichtigungstypen auswählen. Weitere Informationen finden Sie unter „Verwenden der Meldungsprotokollierung“.
   - (Agentenereignisse) Geben Sie die **Abtastfrequenz** an, mit der Daten gesammelt werden sollen, um Audit-Ereignisse zu generieren. Dieses Feld wird nur dann angezeigt, wenn ein ZENworks Endpoint Security Management-Ereignis oder ein ZENworks Agent-Ereignis ausgewählt ist.

7 Klicken Sie auf **OK**, um das Ereignis hinzuzufügen.

Zum Bearbeiten oder Löschen eines Ereignisses wählen Sie das gewünschte Ereignis auf der Seite „Ereigniskonfiguration“ aus und klicken Sie in der Menüleiste auf **Bearbeiten** oder **Löschen**. Sollen mehrere Ereignisse gleichzeitig ausgewählt werden, halten Sie die **Strg-Taste** gedrückt und klicken Sie nacheinander auf die Ereignisse.

Anzeigen eines erzeugten Ereignisses

Wenn ein aktiviertes Ereignis eintritt, wird ein Audit-Ereignis erzeugt.

An den folgenden Stellen können Sie auf die Details zu einem erzeugten Audit-Ereignis zugreifen:

- **Dashboard:** Sie können die Audit-Daten im ZENworks-Kontrollzentrum-Dashboard anzeigen. Das Dashboard enthält die folgenden Registerkarten:
  - **Dashboard:** Auf dieser Registerkarte wird eine Übersicht der Audit-Ereignisse angezeigt, die in der Zone eingetreten sind. Wichtige Ereignisse und betroffene Objekte sind gekennzeichnet, und Sie können die Ereignisprotokollanzeige filtern. Standardmäßig enthält dieses Dashboard einen Überblick über die Ereignisse in den letzten vier Stunden. Sollen weitere Daten angezeigt werden, können Sie den Zeitraum entsprechend ändern.

- **Ereignisse (Audit-Protokoll):** Auf dieser Registerkarte wird eine Übersicht aller Ereignisse angezeigt, die in der Zone eingetreten sind. Die Informationen werden in einem ähnlichen Format wie auf der Seite „Ereigniskonfiguration“ dargestellt. Für Kategorien, in denen Ereignisse erzeugt wurde, wird die Anzahl dieser Ereignisse eingeblendet. Wenn beispielsweise ein Ereignis **Bundle-Zuweisungsverwaltung** erzeugt wurde, ist neben der Kategorie „Bundle-Zuweisungsverwaltung“ in der Baumstruktur die Zahl **1** sichtbar. Wenn Sie auf ein Ereignis klicken, werden die zugehörigen Details im rechten Bereich aufgelistet.

- **(Änderungsereignisse) Objektordner:** Die Registerkarte **Audit** in den Objektordnern (**Geräte**, **Bundles**, **Richtlinien** und **Benutzer**) zeigt die Audit-Ereignisse, die für alle Objekte im ausgewählten Ordner erzeugt wurden. Sie können beispielsweise alle Ereignisse betrachten, die für alle Bundles in einem Bundle-Ordner erzeugt wurden. Alle Ereignisse, die mit Bundles zusammenhängen, sind daher im Bundle-Ordner zu finden. Die Informationen werden ähnlich wie auf der Seite „Ereigniskonfiguration“ in Kategorien gegliedert. Sie können die aufgetretenen Ereignisse durchsuchen und bei Bedarf auf ein Ereignis klicken und so weitere Details zu diesem Ereignis anzeigen.
- **(Änderungsereignisse) Objekte:** Sie können auch die Audit-Ereignisse für ein Objekt im Objektordner anzeigen. Wenn Sie beispielsweise ein bestimmtes Bundle in einem Bundle-Ordner auswählen, werden die Ereignisse aufgeführt, die für dieses Bundle erzeugt wurden.
- **(Agentenereignisse) Geräteordner:** Die Registerkarte **Audit** im Ordner **Geräte** zeigt die Ereignisse, die für ein bestimmtes Gerät (Server oder Arbeitsstation) erzeugt wurden.

So zeigen Sie die Details zu erzeugten Ereignissen an:

1. Melden Sie sich beim ZENworks-Kontrollzentrum an.
2. (Dashboard) Zum Anzeigen der Ereignisse im Dashboard klicken Sie auf **Dashboard** > **Ereignisse**.

   Alternativ:

   (Objektordner) Zum Anzeigen der Ereignisse für alle Objekte in einem Ordner (z. B. in einem Geräte-, Bundle- oder Richtlinienordner) klicken Sie auf den Link **Details** für den Ordner, und wechseln Sie zur Registerkarte **Audit**.

   Alternativ:

   (Objekt) Zum Anzeigen der Ereignisse für ein bestimmtes Objekt (z. B. ein Gerät, ein Bundle oder eine Richtlinie) klicken Sie auf das Objekt, und wechseln Sie zur Registerkarte **Audit**.

   (Geräteordner) Zum Anzeigen der Ereignisse im Geräteordner klicken Sie im linken Bereich auf **Geräte**. Ist das Ereignis auf einem Server in der Zone aufgetreten, klicken Sie auf den Link **Details** für den Server. Falls das Ereignis auf einem verwalteten Gerät eingetreten ist, klicken Sie entsprechend auf den Link **Details** für die Arbeitsstation. Klicken Sie dann auf die Registerkarte **Audit**. Das Fenster mit den Ereignissen wird geöffnet.
3. Klicken Sie auf die Registerkarte **Änderungsereignisse** oder **Agentenereignisse**.
4. Erweitern Sie die Baumstruktur, und navigieren Sie zur gewünschten Kategorie.

   Abhängig davon, ob die Anzahl der Audit-Ereignisse konfiguriert ist, wird die entsprechende Anzahl für die Kategorie angezeigt.
5. Klicken Sie auf das Ereignis.

   Die Details zum erzeugten Ereignis werden im rechten Bereich angezeigt.

HINWEIS: Wenn Sie die Details des Ereignisses in einem neuen Fenster ansehen möchten, klicken Sie auf  .

II Produktverwaltung

Die folgenden Abschnitte enthalten hilfreiche Informationen zur Verwaltung der ZENworks-Produkte. Bevor Sie sich mit diesen Abschnitten beschäftigen, sollten Sie die Konfigurationsaufgaben in Teil I, „Systemkonfiguration“, auf Seite 9 bereits abgeschlossen haben.

7 Kurzübersicht

Nach dem Konfigurieren der Verwaltungszone (siehe Teil I, „Systemkonfiguration“, auf Seite 9) sollten Sie sich mit den Konzepten und Aufgaben in den folgenden Abschnitten für alle ZENworks-Produkte vertraut machen, für die Sie eine Lizenz oder Evaluierungslizenz erworben haben:

Inventarverwaltung

Mit ZENworks Asset Management können Sie die Softwarelizenz-Compliance überwachen, die Softwarenutzung erfassen und Softwareeigentum verfolgen, indem Sie Geräten, Standorten, Abteilungen und Kostenstellen Lizenzen zuweisen.

Aufgabe	Details
Aktivieren der Inventarverwaltung	Wenn die Inventarverwaltung bei der Installation der Verwaltungszone nicht durch Eingabe eines Lizenzschlüssels oder Bereitstellen der Evaluierungslizenz aktiviert wurde, müssen Sie dies nachholen, bevor Sie das Produkt verwenden können. Eine Anleitung dazu finden Sie in „Aktivieren von Asset Management“, auf Seite 71.
Aktivieren des ZENworks Agent zur Durchführung von Inventarverwaltungsvorgängen	Die Inventarverwaltungsfunktion des Agent wird standardmäßig aktiviert, sobald ZENworks Asset Management aktiviert wird (mit Voll- oder Evaluierungslizenz). Überprüfen Sie, ob die Inventarverwaltungsfunktion des Agent nach wie vor aktiviert ist. Wenn Sie Softwarelizenzen nach Benutzer (statt nur nach Geräten) verfolgen möchten, müssen Sie außerdem die Benutzerverwaltungsfunktion aktivieren, die standardmäßig deaktiviert ist. Eine Anleitung dazu finden Sie in „Aktivieren von Asset Management im ZENworks Agent“, auf Seite 71.

Aufgabe	Details
Absuchen von Geräten zum Erfassen von Software- und Hardwareinventar	Sie können Geräte absuchen, um das Software- und Hardwareinventar für die Geräte zu erfassen. Mithilfe der Inventarinformationen können Sie Entscheidungen zur Softwareverteilung und Hardwareaktualisierung treffen. Diese Aufgabe muss ausgeführt werden, bevor Sie die übrigen Aufgaben angehen können. Eine Anleitung dazu finden Sie in „Erfassung des Software- und Hardware-Inventars“, auf Seite 72.
Softwarenutzung überwachen	Generieren Sie Berichte, um zu analysieren, in welchem Umfang und wie oft Softwareprodukte verwendet werden. Eine Anleitung dazu finden Sie in „Überwachen der Softwarenutzung“, auf Seite 74.
Softwarelizenzkonformität überwachen	Überprüfen Sie, ob die installierten Softwareprodukte ordnungsgemäß lizenziert sind oder ob die Lizenzen nicht ausreichen oder zu viele Lizenzen vorhanden sind. Eine Anleitung dazu finden Sie in „Überwachen der Lizenz-Compliance“, auf Seite 74.
Lizenzen zuordnen	Sie können Lizenzen in Ihrem Unternehmen zuordnen, um die Eigentümerschaft und Verteilung der Lizenzen zu überwachen. Lizenzen können zu Geräten oder Demografien (Standorten, Abteilungen oder Kostenstellen) zugeordnet werden. Eine Anleitung dazu finden Sie in „Zuordnen von Lizenzen“, auf Seite 81.

Konfigurationsmanagement

Mit ZENworks Configuration Management können Sie die Konfiguration eines Geräts verwalten, einschließlich Softwareverteilung auf das Gerät, Anwenden von Windows-Konfigurationsrichtlinien sowie Imaging und Anwenden von Images. Darüber hinaus können Sie Gerätehardware- und Softwareinventar erfassen, um informierte Upgrade- und Kaufentscheidungen treffen zu können, und remote auf Geräte zugreifen, um Probleme zu analysieren und zu beheben.

Die folgenden Aufgaben können ggf. in beliebiger Reihenfolge durchgeführt werden.

Aufgabe	Details
Aktivieren des Konfigurationsmanagements	Wenn das Konfigurationsmanagement bei der Installation der Verwaltungszone nicht durch Eingabe eines Lizenzschlüssels oder Bereitstellen der Evaluierungslizenz aktiviert wurde, müssen Sie dies nachholen, bevor Sie das Produkt verwenden können. Eine Anleitung dazu finden Sie in „Aktivieren von Configuration Management“, auf Seite 85.

Aufgabe	Details
Aktivieren des ZENworks Agent zur Durchführung von Konfigurationsmanagementvorgängen	Damit der ZENworks Agent Konfigurationsmanagementvorgänge auf einem Gerät durchführen kann, müssen die entsprechenden Agent-Funktionen aktiviert werden. Diese Funktionen (Bundle-Verwaltung, Image-Verwaltung, Richtlinienverwaltung, Fernverwaltung und Benutzerverwaltung) werden standardmäßig aktiviert, wenn ZENworks Configuration Management aktiviert wird (durch Voll- oder Evaluierungslizenz). Sie sollten überprüfen, ob die Funktionen aktiviert sind. Funktionen, die Sie nicht verwenden möchten, können Sie auch deaktivieren. Eine Anleitung dazu finden Sie in „Aktivieren des Konfigurationsmanagements im ZENworks Agent“, auf Seite 86.
Registrieren von Mobilgeräten	Die Configuration Management-Aktionen (z. B. Bundles bereitstellen oder Sicherheitsrichtlinien anwenden sowie verschiedene Aktionen zur Geräteverwaltung) sind nur dann auf Mobilgeräten verfügbar, wenn Sie die Mobilgeräte in der ZENworks-Verwaltungszone registrieren. Weitere Informationen finden Sie im Handbuch ZENworks Mobile Management Reference (Referenz zu Mobile Management).
Verteilen von Software	Verteilen Sie Software mithilfe von Bundles. Bundles enthalten die Softwaredateien und Anweisungen, die zum Installieren, Starten und Deinstallieren (falls notwendig) der Software erforderlich sind. Sie können Bundles erstellen, um Windows Installer-Anwendungen (MSI und MSP), Windows-fremde Installer-Anwendungen, Weblinks, Thin-Client-Anwendungen, Linux-Anwendungen und Macintosh-Anwendungen zu verteilen. Eine Anleitung dazu finden Sie in „Verteilen von Software“, auf Seite 86.
Anwenden von Richtlinien	Steuern Sie das Verhalten von Geräten durch das Anwenden von Richtlinien. Mit ZENworks können Sie Windows-Gruppenrichtlinien, Richtlinien für zentral gespeicherte Profile, Browserlesezeichenrichtlinien, Druckerrichtlinien usw. erstellen und anwenden. Eine Anleitung dazu finden Sie in „Anwenden von Richtlinien“, auf Seite 88.
Erstellen von Images und Anwenden der Images auf Geräte	Erstellen Sie Images von Geräten, wenden Sie Images auf Geräte an, und führen Sie Imaging-Skripts auf Geräten aus. ZENworks Configuration Management verwendet seine Preboot Services-Funktionalität, um diese Imaging-Aufgaben beim Start auf Geräten auszuführen. Eine Anleitung dazu finden Sie in „Imaging von Geräten“, auf Seite 91.

Aufgabe	Details
Absuchen von Geräten zum Erfassen von Software- und Hardwareinventar	Sie können Geräte absuchen, um das Software- und Hardwareinventar für die Geräte zu erfassen. Mithilfe der Inventarinformationen können Sie Entscheidungen zur Softwareverteilung und Hardwareaktualisierung treffen. Eine Anleitung dazu finden Sie in „Erfassung des Software- und Hardware-Inventars“, auf Seite 111.

Endpoint Security Management

Mit ZENworks Endpoint Security Management können Sie Geräte schützen, indem Sicherheitseinstellungen über Richtlinien erzwungen werden. Sie können den Zugriff eines Geräts auf Wechselmedien, WLANs und Anwendungen kontrollieren. Darüber hinaus können Sie Daten durch Verschlüsselung und Netzwerkkommunikation über Firewall-Erzwingung (Ports, Protokolle und Zugriffssteuerungslisten) sichern. Außerdem können Sie die Sicherheit eines Endpunktgeräts standortabhängig ändern.

Die folgenden Aufgaben müssen in der angegebenen Reihenfolge ausgeführt werden.

Aufgabe	Details
Aktivieren von Endpoint Security Management	Wenn Endpoint Security Management bei der Installation der Verwaltungszone nicht durch Eingabe eines Lizenzschlüssels oder Bereitstellen der Evaluierungslizenz aktiviert wurde, müssen Sie dies nachholen, bevor Sie das Produkt verwenden können. Eine Anleitung dazu finden Sie in „Aktivieren von Endpoint Security Management“, auf Seite 123.
Aktivieren von Endpoint Security Agent	Der Endpoint Security Agent erzwingt die Sicherheitsrichtlinien auf den Geräten. Er muss auf jedem Gerät, auf das Sie Sicherheitsrichtlinien verteilen möchten, installiert und aktiviert werden. Eine Anleitung dazu finden Sie in „Aktivieren des Endpoint Security Agent“, auf Seite 124.
Erstellen von Standorten	Sicherheitsrichtlinien können global sein oder sich auf bestimmte Standorte beziehen. Eine globale Richtlinie wird auf alle Standorte angewendet. Eine standortbasierte Richtlinie wird nur angewendet, wenn der Endpoint Security Agent feststellt, dass die Netzwerkumgebung des Geräts mit der für den Standort definierten Umgebung übereinstimmt. Wenn Sie standortbasierte Richtlinien verwenden möchten, müssen Sie Standorte erstellen. Eine Anleitung dazu finden Sie in „Erstellen von Standorten“, auf Seite 124.

Aufgabe	Details
Erstellen von Sicherheitsrichtlinien	Die Sicherheitseinstellungen eines Geräts werden über Sicherheitsrichtlinien konfiguriert. Es gibt elf Sicherheitsrichtlinien, die Sie erstellen können. Eine Anleitung dazu finden Sie in „Eine Sicherheitsrichtlinie erstellen“, auf Seite 125.
Zuweisen von Richtlinien zu Benutzern und Geräten	Sicherheitsrichtlinien können Benutzern oder Geräten zugewiesen werden. Eine Anleitung dazu finden Sie in „Zuweisen einer Richtlinie zu Benutzern und Geräten“, auf Seite 127.
Zuweisen von Richtlinien zu Zonen	Um sicherzustellen, dass ein Gerät stets geschützt ist, können Sie Standardsicherheitsrichtlinien für jeden Richtlinientyp festlegen, indem Sie der Zone Richtlinien zuweisen. Eine zonenbezogene Richtlinie wird angewendet, wenn ein Gerät nicht von einer benutzer- oder gerätebezogenen Richtlinie abgedeckt ist. Eine Anleitung dazu finden Sie in „Zuweisen einer Richtlinie zur Zone“, auf Seite 128.

Vollständige Festplattenverschlüsselung

ZENworks Full Disk Encryption (vollständige Festplattenverschlüsselung) schützt die Daten eines Geräts vor nicht autorisiertem Zugriff, wenn das Gerät ausgeschaltet wurde bzw. sich im Ruhezustand befindet. Zum Schutz der Daten wird die gesamte Festplatte verschlüsselt, einschließlich temporärer Dateien, Auslagerungsdateien und Betriebssystem. Der Zugriff auf die Daten ist nur möglich, wenn sich ein autorisierter Benutzer anmeldet, nicht jedoch durch Booten des Geräts über Medien wie CD/DVD, Diskette oder USB-Laufwerk. Für einen autorisierten Benutzer unterscheidet sich der Zugriff auf Daten auf der verschlüsselten Festplatte nicht vom Zugriff auf Daten auf einer unverschlüsselten Festplatte.

Die folgenden Aufgaben müssen in der angegebenen Reihenfolge ausgeführt werden.

Aufgabe	Details
Aktivieren der vollständigen Festplattenverschlüsselung (Full Disk Encryption)	Wenn die vollständige Festplattenverschlüsselung bei der Installation der Verwaltungszone nicht durch Eingabe eines Lizenzschlüssels oder Bereitstellen der Evaluierungslizenz aktiviert wurde, müssen Sie dies nachholen, bevor Sie das Produkt verwenden können. Eine Anleitung dazu finden Sie in „Aktivieren der vollständigen Festplattenverschlüsselung (Full Disk Encryption)“, auf Seite 132.
Aktivieren des Agenten zur vollständigen Festplattenverschlüsselung	Der Agent zur vollständigen Festplattenverschlüsselung führt die Festplattenverschlüsselung durch. Er muss auf allen Geräten installiert und aktiviert werden, deren Festplatten Sie verschlüsseln möchten. Eine Anleitung dazu finden Sie in „Aktivieren des Full Disk Encryption Agent“, auf Seite 132.

Aufgabe	Details
Erstellen einer Festplattenverschlüsselungsrichtlinie	Die Informationen, die zum Verschlüsseln der Festplatten von Geräten erforderlich sind, werden mittels einer Festplattenverschlüsselungsrichtlinie an den Agenten zur vollständigen Festplattenverschlüsselung übergeben. Es muss mindestens eine Richtlinie erstellt werden. Eine Anleitung dazu finden Sie in „Erstellen einer Festplattenverschlüsselungsrichtlinie“, auf Seite 133.
Zuweisen der Richtlinie zu Geräten	Festplattenverschlüsselungsrichtlinien können nur Geräten, Gerätegruppen oder Geräteordnern zugewiesen werden. Eine Anleitung dazu finden Sie in „Zuweisen der Richtlinie zu Geräten“, auf Seite 133.

Patchverwaltung

Mit ZENworks Patch Management können Sie den Prozess zur Bewertung von Softwareschwachstellen und Anwendung von Patches zur Behebung dieser Schwächen automatisieren.

Die folgenden Aufgaben müssen in der angegebenen Reihenfolge ausgeführt werden.

Aufgabe	Details
Aktivieren der Patchverwaltung	Wenn die Patchverwaltung bei der Installation der ZENworks-Verwaltungszone nicht durch Eingabe einer Abonnementlizenz oder Bereitstellen der Evaluierungslizenz aktiviert wurde, müssen Sie das Produkt aktivieren. Eine Anleitung dazu finden Sie in „Aktivieren der Patchverwaltung“, auf Seite 140.
Aktivieren des ZENworks Agent zur Durchführung von Patchverwaltungsvorgängen	Damit der ZENworks Agent Patchverwaltungsvorgänge auf einem Gerät durchführen kann, muss die Patchverwaltungsfunktion des Agent aktiviert werden. Die Patchverwaltungsfunktion wird standardmäßig aktiviert, sobald ZENworks Patch Management aktiviert wird (mit Voll- oder Evaluierungslizenz). Überprüfen Sie, ob die Patchverwaltungsfunktion des Agent nach wie vor aktiviert ist. Eine Anleitung dazu finden Sie in „Aktivieren der Patchverwaltung im ZENworks Agent“, auf Seite 141.
Starten des Abonnementdiensts	Der Abonnementdienst muss auf einem ZENworks-Server gestartet werden. Dieser Server lädt die Patches herunter und reproduziert sie auf andere ZENworks-Server (sofern mehr als einer vorhanden ist). Eine Anleitung dazu finden Sie in „Starten des Patch-Abonnementdiensts“, auf Seite 141.

Aufgabe	Details
Erstellen von Patch-Richtlinien	Nachdem Patches vom Abonnementdienst heruntergeladen wurden, wenden Sie die gewünschten Patches an. Eine Anleitung dazu finden Sie in „Erstellen von Patch-Richtlinien“, auf Seite 142.

8 Asset Management

Die folgenden Abschnitte enthalten Erläuterungen und Anleitungen zur Verwendung von ZENworks Asset Management, um Software- und Hardwareinventar von Geräten zu erfassen sowie die Softwarenutzung auf Geräten und die Softwarelizenz-Compliance zu überwachen.

Aktivieren von Asset Management

Wenn Sie die Inventarverwaltung nicht bereits bei der Installation der Verwaltungszone aktiviert haben, indem Sie entweder einen Lizenzschlüssel angegeben oder die Evaluierung eingeschaltet haben, führen Sie folgende Schritte aus:

1. Klicken Sie im ZENworks-Kontrollzentrum auf **Konfiguration**.
2. Klicken Sie in der Kontrollleiste „Lizenzen“ auf **ZENworks 2020 Asset Management**.
3. Wählen Sie „Produkt evaluieren/aktivieren“ aus und füllen Sie anschließend die folgenden Felder aus:

   Evaluierung verwenden: Wählen Sie diese Option aus, um den 60-Tage-Evaluierungszeitraum zu aktivieren. Nach dem 60-Tage-Zeitraum müssen Sie einen Produktlizenzschlüssel anwenden, um das Produkt weiterhin verwenden zu können.

   Produktlizenzschlüssel: Geben Sie den Lizenzschlüssel an, den Sie für Asset Management erworben haben. Eine Produktlizenz können Sie auf der ZENworks Asset Management-Produkt-Website (http://www.novell.com/products/zenworks/assetmanagement) erwerben.
4. Klicken Sie auf **OK**.

Aktivieren von Asset Management im ZENworks Agent

Damit der ZENworks Agent Inventarverwaltungsvorgänge auf einem Gerät durchführen kann, muss die Inventarverwaltungsfunktion des Agent aktiviert werden. Die Inventarverwaltungsfunktion wird standardmäßig aktiviert, sobald ZENworks Asset Management aktiviert wird (mit Voll- oder Evaluierungslizenz).

Überprüfen Sie, ob die Inventarverwaltungsfunktion des Agent aktiviert ist. Wenn Sie Softwarelizenzen nach Benutzer (statt nur nach Geräten) verfolgen möchten, müssen Sie außerdem die Benutzerverwaltungsfunktion aktivieren, die standardmäßig deaktiviert ist. Eine Anleitung dazu finden Sie in „Konfigurieren der ZENworks-Agent-Funktionen“, auf Seite 41.

HINWEIS: Sobald Sie das ZENworks Asset Management-Modul aktiviert haben, führen Sie mit dem Befehl `zac inv -f scannow` eine Komplettabsuche auf allen Geräten aus. Bis zu dieser Absuche enthält der Asset Management-Bericht nicht die richtigen Angaben.

Erfassung des Software- und Hardware-Inventars

Bei der Inventarisierung eines Geräts erfasst ZENworks Asset Management die Software- und auch die Hardwareinformationen auf dem Gerät. Mithilfe des ZENworks-Kontrollzentrums können Sie das Inventar für ein einzelnes Gerät anzeigen oder Berichte für mehrere Geräte auf der Basis spezifischer Kriterien generieren.

Sie können das Softwareinventar für verschiedene Zwecke verwenden; so können Sie die Nutzung bestimmter Anwendungen beobachten und sich vergewissern, dass Sie über ausreichend Lizenzen für alle Kopien der verwendeten Anwendung verfügen. Nehmen Sie beispielsweise an, dass Ihr Unternehmen Eigentümer von 50 Lizenzen einer Textverarbeitungssoftware ist. Sie erstellen ein Softwareinventar und stellen dabei fest, dass diese Software auf 60 Geräten installiert ist, was bedeutet, dass die Compliance mit der Softwarevereinbarung nicht mehr gegeben ist. Wenn Sie sich dann jedoch die Berichte zur Nutzung der Software in den letzten 6 Monaten ansehen, stellen Sie fest, dass die Software nur auf 45 Geräten verwendet wird. Um die Compliance mit der Lizenzvereinbarung herzustellen, deinstallieren Sie die Software von den 15 Geräten, die sie nicht verwenden.

Sie können das Hardwareinventar ebenso für verschiedene Zwecke verwenden; so können Sie sich vergewissern, dass Ihre Hardware die Anforderungen zur Ausführung bestimmter Softwareprogramme erfüllt. Nehmen Sie beispielsweise an, dass Ihre Buchhaltung eine neue Version der Buchhaltungssoftware einführen möchte. Die neue Software hat erhöhte Anforderungen bezüglich Prozessor, Arbeitsspeicher und Festplattenspeicher. Anhand des auf Ihren Geräten erfassten Hardwareinventars können Sie zwei Berichte erstellen. In einem der Berichte werden alle Geräte aufgelistet, die den Anforderungen entsprechen, im anderen die Geräte, die den Anforderungen nicht entsprechen. Basierend auf den Berichten können Sie die Software auf die kompatiblen Geräte verteilen und einen Aktualisierungsplan für die nicht kompatiblen Geräte erstellen.

Standardmäßig werden Geräte um 1:00 Uhr morgens am ersten Tag jedes Monats automatisch überprüft. Sie können den Zeitplan und viele andere **Inventar**-Konfigurationseinstellungen auf der Registerkarte **Konfiguration** im ZENworks-Kontrollzentrum ändern.

In den folgenden Abschnitten finden Sie Anweisungen zur Initiierung einer Geräteabsuche und zur Verwendung des erfassten Inventars:

- „Starten eines Gerätescans“, auf Seite 72
- „Anzeigen von Geräteinventaren“, auf Seite 73
- „Generieren von Inventarberichten“, auf Seite 73
- „Weitere Informationen“, auf Seite 73

Starten eines Gerätescans

Sie können jederzeit einen Gerätescan starten.

1 Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Geräte**.

2 Durchsuchen Sie die Ordner `Server` oder `Arbeitsstationen`, bis Sie die zu scannenden Geräte finden.

3 Klicken Sie auf das Gerät, um seine Details anzuzeigen.

4 Klicken Sie in der Aufgabenliste im linken Navigationsbereich auf **Inventarabsuche nach Servern** oder **Inventarabsuche nach Arbeitsstationen**, um den Scan zu starten.

   Im Dialogfeld Schnellaufgabenstatus wird der Status der Aufgabe angezeigt. Wenn die Aufgabe erledigt ist, können Sie auf die Registerkarte **Inventar** klicken, um die Ergebnisse der Absuche zu sehen.

Zum gleichzeitigen Absuchen mehrerer Geräte können Sie den Ordner öffnen, in dem sich die Geräte befinden, die Kontrollkästchen neben den Geräten aktivieren und anschließend auf **Schnellaufgaben** > **Inventarabsuche** klicken.

Sie können zum Absuchen eines Geräts auch den Befehl `inventory-scan-now` im zman-Dienstprogramm verwenden. Weitere Informationen finden Sie unter „Inventarkommandos“ im Handbuch *ZENworks: Referenz für Befehlszeilen-Dienstprogramme*.

Anzeigen von Geräteinventaren

1 Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Geräte**.

2 Durchsuchen Sie die Ordner `Server` oder `Arbeitsstationen`, bis Sie das Gerät finden, dessen Inventar angezeigt werden soll.

3 Klicken Sie auf das Gerät, um seine Details anzuzeigen.

4 Klicken Sie auf die Registerkarte **Inventar**.

   Auf der Seite „Inventar“ wird eine Zusammenfassung des Hardware-Inventars angezeigt. Klicken Sie zur Anzeige detaillierter Informationen auf **Detailliertes Hardware-/Software-Inventar**.

Generieren von Inventarberichten

ZENworks Asset Management enthält mehrere Standardberichte. Außerdem können Sie benutzerdefinierte Berichte erstellen, um verschiedene Ansichten der Inventarinformationen bereitzustellen.

1 Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Berichte**.

2 Klicken Sie im Bereich der Inventar-Standardberichte auf **Software-Anwendungen**.

3 Klicken Sie auf den Bericht **Betriebssystem**, um den Bericht zu generieren.

   Mithilfe der Optionen unten im Bericht können Sie den generierten Bericht als Microsoft Excel-Arbeitsblatt, CSV-Datei (durch Kommas getrennte Werte), PDF-Datei oder PDF-Grafikdatei speichern.

Weitere Informationen

Weitere Informationen über das Inventar finden Sie im Handbuch *ZENworks: Inventar-Referenz*.

Überwachen der Softwarenutzung

Nach der Inventarisierung von Geräten können Sie Berichte erstellen, die aufzeigen, in welchem Umfang die Anwendungen der Geräte verwendet werden. ZENworks Asset Management enthält Standardberichte für die Anwendungsnutzung nach Produkt, Benutzer und Gerät. Sie können die Berichte auch benutzerdefiniert anpassen, um detailliertere oder konzentriertere Informationen zu bieten. So enthält Asset Management beispielsweise einen vordefinierten benutzerdefinierten Bericht mit den Anwendungen, die in den letzten 90 Tagen nicht verwendet wurden.

So führen Sie einen Bericht aus, in dem aufgezeigt wird, in welchem Umfang eine bestimmte Anwendung verwendet wird:

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Inventarverwaltung** und anschließend auf die Registerkarte **Softwarenutzung**.
2. Klicken Sie in der Kontrollleiste „Standardberichte zur Softwarenutzung“ auf **Anwendungsnutzung**, um die Liste der Berichte zur Anwendungsnutzung anzuzeigen.
3. Klicken Sie in der Kontrollleiste „Berichte“ auf **Lokale Anwendungsnutzung nach Produkt**.

   Im Bericht werden alle auf den Geräten installierten Produkte gruppiert nach Softwarehersteller angezeigt.
4. Suchen Sie einen Hersteller, dessen Produkte Sie anzeigen möchten und klicken Sie anschließend auf die Zahl in der Spalte „Installationen“, um die installierten Produkte anzuzeigen.

   Der resultierende Bericht zeigt die aktuelle Anzahl der Installationen für jedes Produkt an, wie viele der Installationen verwendet werden, wann das Produkt zuletzt verwendet wurde sowie andere Informationen zur Nutzung.
5. Wenn Sie den Zeitraum für den Bericht oder die Liste der angezeigten Produkte (alle Produkte, die verwendeten Produkte oder die nicht verwendeten Produkte) ändern möchten, klicken Sie unten im Bericht auf **Zeitraum/Filter ändern**.

Es sind noch viele weitere Standardberichte und vordefinierten Berichte verfügbar, die Sie verwenden können. Weitere Informationen über Berichte zur Anwendungsnutzung finden Sie im Abschnitt „Berichte“ im Handbuch *ZENworks Asset Management-Referenz*.

Überwachen der Lizenz-Compliance

Mit ZENworks Asset Management können Sie die Compliance der Softwarelizenzvereinbarungen in Ihrem Unternehmen überwachen, indem Sie die gekauften Softwarelizenzen mit den bei Inventarabsuchen ermittelten tatsächlichen Softwareinstallationen vergleichen.

Die Lizenz-Compliance in Asset Management ist ein leistungsfähiges und flexibles Werkzeug. Zur Einrichtung der Lizenz-Compliance können Sie folglich mehrere Ansätze und Methoden verwenden. In den folgenden Abschnitten erhalten Sie grundlegende Anweisungen mit kurzen Erläuterungen, die Sie bei der schnellen Einrichtung eines einzelnen Produkts für die Überwachung der Lizenz-Compliance unterstützen. Nach der Durchführung dieser grundlegenden Schritte finden Sie detailliertere Informationen und Anweisungen im Abschnitt „Lizenz-Compliance“ im Handbuch *ZENworks Asset Management-Referenz*.

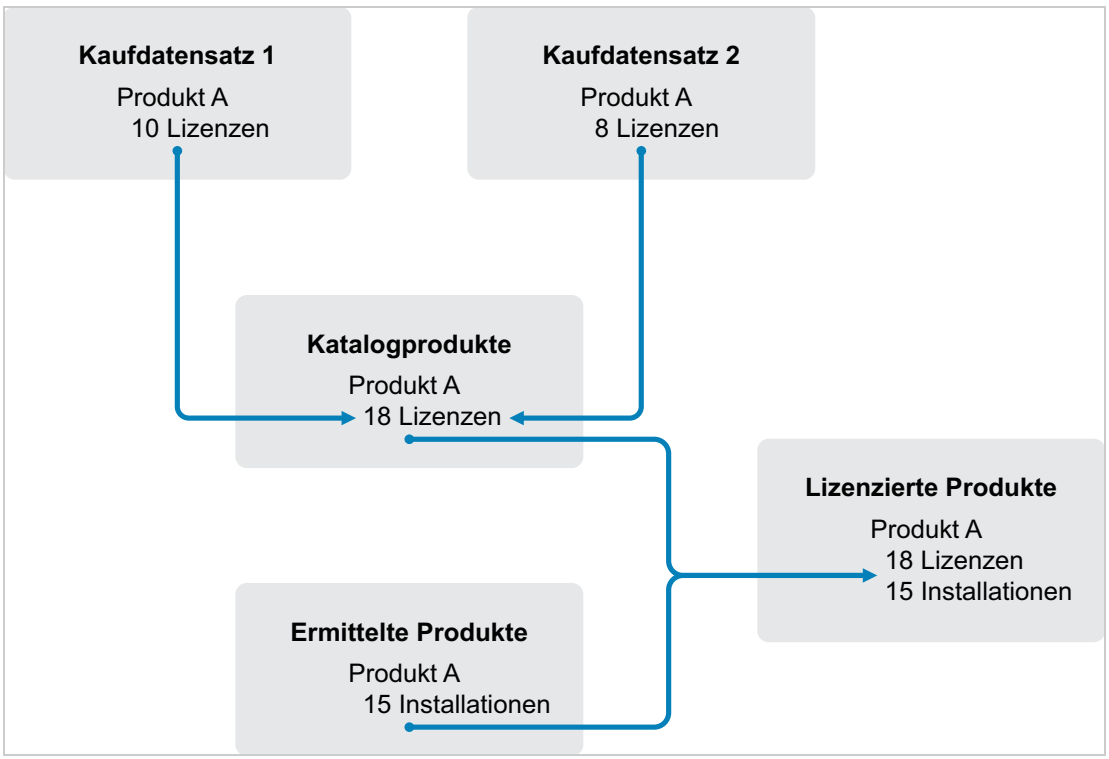
- „Komponenten der Lizenz-Compliance“, auf Seite 75
- „Ermitteln installierter Produkte“, auf Seite 76

- „Erstellen eines Katalogprodukts und eines Kaufdatensatzes“, auf Seite 76
- „Erstellen eines lizenzierten Produkts“, auf Seite 78
- „Anzeigen von Compliance-Daten“, auf Seite 80
- „Weitere Informationen“, auf Seite 81

Komponenten der Lizenz-Compliance

Bevor Sie damit beginnen können, die Compliance-Überwachung zu implementieren, müssen Sie die beteiligten Komponenten und deren Zusammenarbeit verstehen. Dies wird in der folgenden Abbildung und dem dazugehörigen Text erklärt.

Abbildung 8-1 *Komponenten der Lizenz-Compliance*



- Sie suchen die Geräte in Ihrer Verwaltungszone ab, um die Liste der installierten Softwareprodukte zu erstellen. Diese werden als *ermittelte Produkte* bezeichnet. In der Abbildung oben hat die Inventarabsuche ermittelt, dass ProduktA auf 15 Geräten installiert ist.
- Sie erstellen *Katalogprodukte*, um die von Ihrer Organisation gekauften Softwareprodukte darzustellen. Typischerweise entspricht jedes Katalogprodukt einer bestimmten Herstellerartikelnummer. In der Abbildung oben ist ProduktA das einzige Katalogprodukt. Sie verfügen jedoch möglicherweise auch über Katalogprodukte für ProduktA, das ProduktA-Upgrade und ProduktB.
- Sie erstellen *Kaufdatensätze*, um die Aufträge oder Rechnungen für Softwareprodukte darzustellen. Jede Zeile im Kaufdatensatz listet ein Katalogprodukt zusammen mit der Anzahl der gekauften Lizenzen auf. Wenn ein Katalogprodukt in mehreren Kaufdatensätzen aufgeführt ist, entspricht die Gesamtanzahl der Lizenzen für das Katalogprodukt der Auftragsmenge für

beide Kaufdatensätze. In der Abbildung oben enthält ein Kaufdatensatz 10 Lizenzen von ProduktA und ein anderer Kaufdatensatz enthält 8 Lizenzen. Die Gesamtanzahl der Lizenzen für ProduktA beträgt somit 18.

- Sie erstellen *lizenzierte Produkte* und verknüpfen die entsprechenden ermittelten Produkte und Katalogprodukte mit diesen. Daraus ergibt sich ein einzelnes lizenziertes Produkt, das die Anzahl der Lizenzen und Installationen für das Produkt enthält. Daraus ergibt sich ein schneller Überblick darüber, ob die Produktnutzung mit der Lizenzvereinbarung konform ist. In der Abbildung oben sind für ProduktA 18 Lizenzen vorhanden und es ist auf 15 Geräten installiert. Somit ist die Compliance mit der Lizenzvereinbarung für ProduktA gewährleistet.

Ermitteln installierter Produkte

Wenn Sie nicht bereits die Geräte in Ihrer Verwaltungszone abgesucht haben, um Informationen zu den installierten Produkten (den sogenannten **ermittelten Produkten**) zu sammeln, führen Sie die Schritte unter „Erfassung des Software- und Hardware-Inventars“, auf Seite 72 aus.

Wenn Sie Produkte ermittelt haben, wählen Sie ein Produkt aus, dessen Compliance überwacht werden soll.

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Inventarverwaltung** und anschließend auf die Registerkarte **Lizenzverwaltung**.
2. Klicken Sie in der Kontrollleiste „Lizenzverwaltung“ auf **Ermittelte Produkte**, um die Seite „Ermittelte Produkte“ anzuzeigen.
3. Durchsuchen Sie die Liste, um das ermittelte Produkt auszuwählen, das verwendet werden soll.

   Für das Produkt muss in der Spalte **Installierte Menge** mindestens eine Installation aufgeführt sein. Falls möglich, sollten Sie ein Produkt wählen, für das Sie bereits einen Auftrag oder eine Rechnung vorliegen haben. Dadurch können Sie den Vorgang anhand realer Informationen durchführen. Sie können die Kaufinformationen aber auch im Verlauf des Vorgangs erstellen. Merken Sie sich Ihre Produktwahl zur späteren Verwendung.
4. Fahren Sie mit dem nächsten Abschnitt, „Erstellen eines Katalogprodukts und eines Kaufdatensatzes“, auf Seite 76, fort.

Erstellen eines Katalogprodukts und eines Kaufdatensatzes

Ermittelte Produkte enthalten die Installationsinformationen für Produkte. Katalogprodukte und Kaufdatensätze werden erstellt, um Informationen zu Produktkäufen zur Verfügung zu stellen.

Ein Katalogprodukt stellt ein Softwareprodukt dar. Mithilfe eines Kaufdatensatzes wird das Katalogprodukt durch die Anzahl der gekauften Produktlizenzen ergänzt.

In den folgenden Schritten wird erläutert, wie ein Katalogprodukt und ein Kaufdatensatz für das unter „Ermitteln installierter Produkte“, auf Seite 76 gewählte ermittelte Produkt erstellt werden.

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Inventarverwaltung** und anschließend auf die Registerkarte **Lizenzverwaltung**.
2. So erstellen Sie ein Katalogprodukt:
   - **2a** Klicken Sie im Bereich „Lizenzverwaltung“ auf **Katalogprodukte**.
   - **2b** Klicken Sie auf **Neu** > **Katalogprodukt**, um den Assistenten zum Erstellen neuer Katalogprodukte aufzurufen.

2c Füllen Sie die folgenden Felder aus:

Hersteller: Wählen Sie den Softwarehersteller aus der Liste aus. Wenn der entsprechende Hersteller nicht aufgeführt ist, geben Sie den Namen des Herstellers ein (zum Beispiel Novell, Symantec oder Microsoft).

Produkt: Geben Sie den Namen des Produkts ein. Das Produkt sollte das gekaufte Softwareproduktpaket (software product package, SKU) darstellen. Beispielsweise könnte das gekaufte Paket „Einzellizenz für Produkt A“ oder „Paket über 10 Lizenzen für Produkt A“ heißen. Wenn Sie einen Rechnungsdatensatz haben, der das Produkt enthält, für das Sie ein Katalogprodukt erstellen, verwenden Sie den Namen aus der Rechnung.

Lizenzen pro Paket: Geben Sie die Anzahl der Lizenzen an, die im Produktpaket enthalten sind.

Produkttyp – Hinweise: Diese Felder sind optional. Sie können Sie verwenden, um weitere Angaben zum Produkt zu machen.

Ausgeschlossen: Dieses Kontrollkästchen darf nicht aktiviert werden.

2d Klicken Sie auf **Weiter**, um die Seite „Zusammenfassung“ anzuzeigen, und anschließend auf **Fertig stellen**, um das Produkt zur Liste der Katalogprodukte hinzuzufügen.

2e Klicken Sie auf **Lizenzverwaltung** (im Ariadnepfad oben auf der Seite), um zur Seite „Lizenzverwaltung“ zurückzukehren.

3 So erstellen Sie den Kaufdatensatz:

3a Klicken Sie im Bereich „Lizenzverwaltung“ auf **Kaufdatensätze**.

3b Klicken Sie auf **Neu** > **Kaufdatensatz**, um den Assistenten zur Erstellung neuer Kaufdatensätze aufzurufen.

3c Füllen Sie die folgenden Felder aus:

Auftragsnr.: Geben Sie die Auftragsnummer oder die Rechnungsnummer an, die mit dem Kauf des Softwareprodukts verknüpft ist. Wenn Ihnen für dieses Produkt kein Auftrag oder keine Rechnung vorliegt, geben Sie irgendeine Zahl an.

Auftragsdatum: Wählen Sie das Datum aus, an dem die Software gekauft wurde.

Empfänger – Händler: Diese Felder sind optional. Sie können sie verwenden, um weitere Angaben zum Kaufdatensatz zu machen.

3d Klicken Sie auf „Weiter“, um die Seite „Zusammenfassung“ anzuzeigen.

3e Wählen Sie das Feld **Zusätzliche Eigenschaften definieren** aus und klicken Sie anschließend auf **Fertig stellen**, um den Kaufdatensatz zu erstellen und die dazugehörige Seite „Kaufdetails“ anzuzeigen.

3f Klicken Sie auf **Hinzufügen**, um das Dialogfeld „Kaufdetail hinzufügen“ anzuzeigen, und füllen Sie dort die folgenden Felder aus:

Produkt: Klicken Sie auf  , um nach dem unter Schritt 2 erstellten Katalogprodukt zu suchen und es auszuwählen.

Menge: Geben Sie die gekaufte Menge des Produkts an. Wenn es sich bei dem ausgewählten Katalogprodukt beispielsweise um einen 10er-Pack ProduktA handelt und der Auftrag über 5 10er Packs ProduktA erteilt wurde, geben Sie 5 an.

Empfohlener Abgabepreis des Herstellers pro Einheit – Erweiterter Preis: Diese Felder müssen ausgefüllt werden. Geben Sie den empfohlenen Abgabepreis des Herstellers, den Preis, den Sie pro Einheit bezahlt haben, sowie den Angebotspreis an. Wenn Sie das Feld **Angebotspreis** leer lassen, füllt der Assistent es auf, indem er die **Kaufmenge** mit dem **Preis pro Einheit** multipliziert.

Rechnungsnummer – Kommentare: Diese Felder sind optional. Sie können Sie verwenden, um weitere Angaben zum Kauf zu machen.

3g Klicken Sie auf **OK**.

4 Fahren Sie mit dem nächsten Abschnitt, Erstellen eines lizenzierten Produkts, fort.

Asset Management kann Kaufinformationen auch aus elektronischen Dateien importieren. Bei diesem Vorgang werden sowohl der Kaufdatensatz als auch alle Katalogprodukte für im Kaufdatensatz enthaltene Softwareprodukte erstellt. Weitere Informationen finden Sie im Abschnitt „Lizenz-Compliance“ im Handbuch *ZENworks Asset Management-Referenz*.

Erstellen eines lizenzierten Produkts

Der letzte Schritt beim Einrichten der Compliance für das Softwareprodukt besteht darin, ein lizenziertes Produkt zu erstellen und ihm das ermittelte Produkt und das Katalogprodukt zuzuordnen. Dadurch wird das Lizenzprodukt mit den Installations- und Lizenzinformationen aufgefüllt, die zur Festlegung des Lizenz-Compliance-Status erforderlich sind.

In den folgenden Schritten wird erläutert, wie der Assistent für den automatischen Abgleich verwendet wird, um das lizenzierte Produkt zu erstellen und ihm das ermittelte Produkt und das Katalogprodukt zuzuordnen.

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Inventarverwaltung** und anschließend auf die Registerkarte **Lizenzverwaltung**.
2. Klicken Sie im Bereich „Lizenzverwaltung“ auf **Lizenzierte Produkte**.
3. Wählen Sie im Bereich „Lizenzierte Produkte“ die Optionsfolge **Aktion > Automatischer Abgleich: Lizenzierte Produkte erstellen**, um den Assistenten für den automatischen Abgleich aufzurufen. Schließen Sie den Assistenten mithilfe der Informationen aus der folgenden Tabelle ab, um die Felder auszufüllen.

Assistentenseite	Details
Filter für ermittelte Produkte	Der Assistent für den automatischen Abgleich erstellt lizenzierte Produkte aus bereits vorhandenenen ermittelten Produkten. So suchen Sie das ermittelte Produkt: 1. Klicken Sie auf die Option **Unten angegebene Produkte**. 2. Wählen Sie in der Liste **Auswählen** den Hersteller des ermittelten Produkts aus. 3. Geben Sie im Feld **Produkt** den Namen des ermittelten Produkts ein.

Assistentenseite	Details
Zu erstellende lizenzierte Produkte auswählen	Basierend auf den auf der Seite „Filter für ermittelte Produkte“ angegebenen Informationen sollten auf dieser Seite das ermittelte Produkt und die für das Produkt erstellte Lizenz angezeigt werden. Der Assistent versucht, das Katalogprodukt und das ermittelte Produkt abzugleichen, indem er die Felder „Hersteller“ und „Produkt“ vergleicht. Wenn der Assistent eine Übereinstimmung zwischen dem erstellten Katalogprodukt und dem ermittelten Produkt feststellt, wird das Katalogprodukt ebenfalls aufgeführt. Wählen Sie das Katalogprodukt aus, um es dem lizenzierten Produkt zuzuordnen. Wenn der Assistent keine Übereinstimmung zwischen dem Katalogprodukt und dem ermittelten Produkt feststellen kann, müssen Sie das Katalogprodukt nach Abschließen des Assistenten manuell zuweisen.
Zielordner	Wählen Sie den Ordner aus, in dem das neu lizenzierte Produkt gespeichert werden soll. Das Feld enthält standardmäßig den aktuellen Ordner (den Ordner, von dem aus Sie den Assistenten für automatischen Abgleich gestartet haben). Um einen anderen Ordner anzugeben, klicken Sie auf  , navigieren Sie zum gewünschten Ordner und wählen Sie ihn aus. Der Ordner muss bereits vorhanden sein. Sie können im Auswahldialogfeld keinen neuen Ordner erstellen.
Lizenzberechtigungen	Jedes lizenzierte Produkt muss mindestens eine Berechtigung und ein Lizenzmodell haben. Eine Berechtigung stellt typischerweise eine Lizenzvereinbarung dar. In vielen Fällen enthält ein lizenziertes Produkt möglicherweise nur eine Berechtigung. Wenn Sie jedoch mehrere Berechtigungen zulassen, können Sie die Compliance für ein lizenziertes Produkt feststellen, das über mehrere Lizenzvereinbarungen verfügt. Sie haben beispielsweise für ein Produkt sowohl eine Volllizenzvereinbarung als auch eine Upgrade-Lizenzvereinbarung. Anstatt zwei separate Lizenzprodukte für ein und dasselbe Produkt zu erstellen, können Sie ein einziges lizenziertes Produkt mit zwei unterschiedlichen Berechtigungen erstellen. Durch das Lizenzmodell wird festgelegt, wie die Lizenzen gezählt werden. Lizenzen können pro Installation, pro Benutzer oder pro Gerät gezählt werden. Geben Sie in diesem Fall **Pro Installation** als Beschreibung an und wählen Sie **Pro Installation** als Lizenzmodell aus. Dadurch verbraucht jede Installation des Produkts eine Lizenz.
Zusammenfassung für automatischen Abgleich erstellen	Überprüfen Sie Ihre Daten.

4 Falls nicht bereits geschehen, klicken Sie auf **Fertig stellen**, um das lizenzierte Produkt zu erstellen und es zur Liste der lizenzierten Produkte hinzuzufügen.

5 Gehen Sie folgendermaßen vor, wenn der Assistent für den automatischen Abgleich dem Katalogprodukt kein lizenziertes Produkt zuordnen konnte:

5a Klicken Sie auf das lizenzierte Produkt.

5b Klicken Sie auf die Registerkarte **Lizenzberechtigungen**.

5c Klicken Sie in der Kontrollleiste „Berechtigungen“ auf die entsprechende Berechtigung.

5d Klicken Sie auf die Registerkarte **Eigentumsnachweis**.

5e Klicken Sie im Bereich „Katalogprodukte“ auf **Hinzufügen**.

5f Wählen Sie das Katalogprodukt aus und klicken Sie anschließend auf **OK**, um es der Kontrollleiste „Katalogprodukte“ hinzuzufügen.

In der Kontrollleiste „Katalogprodukte“ wird die Kaufmenge des Katalogprodukts angezeigt, also die Anzahl der Einheiten des (laut Kaufdatensatz) gekauften Katalogprodukts. Es wird auch die Lizenzmenge angezeigt, also die gesamte Anzahl der in den gekauften Einheiten enthaltenen Lizenzen.

6 Weitere Informationen zur Überwachung der Compliance finden Sie im nächsten Abschnitt, Anzeigen von Compliance-Daten.

Anzeigen von Compliance-Daten

Zur Anzeige des Compliance-Status Ihrer lizenzierten Produkte stehen Ihnen zwei Ansichten zur Verfügung. Sie können die Seite „Lizenzierte Produkte“ anzeigen, um eine Software-Compliance-Zusammenfassung für alle Produkte zu erhalten. Sie können aber auch den Software-Compliance-Bericht generieren, um detailliertere Informationen zu erhalten.

- „Anzeigen der Software-Compliance-Zusammenfassung“, auf Seite 80
- „Generieren des Software-Compliance-Berichts“, auf Seite 81

Anzeigen der Software-Compliance-Zusammenfassung

1 Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Inventarverwaltung** und anschließend auf die Registerkarte **Lizenzverwaltung**.

2 Klicken Sie in der Kontrollleiste „Lizenzverwaltung“ auf **Lizenzierte Produkte**, um die Seite „Lizenzierte Produkte“ anzuzeigen.

In der Liste „Lizenzierte Produkte“ werden alle lizenzierten Produkte und deren aktueller Compliance-Status angezeigt:

- Das Softwareprodukt ist ordnungsgemäß lizenziert. Die Anzahl der gekauften Lizenzen entspricht der Anzahl der Installationen.
- Für das Softwareprodukt sind zu viele Lizenzen vorhanden. Es sind mehr gekaufte Lizenzen als Installationen vorhanden.
- Für das Softwareprodukt sind nicht genügend Lizenzen vorhanden. Es sind weniger gekaufte Lizenzen als Installationen vorhanden.

Generieren des Software-Compliance-Berichts

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Inventarverwaltung** und anschließend auf die Registerkarte **Lizenzverwaltung**.
2. Klicken Sie im Bereich „Lizenzverwaltung“ auf **Lizenzverwaltungsberichte**.
3. Klicken Sie im Bereich „Standardmäßige Lizenzverwaltungsberichte“ auf **Software-Compliance**.
4. Klicken Sie im Bereich „Berichte“ auf **Compliance-Bericht**.

   Daraufhin wird ein Bericht angezeigt, in dem die Compliance-Daten nach Lizenz sortiert sind. Sie können die Daten anhand des Compliance-Status, des Herstellers und Werts oder anhand demografischer Daten filtern. Erweitern Sie die Anzeige bis zum Eintrag **Lizenzmenge**, um die Compliance-Details für ein bestimmtes lizenziertes Produkt anzuzeigen. Informationen zu anderen Berichten finden Sie im Handbuch *ZENworks Asset Management-Referenz*.

Weitere Informationen

Das in den vorigen Abschnitten beschriebene Szenario zeigt nur einen kleinen Teil der in ZENworks Asset Management verfügbaren Lizenz-Compliance-Funktionen. Weitere Informationen finden Sie im Abschnitt „Lizenz-Compliance“ im Handbuch *ZENworks Asset Management-Referenz*.

Zuordnen von Lizenzen

Mit ZENworks Asset Management können Sie Lizenzen innerhalb Ihres Unternehmens zuordnen, um die Eigentümerschaft und Verteilung der Lizenzen zu überwachen. Lizenzen können zu Geräten oder Demografien (Standorten, Abteilungen oder Kostenstellen) zugeordnet werden.

Unter einer *Gerätezuordnung* versteht man die Zuweisung einer Lizenz zu einem bestimmten Gerät. Auf dem Gerät kann das Produkt installiert sein oder auch nicht. Sie kaufen beispielsweise 10 Lizenzen von ProduktA. Sie können die Lizenzen den Zielgeräten zuordnen, bevor ProduktA überhaupt auf den Geräten installiert wird.

Unter einer *demografischen Zuordnung* versteht man die Zuweisung mindestens einer Lizenz zu einem Standort, einer Abteilung oder einer Kostenstelle. Jedes Gerät, das der Demografie zugewiesen wurde und auf dem das Produkt installiert ist, wird als eine mit der Zuordnung verknüpfte Installation angezeigt. Sie kaufen beispielsweise 15 Lizenzen von ProduktA und ordnen sie AbteilungQ zu. AbteilungQ sind 20 Geräte zugewiesen. ProduktA ist auf 12 dieser 20 Geräte installiert. Folglich zeigt die Zuordnung für AbteilungQ 15 zugeordnete Lizenzen mit 12 Installationen an.

In den folgenden Schritten wird erläutert, wie Lizenzen zu Geräten zugeordnet werden. Informationen zum Zuordnen von Lizenzen zu Demografien finden Sie im Abschnitt „Lizenzzuordnung“ im Handbuch *ZENworks Asset Management-Referenz*.

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Inventarverwaltung**.
2. Klicken Sie auf der Seite „Lizenzverwaltung“ auf **Lizenzierte Produkte**.
3. Klicken Sie in der Liste der lizenzierten Produkte auf das lizenzierte Produkt, für das Lizenzen zugeordnet werden sollen.

4 Standardmäßig wird zum Verfolgen des Produktlizenzeigentums nur die Gerätezuordnung aktiviert. Zum Zuordnen von Lizenzen zu Demografien muss ein Benutzer die folgenden Schritte ausführen, um die demografische Zuordnung für das Produkt zu aktivieren:

4a Klicken Sie auf das Register **Allgemein**.

4b Füllen Sie in der Kontrollleiste „Einstellungen für Lizenzzuordnungen“ die folgenden Felder aus:

Demografische Zuordnungen aktivieren: Wählen Sie diese Option.

Demografischer Zuordnungstyp: Alle demografischen Zuordnungen für ein einzelnes lizenziertes Produkt müssen denselben Typ aufweisen. Wählen Sie den Typ (**Standort**, **Abteilung**, **Kostenstelle**) aus, der für dieses Produkt verwendet werden soll.

Aktualisierung von Lizenzzuordnungen mit demografischen Daten aus Importen von zukünftigen Kaufdatensätzen: Wählen Sie diese Option aus, wenn beim Importieren zukünftiger Kaufdatensätze für das Produkt die zugeordnete Lizenzmenge auf Basis der demografischen Daten des Kaufdatensatzes automatisch aktualisiert werden soll.

Nehmen Sie beispielsweise an, dass das Produkt Abteilungszuordnungen verwendet. Sie importieren einen Kaufdatensatz, der AbteilungQ zugewiesene Lizenzen verwendet. Die Lizenzen werden der demografischen Zuordnung zu AbteilungQ hinzugefügt.

Erstellt gegebenenfalls auch neue Zuordnungen. Wenn der Kaufdatensatz beispielsweise Lizenzen für ProduktA enthält, die einer AbteilungZ zugewiesen wurden (einer neuen Abteilung, die nicht in den Zuordnungen von ProduktA aufgeführt ist), so wird eine neue Zuordnung für AbteilungZ erstellt.

Zugeordnete Menge: Zeigt die gesamte Anzahl zugeordneter Lizenzen an, entweder zu Geräten oder zu Demografien.

4c Klicken Sie auf **Anwenden**, um Änderungen zu speichern.

5 Klicken Sie auf die Registerkarte **Lizenzzuordnungen**.

6 (Optional) Um festzustellen, auf welchen Geräten das Produkt installiert ist, obwohl diesen keine Lizenz zugeordnet wurde, klicken Sie in der Kontrollleiste „Gerätezuordnungen“ auf die Zahl für **Installationen ohne Zuordnungen**.

7 Klicken Sie auf **Hinzufügen** > **Geräte mit installiertem Produkt**, wenn auf dem Gerät, dem eine Lizenz zugeordnet werden soll, das Produkt installiert ist.

oder

Klicken Sie auf **Hinzufügen** > **Beliebige Geräte**, wenn auf dem Gerät, dem eine Lizenz zugeordnet werden soll, das Produkt nicht installiert ist.

Das Dialogfeld „Gerät suchen“ wird angezeigt.

8 Wählen Sie im Feld **Gerätetyp** aus, ob **Verwaltete Geräte**, **Inventarisierte Geräte**, **Verwaltete oder inventarisierte Geräte**, **Migrierte ZAM-Geräte** oder **Alle** gesucht werden sollen.

Wenn Sie nicht sicher sind, um welchen Gerätetyp es sich handelt, wählen Sie **Alle** aus.

9 Verwenden Sie zur Eingrenzung der Suche die Option Filter, um die Suchkriterien zu erstellen.

Wenn Sie keine Filter erstellen, werden alle Geräte (oder alle Geräte mit dem installierten Produkt) angezeigt, bis die maximale Anzahl für die Anzeige erreicht ist.

10 Geben Sie die maximale Anzahl von Geräten an, die im Suchergebnis angezeigt werden soll.

11 Wählen Sie die Spalten aus, die im Dialogfeld mit dem Suchergebnis angezeigt werden sollen. Halten Sie die Strg-Taste gedrückt und klicken Sie auf die Felder, die ausgewählt werden sollen.

12 Klicken Sie auf **Suchen**, um ein Dialogfeld „Gerät auswählen“ anzuzeigen, in dem die Suchergebnisse aufgeführt sind.

13 Wählen Sie die Geräte aus, denen Lizenzen zugeordnet werden sollen, und klicken Sie anschließend auf **OK**.

Für die Zuordnung werden folgende Informationen angezeigt:

- **Computername, Anmeldename und IP-Adresse:** Standardinformationen zu dem Gerät, einschließlich des Anmeldenamens des Benutzers, der zum Zeitpunkt der Inventarisierung des Geräts angemeldet war.
- **Standort, Abteilung, Kostenstelle:** Demografische Daten zu dem Gerät. Wenn mindestens eines der Felder leer ist, sind diese Informationen nicht in den Inventardaten des Geräts enthalten.
- **Installierte Menge:** Die Anzahl der Installationen des lizenzierten Produkts auf dem Gerät. Diese sollte typischerweise 1 lauten.
- **Doppelte Zuordnung:** Ist mit einem Häkchen versehen, wenn die Intallation des Geräts auch in einer demografischen Zuordnung enthalten ist.
- **Installationen ohne Zuordnungen:** Zeigt die Anzahl der Installationen an, die nicht durch eine demografische Zuordnung oder eine Gerätezuordnung einer Lizenz zugeordnet sind. Klicken Sie auf die Zahl, um die Liste der Installationen anzuzeigen.

9 Konfigurationsmanagement

Die folgenden Abschnitte enthalten Erläuterungen und Anweisungen für die Aufgaben, die Sie mit ZENworks Configuration Management ausführen können. Je nach Umgebung und den Funktionen, die Sie verwenden möchten, müssen Sie möglicherweise nicht wissen, wie alle Aufgaben durchgeführt werden. Diejenigen, über die Sie mehr erfahren möchten, können Sie in beliebiger Reihenfolge überprüfen.

Aktivieren von Configuration Management

Wenn Sie Configuration Management nicht bereits bei der Installation der Verwaltungszone aktiviert haben, indem Sie entweder einen Lizenzschlüssel angegeben oder die Evaluierung eingeschaltet haben, führen Sie folgende Schritte aus:

1. Klicken Sie im ZENworks-Kontrollzentrum auf **Konfiguration**.
2. Klicken Sie in der Kontrollleiste „Lizenzen“ auf **ZENworks 2020 Configuration Management**.
3. Wählen Sie „Produkt evaluieren/aktivieren“ aus und füllen Sie anschließend die folgenden Felder aus:

   Evaluierung verwenden: Wählen Sie diese Option aus, um den 60-Tage-Evaluierungszeitraum zu aktivieren. Nach dem 60-Tage-Zeitraum müssen Sie einen Produktlizenzschlüssel anwenden, um das Produkt weiterhin verwenden zu können.

   Produktlizenzschlüssel: Geben Sie den Lizenzschlüssel an, den Sie für Configuration Management erworben haben. Eine Produktlizenz können Sie auf der Novell ZENworks Configuration Management-Produkt-Website (http://www.novell.com/products/zenworks/configurationmanagement) erwerben.
4. Klicken Sie auf **OK**.

Aktivieren des Konfigurationsmanagements im ZENworks Agent

Damit der ZENworks Agent Konfigurationsmanagementvorgänge auf einem Gerät durchführen kann, müssen die entsprechenden Agent-Funktionen aktiviert werden. Diese Funktionen (Bundle-Verwaltung, Image-Verwaltung, Richtlinienverwaltung, Fernverwaltung und Benutzerverwaltung) werden standardmäßig aktiviert, wenn ZENworks Configuration Management aktiviert wird (durch Voll- oder Evaluierungslizenz).

Sie sollten überprüfen, ob die Funktionen aktiviert sind. Funktionen, die Sie nicht verwenden möchten, können Sie auch deaktivieren. Eine Anleitung dazu finden Sie in „Konfigurieren der ZENworks-Agent-Funktionen“, auf Seite 41.

Verteilen von Software

ZENworks Configuration Management bietet Ihnen große Flexibilität beim Verteilen von Software. Sie können Anwendungen und einzelne Dateien verteilen, Änderungen an vorhandenen Dateien auf einem Gerät vornehmen sowie Anwendungen auf Ihren Geräten installieren, entfernen und zurücksetzen.

Software wird mithilfe von Bundles verteilt. Ein Bundle umfasst alle Dateien, Konfigurationseinstellungen, Installationsanweisungen usw., die zur Bereitstellung und Verwaltung der Anwendung oder Dateien auf einem Gerät erforderlich sind. Wenn Sie ein Bundle einem Gerät zuweisen, können Sie es auf dem Gerät gemäß der von Ihnen definierten Zeitpläne (Verteilung, Start und Verfügbarkeit) installieren und starten.

Sie können auch die Zusammenfassung des Zuweisungs-, Verteilungs-, Installations- und Startstatus für das Bundle über das Bundle-Dashboard anzeigen. Weitere Informationen finden Sie im Handbuch ZENworks: Referenz zur Softwareverteilung.

Es gibt vier Arten von Bundles, die Sie erstellen können:

- **iOS-Bundle:** Ermöglicht es Ihnen, Anwendungen auf iOS-Geräten zu konfigurieren und zu verwalten.
- **Linux-Bundle:** Ermöglicht es Ihnen, Anwendungen auf Linux-Geräten zu konfigurieren und zu verwalten.
- **Linux-Abhängigkeits-Bundle:** Ermöglicht es, dass Softwarepakete auf Linux-Geräten verfügbar sind, um Paketabhängigkeiten aufzulösen.
- **Macintosh-Bundle:** Ermöglicht es Ihnen, Anwendungen auf Macintosh-Geräten zu konfigurieren und zu verwalten.
- **Preboot-Bundle:** Ermöglicht es Ihnen, einen Satz von Aufgaben auf einem verwalteten oder nicht verwalteten Gerät durchzuführen, bevor das Betriebssystem auf dem Gerät bootet.
- **Windows-Bundle:** Ermöglicht es Ihnen, Anwendungen auf Windows-Geräten zu konfigurieren und zu verwalten.

Android-Bundles (Arbeits-Apps für Android im Unternehmen) und Apple VPP-Bundles werden automatisch erstellt, sobald ZENworks mit dem entsprechenden Google- bzw. Apple-Server synchronisiert wird. Sie können jedoch zusätzliche Android- oder Apple VPP-Bundles erstellen. Weitere Informationen finden Sie unter Provisioning Applications (Bereitstellen von Anwendungen).

Die in einem Bundle enthaltene Software wird auf das ZENworks-Server-Repository heraufgeladen. Das ermöglicht dem ZENworks-Server, die Software zu verteilen, ohne Zugriff auf andere Netzwerkspeicherorte zu verlangen.

 In den folgenden Videos wird die Verteilung von Software auf Windows-, Linux- und Macintosh-Geräten erläutert:

- Bereitstellen von Windows-Software mit ZENworks
- Bereitstellen von Linux-Software mit ZENworks
- Mac-Management mit ZENworks: Agentenbereitstellung
- Mac-Verwaltung mit ZENworks: Standardisierte Anwendungsbereitstellung

---

Erstellen eines Bundles

Zum Erstellen eines Software-Bundles verwenden Sie den Assistenten zum Erstellen neuer Bundles. Außer beim Erstellen des Bundles unterstützt Sie der Assistent auch beim Zuweisen zu Geräten und Benutzern sowie beim Erstellen von Verteilungs-, Start- und Verfügbarkeitszeitplänen.

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Bundles**.
2. Klicken Sie im Bundles-Bereich auf **Neu** > **Bundle**, um den Assistenten zum Erstellen neuer Bundles zu starten.
3. Folgen Sie den Eingabeaufforderungen, um das Bundle zu erstellen.

   Klicken Sie auf den einzelnen Seiten des Assistenten auf die Schaltfläche **Hilfe**, um detaillierte Informationen zur jeweiligen Seite anzuzeigen.

   Wenn Sie den Assistenten fertig stellen, wird das Bundle dem Bundles-Bereich hinzugefügt. Durch Klicken auf das Bundle können Sie die Bundle-Details anzeigen und ändern.
4. Fahren Sie mit dem nächsten Abschnitt, Zuweisen eines Bundles, fort.

Zum Erstellen eines Software-Bundles können Sie auch den Befehl `bundle-create` im zman-Dienstprogramm verwenden. Weitere Informationen finden Sie unter „Bundle-Kommandos“ im Handbuch *ZENworks: Referenz für Befehlszeilen-Dienstprogramme*.

Zuweisen eines Bundles

Nach dem Erstellen eines Bundles müssen Sie es den Geräten zuweisen, auf denen es installiert werden soll. Zuweisungen können für Geräte oder Benutzer vorgenommen werden.

1. Wählen Sie in der Kontrollleiste „Bundles“ das Bundle aus, das Sie zuweisen möchten, indem Sie das zugehörige Kontrollkästchen aktivieren.
2. Klicken Sie auf **Aktion** > **Zu Gerät zuweisen**.

   oder

   Klicken Sie auf **Aktion** > **Benutzer zuweisen.**
3. Folgen Sie den Eingabeaufforderungen, um das Bundle zuzuweisen.

Klicken Sie auf den einzelnen Seiten des Assistenten auf die Schaltfläche **Hilfe**, um detaillierte Informationen zur jeweiligen Seite anzuzeigen.

Wenn Sie den Assistenten fertig stellen, werden die zugewiesenen Geräte oder Benutzer auf der Seite „Beziehungen“ des Bundles hinzugefügt. Die Zuweisungen können Sie durch Klicken auf das Bundle anzeigen.

Zum Zuweisen eines Bundles können Sie auch das Kommando `bundle-assign` im zman-Dienstprogramm verwenden. Weitere Informationen finden Sie unter „Bundle-Kommandos“ im Handbuch *ZENworks: Referenz für Befehlszeilen-Dienstprogramme*.

Weitere Informationen

Weitere Informationen über das Verteilen von Software finden Sie im Handbuch *ZENworks: Referenz zur Softwareverteilung*.

Weitere Informationen zum Verteilen von Apps an Mobilgeräte finden Sie in der *ZENworks Mobile Management Reference* (Referenz zu Mobile Management).

Anwenden von Richtlinien

In ZENworks Configuration Management können Sie mittels Richtlinien bestimmte Konfigurationen erstellen, die den angegebenen verwalteten Geräten zugewiesen werden. Dadurch lassen sich Geräte identisch konfigurieren, ohne dass der Konfigurationsvorgang auf den einzelnen Geräten separat wiederholt werden muss.

Mithilfe der Richtlinien in ZENworks Configuration Management können Sie externe Dienste, auf Puppet-Richtlinien bezogene Einstellungen, Internet Explorer-Favoriten, Windows-Gruppenrichtlinien, lokale Dateirechte, Energieverwaltungseinstellungen, Drucker, SNMP-Diensteinstellungen und zentral gespeicherte Profile verwalten sowie dynamische lokale Benutzerkonten konfigurieren und diese auf verwalteten Geräten verwalten. Außerdem können Sie über Richtlinien das Verhalten bzw. die Ausführung einer Fernverwaltungssitzung auf dem verwalteten Gerät konfigurieren und das Verhalten sowie die Funktionen von ZENworks Explorer zentral steuern.

Der folgende Abschnitt enthält die Liste der Windows-Konfigurationsrichtlinien, die erstellt und einem Benutzer oder einem verwalteten Gerät zugewiesen werden können.

- **Richtlinie für Browser-Lesezeichen:** Konfiguriert die Favoriten im Internet Explorer für Windows-Geräte und -Benutzer.
- **Richtlinie für dynamische lokale Benutzer:** Konfiguriert die auf Windows XP-, Windows Vista- und Windows 7-Arbeitsstationen und auf Windows 2003-, Windows 2008- und Windows 2008 R2-Terminalservern angelegten Benutzer, nachdem diese Benutzer erfolgreich in Novell eDirectory authentifiziert wurden.
- **Richtlinie für lokale Dateirechte:** Konfiguriert die Rechte für Dateien oder Ordner, die sich auf dem NTFS-Dateisystem befinden.

  Mithilfe dieser Richtlinie können Sie Basis- und erweiterte Berechtigungen sowohl für lokale Benutzer als auch für Domänenbenutzer oder Gruppen konfigurieren. Damit kann ein Administrator auf verwalteten Geräten benutzerdefinierte Gruppen anlegen.
- **Energieverwaltungsrichtlinie:** Konfiguriert Energieverwaltungseinstellungen auf verwalteten Geräten.

Schauen Sie sich ein Video über die Konfiguration einer Energieverwaltungsrichtlinie an.

- **Druckerrichtlinie:** Konfiguriert lokale Drucker sowie SMB, HTTP, TCP/IP, CUPS, und iPrint-Drucker für Windows-Geräte und Benutzer.
- **Fernverwaltungsrichtlinie:** Konfiguriert das Verhalten oder die Ausführung einer Fernverwaltungssitzung auf einem verwalteten Gerät. Die Richtlinie enthält Eigenschaften wie Fernverwaltungsvorgänge, -sicherheit usw. Eine Fernverwaltungsrichtlinie kann Benutzern und verwalteten Geräten zugewiesen werden.
- **Richtlinie für zentral gespeicherte Profile:** Ermöglicht es dem Benutzer, den Pfad zu konfigurieren, unter dem sein Benutzerprofil gespeichert werden soll.

  Ein Benutzerprofil enthält Informationen zu den Desktopeinstellungen eines Benutzers sowie dessen persönliche Einstellungen, die von Sitzung zu Sitzung beibehalten werden.

  Jedes in einem Netzwerkpfad gespeicherte Benutzerprofil wird als zentral gespeichertes Profil bezeichnet. Bei jeder Anmeldung eines Benutzers an einem Gerät wird dessen Profil aus dem Netzwerkpfad geladen. Damit werden die persönlichen Einstellungen eines Benutzers konsistent beibehalten, auch wenn er von Computer zu Computer wechselt.
- **SNMP-Richtlinie:** Konfiguriert die SNMP-Parameter auf den verwalteten Geräten.
- **Windows-Gruppenrichtlinie:** Konfiguriert die Gruppenrichtlinie für Windows-Geräte und -Benutzer.
- **ZENworks Explorer-Konfigurationsrichtlinie:** Ermöglicht Ihnen die zentrale Verwaltung des Verhaltens und der Funktionen des ZENworks Explorer.

Der folgende Abschnitt enthält die Liste der Linux-Konfigurationsrichtlinien, die erstellt und einem Benutzer oder einem verwalteten Gerät zugewiesen werden können.

- **Richtlinie für externe Dienste:** Konfiguriert die externen Dienste auf einem verwalteten Linux-Gerät für die YUM-, ZYPP- oder MOUNT-Repositorys. Sie bietet einem Administrator die Möglichkeit, Softwarepakete oder Aktualisierungen von diesen Repositorys herunterzuladen und auf den verwalteten Geräten zu installieren.
- **Puppet-Richtlinie:** Gibt an, wie Puppet-Manifeste oder -Module auf verwalteten Geräten ausgeführt und Skript-Dateien heraufgeladen werden und ob ein Probelauf des Skripts auf dem Gerät durchgeführt werden sollte.

Der nachfolgende Abschnitt zeigt die Richtlinien für die in der Zone registrierten Mobilgeräte.

- **Richtlinie zur Mobilgerätesteuerung:** Hiermit können Sie den Zugriff der Benutzer auf die verschiedenen Funktionen des Mobilgeräts zulassen oder einschränken.
- **E-Mail-Richtlinie für Mobilgeräte:** Hiermit verwalten Sie das Unternehmens-E-Mail-Konto auf Mobilgeräten.
- **Richtlinie zur Mobilregistrierung:** Hiermit legen Sie fest, welche Benutzer welche Mobilgeräte registrieren können. Außerdem geben Sie den Modus für die Registrierung der Mobilgeräte sowie den Standort und die Benennung der Geräte an.
- **Sicherheitsrichtlinie für Mobilgeräte:** Hiermit konfigurieren Sie die Passworteinschränkungen, die Verschlüsselungseinstellungen und die Einstellungen zur Inaktivität von Geräten.
- **Mobilgeräte-Compliance-Richtlinie:** Stellt sicher, dass die Geräte mit den auf diese Geräte angewendeten Regeln konform sind.

- **Android Enterprise-Registrierungsrichtlinie:** Ermöglicht es Benutzern, Ihre Android-Geräte im Arbeitsprofilmodus oder im Modus für verwaltete Unternehmensgeräte als Bestandteil des Android Enterprise-Programms zu registrieren.
- **iOS Intune-App-Schutzrichtlinie:** Erzwingt Beschränkungen für Microsoft Intune-Apps wie Aktionen zum Ausschneiden, Kopieren und Einfügen in der App und erzwingt die Verwendung einer PIN für den Zugriff auf eine Intune-App.

Erstellen einer Richtlinie

Zum Erstellen einer Richtlinie verwenden Sie den Assistenten zum Erstellen neuer Richtlinien. Außer beim Erstellen der Richtlinie unterstützt Sie der Assistent auch beim Zuweisen zu Geräten und Benutzern sowie bei Ihrer Entscheidung, die Richtlinie unverzüglich durchzusetzen oder bis zum Aktualisieren der Geräteinformationen zu warten.

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Richtlinien**.
2. Klicken Sie im Bereich „Richtlinien“ auf **Neu** > **Richtlinie**. Die Seite „Plattform auswählen“ wird geöffnet.
3. Wählen Sie die Richtlinienkategorie aus und klicken Sie auf **Weiter**. Die Seite „Richtlinienkategorie auswählen“ wird geöffnet.
4. Wählen Sie die Kategorie der zu konfigurierenden Richtlinie aus und klicken Sie auf **Weiter**.
5. Wählen Sie einen Richtlinientyp in der Liste der verfügbaren Richtlinien aus. Folgen Sie den Bildschirmanweisungen, um die Richtlinie zu erstellen.

   Klicken Sie auf den einzelnen Seiten des Assistenten auf die Schaltfläche **Hilfe**, um detaillierte Informationen zur jeweiligen Seite anzuzeigen.

   Wenn Sie den Assistenten fertig stellen, wird die Richtlinie Richtlinienbereich hinzugefügt. Sie können auf die Richtlinie klicken, um ihre Details anzuzeigen und um Zuweisungen zu bearbeiten.

Zum Erstellen einer Richtlinie können Sie auch den Befehl `policy-create` im zman-Dienstprogramm verwenden. Weitere Informationen finden Sie unter „Richtlinienkommandos“ im Handbuch *ZENworks: Referenz für Befehlszeilen-Dienstprogramme*.

Eine Richtlinie zuweisen

Nach dem Erstellen einer Richtlinie müssen Sie sie den Geräten zuweisen, auf denen sie angewendet werden soll. Zuweisungen können für Geräte oder Benutzer vorgenommen werden.

1. Wählen Sie in der Kontrollleiste „Richtlinien“ die Richtlinie aus, die Sie zuweisen möchten, indem Sie das zugehörige Kontrollkästchen aktivieren.
2. Klicken Sie auf **Aktion** > **Zu Gerät zuweisen**.

   oder

   Klicken Sie auf **Aktion** > **Benutzer zuweisen.**
3. Folgen Sie den Eingabeaufforderungen, um die Richtlinie zuzuweisen.

Klicken Sie auf den einzelnen Seiten des Assistenten auf die Schaltfläche **Hilfe**, um detaillierte Informationen zur jeweiligen Seite anzuzeigen.

Wenn Sie den Assistenten fertig stellen, werden die zugewiesenen Geräte oder Benutzer auf der Seite „Beziehungen“ der Richtlinie hinzugefügt. Sie können auf die Richtlinie klicken, um die Zuweisungen anzuzeigen.

Zum Zuweisen einer Richtlinie können Sie auch das Kommando `policy-assign` im zman-Dienstprogramm verwenden. Weitere Informationen finden Sie unter „Richtlinienkommandos“ im Handbuch *ZENworks: Referenz für Befehlszeilen-Dienstprogramme*.

Weitere Informationen

Weitere Informationen über das Anwenden von Richtlinien finden Sie im Handbuch *ZENworks: Referenz für Konfigurationsrichtlinien*.

Weitere Informationen zum Anwenden von Richtlinien auf Mobilgeräten finden Sie in der *ZENworks Mobile Management Reference* (Referenz zu Mobile Management).

Imaging von Geräten

ZENworks Configuration Management beinhaltet Preboot Services, mit dem Sie vor dem Startvorgang der Betriebssysteme Aufgaben auf den Geräten ausführen können. Mit Preboot Services können Sie die folgenden Aufgaben beim Starten eines Geräts automatisch oder manuell durchführen:

- Ausführen von ZENworks-Imaging-Skripten mit den gleichen Befehlen, die Sie auch über die Bash-Eingabeaufforderung ausführen können
- Erstellen eines Images der Festplatten und anderer Speichergeräte
- Wiederherstellen eines Images auf dem Gerät
- Teilnehmen an einer Sitzung, in der ein vorhandenes Image auf mehrere Geräte angewendet wird, per Multicast
- Erstellen oder Wiederherstellen eines WIM-Images mittels ImageX
- Erstellen oder Wiederherstellen eines Ghost-Image mittels Symantec Ghost

Einige dieser Aufgaben werden automatisch ausgeführt, wenn auf den Geräten PXE (Preboot Execution Environment) aktiviert ist und die Preboot-fähigen Aufgaben im ZENworks-Kontrollzentrum konfiguriert und den Geräten zugewiesen sind. Anschließend können diese Aufgaben automatisch von den Geräten während des Startvorgangs implementiert werden.

Wenn Sie die Aufgaben manuell implementieren möchten, können Sie die Geräte so konfigurieren, dass beim Booten ein Benutzereingriff erforderlich wird.

Mithilfe des ZENworks-Kontrollzentrums können Sie auch die Änderungen am `tftp`-Verzeichnis von einem Primärserver auf andere Imaging-Server (Primärserver oder Satellitengeräte mit der Imaging-Rolle) reproduzieren.

- „Einrichten von Preboot Services“, auf Seite 92
- „Erstellen eines Images“, auf Seite 95

- „Anwenden eines Images“, auf Seite 97
- „Weitere Informationen“, auf Seite 100

Einrichten von Preboot Services

Um Preboot Services zu verwenden, müssen Sie die Aufgaben in den folgenden Abschnitten ausführen:

- „Aktivieren von PXE auf einem Gerät“, auf Seite 92
- „Einrichten eines Imaging-Servers“, auf Seite 92
- „Konfigurieren der Imaging-Einstellungen von Drittanbietern“, auf Seite 92
- „Konfigurieren der Einstellungen eines Drittanbieter-NTFS-Treibers“, auf Seite 95

Aktivieren von PXE auf einem Gerät

Preboot Services benötigen PXE (Preboot eXecution Environment), damit sie auf einem verwalteten Gerät aktiviert werden können, um ein Image zu erstellen oder anzuwenden.

Wenn Sie überprüfen möchten, ob PXE auf einem Gerät aktiviert ist, starten Sie das Gerät neu und wählen Sie die Bootoption (auf den meisten Geräten F12). PXE ist aktiviert, wenn es eine Netzwerk-Bootoption gibt.

Wenn PXE auf einem Gerät nicht aktiviert ist, bearbeiten Sie das BIOS des Geräts, um PXE zu aktivieren. Um sicherzustellen, dass die PXE-Umgebung bei jedem Start des Geräts zur Verfügung steht, können Sie die Bootreihenfolge auch so ändern, dass die Option für die Netzwerkschnittstellenkarte (Network Interface Card, NIC) in der Liste der Bootoptionen vor den anderen Bootoptionen steht.

Einrichten eines Imaging-Servers

Der Imaging-Server ist der PXE-Server, mit dem die PXE-Engine eines Geräts eine Verbindung aufbaut. Damit ZENworks-Server als Imaging-Server fungieren kann, müssen Sie einfach nur den Novell Proxy DHCP-Service auf dem ZENworks-Server starten. Wenn Sie den Dienst starten, sollten Sie auch den Starttyp von „Manuell“ in „Automatisch“ ändern, damit er bei jedem Server-Neuboot startet.

Konfigurieren der Imaging-Einstellungen von Drittanbietern

Wenn Imaging-Lösungen von Drittanbietern verwendet werden sollen, müssen Sie im ZENworks-Kontrollzentrum die Imaging-Einstellungen von Drittanbietern konfigurieren. ZENworks unterstützt die folgenden Imaging-Tools von Drittanbietern:

- Microsoft ImageX, das das Imagedateiformat WIM und WINPE als Verteilung verwendet
- Symantec Ghost, das das Imagedateiformat Ghost und WINPE als Verteilung verwendet

Das Drittanbieter-Imaging von ZENworks unterstützt nur PXE als Bootmechanismus.

So konfigurieren Sie die Einstellungen für das Drittanbieter-Imaging:

1 Installieren Sie ZENworks Configuration Management auf Ihrem Imaging-Server.

Weitere Informationen zum Installieren von ZENworks 2020 finden Sie unter „Installieren eines ZENworks-Primärservers unter Windows“ im Handbuch *ZENworks-Server-Installation*.

2 Konfigurieren Sie die Drittanbieter-Imaging-Einstellungen im ZENworks-Kontrollzentrum.

2a Das Microsoft Windows Automated Installation Kit (WAIK) oder das Windows Assessment and Deployment Kit (WADK) muss auf dem Gerät installiert sein, auf dem das ZENworks-Kontrollzentrum ausgeführt wird.

2b Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Konfiguration**.

2c Klicken Sie im Bereich **Verwaltungszoneneinstellungen** auf **Geräteverwaltung** > **Preboot Services** und anschließend auf den Bereich **Einstellungen für Drittanbieter-Imaging**.

2d **Einstellungen für 32-Bit-Upload:**

WinPE-Basisdistribution hochladen (Windows AIK/Windows ADK erforderlich): Klicken Sie zum Heraufladen der WIM-Imaging-Datei auf das . Führen Sie im Dialogfeld „WIM-Imaging-Datei hochladen“ die folgenden Schritte durch:

1. So laden Sie die 32-Bit-Datei `winpe.wim` herauf:

   Mit dem WAIK: Wechseln Sie im Installationsverzeichnis zum Ordner `Windows AIK\Tools\PETools\x86` und wählen Sie die Datei `winpe.wim` aus.

   Mit dem WADK: Wechseln Sie im Installationsverzeichnis zum Ordner `Windows Kits\<Version>\Assessment and Deployment Kit\Windows Preinstallation Environment\x86\en-us` und wählen Sie die Datei `winpe.wim` aus.

   <Version> bezeichnet dabei eine Windows-Betriebssystemversion.

   HINWEIS: Durch erneutes Hochladen der Datei `winpe.wim` wird die bisherige Instanz dieser Datei vom Server überschrieben.

   ---

2. Klicken Sie auf **OK**.

   Die Imaging-Dateien werden vom Server auf das Gerät heruntergeladen, mit dem Sie auf das ZENworks-Kontrollzentrum zugreifen, und die Datei `winpe.wim` wird mit Imaging-Dateien neu aufgebaut. Anschließend werden die Dateien vom Gerät auf den Server heraufgeladen. Der Fortschritt des Download- und Upload-Prozesses der Dateien wird im Feld **Status** angezeigt.

ImageX-Dateien zur Unterstützung von WIM-Imaging hochladen (ImageX.exe):

1. Klicken Sie auf das , navigieren Sie auf dem Gerät, mit dem Sie auf das ZENworks-Kontrollzentrum zugreifen, zur Microsoft Imaging-Engine (`imagex.exe`) und wählen Sie diese Engine aus.
2. Klicken Sie nach der Konfiguration der Einstellungen für Drittanbieter-Imaging auf **Anwenden**.
3. Klicken Sie auf **Status**, um den Status der Inhaltsreproduktion auf allen Primärservern und Satelliten mit der Imaging-Rolle der Verwaltungszone anzuzeigen. Sie können eine Imaging-Aktion nur starten, wenn der Status „Verfügbar“ lautet.

   HINWEIS: Wenn Sie sowohl 32-Bit- als auch 64-Bit-ImageX-Dateien hochladen, so müssen diese Dateien in verschiedenen Instanzen hochgeladen werden.

Dateien von Ghost 11.5 oder höher zur Unterstützung von Ghost-Imaging heraufladen (Ghost32.exe):

1. Klicken Sie auf das , navigieren Sie auf dem Gerät, mit dem Sie auf das ZENworks-Kontrollzentrum zugreifen, zur Symantec GHOST-Engine (`ghost32.exe`) und wählen Sie diese Engine aus.
2. Klicken Sie nach der Konfiguration der Einstellungen für Drittanbieter-Imaging auf **Anwenden**.
3. Klicken Sie auf **Status**, um den Status der Inhaltsreproduktion auf allen Primärservern und Satelliten mit der Imaging-Rolle der Verwaltungszone anzuzeigen. Sie können eine Imaging-Aktion nur starten, wenn der Status „Verfügbar“ lautet.

2e **Einstellungen für 64-Bit-Upload:**

WinPE-Basisdistribution hochladen (Windows AIK/Windows ADK erforderlich): Klicken Sie zum Heraufladen der WIM-Imaging-Datei auf das . Führen Sie im Dialogfeld „WIM-Imaging-Datei hochladen“ die folgenden Schritte durch:

1. Zum Hochladen der 64-Bit-Datei `winpe.wim` mit dem WADK wechseln Sie im Installationsverzeichnis zum Ordner `Windows Kits\<Version>\Assessment and Deployment Kit\Windows Preinstallation environment\amd64\en-us` und wählen Sie die Datei `winpe.wim` aus. verwenden.

   <Version> bezeichnet dabei eine Windows-Betriebssystemversion.
2. Klicken Sie auf **OK**.

   Die Imaging-Dateien werden vom Server auf das Gerät heruntergeladen, mit dem Sie auf das ZENworks-Kontrollzentrum zugreifen, und die Datei `winpe.wim` wird mit Imaging-Dateien neu aufgebaut. Anschließend werden die Dateien vom Gerät auf den Server heraufgeladen. Der Fortschritt des Download- und Upload-Prozesses der Dateien wird im Feld **Status** angezeigt.

ImageX-Dateien zur Unterstützung von WIM-Imaging hochladen (ImageX.exe):

1. Klicken Sie auf das , navigieren Sie auf dem Gerät, mit dem Sie auf das ZENworks-Kontrollzentrum zugreifen, zur Microsoft Imaging-Engine (`imagex.exe`) und wählen Sie diese Engine aus.
2. Klicken Sie nach der Konfiguration der Einstellungen für Drittanbieter-Imaging auf **Anwenden**.
3. Klicken Sie auf **Status**, um den Status der Inhaltsreproduktion auf allen Primärservern und Satelliten mit der Imaging-Rolle der Verwaltungszone anzuzeigen. Sie können eine Imaging-Aktion nur starten, wenn der Status „Verfügbar“ lautet.

HINWEIS: Wenn Sie sowohl 32-Bit- als auch 64-Bit-ImageX-Dateien hochladen, so müssen diese Dateien in verschiedenen Instanzen hochgeladen werden.

Dateien von Ghost 11.5 oder höher zur Unterstützung von Ghost-Imaging heraufladen (Ghost64.exe):

1. Klicken Sie auf das , navigieren Sie auf dem Gerät, mit dem Sie auf das ZENworks-Kontrollzentrum zugreifen, zur Symantec GHOST-Engine (`ghost64.exe`) und wählen Sie diese Engine aus.

2. Klicken Sie nach der Konfiguration der Einstellungen für Drittanbieter-Imaging auf **Anwenden**.
3. Klicken Sie auf **Status**, um den Status der Inhaltsreproduktion auf allen Primärservern und Satelliten mit der Imaging-Rolle der Verwaltungszone anzuzeigen. Sie können eine Imaging-Aktion nur starten, wenn der Status „Verfügbar“ lautet.

3 Aktivieren Sie PXE auf dem Gerät.

4 Vergewissern Sie sich, dass Sie einen DHCP-Standardserver auf dem Imaging-Server oder auf einem anderen Netzwerkserver verwenden.

Konfigurieren der Einstellungen eines Drittanbieter-NTFS-Treibers

Sie können den neuesten leistungsfähigen NTFS-Treiber herunterladen und auf Ihrem System speichern. Sie können den Inhaltsreproduktionsstatus auf allen Primär- und Satellitenservern mit der Imaging-Rolle in der Verwaltungszone anzeigen. Sie können eine Imaging-Aktion über den Drittanbieter-NTFS-Treiber starten, wenn der Status „Verfügbar“ lautet.

Zum Konfigurieren dieser Einstellungen klicken Sie im linken Bereich auf **Konfiguration**, um die Registerkarte **Konfiguration** anzuzeigen. Klicken Sie auf **Verwaltungszoneneinstellungen**, klicken Sie dann auf **Geräteverwaltung** > **Preboot Services**, um die Seite „Preboot Services“ anzuzeigen.

Erstellen eines Images

Sie können ZENworks-Images mit ZENworks Imaging auf einem Gerät erstellen und wiederherstellen, und das Drittanbieter-Imaging-Dienstprogramm von ZENworks ermöglicht das Erstellen und Wiederherstellen von Drittanbieter-Images. Mit diesem Programm können Sie ein Image im Windows Imaging(WIM)- oder Ghost Imaging-Format erstellen und auf einem lokalen Gerät oder Server wiederherstellen.

1 Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Geräte**.

2 Durchsuchen Sie die Ordner `Server` oder `Arbeitsstationen`, bis Sie das Gerät finden, vom dem Sie ein Image erstellen möchten.

3 Klicken Sie auf das Gerät, um seine Details anzuzeigen.

4 Klicken Sie in der Aufgabenliste im linken Navigationsbereich auf **Image erstellen**, um den Assistenten zum Erstellen eines Images zu starten.

5 Füllen Sie auf der Seite mit den Dateiinformationen die folgenden Felder aus, und klicken Sie dann auf **Weiter**.

Geben Sie Folgendes für ZENworks Imaging an:

Image-Format: Wählen Sie das Format des Image aus, das für das Gerät verwendet werden soll

Server- und Dateipfad: Klicken Sie auf , um das Dialogfeld „Server- und Pfadinformationen“ zu öffnen. Konfigurieren Sie die folgenden Optionen.

- **Serverobjekt, IP oder DNS:** Klicken Sie auf , um das Objekt, die IP-Adresse oder den DNS-Namen des Primärservers oder des Geräts, das auf die Imaging-Serverrolle hochgestuft wird, zu suchen und auszuwählen.
- **Dateipfad auf Server:** Klicken Sie auf , um nach einer Imagedatei zu suchen und diese auszuwählen. Bei der Imagedatei muss es sich um eine gültige ZENworks-Imagedatei handeln, sie muss also die Erweiterung `.zmg` haben.

HINWEIS: Sie können nicht zu dem angegebenen Dateisystem navigieren, wenn mehrere Suchdomänen mit DHCP für Linux konfiguriert sind und wenn sich der Server auf Windows befindet.

Geben Sie Folgendes für das Drittanbieter-Imaging an:

Freigegebener Netzwerkpfad der Imagedatei: Geben Sie den freigegebenen Netzwerkpfad an, in dem die `.wim`- oder `.gho`-Datei gespeichert werden soll. Das Verzeichnis muss eine Windows-Freigabe oder eine Linux SMB- bzw. CIFS-Freigabe sein.

Wenn auf diesem Gerät die Novell File Upload-Erweiterung nicht installiert ist, müssen Sie zunächst die Installation vornehmen, um die zu installierenden Verzeichnisse hochladen zu können.

Imagedateiname: Geben Sie den Dateinamen an, unter dem die `.wim`- oder `.gho`-Datei gespeichert werden soll. Diese Option wird nur angezeigt für das Windows-Imaging-Format (`.wim`) und das GHOST-Imaging-Format (`.gho`).

Netzwerk-Berechtigungsnachweis: Klicken Sie auf  , um die Netzwerk-Berechtigungsnachweise zu suchen und auszuwählen, die für den Zugriff auf das Gerät, auf dem die `.wim`-Dateien gespeichert sind, verwendet werden sollen. Diese Option wird nur für das Windows-Image-Format (`.wim`) und das Ghost-Image-Format (`.gho`) angezeigt.

Komprimierung verwenden: Eine Komprimierung ist erforderlich. Wählen Sie eine der folgenden Optionen aus:

- **Ausgewogen:** Stellt für die Komprimierung automatisch das bestmögliche Verhältnis zwischen der durchschnittlichen Zurückspielgeschwindigkeit und dem verfügbaren Speicherplatz für die Imagedatei her. Diese Option wird nur für das ZENworks-Image-Format angezeigt
- **Keine:** Diese Option wird nur für das Windows-Image-Format und das Ghost-Image-Format angezeigt.
- **Zeitoptimiert:** Optimiert die Komprimierung, um ein schnellstmögliches Zurückspielen des Image zu ermöglichen. Wählen Sie diese Option aus, wenn CPU-Geschwindigkeit ein Problem ist.
- **Platzoptimiert:** Optimiert die Komprimierung, um die Größe der Imagedatei zu minimieren und so Speicherplatz zu sparen. Dies kann dazu führen, dass das Neueinspielen des Image mehr Zeit benötigt.

Ausgewogen ist die Standardoption für das ZENworks-Image-Format und **Zeitoptimiert** ist die Standardoption für das Windows-Image-Format und das GHOST-Image-Format.

Image-Bundle erstellen: Lassen Sie dieses Feld deaktiviert.

6 Überprüfen Sie die Informationen auf der Dateizusammenfassungsseite, klicken Sie auf **Fertig** und dann auf **OK**.

Da Imaging-Aufgaben von Preboot Services ausgeführt werden, wird das Image des Geräts beim nächsten Neustart des Geräts erstellt. Im Imaging-Bereich, den Sie auf der Zusammenfassungsseite des Geräts finden, wird angezeigt, dass die Arbeit geplant ist. Nach Abschluss der Arbeit wird die Aufgabe aus diesem Bereich entfernt.

7 Um das Gerät unverzüglich zu starten und die Imaging-Arbeit zu beginnen, klicken Sie im linken Navigationsbereich auf **Arbeitsstation neu booten/herunterfahren** (oder auf **Server neu booten/herunterfahren**).

Die zum Erstellen des Image benötigte Zeit hängt von der Größe der Laufwerke des Geräts ab.

Anwenden eines Images

Zum Anwenden eines Images auf ein Gerät verwenden Sie den Assistenten zum Erstellen neuer Bundles und erstellen ein Imaging-Bundle. Das Bundle enthält das Image, das Sie anwenden möchten. Außer beim Erstellen des Bundles unterstützt Sie der Assistent auch beim Zuweisen des Bundles zu Geräten. Nach dem Erstellen des Imaging-Bundles starten Sie den Imaging-Prozess.

- „Erstellen des ZENworks Image-Bundles“, auf Seite 97
- „Erstellen des Drittanbieter-Image-Bundles“, auf Seite 98
- „Initiieren des Imaging-Vorgangs“, auf Seite 99

 In den folgenden Videos wird die Bereitstellung von Windows 7- und Linux-Images auf Geräten erläutert:

- Bereitstellen eines Windows 7-Image mit ZENworks
- Bereitstellen von Linux mit ZENworks

Erstellen des ZENworks Image-Bundles

Um ZENworks-Images auf einem Gerät wiederherstellen zu können, müssen Sie ein ZENworks Image-Bundle erstellen.

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Bundles**.
2. Klicken Sie im Bundles-Bereich auf **Neu** > **Bundle**, um den Assistenten zum Erstellen neuer Bundles zu starten.
3. Wählen Sie auf der Seite „Bundle-Typ auswählen“ die Option **Preboot-Bundle** und klicken Sie dann auf **Weiter**.
4. Wählen Sie auf der Seite „Bundle-Kategorie auswählen“ die Option **ZENworks-Image** aus und klicken Sie anschließend auf **Weiter**.
5. Schließen Sie den Assistenten mithilfe der Informationen aus der folgenden Tabelle ab, um die Felder auszufüllen.

Assistentenseite	Details
Seite „Details definieren“	Geben Sie einen Namen für die Aufgabe ein. Der Name darf keines der folgenden ungültigen Zeichen enthalten: / \ * ? : „ ' < > | ` % ~

Assistentenseite	Details
Seite „ZENworks-Imagedatei auswählen“	So wählen Sie die Imagedatei aus: 1. Klicken Sie auf , um das Dialogfeld „Server- und Pfadinformationen“ zu öffnen. 2. Füllen Sie die folgenden Felder aus: **Geräteobjekt, IP oder DNS:** Wählen Sie den ZENworks-Server aus, auf dem Sie das Image gespeichert haben. **Dateipfad auf Server:** Suchen Sie die Imagedatei und wählen Sie sie aus. Das standardmäßige Speicherverzeichnis für Imagedateien ist `\Novell\ZENworks\work\content-repo\images`. 3. Klicken Sie auf **OK**.
Seite „Zusammenfassung“	Klicken Sie auf **Weiter**, um den Assistenten fortzusetzen und das Bundle dem Zielgerät zuzuweisen.
Seite „Bundle-Gruppen“	Sie sollten das Image-Bundle keiner Gruppe zuweisen. Klicken Sie auf **Weiter**, um diese Seite zu überspringen.
Seite „Zuweisungen hinzufügen“	Wählen Sie das Gerät aus, auf dem Sie das Image anwenden möchten.
Seite „Zeitpläne“	Sie sollten dem Image-Bundle keinen Zeitplan zuweisen. Klicken Sie auf **Weiter**, um diese Seite zu überspringen.
Seite „Fertig stellen“	Klicken Sie auf **Fertig stellen**, um das Bundle zu erstellen und dem ausgewählten Gerät zuzuweisen.

Erstellen des Drittanbieter-Image-Bundles

Um Drittanbieter-Images wiederherstellen zu können, müssen Sie ein Drittanbieter-Image-Bundle erstellen.

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Bundles**.
2. Klicken Sie im Bundles-Bereich auf **Neu** > **Bundle**, um den Assistenten zum Erstellen neuer Bundles zu starten.
3. Wählen Sie auf der Seite „Bundle-Typ auswählen“ die Option **Preboot-Bundle** und klicken Sie dann auf **Weiter**.
4. Klicken Sie auf der Seite „Bundle-Kategorie auswählen“ auf **Drittanbieter-Image** und anschließend auf **Weiter**.
5. Schließen Sie den Assistenten mithilfe der Informationen aus der folgenden Tabelle ab, um die Felder auszufüllen.

Assistentenseite	Details
Seite „Details definieren“	Geben Sie einen Namen für die Aufgabe ein. Der Name darf keines der folgenden ungültigen Zeichen enthalten: / \ * ? : „ ' < > | ` % ~

Assistentenseite	Details
Seite „Datei mit einem Drittanbieter-Image auswählen“	So wählen Sie eine Datei mit einem Drittanbieter-Image aus: 1. Wählen Sie den Image-Typ für das Bundle aus. In ZENworks Configuration Management stehen nur das Windows-Image-Format (`.wim`) und das Ghost-Image-Format (`.gho`) zur Verfügung. 2. Geben Sie das freigegebene Netzwerkverzeichnis an, in dem sich die `.wim`- oder `.gho`-Dateien befinden. Das Verzeichnis muss eine Windows-Freigabe oder eine Linux SMB- bzw. CIFS-Freigabe sein. 3. Klicken Sie auf  , um die Netzwerk-Berechtigungsnachweise zu suchen und auszuwählen, die für den Zugriff auf das Gerät, auf dem die `.wim`- oder `.gho`-Dateien gespeichert sind, verwendet werden sollen. 4. Wenn das WIM-Bundle als Zusatzimage verwendet werden soll, wählen Sie **WIM als Zusatzimage wiederherstellen** aus und konfigurieren Sie die folgenden Optionen: **Image-Nummer (nur WIM):** Wählen Sie die Index-Nummer des wiederherzustellenden Image aus. **Pfad für Wiederherstellung des Zusatzimage:** Geben Sie das Verzeichnis auf dem Gerät an, in dem das Zusatzimage wiederhergestellt werden soll. 5. Klicken Sie auf **OK**.
Seite „Zusammenfassung“	Klicken Sie auf **Weiter**, um den Assistenten fortzusetzen und das Bundle dem Zielgerät zuzuweisen.
Seite „Bundle-Gruppen“	Sie sollten das Image-Bundle keiner Gruppe zuweisen. Klicken Sie auf **Weiter**, um diese Seite zu überspringen.
Seite „Zuweisungen hinzufügen“	Wählen Sie das Gerät aus, auf dem Sie das Image anwenden möchten.
Seite „Zeitpläne“	Sie sollten dem Image-Bundle keinen Zeitplan zuweisen. Klicken Sie auf **Weiter**, um diese Seite zu überspringen.
Seite „Fertig stellen“	Klicken Sie auf **Fertig stellen**, um das Bundle zu erstellen und dem ausgewählten Gerät zuzuweisen.

Initiieren des Imaging-Vorgangs

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Geräte**.
2. Durchsuchen Sie die Ordner `Server` oder `Arbeitsstationen`, bis Sie das Gerät gefunden haben, auf dem Sie das Image anwenden möchten.
3. Klicken Sie auf das Gerät, um seine Details anzuzeigen.
4. Klicken Sie in der Aufgabenliste im linken Navigationsbereich auf **Zugewiesenes Imaging-Bundle anwenden**, um den Vorgang zu planen.

Da Imaging-Aufgaben von Preboot Services ausgeführt werden, wird das Image beim nächsten Neustart des Geräts auf das Gerät angewendet. Im Imaging-Bereich, den Sie auf der Zusammenfassungsseite des Geräts finden, wird angezeigt, dass die Arbeit geplant ist. Nach Abschluss der Arbeit wird die Aufgabe aus diesem Bereich entfernt.

5 Um das Gerät unverzüglich zu starten und die Imaging-Arbeit zu beginnen, klicken Sie im linken Navigationsbereich auf **Arbeitsstation neu booten/herunterfahren** (oder auf **Server neu booten/herunterfahren**).

Weitere Informationen

Weitere Informationen über Imaging und Preboot Services finden Sie im Handbuch *Novell ZENworks – Referenz für Preboot Services und Imaging*.

Fernverwalten von Geräten

ZENworks Configuration Management stellt Fernverwaltungsfunktionen bereit, mit denen Sie Geräte fernverwalten können. Das Modul für die Fernverwaltung unterstützt folgende entfernten Vorgänge:

Fernvorgang	Beschreibung	Zusätzliche Details
Fernsteuerung	Ermöglicht es Ihnen, ein verwaltetes Gerät von der Verwaltungskonsole aus zu steuern, um Benutzer zu unterstützen und beim Lösen von Problemen zu helfen. Sie können alle Vorgänge ausführen, die auch ein Benutzer auf dem Gerät ausführen kann. Weitere Informationen zur Fernsteuerung eines Windows-Geräts finden Sie unter „Durchführen von Vorgängen für die Fernsteuerung, die Fernansicht und die Fernausführung auf einem Windows-Gerät“, auf Seite 104. Weitere Informationen zur Fernsteuerung eines Linux-Geräts finden Sie unter „Durchführen von Fernsteuerungs-, Fernansichts- und Fernanmeldungsvorgängen auf einem Linux-Gerät“, auf Seite 109.	

Fernvorgang	Beschreibung	Zusätzliche Details
Fernansicht	Ermöglicht es Ihnen, eine Verbindung zu einem verwalteten Gerät so aufzubauen, dass Sie das verwaltete Gerät sehen anstatt es zu steuern. Auf diese Weise können Sie Benutzern bei der Lösung auftretender Probleme behilflich sein. Beispielsweise können Sie überprüfen, wie der Benutzer an einem verwalteten Gerät bestimmte Aufgaben erledigt, um sicherzustellen, dass eine Aufgabe korrekt ausgeführt wird. Weitere Informationen zur Fernansicht eines Windows-Geräts finden Sie unter „Durchführen von Vorgängen für die Fernsteuerung, die Fernansicht und die Fernausführung auf einem Windows-Gerät“, auf Seite 104. Weitere Informationen zur Fernansicht eines Linux-Geräts finden Sie unter „Durchführen von Fernsteuerungs-, Fernansichts- und Fernanmeldungsvorgängen auf einem Linux-Gerät“, auf Seite 109.	
Fernausführung	Ermöglicht es Ihnen, über die Verwaltungskonsole beliebige ausführbare Dateien auf einem verwalteten Gerät auszuführen. Für die entfernte Ausführung einer Anwendung geben Sie den Namen der ausführbaren Datei im Dialogfeld „Fernausführung“ an. Wenn die Anwendung auf dem verwalteten Gerät nicht unter dem Systempfad zu finden ist, geben Sie den vollständigen Pfad der Anwendung an. Sie können beispielsweise den Befehl `regedit` ausführen, um auf dem verwalteten Gerät den Registrierungseditor zu öffnen. Im Dialogfeld „Remoteausführung“ wird der Status der Befehlsausführung angezeigt. Weitere Informationen zur Fernausführung eines Windows-Geräts finden Sie unter „Durchführen von Vorgängen für die Fernsteuerung, die Fernansicht und die Fernausführung auf einem Windows-Gerät“, auf Seite 104.	Dieser Vorgang wird nur auf verwalteten Windows-Geräten unterstützt.

Fernvorgang	Beschreibung	Zusätzliche Details
Ferndiagnose	Ermöglicht es Ihnen, die Probleme auf einem verwalteten Gerät zu diagnostizieren und zu analysieren. Hiermit können Sie die Zeiten für die Problemlösung verkürzen und Benutzern Unterstützung bieten, ohne das jeweilige Gerät aufzusuchen. Dadurch wird die Benutzerproduktivität erhöht, da auf den Desktops ohne Unterbrechung weitergearbeitet werden kann. Weitere Informationen zur Ferndiagnose eines Geräts finden Sie unter „Durchführen von Vorgängen zur Ferndiagnose“, auf Seite 106.	Dieser Vorgang wird nur auf verwalteten Windows-Geräten unterstützt.
Dateiübertragung	Ermöglicht Ihnen, Dateien zwischen der Verwaltungskonsole und einem verwalteten Gerät zu übertragen. Weitere Informationen zur Dateiübertragung finden Sie unter „Durchführen von Vorgängen zur Dateiübertragung“, auf Seite 108.	Dieser Vorgang wird nur auf verwalteten Windows-Geräten unterstützt.
Fernanmeldung	Ermöglicht die Anmeldung bei einem verwalteten Gerät über die Verwaltungskonsole und das Starten einer neuen grafischen Sitzung, ohne dass der Benutzer am verwalteten Gerät gestört wird. Der Benutzer am verwalteten Gerät kann allerdings nicht die Fernanmeldungssitzung anzeigen. Weitere Informationen zur Fernanmeldung auf einem Linux-Geräts finden Sie unter „Durchführen von Fernsteuerungs-, Fernansichts- und Fernanmeldungsvorgängen auf einem Linux-Gerät“, auf Seite 109.	Dieser Vorgang wird nur auf verwalteten Linux-Geräten unterstützt. Melden Sie sich mit einem Nicht-`Root`-Berechtigungsnachweis beim Gerät an.
Remote-SSH	Hier können Sie eine sichere Verbindung zu einem entfernten Linux-Gerät herstellen und sicher Befehle auf dem Gerät ausführen. Weitere Informationen zur Fernanmeldung auf einem Linux-Gerät finden Sie unter „Durchführen eines Fern-SSH-Vorgangs auf einem Linux-Gerät“, auf Seite 110.	Dieser Vorgang wird nur auf verwalteten Linux-Geräten unterstützt.

In folgenden Abschnitten wird erläutert, wie das Modul für die Fernverwaltung eingerichtet wird und die einzelnen Vorgänge ausgeführt werden:

- „Erstellen von Fernverwaltungsrichtlinien“, auf Seite 103
- „Konfigurieren von Fernverwaltungseinstellungen“, auf Seite 104
- „Durchführen von Vorgängen für die Fernsteuerung, die Fernansicht und die Fernausführung auf einem Windows-Gerät“, auf Seite 104
- „Durchführen von Vorgängen zur Ferndiagnose“, auf Seite 106
- „Durchführen von Vorgängen zur Dateiübertragung“, auf Seite 108

- „Durchführen von Fernsteuerungs-, Fernansichts- und Fernanmeldungsvorgängen auf einem Linux-Gerät“, auf Seite 109
- „Durchführen eines Fern-SSH-Vorgangs auf einem Linux-Gerät“, auf Seite 110
- „Weitere Informationen“, auf Seite 110

 Betrachten Sie ein Video über die Fernverwaltung von Geräten.

Erstellen von Fernverwaltungsrichtlinien

Standardmäßig wird auf dem verwalteten Gerät eine sichere Fernverwaltungsrichtlinie erstellt, wenn ZENworks Agent mit der Fernverwaltungskomponente auf dem Gerät bereitgestellt wird. Die Standardrichtlinie kann zur Fernverwaltung eines Geräts verwendet werden. Mithilfe der Standardrichtlinie können alle Fernverwaltungsvorgänge auf einem Gerät ausgeführt werden. Um die Standardrichtlinie zu überschreiben, kann eine Fernverwaltungsrichtlinie explizit für das Gerät erstellt werden.

Eine Fernverwaltungsrichtlinie kann Geräten oder Benutzern zugewiesen werden.

So erstellen Sie eine Fernverwaltungsrichtlinie:

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Richtlinien**.
2. Klicken Sie im Richtlinienbereich auf **Neu** > **Richtlinie**, um den Assistenten zum Erstellen neuer Richtlinien zu starten.
3. Wählen Sie **Windows-Konfigurationsrichtlinien** und klicken Sie dann auf **Weiter**.
4. Folgen Sie den Eingabeaufforderungen, um die Fernverwaltungsrichtlinie zu erstellen.

   Klicken Sie auf den einzelnen Seiten des Assistenten auf die Schaltfläche **Hilfe**, um detaillierte Informationen zur jeweiligen Seite anzuzeigen. Wenn Sie den Assistenten fertig stellen, wird die Richtlinie dem Richtlinienbereich hinzugefügt. Sie können auf die Richtlinie klicken, um ihre Details anzuzeigen und um Zuweisungen, Zeitpläne usw. zu modifizieren.
5. Weisen Sie die Fernverwaltungsrichtlinie Benutzern und Geräten zu:
   - **5a** Aktivieren Sie in der Kontrollleiste „Richtlinien“ das Kontrollkästchen neben der Richtlinie.
   - **5b** Klicken Sie auf **Aktion** > **Zu Gerät zuweisen**.

     oder

     Klicken Sie auf **Aktion** > **Benutzer zuweisen.**
   - **5c** Folgen Sie den Eingabeaufforderungen, um die Richtlinie zuzuweisen.

     Klicken Sie auf den einzelnen Seiten des Assistenten auf die Schaltfläche **Hilfe**, um detaillierte Informationen zur jeweiligen Seite anzuzeigen.

     Wenn Sie den Assistenten fertig stellen, werden die zugewiesenen Geräte oder Benutzer auf der Seite „Beziehungen“ der Richtlinie hinzugefügt. Sie können auf die Richtlinie klicken, um die Zuweisungen anzuzeigen.

Konfigurieren von Fernverwaltungseinstellungen

Im Bereich mit den Fernverwaltungs-Konfigurationseinstellungen auf der Seite „Konfiguration“ können Sie u. a. Einstellungen hinsichtlich des Fernverwaltungs-Ports, der Sitzungsleistung und der verfügbaren Diagnoseanwendungen angeben.

Diese Einstellungen sind gemäß der gängigsten Konfiguration vordefiniert. Gehen Sie folgendermaßen vor, wenn Sie die Einstellungen ändern möchten:

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Konfiguration**.
2. Wählen Sie im Bereich „Verwaltungszoneneinstellungen“ die Optionsfolge **Geräteverwaltung** > **Fernverwaltung**.
3. Bearbeiten Sie die Einstellungen nach Bedarf.

   Klicken Sie auf die Schaltfläche **Hilfe**, um ausführliche Informationen zur jeweiligen Seite zu erhalten.
4. Wenn Sie die Bearbeitung der Einstellungen abgeschlossen haben, klicken Sie auf **Anwenden** bzw. **OK**, um die vorgenommenen Änderungen zu speichern.

Durchführen von Vorgängen für die Fernsteuerung, die Fernansicht und die Fernausführung auf einem Windows-Gerät

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Geräte**.
2. Navigieren Sie im Ordner `Server` oder `Arbeitsstationen` zu dem Gerät, das Sie verwalten möchten.
3. Wählen Sie das Gerät aus, indem Sie das Kontrollkästchen vor dem Gerät markieren.
4. Klicken Sie in der Taskliste im linken Navigationsbereich auf **Arbeitsstation fernsteuern** oder **Server fernsteuern**, um das Dialogfeld „Fernverwaltung“ zu öffnen.
5. Füllen Sie im Dialogfeld „Fernverwaltung“ die folgenden Felder aus:

   Gerät: Geben Sie den Namen oder die IP-Adresse des Gerätes an, das Sie dezentral verwalten möchten.

   Für alle Geräte immer standardmäßig die IP-Adresse verwenden: Wählen Sie dies aus, wenn im System die IP-Adresse des Geräts anstelle des DNS-Namens angezeigt werden soll.

   Die Werte, die Sie für den Zugriff auf ein Gerät während eines Fernsteuerungsvorgangs angeben, werden im System gespeichert, sobald Sie auf **OK** klicken. Einige dieser Werte werden in Abhängigkeit vom Gerät bzw. dem Fernoperator automatisch während der nachfolgenden Fernsteuerungsvorgänge ausgewählt.

   Operation: Wählen Sie die Art des entfernten Vorgangs (Fernsteuerung, Fernansicht oder Fernausführung) aus, den Sie auf dem verwalteten Gerät durchführen möchten:

   Authentifizierung: Wählen Sie den gewünschten Modus aus, um sich am verwalteten Gerät zu authentifizieren. Es stehen zwei Optionen zur Verfügung:

   - **Passwort:** Stellt eine auf einem Passwort basierende Authentifizierung zum Durchführen eines Fernsteuervorgangs bereit. Sie müssen das korrekte Passwort eingeben, das vom Benutzer auf dem verwalteten Gerät festgelegt oder vom Administrator in den Sicherheitseinstellungen der Fernverwaltungsrichtlinie konfiguriert wurde. Das vom Benutzer festgelegte Passwort hat Vorrang vor dem vom Administrator konfigurierten Passwort.

- **Rechte:** Diese Option ist nur dann verfügbar, wenn Sie das verwaltete Gerät ausgewählt haben, auf dem Sie den Fernvorgang durchführen möchten. Wenn Ihnen der Administrator bereits Fernverwaltungsrechte erteilt hat, um den gewünschten Fernvorgang auf dem ausgewählten verwalteten Gerät durchzuführen, erhalten Sie automatisch Zugriff, wenn die Sitzung gestartet wird.

Port: Geben Sie die Nummer des Ports an, den der Fernverwaltungsagent überwacht. Standardmäßig lautet die Portnummer 5950.

Sitzungsmodus: Wählen Sie einen der folgenden Modi für die Sitzung aus:

- **Zusammenarbeit:** Mithilfe dieser Option können Sie eine Fernsteuerungssitzung und Fernansichtssitzung im Modus „Zusammenarbeit“ starten. Es ist jedoch nicht möglich, als Erstes eine Fernansichtssitzung auf dem verwalteten Gerät zu starten. Wenn Sie die Fernsteuerungssitzung auf dem verwalteten Gerät starten, erhalten Sie alle Privilegien eines Master-Fernoperators, darunter folgende:
  - Einladen anderer Fernoperatoren zur Teilnahme an der Fernsitzung.
  - Delegieren von Fernsteuerungsrechten an einen Fernoperator.
  - Wiedererlangen der Steuerung vom Fernoperator.
  - Beenden einer Fernsitzung

  Nachdem die Fernsteuerungssitzung für das verwaltete Gerät im Zusammenarbeitsmodus eingerichtet wurde, handelt es sich bei den anderen Fernsitzungen auf dem verwalteten Gerät und Fernansichtssitzungen.
- **Freigegeben:** Ermöglicht mehreren Fernoperatoren gleichzeitig die Steuerung des verwalteten Geräts.
- **Exklusiv:** Ermöglicht Ihnen eine exklusive Fernsitzung auf dem verwalteten Gerät Nachdem eine Sitzung im exklusiven Modus gestartet wurde, kann keine andere Fernsitzung auf dem verwalteten Gerät gestartet werden.

Sitzungsverschlüsselung: Gewährleistet, dass die Fernsitzung mithilfe der SSL(Secure Sockets Layer)-Verschlüsselung (TLSv1-Protokoll) geschützt wird.

Caching aktivieren: Dadurch können entfernte Verwaltungssitzungsdaten im Cache gespeichert werden, um die Geschwindigkeit zu erhöhen. Diese Option steht nur für den Vorgang der Fernsteuerung zur Verfügung. Diese Option wird zurzeit nur auf Windows unterstützt.

Dynamische Bandbreitenoptimierung: Verbessert die Leistung durch Erkennung der verfügbaren Netzwerkbandbreite und Anpassung der Sitzungseinstellungen an die erkannte Bandbreite. Diese Option steht nur für den Vorgang der Fernsteuerung zur Verfügung.

Protokollierung aktivieren: Protokolliert Informationen zur Sitzung und zum Debugging in der Datei `novell-zenworks-vncviewer.txt`. Die Datei wird standardmäßig auf dem Desktop gespeichert, wenn Sie das ZENworks-Kontrollzentrum über Internet Explorer starten. Sie wird im Mozilla-Installationsverzeichnis gespeichert, wenn Sie das ZENworks-Kontrollzentrum über Mozilla Firefox starten.

Durch Proxy weiterleiten: Ermöglicht, dass der Fernverwaltungsbetrieb des verwalteten Geräts durch einen Proxyserver geleitet werden kann. Wenn sich das verwaltete Gerät in einem privaten Netzwerk oder auf der anderen Seite einer Firewall oder eines Routers befindet, die/der NAT (Network Address Translation) verwendet, kann der Fernverwaltungsbetrieb des Geräts durch einen Proxy-Server geleitet werden. Füllen Sie die folgenden Felder aus:

- **Proxy:** Geben Sie den DNS-Namen bzw. die IP-Adresse des Proxyservers an. Standardmäßig wird der Proxyserver, der in der Kontrollleiste Proxy-Einstellungen für den Fernbetrieb auf dem Gerät konfiguriert wurde, in diesem Feld eingegeben. Sie können einen anderen Proxyserver angeben.
- **Proxy-Port:** Geben Sie die Portnummer an, die der Proxyserver überwacht. Standardmäßig lautet die Portnummer 5750.

Das folgende Schlüsselpaar zur Identifizierung verwenden: Wenn eine interne Zertifizierungsstelle (CA) genutzt wird, werden die folgenden Optionen nicht angezeigt. Wenn eine externe Zertifizierungsstelle (CA) genutzt wird, füllen Sie die folgenden Felder aus:

- **Privater Schlüssel:** Klicken Sie auf **Durchsuchen**, um zum privaten Schlüssel des Fernoperators zu navigieren und diesen auszuwählen.
- **Zertifikat:** Klicken Sie auf **Durchsuchen**, um zum Zertifikat zu navigieren, das dem privaten Schlüssel entspricht, und dieses auszuwählen. Dieses Zertifikat muss mit der Zertifizierungsstelle verknüpft sein, die für die Zone konfiguriert ist.

  Die unterstützten Formate für den Schlüssel und das Zertifikat lauten DER und PEM.

Fernverwaltungs-Viewer installieren: Klicken Sie auf den Link **Fernverwaltungs-Viewer installieren**, um das Fernverwaltungs-Anzeigeprogramm zu installieren. Dieser Link wird nur angezeigt, wenn Sie die Fernverwaltungssitzung auf dem verwalteten Gerät erstmalig durchführen, oder wenn der Fernverwaltungs-Viewer nicht auf dem verwalteten Gerät installiert ist.

6 Klicken Sie auf **OK**, um die Sitzung zu starten.

Durchführen von Vorgängen zur Ferndiagnose

1 Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Geräte**.

2 Navigieren Sie im Ordner `Server` oder `Arbeitsstationen` zu dem Gerät, das Sie verwalten möchten.

3 Wählen Sie das Gerät aus, indem Sie das Kontrollkästchen vor dem Gerät markieren.

4 Klicken Sie in der Aufgabenliste im linken Navigationsbereich auf **Ferndiagnose**, um das Dialogfeld „Ferndiagnose“ anzuzeigen.

5 Füllen Sie im Dialogfeld „Ferndiagnose“ folgenden Felder aus:

Gerät: Geben Sie den Namen oder die IP-Adresse des Gerätes an, das Sie ferndiagnostizieren möchten.

Für alle Geräte immer standardmäßig die IP-Adresse verwenden: Wählen Sie dies aus, wenn im System die IP-Adresse des Geräts anstelle des DNS-Namens angezeigt werden soll.

Die Werte, die Sie für den Zugriff auf ein Gerät während eines Fernsteuerungsvorgangs angeben, werden im System gespeichert, sobald Sie auf **OK** klicken. Einige dieser Werte werden in Abhängigkeit vom Gerät bzw. dem Fernoperator automatisch während der nachfolgenden Fernsteuerungsvorgänge ausgewählt.

Anwendung: Wählen Sie die Anwendung aus, die Sie auf dem Gerät für die Ferndiagnose verwenden möchten.

Authentifizierung: Wählen Sie den gewünschten Modus aus, um sich am verwalteten Gerät zu authentifizieren. Es stehen zwei Optionen zur Verfügung:

- **Passwort:** Stellt eine auf einem Passwort basierende Authentifizierung zum Durchführen eines Ferndiagnosevorgangs bereit. Sie müssen das korrekte Passwort eingeben, das vom Benutzer auf dem verwalteten Gerät festgelegt oder vom Administrator in den Sicherheitseinstellungen der Fernverwaltungsrichtlinie konfiguriert wurde. Das vom Benutzer festgelegte Passwort hat Vorrang vor dem vom Administrator konfigurierten Passwort.
- **Rechte:** Diese Option ist nur dann verfügbar, wenn Sie das verwaltete Gerät ausgewählt haben, auf dem Sie den Fernvorgang durchführen möchten. Wenn Ihnen der Administrator bereits Fernverwaltungsrechte erteilt hat, um den gewünschten Fernvorgang auf dem ausgewählten verwalteten Gerät durchzuführen, erhalten Sie automatisch Zugriff, wenn die Sitzung gestartet wird.

Port: Geben Sie die Nummer des Ports an, den der Fernverwaltungsagent überwacht. Standardmäßig lautet die Portnummer 5950.

Sitzungsmodus: Ist für den Ferndiagnosevorgang nicht relevant.

Sitzungsverschlüsselung: Gewährleistet, dass die Fernsitzung mithilfe der SSL(Secure Sockets Layer)-Verschlüsselung (TLSv1-Protokoll) geschützt wird.

Caching aktivieren: Dadurch können entfernte Verwaltungssitzungsdaten im Cache gespeichert werden, um die Geschwindigkeit zu erhöhen. Diese Option wird zurzeit nur auf Windows unterstützt.

Dynamische Bandbreitenoptimierung: Mithilfe dieser Option kann die verfügbare Netzwerkbandbreite erkannt und die Sitzungseinstellungen zur Erhöhung der Geschwindigkeit angepasst werden.

Protokollierung aktivieren: Protokolliert Informationen zur Sitzung und zum Debugging in der Datei `novell-zenworks-vncviewer.txt`. Die Datei wird standardmäßig auf dem Desktop gespeichert, wenn Sie das ZENworks-Kontrollzentrum über Internet Explorer starten. Sie wird im Mozilla-Installationsverzeichnis gespeichert, wenn Sie das ZENworks-Kontrollzentrum über Mozilla Firefox starten.

Durch Proxy weiterleiten: Ermöglicht, dass der Fernverwaltungsbetrieb des verwalteten Geräts durch einen Proxyserver geleitet werden kann. Wenn sich das verwaltete Gerät in einem privaten Netzwerk oder auf der anderen Seite einer Firewall oder eines Routers befindet, die/der NAT (Network Address Translation) verwendet, kann der Fernverwaltungsbetrieb des Geräts durch einen Proxy-Server geleitet werden. Füllen Sie die folgenden Felder aus:

- **Proxy:** Geben Sie den DNS-Namen bzw. die IP-Adresse des Proxyservers an. Standardmäßig wird der Proxyserver, der in der Kontrollleiste Proxy-Einstellungen für den Fernbetrieb auf dem Gerät konfiguriert wurde, in diesem Feld eingegeben. Sie können einen anderen Proxyserver angeben.
- **Proxy-Port:** Geben Sie die Portnummer an, die der Proxyserver überwacht. Standardmäßig lautet die Portnummer 5750.

6 Klicken Sie auf **OK**, um die Sitzung zu starten.

Durchführen von Vorgängen zur Dateiübertragung

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Geräte**.
2. Navigieren Sie im Ordner `Server` oder `Arbeitsstationen` zu dem Gerät, das Sie verwalten möchten.
3. Wählen Sie das Gerät aus, indem Sie das Kontrollkästchen vor dem Gerät markieren.
4. Klicken Sie in der Aufgabenliste im linken Navigationsbereich auf **Dateien übertragen**, um das Dialogfeld „Dateiübertragung“ anzuzeigen.
5. Füllen Sie im Dialogfeld „Dateiübertragung“ folgende Felder aus:

   Gerät: Geben Sie den Namen oder die IP-Adresse des Geräts an, auf das Sie zugreifen möchten.

   Für alle Geräte immer standardmäßig die IP-Adresse verwenden: Wählen Sie dies aus, wenn im System die IP-Adresse des Geräts anstelle des DNS-Namens angezeigt werden soll. Die Werte, die Sie für den Zugriff auf ein Gerät während eines Fernsteuerungsvorgangs angeben, werden im System gespeichert, sobald Sie auf **OK** klicken. Einige dieser Werte werden in Abhängigkeit vom Gerät bzw. dem Fernoperator automatisch während der nachfolgenden Fernsteuerungsvorgänge ausgewählt.

   Authentifizierung: Wählen Sie den gewünschten Modus aus, um sich am verwalteten Gerät zu authentifizieren. Es stehen zwei Optionen zur Verfügung:

   - **Passwort:** Stellt die passwortbasierte Authentifizierung für die Durchführung eines Vorgangs bereit. Sie müssen das korrekte Passwort eingeben, das vom Benutzer auf dem verwalteten Gerät festgelegt oder vom Administrator in den Sicherheitseinstellungen der Fernverwaltungsrichtlinie konfiguriert wurde. Das vom Benutzer festgelegte Passwort hat Vorrang vor dem vom Administrator konfigurierten Passwort.
   - **Rechte:** Diese Option ist nur dann verfügbar, wenn Sie das verwaltete Gerät ausgewählt haben, auf dem Sie den Fernvorgang durchführen möchten. Wenn Ihnen der Administrator bereits Fernverwaltungsrechte erteilt hat, um den gewünschten Fernvorgang auf dem ausgewählten verwalteten Gerät durchzuführen, erhalten Sie automatisch Zugriff, wenn die Sitzung gestartet wird.

   Port: Geben Sie die Nummer des Ports an, den der Fernverwaltungsagent überwacht. Standardmäßig lautet die Portnummer 5950.

   Sitzungsmodus: Ist für den Dateiübertragungsvorgang nicht relevant.

   Sitzungsverschlüsselung: Gewährleistet, dass die Fernsitzung mithilfe der SSL(Secure Sockets Layer)-Verschlüsselung (TLSv1-Protokoll) geschützt wird.

   Protokollierung aktivieren: Protokolliert Informationen zur Sitzung und zum Debugging in der Datei `novell-zenworks-vncviewer.txt`. Die Datei wird standardmäßig auf dem Desktop gespeichert, wenn Sie das ZENworks-Kontrollzentrum über Internet Explorer starten. Sie wird im Mozilla-Installationsverzeichnis gespeichert, wenn Sie das ZENworks-Kontrollzentrum über Mozilla Firefox starten. Auf einer Linux-Verwaltungskonsole wird die Datei im Basisverzeichnis des angemeldeten Benutzers gespeichert.

Durch Proxy weiterleiten: Ermöglicht, dass der Fernverwaltungsbetrieb des verwalteten Geräts durch einen Proxyserver geleitet werden kann. Wenn sich das verwaltete Gerät in einem privaten Netzwerk oder auf der anderen Seite einer Firewall oder eines Routers befindet, die/der NAT (Network Address Translation) verwendet, kann der Fernverwaltungsbetrieb des Geräts durch einen Proxy-Server geleitet werden. Füllen Sie die folgenden Felder aus:

- **Proxy:** Geben Sie den DNS-Namen bzw. die IP-Adresse des Proxyservers an. Standardmäßig wird der Proxyserver, der in der Kontrollleiste Proxy-Einstellungen für den Fernbetrieb auf dem Gerät konfiguriert wurde, in diesem Feld eingegeben. Sie können einen anderen Proxyserver angeben.
- **Proxy-Port:** Geben Sie die Portnummer an, die der Proxyserver überwacht. Standardmäßig lautet die Portnummer 5750.

6 Klicken Sie auf **OK**, um die Sitzung zu starten.

Durchführen von Fernsteuerungs-, Fernansichts- und Fernanmeldungsvorgängen auf einem Linux-Gerät

1 Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Geräte**.

2 Navigieren Sie im Ordner `Server` oder `Arbeitsstationen` zu dem Gerät, das Sie verwalten möchten.

3 Wählen Sie ein Linux-Gerät aus, indem Sie das Kontrollkästchen vor dem Gerät aktivieren.

4 Klicken Sie auf **Aktion** > **Fernsteuerung**, um das Dialogfeld „Fernverwaltung“ anzuzeigen.

5 Füllen Sie im Dialogfeld „Fernverwaltung“ die folgenden Felder aus:

Gerät: Geben Sie den Namen oder die IP-Adresse des Gerätes an, das Sie dezentral verwalten möchten.

Für alle Geräte immer standardmäßig die IP-Adresse verwenden: Wählen Sie dies aus, wenn im System die IP-Adresse des Geräts anstelle des DNS-Namens angezeigt werden soll.

Die Werte, die Sie für den Zugriff auf ein Gerät während eines Fernsteuerungsvorgangs angeben, werden im System gespeichert, sobald Sie auf **OK** klicken. Einige dieser Werte werden in Abhängigkeit vom Gerät bzw. dem Fernoperator automatisch während der nachfolgenden Fernsteuerungsvorgänge ausgewählt.

Operation: Wählen Sie die Art des entfernten Vorgangs (Fernsteuerung, Fernansicht oder Fernausführung) aus, den Sie auf dem verwalteten Gerät durchführen möchten:

Port: Geben Sie die Nummer des Ports an, den der Fernverwaltungsagent überwacht. Die Portnummer für Fernsteuerungs- und Fernansichtsvorgänge lautet standardmäßig 5950 und für Fernanmeldungsvorgänge 5951.

Protokollierung aktivieren: Protokolliert Informationen zur Sitzung und zum Debugging in der Datei `novell-zenworks-vncviewer.txt`. Die Datei wird standardmäßig auf dem Desktop gespeichert, wenn Sie das ZENworks-Kontrollzentrum über Internet Explorer starten. Sie wird im Mozilla-Installationsverzeichnis gespeichert, wenn Sie das ZENworks-Kontrollzentrum über Mozilla Firefox starten. Auf einer Linux-Verwaltungskonsole wird die Datei im Basisverzeichnis des angemeldeten Benutzers gespeichert.

Durch Proxy weiterleiten: Ermöglicht, dass der Fernverwaltungsbetrieb des verwalteten Geräts durch einen Proxyserver geleitet werden kann. Wenn sich das verwaltete Gerät in einem privaten Netzwerk oder auf der anderen Seite einer Firewall oder eines Routers befindet, die/der NAT (Network Address Translation) verwendet, kann der Fernverwaltungsbetrieb des Geräts durch einen Proxy-Server geleitet werden. Füllen Sie die folgenden Felder aus:

- **Proxy:** Geben Sie den DNS-Namen bzw. die IP-Adresse des Proxyservers an. Standardmäßig wird der Proxyserver, der in der Kontrollleiste Proxy-Einstellungen für den Fernbetrieb auf dem Gerät konfiguriert wurde, in diesem Feld eingegeben. Sie können einen anderen Proxyserver angeben.
- **Proxy-Port:** Geben Sie die Portnummer an, die der Proxyserver überwacht. Standardmäßig lautet die Portnummer 5750.

Fernverwaltungs-Viewer installieren: Klicken Sie auf den Link **Fernverwaltungs-Viewer installieren**, um das Fernverwaltungs-Anzeigeprogramm zu installieren. Dieser Link wird nur angezeigt, wenn Sie die Fernverwaltungssitzung auf dem verwalteten Gerät erstmalig durchführen, oder wenn der Fernverwaltungs-Viewer nicht auf dem verwalteten Gerät installiert ist.

6 Klicken Sie auf **OK**, um die Sitzung zu starten.

Durchführen eines Fern-SSH-Vorgangs auf einem Linux-Gerät

1 Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Geräte**.

2 Navigieren Sie im Ordner `Server` oder `Arbeitsstationen` zu dem Gerät, das Sie verwalten möchten.

3 Wählen Sie ein Linux-Gerät aus, indem Sie das Kontrollkästchen vor dem Gerät aktivieren.

4 Klicken Sie auf **Aktion** > **Fern-SSH**, um das Dialogfeld „Fern-SSH“ anzuzeigen.

5 Füllen Sie im Dialogfeld „Fern-SSH“ die folgenden Felder aus:

Gerät: Geben Sie den Namen oder die IP-Adresse des Geräts an, mit dem Sie eine Fernverbindung herstellen möchten. Wenn sich das Gerät nicht im selben Netzwerk befindet, müssen Sie die IP-Adresse des Geräts angeben.

Benutzername: Geben Sie den Benutzernamen für die Anmeldung bei dem Remote-Gerät an. Standardmäßig lautet er `root`.

Anschluss: Geben Sie die Portnummer für den Remote-SSH-Service an. Standardmäßig lautet die Portnummer 22.

Wenn Sie auf **OK** klicken, werden Sie aufgefordert, Remote SSH Java Web Start Launcher zu starten. Klicken Sie auf „Ja“, um das Zertifikat zu akzeptieren, und klicken Sie dann auf **Ausführen**. Um die Verbindung mit dem Gerät fortzusetzen, klicken Sie auf **Ja**. Sie werden aufgefordert, das Passwort für die Verbindung mit dem verwalteten Gerät einzugeben.

6 Klicken Sie auf **OK**, um die Sitzung zu starten.

Weitere Informationen

Weitere Informationen über die Fernverwaltung von Geräten erhalten Sie im Handbuch *ZENworks: Fernverwaltungsreferenz*.

Erfassung des Software- und Hardware-Inventars

Mit ZENworks Configuration Management können Sie Software- und Hardwareinformationen von Geräten erfassen. Sie können das Inventar eines einzelnen Geräts anzeigen und Inventarberichte basierend auf spezifischen Kriterien generieren.

Sie möchten beispielsweise eine Softwareanwendung verteilen, die bestimmte Anforderungen an den Prozessor, Arbeitsspeicher und Festplattenspeicherplatz aufweist. Sie erstellen zwei Berichte, einen, in dem alle Geräte aufgelistet werden, die die Anforderungen erfüllen, und einen, in dem die Geräte aufgelistet werden, die die Anforderungen nicht erfüllen. Basierend auf den Berichten können Sie die Software auf die kompatiblen Geräte verteilen und einen Aktualisierungsplan für die nicht kompatiblen Geräte erstellen.

Standardmäßig werden Geräte um 1:00 Uhr morgens am ersten Tag jedes Monats automatisch überprüft. Sie können den Zeitplan und viele andere **Inventar**-Konfigurationseinstellungen auf der Registerkarte **Konfiguration** im ZENworks-Kontrollzentrum modifizieren.

Starten eines Gerätescans

Sie können jederzeit einen Gerätescan starten.

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Geräte**.
2. Durchsuchen Sie die Ordner `Server` oder `Arbeitsstationen`, bis Sie die zu scannenden Geräte finden.
3. Klicken Sie auf das Gerät, um seine Details anzuzeigen.
4. Klicken Sie in der Aufgabenliste im linken Navigationsbereich auf **Inventarabsuche nach Servern** oder **Inventarabsuche nach Arbeitsstationen**, um den Scan zu starten.

   Im Dialogfeld Schnellaufgabenstatus wird der Status der Aufgabe angezeigt. Nach Abschluss der Aufgabe können Sie auf die Registerkarte **Inventar** klicken, um die Ergebnisse des Scans anzuzeigen.

Sie können zum Absuchen eines Geräts auch den Befehl `inventory-scan-now` im zman-Dienstprogramm verwenden. Weitere Informationen finden Sie unter „Inventarkommandos“ im Handbuch *ZENworks: Referenz für Befehlszeilen-Dienstprogramme*.

Anzeigen von Geräteinventaren

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Geräte**.
2. Durchsuchen Sie die Ordner `Server` oder `Arbeitsstationen`, bis Sie die zu scannenden Geräte finden.
3. Klicken Sie auf das Gerät, um seine Details anzuzeigen.
4. Klicken Sie auf den Karteireiter **Inventar**.

Generieren von Inventarberichten

ZENworks Configuration Management umfasst mehrere Standardberichte. Außerdem können Sie benutzerdefinierte Berichte erstellen, um verschiedene Ansichten der Inventarinformationen bereitzustellen.

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte .
2. Klicken Sie im Bereich der Inventar-Standardberichte auf **Software-Anwendungen**.
3. Klicken Sie auf den Bericht **Betriebssystem**, um den Bericht zu generieren.

   Mithilfe der Optionen unten im Bericht können Sie den generierten Bericht als Microsoft Excel-Arbeitsblatt, CSV-Datei (durch Kommas getrennte Werte), PDF-Datei oder PDF-Grafikdatei speichern.

Weitere Informationen

Weitere Informationen über das Inventar finden Sie im Handbuch *ZENworks: Inventar-Referenz*.

Linux Management

Linux Management macht es Ihnen einfach, Linux in Ihre bestehende Umgebung einzubinden und es zu erweitern. Linux-Ressourcen werden automatisch und richtliniengesteuert implementiert, bereitgestellt, verwaltet und gewartet. Die automatischen und intelligenten Richtlinien ermöglichen es Ihnen, eine zentrale Steuerung während des gesamten Lebenszyklus von Linux-Systemen zu bieten, sodass das Sperren, das Erstellen von Images, die Fernverwaltung und die Inventar- sowie die Softwareverwaltung von Desktops möglich werden. Das Ergebnis ist eine umfassende Linux-Verwaltungslösung, die die anfallenden IT-Arbeiten drastisch reduziert, indem der erforderliche Overhead reduziert wird, der für die Verwaltung von Linux-Systemen erforderlich ist.

Zum Patchen Ihrer Linux-Geräte können Sie eine der folgenden Optionen verwenden:

- Patchverwaltung
- Linux-Paketverwaltung

Patchverwaltung

Die Patchverwaltung ist eine vollständig in ZENworks integrierte Funktion, die Agent-bezogene Patches, Patches zum Beheben von Schwachstellen und eine Compliance-Verwaltungslösung zur Verfügung stellt.

Die Patchverwaltung bietet folgende Funktionen:

- Verwendet Signaturen zur Bestimmung der erforderlichen Patches und gibt Rückmeldung, um die Berichterstellung zu erleichtern.
- Implementiert obligatorische Grundkonfigurationen für bestimmte Patches, damit diese auf einem Gerät stets vorhanden sind.
- Führt nur Patches für die SLES- und RHEL-Verteilungen durch.

Weitere Informationen finden Sie in Kapitel 12, „Patch Management“, auf Seite 137.

Linux-Paketverwaltung

Die Linux-Paketverwaltung dient zur Abwicklung der Paketverwaltungsfunktion von ZENworks Configuration Management für Linux-Geräte (Server und Desktops).

Die Linux-Paketverwaltung bietet die folgenden Funktionen:

- Stellt eine zentrale Verwaltung für das Patchen, Installieren und Aktualisieren von Paketen für eine große Anzahl von Linux-Geräten auf Unternehmensebene zur Verfügung.
- Spiegelt Aktualisierungen und Pakete von den NU-, RHN-, RCE- und YUM-Repositorys für Patches und Pakete als ZENworks-Bundles. Diese Bundles können Sie verwalteten Linux-Geräten zum Zwecke der Paketverwaltung zuweisen.
- Unterstützt das Herunterladen von Delta-RPMs auf die verwalteten Geräte, sobald die Delta-RPMs verfügbar und anwendbar sind. Dadurch wird die erforderliche Bandbreite beim Patchen reduziert.
- Bietet Ihnen die Möglichkeit, die Kataloge, Pakete und Bundles auszuwählen, die Sie spiegeln möchten.
- Ermöglicht es Ihnen, OES-Server zu patchen.

Verwalten von Mobilgeräten

Die Seite **Erste Schritte für Mobile Management** im ZENworks-Kontrollzentrum führt Sie durch die nötigen Schritte zum Registrieren und Verwalten von Mobilgeräten in der Zone.

So öffnen Sie die Seite **Erste Schritte für Mobile Management**:

1. Klicken Sie im ZENworks-Kontrollzentrum auf **Mobile Management** (im linken Navigationsbereich).

   Die einzelnen Konfigurationsaufgaben auf der Seite sind mit dem Symbol ⛔ oder ✅ für den Bearbeitungsstatus versehen und bieten mindestens einen Link auf die Seite, auf der Sie die Aufgabe ausführen.

   Mit dem Symbol ⓘ neben den Aufgaben und mit dem Link **Hilfe** oben rechts auf den Seiten erhalten Sie jeweils weitere Informationen zur betreffenden Aufgabe.

2. Führen Sie die nötigen **Konfigurationsaufgaben** aus, mit denen die Geräte in der Zone registriert werden. Anschließend können Sie diese Geräte mit den Aufgaben unter **Weitere Vorgehensweise** verwalten.

   Weitere Informationen zu den einzelnen Aufgaben finden Sie im Handbuch ZENworks Mobile Management Reference (Referenz zu Mobile Management).

Registrieren von Mobilgeräten

Registrieren eines iOS DEP-Geräts

Für Endbenutzer ist das Registrieren eines DEP-Geräts einfach, da Sie dem Benutzer ermöglichen können, die meisten Eingabeaufforderungen zur Geräteaktivierung zu überspringen, indem Sie das DEP-Profil ändern. Stellen Sie vor dem Registrieren eines DEP-Geräts sicher, dass die folgenden Voraussetzungen erfüllt sind:

Voraussetzungen

- Fügen Sie einen DEP-Server im ZCC hinzu, der den ZENworks-MDM-Server und den virtuellen MDM-Server im Apple-Portal verknüpft.
- Weisen Sie dem virtuellen MDM-Server im Apple-Portal Geräte zu. Diese Geräte werden dann von ZENworks ermittelt und im ZCC ausgefüllt.
- (Optional) Weisen Sie dem Gerät einen Benutzer zu, wenn Sie möchten, dass das Gerät bei der DEP-Registrierung nur mit diesem Benutzer verbunden werden soll.
- (Optional) Ändern Sie die DEP-Profileinstellungen, um den Registrierungsprozess zu verbessern.
- (Bedingt) Wenn Sie das DEP-Profil bearbeiten, stellen Sie sicher, dass das bearbeitete DEP-Profil dem Apple-Portal erfolgreich zugewiesen wird.

Ferner:

- Weisen Sie eine Mobilgeräte-Registrierungsrichtlinie zu.
- (Bedingt) Wenn Sie ein Gerät, das von einem anderen Benutzer stillgelegt wurde, erneut registrieren, stellen Sie sicher, dass das vorherige Geräteobjekt im ZCC gelöscht wurde.
- (Optional) Weisen Sie eine E-Mail-Richtlinie für Mobilgeräte zu, um das E-Mail-Konto auf dem Gerät zu konfigurieren.

Weitere Informationen zu den einzelnen Aufgaben finden Sie im Handbuch ZENworks Mobile Management Reference (Referenz zu Mobile Management).

Verfahren

Folgen Sie den Eingabeaufforderungen des Setup-Programms, um das Gerät zu registrieren. Nachdem der Benutzer die Wi-Fi-Einstellungen konfiguriert hat, melden Sie sich mit dem Berechtigungsnachweis des Benutzers bei dem Gerät an. Wenn das Gerät einem bestimmten Benutzer zugewiesen ist, darf nur der Berechtigungsnachweis dieses Benutzers eingegeben werden, sonst schlägt die Registrierung fehl.

Nach der Registrierung des Geräts können Sie den **Bereitstellungsstatus** des Geräts im ZCC anzeigen, der sich von **Ermittelt** in **Verwaltet** geändert haben sollte. Sie können den Status auf der Zusammenfassungsseite des Geräts anzeigen.

Registrieren eines iOS-Geräts über Apple Configurator

Apple Configurator ist ein Werkzeug in Mac OS X, das Administratoren bei der Bereitstellung von iOS-Geräten in Unternehmens- oder Bildungsumgebungen hilft. Apple Configurator vereinfacht und beschleunigt die erneute Zuweisung von Geräten, sodass der nächste Benutzer auf dem Gerät in Bezug auf den Inhalt ganz von vorn beginnen kann.

Voraussetzungen

- Weisen Sie eine Mobilgeräte-Registrierungsrichtlinie zu.

- Kopieren Sie die Apple-Registrierungs-URL, die den MDM-Server für die Registrierung des Geräts angibt. Um diese zu erhalten, navigieren Sie im ZCC zu **Konfiguration** > **Infrastrukturverwaltung** > **MDM-Server**. Wählen Sie einen MDM-Server aus und klicken Sie auf **Apple-Registrierungs-URL**.
- (Optional) Weisen Sie eine E-Mail-Richtlinie für Mobilgeräte zu, um das E-Mail-Konto auf dem Gerät zu konfigurieren.

Weitere Informationen zu den einzelnen Aufgaben finden Sie im Handbuch ZENworks Mobile Management Reference (Referenz zu Mobile Management).

Verfahren

1. Verbinden Sie das Gerät über den USB-Port mit dem MAC.
2. Klicken Sie mit der rechten Maustaste und wählen Sie **Vorbereiten** aus oder wählen Sie in der oberen Menüleiste des Apple Configurator **Vorbereiten** aus.
3. Wählen Sie im Dropdown-Menü **Konfiguration** die Option **Manuell** aus. Klicken Sie auf **Weiter**.
4. Wählen Sie den MDM-Server aus, auf dem das Gerät registriert werden soll. Wenn Sie den MDM-Server im Dropdown-Menü nicht gespeichert haben, wählen Sie **Neuer Server** aus.
5. Geben Sie einen Namen für den Server an und fügen Sie die aus dem ZCC kopierte Apple-Registrierungs-URL ein. Um diese zu erhalten, navigieren Sie im ZCC zu **Konfiguration** > **Infrastrukturverwaltung** > **MDM-Server**. Wählen Sie einen MDM-Server aus und klicken Sie auf **Apple-Registrierungs-URL**. Kopieren Sie die URL und fügen Sie sie auf der Seite „MDM-Server festlegen“ im Apple Configurator ein. Dieser MDM-Server wird zur zukünftigen Verwendung gespeichert.
6. Wählen Sie **Betreuen von Geräten** aus, wenn Sie festlegen möchten, dass das Gerät betreut wird. Das Kontrollkästchen **Geräten erlauben, sich mit anderen Computern zu koppeln** ist automatisch aktiviert.
7. Wählen Sie die Organisation aus, die diese Geräte betreut.
8. Wählen Sie die entsprechende Option im Dropdown-Menü **Einrichtungsassistent**, wenn Sie möchten, dass bestimmte Einrichtungsschritte bei der Registrierung des Geräts übersprungen werden. Prüfen Sie die Einrichtungselemente, die bei der Geräteregistrierung angezeigt werden sollen.
9. Klicken Sie auf **Vorbereiten**, um das verbundene Gerät vorzubereiten.

Nach der Vorbereitungsphase wird das iOS-Gerät auf seine Werkseinstellungen zurückgesetzt. Sobald das Gerät zurückgesetzt wurde, befolgen Sie die Anweisungen auf dem iOS-Gerät, die auf der Seite **Configure iOS Setup Assistant** (iOS-Setup-Assistent konfigurieren) in Apple Configurator konfiguriert wurden. Nach der Eingabe des Wi-Fi-Passworts wird der Benutzer aufgefordert, den Benutzerberechtigungsnachweis einzugeben.

Registrieren eines iOS-Geräts über das ZENworks-Benutzerportal

In diesem Szenario wird erläutert, wie Sie ein iOS-Gerät als vollständig verwaltetes Gerät in der ZENworks-Verwaltungszone registrieren. Bei dieser Registrierung wird ein MDM-Profil auf dem Gerät angelegt, mit dem Sie Einschränkungen auf dem Gerät anwenden und Apps bereitstellen können.

Voraussetzungen

- ZENworks unterstützt Geräte mit iOS-Version 8 (oder höher).
- Eine Benutzerquelle für die Mobilgeräteregistrierung wurde konfiguriert und aktiviert.
- Eine Registrierungsrichtlinie wurde erstellt und dem Benutzer zugewiesen.
- Einem Primärserver wurde eine MDM-Rolle zugewiesen.
- Push-Benachrichtigungen für iOS-Geräte.
- Sollen E-Mails für Exchange ActiveSync-Konten mit ZENworks synchronisiert werden, ist ein ActiveSync-Server zu konfigurieren. Außerdem ist eine E-Mail-Richtlinie für Mobilgeräte für den ZENworks-Server, der als Proxyserver für den ActiveSync-Server fungiert, zu erstellen und zuzuweisen. So kann ZENworks die Unternehmens-E-Mails verwalten, die auf dem Gerät gesendet und empfangen werden.
- Die Registrierung von iOS-Geräten mit dem Safari-Browser im privaten Modus wird nur unter iOS 11 (oder höher) unterstützt.

Verfahren

1 Geben Sie *ZENworks_Serveradresse*/zenworks-eup in den Safari-Browser auf dem Gerät ein. *ZENworks_Serveradresse* bezeichnet hierbei den DNS-Namen oder die IP-Adresse des ZENworks-MDM-Servers.

   Der Anmeldebildschirm für das ZENworks-Benutzerportal wird geöffnet.

2 Geben Sie den Benutzernamen und das Passwort des Benutzers ein. Falls die Option **Einfache Registrierung zulassen** für die Benutzerquelle aktiviert ist, zu der der Benutzer gehört, müssen Sie die Registrierungsdomäne nicht angeben; ansonsten geben Sie die Registrierungsdomäne an.

   Alle mit dem Benutzer verknüpften Geräte werden im ZENworks-Benutzerportal angezeigt.

3 Tippen Sie oben rechts auf **Registrieren**. Die Registrierungsoptionen für das Gerät werden angezeigt.

4 Tippen Sie auf **Nur verwaltetes Gerät**. Der Bildschirm **Geräteoptionen registrieren** wird geöffnet. Wenn in der Mobilgeräte-Registrierungsrichtlinie konfiguriert ist, dass Sie das Eigentum am Mobilgerät definieren können (Unternehmen oder persönlich), werden Sie aufgefordert, diese Informationen anzugeben. Wählen Sie die Option für das Eigentum am Gerät und klicken Sie auf **OK**.

5 Tippen Sie auf **Zertifikat herunterladen**. Der Bildschirm **Profil installieren** wird geöffnet.

HINWEIS: Wenn Sie ein Gerät mit iOS 12.1.2 oder ein älteres Gerät registrieren und auf „Zertifikat herunterladen“ klicken, werden Sie zum Bildschirm für die Installation des Profils weitergeleitet. Klicken Sie auf „Installieren“ und folgen Sie den Eingabeaufforderungen, um das Profil zu installieren.

   5a Erlauben Sie der Website, das Konfigurationsprofil herunterzuladen.

   5b Das Konfigurationsprofil wird heruntergeladen. Anschließend können Sie das Profil über das Menü „Einstellungen“ herunterladen.

   5c Navigieren Sie zum Menü „Einstellungen“ und klicken Sie auf **Allgemein** > **Profile**.

5d Tippen Sie auf **ZENworks-Verbürgungsprofil**.

5e Installieren Sie das Profil.

6 (Bedingt) Aktivieren Sie das Registrierungszertifikat auf dem Gerät. Dieser Schritt wird auf Geräten mit iOS-Version 10.3 oder höher angezeigt. So aktivieren Sie das Zertifikat:

6a Navigieren Sie zum Menü **Einstellungen** auf dem Gerät und klicken Sie auf **Allgemein**.

6b Klicken Sie auf **Info**.

6c Klicken Sie auf **Zertifikatsvertrauenseinstellungen**.

6d Aktivieren Sie das auf dem Bildschirm angezeigte Root-Zertifikat.

7 Tippen Sie im Bildschirm „Als verwaltetes Gerät registrieren“ auf **Profil herunterladen**. Der Bildschirm „Profil installieren“ wird geöffnet.

HINWEIS: Wenn der Benutzer ein Gerät mit iOS 12.1.2 oder älter registriert und auf **Zertifikat herunterladen** klickt, wird er zum Bildschirm für die Installation des Profils weitergeleitet. Tippen Sie auf **Installieren** und folgen Sie den Eingabeaufforderungen, um das Profil zu installieren.

7a Erlauben Sie der Website, das Profil herunterzuladen.

7b Das Konfigurationsprofil wird heruntergeladen. Anschließend können Sie das Profil über das Menü „Einstellungen“ herunterladen.

7c Navigieren Sie zum Menü **Einstellungen**auf dem Gerät, um das Profil zu installieren, und tippen Sie auf **Allgemein** > **Profile**.

7d Tippen Sie auf **ZENworks Device Enrollment Program Profile** (Profil für das ZENworks-Geräteregistrierungsprogramm). Das Profil für das ZENworks-Geräteregistrierungsprogramm enthält das MDM-Profil zur Verwaltung des Geräts durch ZENworks.

7e Tippen Sie auf **Installieren**und folgen Sie den Eingabeaufforderungen, um das Profil zu installieren.

8 Navigieren Sie zurück zur EUP-Seite. Das Gerät wird in der Liste „Eigene Geräte“ mit dem Status **Registrierung wird durchgeführt** angezeigt. Aktualisieren Sie den Browser, damit der Status zu Gerät ist aktiv wechselt.

Nun können Sie den Registrierungsmodus im ZCC auf der Seite „Geräteinformationen“ abrufen. Zum Abrufen der Geräteinformationen klicken Sie im ZCC im linken Navigationsbereich auf **Geräte** > **Mobilgeräte** (oder navigieren Sie zum Ordner, der in der Mobilgeräte-Registrierungsrichtlinie konfiguriert ist) und wählen Sie das Gerät aus. Der Registrierungsmodus lautet **iOS MDM**.

9 Auf der Grundlage der E-Mail-Richtlinie für Mobilgeräte, die dem Benutzer oder dem Gerät zugewiesen ist, wird auf dem Gerät automatisch ein E-Mail-Konto eingerichtet.

Registrieren von Android-Geräten im Arbeitsprofilmodus

Im Arbeitsprofilmodus werden dedizierte Container auf Geräten für Unternehmens-Apps und -daten erstellt, wodurch es Organisationen ermöglicht wird, ausschließlich die Unternehmensdaten zu verwalten. Dieser Modus ist für das BYOD-Szenario vorgesehen, in dem der Benutzer eigene Geräte zum Arbeitsplatz mitbringt.

Voraussetzungen

Obligatorische Einstellungen

- Erstellen Sie ein Android Enterprise-Abonnement.
- Erstellen Sie eine Mobilgeräte-Registrierungsrichtlinie und weisen Sie diese zu.
- Erstellen Sie eine Android-Profilregistrierungsrichtlinie und weisen Sie diese zu.
- Für den Arbeitsprofilmodus ist die Android-Version 5.0 (oder höher) erforderlich, für den Modus für verwaltete Unternehmensgeräte die Version 6.0 (oder höher).

Optionale Einstellungen

- Fordern Sie die Benutzer auf, ihre Geräte zu registrieren.

Weitere Informationen zu den einzelnen Aufgaben finden Sie im Handbuch ZENworks Mobile Management Reference (Referenz zu Mobile Management).

Verfahren

Das in diesem Abschnitt vorgestellte Szenario richtet sich an Benutzer, die ihre Geräte erstmalig bei ZENworks registrieren. Weitere Informationen für Benutzer, die ihre Geräte bereits im Basismodus (nur Android-App) registriert haben und nun die Registrierung im Arbeitsprofilmodus vornehmen möchten, finden Sie unter Arbeitsprofilregistrierung für vorhandene Benutzer.

Verfahren

1. Installieren Sie die ZENworks-Agent-App aus dem Google Play Store. Alternativ kann der Benutzer die ZENworks-Agent-App gemäß den Anweisungen im Einladungsschreiben herunterladen.
2. Klicken Sie nach der Installation auf **Öffnen**. Eine kurze Beschreibung des ZENworks-Agenten wird angezeigt. Der Benutzer klickt auf **Weiter**.
3. Soll die Geräteverwaltung über die App aktiviert werden, klicken Sie auf **Diesen Geräteadministrator aktivieren**.
4. Melden Sie sich mit den folgenden Angaben bei der App an:

   Benutzername, Passwort, Domäne, Server -URL: Geben Sie den Benutzernamen, das Passwort und die Registrierungsdomäne (wenn **Einfache Registrierung zulassen** für den Benutzer deaktiviert ist) sowie die Server-URL des ZENworks-MDM-Servers ein. Der Benutzer findet diese Informationen im Einladungsschreiben.
5. Legen Sie das Eigentum am Gerät fest (Unternehmen oder persönlich), wenn Sie in der Mobilgeräte-Registrierungsrichtlinie konfiguriert haben, dass der Benutzer das Eigentum festlegen kann. Tippen Sie auf **OK**.

6 Befolgen Sie die Anweisungen auf den nachfolgenden Bildschirmen. Das Gerät richtet automatisch ein Arbeitsprofil ein und registriert sich bei ZENworks. Der Startbildschirm der ZENworks-Agent-App wird geöffnet und das Gerät wird als registriert und aktiv angezeigt.

7 Prüfen Sie die Geräteinformationen im ZCC. Klicken Sie im ZCC im linken Navigationsbereich auf **Geräte**> **Mobilgeräte** (oder navigieren Sie zum Ordner, der in der Mobilgeräte-Registrierungsrichtlinie konfiguriert ist). Klicken Sie auf das entsprechende Gerät und prüfen Sie die Details auf der Seite **Zusammenfassung**. Der Registrierungsmodus wird als **Android-App** angezeigt und der **Arbeitsprofilmodus** ist ebenfalls aktiviert.

Nach erfolgter Registrierung Ihres Geräts wird ein Badge-Symbol neben dem Symbol der ZENworks-Agent-App angezeigt und andere System-Apps tragen dazu bei, Arbeits-Apps von persönlichen Apps zu unterscheiden.

Arbeitsprofilregistrierung für vorhandene Benutzer

Wenn die Benutzer sich bereits mit dem Basis-Registrierungsmodus (nur Android-App) registriert haben und sich nun im Arbeitsprofilmodus registrieren möchten, weisen Sie diesen Benutzern die Android-Profilregistrierungsrichtlinie zu.

Sobald den Benutzern die Mobilgerät-Registrierungsrichtlinie zugewiesen wurde, erhalten die Benutzer eine Benachrichtigung auf ihren Geräten, mit der sie aufgefordert werden, ein Arbeitsprofil anzulegen, sobald sie die ZENworks-Agent-App öffnen.

Der Benutzer klickt auf **Einrichten** und befolgt die Anweisungen zum Einrichten des Arbeitsprofils. Das Gerät richtet das Arbeitsprofil automatisch ein.

Registrieren eines Android-Geräts im Modus für verwaltete Unternehmensgeräte

Durch den Modus für verwaltete Unternehmensgeräte können Administratoren das gesamte Gerät verwalten und damit das Gerät auf die ausschließliche Unternehmensnutzung beschränken. Dieser Modus ist vorwiegend für Geräte vorgesehen, die Eigentum des Unternehmens sind.

Voraussetzungen

Obligatorische Einstellungen

- Erstellen Sie ein Android Enterprise-Abonnement.
- Erstellen Sie eine Mobilgeräte-Registrierungsrichtlinie und weisen Sie diese zu.
- Erstellen Sie eine Android-Profilregistrierungsrichtlinie und weisen Sie diese zu.
- Für den Arbeitsprofilmodus ist die Android-Version 5.0 (oder höher) erforderlich, für den Modus für verwaltete Unternehmensgeräte die Version 6.0 (oder höher).

Verfahren

1 Bearbeiten Sie die grundlegenden Einrichtungsbildschirme, z. B. Spracheinrichtung und WLAN-Konfiguration.

2 Legen Sie die AFW-Kennung (afw#zenworks) im Einrichtungsbildschirm fest, auf dem das Feld „E-Mail-ID“ angezeigt wird.

3 Klicken Sie auf der Seite „Android Enterprise“ auf **Weiter** und setzen Sie die Installation der ZENworks-App fort.

   Die ZENworks-Agent-App wird automatisch auf das Gerät heruntergeladen.

4 Klicken Sie auf **Installieren**. Die App wird auf dem Gerät installiert. Befolgen Sie dann die Anweisungen zum Einrichten des Geräts.

5 Befolgen Sie die Anweisungen in den restlichen Bildschirmen zum Einrichten eines verwalteten Unternehmensgeräts. Das Gerät ist nun eingerichtet, muss jedoch noch als verwaltetes Unternehmensgerät registriert werden.

6 Melden Sie sich mit den folgenden Angaben bei der App an:

   Benutzername, Passwort, Domäne, Server -URL: Geben Sie den Benutzernamen, das Passwort und die Registrierungsdomäne (wenn **Einfache Registrierung zulassen** für den Benutzer deaktiviert ist) sowie die Server-URL des ZENworks-MDM-Servers ein.

   Das verwaltete Unternehmensgerät wird automatisch auf dem Gerät eingerichtet.

Prüfen Sie die Geräteinformationen im ZCC. Klicken Sie im ZCC im linken Navigationsbereich auf **Geräte**> **Mobilgeräte** (oder navigieren Sie zum Ordner, der in der Mobilgeräte-Registrierungsrichtlinie konfiguriert ist). Klicken Sie auf das entsprechende Gerät und prüfen Sie die Details auf der Seite **Zusammenfassung**. Der Registrierungsmodus wird als **Android-App** angezeigt und der **Modus für verwaltete Unternehmensgeräte** ist ebenfalls aktiviert.

Registrieren eines Nur-ActiveSync-Geräts

Voraussetzungen

Vor dem Registrieren eines Mobilgeräts als vollständig verwaltetes Gerät bzw. als Nur-E-Mail-Gerät müssen die folgenden Voraussetzungen erfüllt sein:

- ZENworks unterstützt Geräte mit ActiveSync 12.1 (oder höher).
- Eine Benutzerquelle für die Mobilgeräteregistrierung wurde konfiguriert und aktiviert.
- Eine Registrierungsrichtlinie wurde erstellt und dem Benutzer zugewiesen.
- Einem Primärserver wurde eine MDM-Rolle zugewiesen.
- Push-Benachrichtigungen für ein Android-Gerät.
- Sollen E-Mails für Exchange ActiveSync-Konten mit ZENworks synchronisiert werden, ist ein ActiveSync-Server zu konfigurieren. Außerdem ist eine E-Mail-Richtlinie für Mobilgeräte für den ZENworks-Server, der als Proxyserver für den ActiveSync-Server fungiert, zu erstellen und zuzuweisen.

Verfahren

In diesem Szenario wird erläutert, wie Sie ein Gerät als Nur-E-Mail-Gerät in der ZENworks-Verwaltungszone registrieren. Dieses Szenario zeigt die Registrierung eines iOS-Geräts als Nur-E-Mail-Gerät.

1. Geben Sie *ZENworks_Serveradresse*/zenworks-eup in den Browser auf dem Gerät ein. *ZENworks_Serveradresse* bezeichnet hierbei den DNS-Namen oder die IP-Adresse des ZENworks-MDM-Servers.

   Der Anmeldebildschirm für das ZENworks-Benutzerportal wird geöffnet.

2. Geben Sie den Benutzernamen und das Passwort des Benutzers in das ZENworks-Benutzerportal ein. Falls die Option **Einfache Registrierung zulassen** für die Benutzerquelle aktiviert ist, zu der der Benutzer gehört, müssen Sie die Registrierungsdomäne nicht angeben; ansonsten geben Sie die Registrierungsdomäne an.

3. Tippen Sie oben rechts auf **Registrieren**. Die Registrierungsoptionen für das Gerät werden angezeigt.

4. Tippen Sie auf **Nur E-Mail**. Der Bildschirm **Nur als E-Mail registrieren** wird geöffnet. Erstellen Sie anhand der angezeigten Informationen ein E-Mail-Konto für den Benutzer.

   Sobald der Benutzer das E-Mail-Konto konfiguriert hat, wird eine E-Mail mit dem Hinweis, dass die Registrierung noch abgeschlossen werden muss, an den Benutzer gesendet. Der Inhalt dieser E-Mail kann im ZCC bearbeitet werden. Navigieren Sie zu **Konfiguration** > **Verwaltungszoneneinstellungen** > **Ereignis und Messaging** > **E-Mail-Benachrichtigungen**. Klicken Sie auf die E-Mail und bearbeiten Sie ihren Inhalt.

5. Klicken Sie in der E-Mail auf den Link zum ZENworks-Endbenutzerportal oder öffnen Sie das ZENworks-Endbenutzerportal gemäß den Anweisungen in Schritt 1.

   Das Gerät wird im ZENworks-Benutzerportal in der Liste „Eigene Geräte“ aufgeführt. Das Gerät wurde bereits in die ZENworks-Verwaltungszone aufgenommen, muss jedoch noch registriert werden.

6. Tippen Sie auf **Vollständige Registrierung**.

   Wenn in der Mobilgeräte-Registrierungsrichtlinie konfiguriert ist, dass Sie das Eigentum am Mobilgerät definieren können (Unternehmen oder persönlich), werden Sie aufgefordert, diese Informationen anzugeben. Geben Sie die erforderlichen Registrierungsinformationen auf dem Gerät an und tippen Sie auf **OK**.

   Die Liste „Eigene Geräte“ wird aktualisiert und das Gerät wird als registriert und aktiv angezeigt.

7. Prüfen Sie, ob E-Mails auf dem Gerät empfangen werden können. Senden Sie hierzu eine E-Mail von einem anderen Konto aus an den Benutzer.

   Sobald das Gerät in der ZENworks-Verwaltungszone registriert wurde, wird im ZCC auf der Seite „Geräteinformationen“ der Registrierungsmodus **ActiveSync** für das Gerät angezeigt. Zum Abrufen der Geräteinformationen klicken Sie im ZCC im linken Navigationsbereich auf **Geräte** > **Mobilgeräte** (oder navigieren Sie zum Ordner, der in der Mobilgeräte-Registrierungsrichtlinie konfiguriert ist) und wählen Sie das Gerät aus.

10 Endpoint Security Management

ZENworks Endpoint Security Management vereinfacht die Endpunktsicherheit durch die zentrale Verwaltung von Sicherheitsrichtlinien für Ihre verwalteten Geräte. Sie können den Zugriff eines Geräts auf Wechselmedien, WLANs und Anwendungen kontrollieren. Darüber hinaus können Sie Daten durch Verschlüsselung und Netzwerkkommunikation über Firewall-Erzwingung (Ports, Protokolle und Zugriffssteuerungslisten) sichern. Außerdem können Sie die Sicherheit eines Endpunktgeräts standortabhängig ändern.

In den folgenden Abschnitten wird erläutert, wie Sie Endpoint Security Management zur Sicherung Ihrer Geräte verwenden, unabhängig davon, ob diese sich im Büro, zu Hause oder an einem öffentlichen Flughafenterminal befinden:

Aktivieren von Endpoint Security Management

Wenn Sie Endpoint Security Management nicht bereits bei der Installation der Verwaltungszone aktiviert haben, indem Sie entweder einen Lizenzschlüssel angegeben oder die Evaluierung eingeschaltet haben, führen Sie folgende Schritte aus:

1. Klicken Sie im ZENworks-Kontrollzentrum auf **Konfiguration**.
2. Klicken Sie in der Kontrollleiste „Lizenzen“ auf **ZENworks 2020 Endpoint Security Management**.
3. Wählen Sie **Produkt evaluieren/aktivieren** aus und füllen Sie anschließend die folgenden Felder aus:

   Evaluierung verwenden: Wählen Sie diese Option aus, um den 60-Tage-Evaluierungszeitraum zu aktivieren. Nach dem 60-Tage-Zeitraum müssen Sie einen Produktlizenzschlüssel anwenden, um das Produkt weiterhin verwenden zu können.

   Produktlizenzschlüssel: Geben Sie den Lizenzschlüssel an, den Sie für Endpoint Security Management erworben haben. Eine Produktlizenz können Sie auf der ZENworks Endpoint Security Management-Produkt-Website (http://www.novell.com/products/zenworks/endpointsecuritymanagement) erwerben.
4. Klicken Sie auf **OK**.

Aktivieren des Endpoint Security Agent

Der ZENworks Agent ist verantwortlich für die Geräteregistrierung, die Inhaltsverteilung und die Softwareaktualisierungen für ein Gerät.

Zusätzlich zum ZENworks Agent wird der Endpoint Security Agent auf Geräten installiert, wenn ZENworks Endpoint Security Management aktiviert wird (Volllizenz oder Evaluierung). Der Endpoint Security Agent ist verantwortlich für die Erzwingung von Sicherheitsrichtlinieneinstellungen auf dem Gerät.

Sie sollten überprüfen, ob der Endpoint Security Agent aktiviert ist. Eine Anleitung dazu finden Sie in „Konfigurieren der ZENworks-Agent-Funktionen“, auf Seite 41.

Erstellen von Standorten

Die Sicherheitsanforderungen für ein Gerät können sich von Standort zu Standort unterscheiden. Zum Beispiel kann die persönliche Firewall bei einem Gerät in einem Flughafen-Terminal andere Einschränkungen haben als ein Gerät in einem Büro innerhalb der Firewall in Ihrem Unternehmen.

Um sicherzustellen, dass die Sicherheitsanforderungen eines Geräts für den jeweiligen Standort geeignet sind, unterstützt Endpoint Security Management sowohl die globalen Richtlinien als auch die standortbasierten Richtlinien. Globale Richtlinien werden unabhängig vom Standort des Geräts angewendet. Standortbasierte Richtlinien werden nur angewendet, wenn der aktuelle Standort des Geräts die Kriterien für einen mit der Richtlinie verknüpften Standort erfüllt. Wenn Sie beispielsweise eine standortbasierte Richtlinie für Ihr Firmenbüro erstellen und diese einem Notebook zuweisen, gilt die Richtlinie nur, wenn es sich bei dem Standort des Notebooks um das Firmenbüro handelt.

Wenn standortbasierte Richtlinien verwendet werden sollen, müssen Sie zunächst die Standorte definieren, die für Ihre Organisation sinnvoll sind. Ein Standort stellt einen Ort oder einen Ortstyp dar, für den spezifische Sicherheitsanforderungen gelten. So können beispielsweise unterschiedliche Anforderungen für ein Gerät gelten, je nachdem, ob es im Büro, zu Hause oder in einem Flughafen verwendet wird.

Standorte sind durch Netzwerkumgebungen definiert. Angenommen, Sie haben ein Büro in New York und ein Büro in Tokio. Für beide Büros gelten dieselben Sicherheitsanforderungen. Daher erstellen Sie einen Standort vom Typ „Büro“ und verknüpfen ihn mit zwei Netzwerkumgebungen: „Netzwerk von Büro New York“ und „Netzwerk von Büro Tokio“. Jede dieser Umgebungen ist explizit durch eine Menge von Services für Gateways, DNS-Server und drahtlose Zugriffspunkte definiert. Wenn der Endpoint Security Agent feststellt, dass seine aktuelle Umgebung mit dem Netzwerk von Büro New York oder dem Netzwerk von Büro Tokio übereinstimmt, legt er seinen Standort als Standort vom Typ „Büro“ fest und wendet die Sicherheitsrichtlinien an, die mit dem Standort vom Typ „Büro“ verknüpft sind.

Ausführliche Informationen zum Erstellen von Standorten finden Sie unter „Erstellen von Standorten“, auf Seite 36.

Eine Sicherheitsrichtlinie erstellen

Es sind 12 verschiedene Sicherheitsrichtlinien vorhanden:

Die Sicherheitseinstellungen eines Geräts werden von den Sicherheitsrichtlinien gesteuert, die vom Endpoint Security Agent angewendet wurden. Es sind acht Sicherheitsrichtlinien vorhanden, die eine Reihe von sicherheitsrelevanten Funktionen steuern. Je nach den Anforderungen in Ihrem Unternehmen können Sie alle oder einige der Richtlinien verwenden.

Richtlinie	Beschreibung
Anwendungssteuerung	Blockiert die Ausführung von Anwendungen oder verweigert den Internetzugriff durch Anwendungen. Sie geben die Anwendungen an, die gesperrt sind oder denen der Internetzugriff verweigert wird.
Kommunikationshardware	Deaktiviert die folgende Kommunikationshardware: 1394-Firewire, IrDA-Infrared, Bluetooth, seriell/parallel, Dialup, kabelgebunden und kabellos. Jede Kommunikationshardware wird einzeln konfiguriert, was bedeutet, dass Sie einige Hardwaretypen (wie zum Beispiel Bluetooth und Dialup) deaktivieren und andere aktiviert lassen können.
Datenverschlüsselung	Aktiviert die Datenverschlüsselung von Dateien auf Wechselspeichergeräten.
Firewall	Steuert die Netzwerk-Konnektivität durch Deaktivieren von Ports, Protokollen und Netzwerkadressen (IP und MAC).
Microsoft-Datenverschlüsselung	Steuert die Verschlüsselung von Wechseldatenträgern und Ordnern auf Festplatten mit Microsoft BitLocker bzw. Microsoft Encrypting File System (EFS).
Skripts	Führt ein Skript (JScript oder VBScript) auf einem Gerät aus. Sie können die Auslöser angeben, die die Ausführung des Skripts bewirken. Auslöser können auf Endpoint Security Agent-Aktionen (Aktionen der Endpunktsicherheitsverwaltung), Standortänderungen oder Zeitintervallen beruhen.
Steuerelement für Speichergerätsteuerung	Steuert den Zugriff auf CD/DVD-Laufwerke, Diskettenlaufwerke und Wechselspeicherlaufwerke. Jeder Speichergerätetyp wird einzeln konfiguriert, was bedeutet, dass Sie einige deaktivieren und andere aktivieren können.
USB-Konnektivität	Steuert den Zugriff auf USB-Geräte wie Wechselspeichergeräte, Drucker, Eingabegeräte (Tastaturen, Mausgeräte etc.). Sie können einzelne Geräte oder Gerätegruppen angeben. Sie können beispielsweise den Zugriff auf einen bestimmten Drucker deaktivieren und den Zugriff auf alle Sandisk-USB-Geräte aktivieren.
VPN-Erzwingung	Erzwingt eine auf dem Standort des Geräts basierende VPN-Verbindung. Wenn beispielsweise der Standort eines Geräts unbekannt ist, können Sie eine VPN-Verbindung erzwingen, über die der Internetverkehr insgesamt geroutet wird.
Wi-Fi	Deaktiviert Funkadapter, blockiert Funkverbindungen, steuert Verbindungen zu kabellosen Zugriffspunkten und so weiter.

Zusätzlich zu den oben genannten Sicherheitsrichtlinien können die folgenden Sicherheitsrichtlinien zum Schutz und zur Konfiguration des Endpoint Security Agent verwendet werden. Aufgrund der Eigenschaften dieser beiden Richtlinien empfehlen wir Ihnen, sie zunächst zu erstellen und zuzuweisen.

Richtlinie	Beschreibung
Sicherheitseinstellungen	Schützt den Endpoint Security Agent vor Manipulation und Deinstallation. Informationen zum Konfigurieren von ZENworks Agent Security-Einstellungen finden Sie unter „Konfigurieren der ZENworks-Agent-Sicherheit“, auf Seite 43.
Standortzuweisung	Enthält die Liste der zulässigen Standorte für ein Gerät oder einen Benutzer. Der Endpoint Security Agent evaluiert seine aktuelle Netzwerkumgebung, um zu ermitteln, ob sie mit einem der zulässigen Standorte übereinstimmt. Wenn dies der Fall ist, wird der Standort zum Sicherheitsstandort und der Agent wendet alle mit dem Standort verknüpften Sicherheitsrichtlinien darauf an. Wenn sie mit keinem der Standorte in der Liste übereinstimmt, werden die Sicherheitsrichtlinien angewendet, die mit dem Standort „Unbekannt“ verknüpft sind. Wenn Sie vorhaben, standortbasierte Richtlinien zu verwenden, sollten Sie sicher stellen, dass jedem Gerät oder Benutzer eine Standortzuweisungsrichtlinie zugewiesen wurde. Wenn einem Gerät bzw. Benutzer des Geräts keine Standortzuweisungsrichtlinie zugewiesen wurde, kann der Endpoint Security Agent keine standortbasierte Richtlinien auf das Gerät anwenden.

So erstellen Sie eine Sicherheitsrichtlinie:

1. Klicken Sie im ZENworks-Kontrollzentrum auf **Richtlinien**, um die Seite „Richtlinien“ anzuzeigen.
2. Klicken Sie im Richtlinienbereich auf **Neu** > **Richtlinie**, um den Assistenten zum Erstellen neuer Richtlinien zu starten.
3. Wählen Sie auf der Seite „Plattform auswählen“ die Option **Windows** aus und klicken Sie anschließend auf **Weiter**.
4. Wählen Sie auf der Seite „Richtlinienkategorie auswählen“ die Option **Windows Endpoint Security-Richtlinien** aus und klicken Sie anschließend auf **Weiter**.
5. Wählen Sie auf der Seite „Richtlinientyp auswählen“ den zu erstellenden Richtlinientyp aus und klicken Sie anschließend auf **Weiter**.

   Wenn Sie Standorte erstellt haben und vorhaben, standortbasierte Richtlinien zu verwenden, müssen Sie mindestens eine Standortzuweisungsrichtlinie erstellen und diese den Geräten oder den Benutzern der Geräte zuweisen. Anderfalls ist keiner der estellten Standorte für die Geräte verfügbar, was bedeutet, dass keine der standortbasierten Richtlinien angewendet werden kann.
6. Geben Sie auf der Seite „Details definieren“ einen Namen für die Richtlinie an und wählen Sie den Ordner aus, in dem die Richtlinie abgelegt werden soll.

   Der Name muss unter allen anderen im ausgewählten Ordner befindlichen Richtlinien eindeutig sein.

7 (Bedingt) Wenn die Seite „Vererbung und Standortzuweisungen konfigurieren“ angezeigt wird, konfigurieren Sie die folgenden Einstellungen und klicken Sie anschließend auf **Weiter**.

- **Vererbung:** Lassen Sie die Einstellung **Aus Richtlinienhierarchie übernehmen** ausgewählt, wenn diese Richtlinie aktiviert werden soll, um Einstellungen von Richtlinien desselben Typs zu übernehmen, die in der Richtlinienhierarchie übergeordnet sind. Wenn Sie beispielsweise diese Richtlinie einem Gerät zuweisen und eine andere Richtlinie (desselben Typs) dem Ordner des Geräts, kann diese Richtlinie durch Aktivieren dieser Option Einstellungen von derjenigen Richtlinie übernehmen, die dem Ordner des Geräts zugewiesen sind. Heben Sie die Auswahl der Einstellung **Aus Richtlinienhierarchie übernehmen** auf, wenn diese Richtlinie keine Richtlinieneinstellungen übernehmen soll.
- **Standortzuweisungen:** Richtlinien können global oder standortbasiert sein. Eine globale Richtlinie kann unabängig vom Standort angewendet werden. Eine standortbasierte Richtlinie wird nur angewendet, wenn das Gerät erkennt, dass es zu den Standorten gehört, die der Richtlinie zugewiesen wurden.

  Wählen Sie aus, ob diese Richtlinie global oder standortbasiert ist. Wenn Sie standortbasiert auswählen, klicken Sie auf **Hinzufügen**, wählen Sie die Standorte aus, denen die Richtlinie zugewiesen werden soll und klicken Sie anschließend auf **OK**, um sie der Liste hinzuzufügen.

8 Konfigurieren Sie die richtlinienspezifischen Einstellungen und klicken Sie anschließend auf **Weiter**, bis Sie auf der Seite „Zusammenfassung“ angelangt sind.

Weitere Informationen über die Einstellungen der Richtlinie erhalten Sie, wenn Sie im ZENworks-Kontrollzentrum auf **Hilfe** > **Aktuelle Seite** klicken.

9 Überprüfen Sie die Informationen auf der Seite „Zusammenfassung“, um sicherzustellen, dass sie korrekt sind. Falls Sie nicht korrekt sind, können Sie auf die Schaltfläche **Zurück** klicken, um die entsprechende Assistentenseite erneut zu besuchen und Änderungen vorzunehmen. Wenn die Informationen korrekt sind, wählen Sie eine der folgenden Optionen aus (falls gewünscht) und klicken Sie anschließend auf **Fertig stellen**.

- **Als Sandbox erstellen:** Wählen Sie diese Option aus, um die Richtlinie als Sandbox-Version zu erstellen. Benutzer und Geräte haben erst Zugriff auf die Sandbox-Version, wenn Sie sie veröffentlichen. Sie können sie beispielsweise Benutzern und Geräten zuweisen, sie wird jedoch erst angewendet, nachdem Sie sie veröffentlicht haben.
- **Zusätzliche Eigenschaften definieren:** Wählen Sie diese Option aus, um die Eigenschaftenseiten der Richtlinie anzuzeigen. Auf diesen Seiten können Sie Richtlinieneinstellungen bearbeiten und die Richtlinie Benutzern und Geräten zuweisen.

Zuweisen einer Richtlinie zu Benutzern und Geräten

Nachdem Sie eine Richtlinie erstellt haben, müssen Sie sie auf Geräte anwenden, indem Sie die Richtlinie Geräten oder Gerätebenutzern zuweisen.

1 Aktivieren Sie in der Kontrollleiste „Richtlinien“ das Kontrollkästchen neben der Richtlinie, die zugewiesen werden soll.

2 Klicken Sie auf **Aktion** > **Zu Gerät zuweisen**.

oder

Klicken Sie auf **Aktion** > **Benutzer zuweisen.**

3 Folgen Sie den Eingabeaufforderungen, um die Richtlinie zuzuweisen.

Klicken Sie auf den einzelnen Seiten des Assistenten auf die Schaltfläche **Hilfe**, um detaillierte Informationen zur jeweiligen Seite anzuzeigen.

Wenn Sie den Assistenten fertig stellen, werden die zugewiesenen Geräte oder Benutzer auf der Seite „Beziehungen“ der Richtlinie hinzugefügt. Sie können auf die Richtlinie klicken, um die Zuweisungen anzuzeigen.

Zuweisen einer Richtlinie zur Zone

Sie können Sicherheitsrichtlinien der Verwaltungszone zuweisen. Bei der Festlegung der effektiven Richtlinien, die auf einem Gerät erzwungen werden sollen, werden die Zonenrichtlinien nach allen anderen Richtlinien, die Benutzern und Geräten zugewiesen wurden, evaluiert. Betrachten Sie folgende Situationen:

- Einem Gerät bzw. dem Benutzer des Geräts sind keine Firewall-Richtlinien zugewiesen (weder direkt noch über eine Gruppe oder einen Ordner). Die Firewall-Richtlinie der Zone wird die effektive Richtlinie für das Gerät und wird auf dem Gerät erzwungen.
- Firewall-Richtlinien sind einem Gerät und dem Benutzer des Geräts zugewiesen. Beide Richtlinien werden ausgewertet und zusammengeführt, um die effektive Firewall-Richtlinie festzulegen die auf das Gerät angewendet werden soll. Nachdem die effektive Richtlinie aus den dem Benutzer bzw. dem Gerät zugewiesenen Richtlinien ermittelt wurde, wird die Firewall-Richtlinie der Zone verwendet, um Werte bereitzustellen, die 1) in der effektiven Firewall-Richtlinie nicht festgelegt sind und 2) sich ergänzen (z. B. die mehrwertigen Tabellen für Port-/Protokollregeln).

Zonenrichtlinien können auf drei Ebenen definiert werden. Dadurch können Sie unterschiedlichen Geräten in Ihrer Verwaltungszone unterschiedliche Richtlinien zuweisen.

- **Verwaltungszone:** Die Richtlinien, die Sie in der Verwaltungszone zuweisen, werden zu den Zonenrichtlinien für alle Geräte, sofern Sie nicht andere Zonenrichtlinien auf der Geräteordner- oder Geräteebene angeben.
- **Geräteordner:** Die Richtlinien, die Sie für Geräteordner definieren, setzen die Richtlinien für die Verwaltungszone (und etwaige übergeordnete Geräteordner) außer Kraft und werden zu den Zonenrichtlinien für alle in der Ordnerstruktur enthaltenen Geräte, sofern Sie nicht andere Zonenrichtlinien für einen Unterordner oder ein Einzelgerät angeben.
- **Gerät:** Die Richtlinien, die Sie für ein Einzelgerät definieren, setzen die Richtlinien für die Verwaltungszone und für den Geräteordner außer Kraft und werden zu den Zonenrichtlinien für das Gerät.

In den folgenden Schritten erhalten Sie Anweisungen zum Zuweisen von Richtlinien in der Verwaltungszone.

1. Klicken Sie im ZENworks-Kontrollzentrum auf **Konfiguration**, um die Seite „Konfiguration“ anzuzeigen.
2. Klicken Sie in der Kontrollleiste „Verwaltungszoneneinstellungen“ auf **Endpoint Security Management**.
3. Klicken Sie auf **Zonenrichtlinieneinstellungen**, um die Seite „Zonenrichtlinieneinstellungen“ anzuzeigen.

4 Klicken Sie auf **Hinzufügen**, suchen Sie die Richtlinien, die der Zone zugewiesen werden sollen, wählen Sie sie aus und klicken Sie anschließend auf **OK**, um sie der Liste hinzuzufügen.

5 Klicken Sie auf **OK**, wenn Sie die Richtlinien hinzugefügt haben.

Weitere Informationen

Weitere Informationen zur Verwendung von ZENworks Endpoint Security Management finden Sie in den folgenden Handbüchern:

- *ZENworks Endpoint Security Policies Reference*
- *ZENworks Endpoint Security Agent Reference*
- *ZENworks: Referenz für Endpoint Security-Dienstprogramme*
- *ZENworks: Referenz für Endpoint Security-Skripterstellung*

11 Vollständige Festplattenverschlüsselung

ZENworks Full Disk Encryption (vollständige Festplattenverschlüsselung) schützt die Daten eines Geräts vor nicht autorisiertem Zugriff, wenn das Gerät ausgeschaltet wurde bzw. sich im Ruhezustand befindet. Dadurch wird eine Kombination aus Festplattenverschlüsselung und Preboot-Authentifizierung verwendet.

Die vollständige Festplattenverschlüsselung bietet eine softwarebasierte Verschlüsselung für Standard-, Solid State- und selbstverschlüsselte Festplatten. Alle Festplatten-Volumes (oder ausgewählte Festplatten-Volumes) werden verschlüsselt, einschließlich Temporärdateien, Auslagerungsdateien und Betriebssystemdateien zu den Volumes. Der Zugriff auf die Daten ist nur möglich, wenn sich ein gültiger Benutzer anmeldet, nicht jedoch durch Booten des Geräts über Medien wie CD/DVD, Diskette oder USB-Laufwerk. Für einen authentifizierten Benutzer unterscheidet sich der Zugriff auf Daten auf der verschlüsselten Festplatte nicht vom Zugriff auf Daten auf einer unverschlüsselten Festplatte.

Die vollständige Festplattenverschlüsselung ermöglicht eine optionale Preboot-Authentifizierung für Festplatten. Die ZENworks-Komponente für die Preboot-Authentifizierung (PBA) wird als kleine Linux-Partition auf der Festplatte installiert. Die Anmeldung erfolgt über die ZENworks-PBA, die durch MDT-Prüfsummen gegen Manipulation und durch starke Verschlüsselung für die Schlüssel gegen Passwortextrahierung geschützt ist.

Die ZENworks-PBA unterstützt Single Sign-On mit der Windows-Anmeldung, sodass die Benutzer lediglich einen einzigen Berechtigungsnachweis (entweder Benutzername/Passwort oder Smartcard) verwenden müssen, um sich sowohl über den Windows-Client als auch über die ZENworks-PBA anzumelden.

Aktivieren der vollständigen Festplattenverschlüsselung (Full Disk Encryption)

Wenn Sie die vollständige Festplattenverschlüsselung nicht bereits bei der Installation der Verwaltungszone aktiviert haben, indem Sie entweder einen Lizenzschlüssel angegeben oder die Evaluierung eingeschaltet haben, müssen Sie dies nun nachholen.

So aktivieren Sie die vollständige Festplattenverschlüsselung (Full Disk Encryption):

1. Klicken Sie im ZENworks-Kontrollzentrum auf **Konfiguration**.
2. Klicken Sie im Bereich „Lizenzen“ auf **ZENworks 2020 Full Disk Encryption**.
3. Wählen Sie **Produkt evaluieren/aktivieren** aus und füllen Sie anschließend die folgenden Felder aus:

   Evaluierung verwenden: Wählen Sie diese Option aus, um den 60-Tage-Evaluierungszeitraum zu aktivieren. Nach dem 60-Tage-Zeitraum müssen Sie einen Produktlizenzschlüssel anwenden, um das Produkt weiterhin verwenden zu können.

   Produktlizenzschlüssel: Geben Sie den Lizenzschlüssel ein, den Sie für ZENworks Full Disk Encryption erworben haben. Eine Produktlizenz können Sie auf der ZENworks Endpoint Security Management-Produkt-Website (http://www.novell.com/products/zenworks/full-disk-encryption) erwerben.
4. Klicken Sie auf **OK**.

Aktivieren des Full Disk Encryption Agent

Der ZENworks Agent ist verantwortlich für die Geräteregistrierung, die Inhaltsverteilung und die Softwareaktualisierungen für ein Gerät.

Zusätzlich zum ZENworks Agent wird der Full Disk Encryption Agent auf Geräten installiert, wenn ZENworks Full Disk Encryption aktiviert wird (Volllizenz oder Evaluierung). Der Full Disk Encryption Agent ist für die Ver- und Entschlüsselung von Festplatten gemäß der für ein Gerät geltenden Festplattenverschlüsselungsrichtlinie zuständig.

Sie sollten sich vergewissern, dass der Full Disk Encryption Agent aktiviert ist. Eine Anleitung dazu finden Sie in Konfigurieren der ZENworks-Agent-Funktionen.

WICHTIG: ZENworks Full Disk Encryption bietet keine Unterstützung für die Windows-Funktion „Sicherer Start“. Diese Funktion muss vor der Installation des Agenten zur vollständigen Festplattenverschlüsselung auf Geräten deaktiviert werden. Weitere Informationen über Systemanforderungen finden Sie unter „System Requirements“ (Systemanforderungen) im Handbuch *ZENworks Full Disk Encryption Agent Reference* (ZENworks-Referenz für den Agenten zur vollständigen Festplattenverschlüsselung).

Erstellen einer Festplattenverschlüsselungsrichtlinie

Die Verschlüsselung der Festplatten eines Geräts und die Verwendung der (optionalen) Preboot-Authentifizierung von ZENworks werden beide über die Festplattenverschlüsselungsrichtlinie gesteuert.

So erstellen Sie eine Festplattenverschlüsselungsrichtlinie:

1. Klicken Sie im ZENworks-Kontrollzentrum auf **Richtlinien**, um die Seite „Richtlinien“ anzuzeigen.
2. Klicken Sie im Richtlinienbereich auf **Neu** > **Richtlinie**, um den Assistenten zum Erstellen neuer Richtlinien zu starten.
3. Wählen Sie auf der Seite „Plattform auswählen“ die Option **Windows** aus und klicken Sie anschließend auf **Weiter**.
4. Wählen Sie auf der Seite „Richtlinienkategorie auswählen“ die Option **Richtlinien für die vollständige Festplattenverschlüsselung unter Windows** aus und klicken Sie anschließend auf **Weiter**.
5. Wählen Sie auf der Seite „Richtlinientyp auswählen“ die Option **Festplattenverschlüsselungsrichtlinie** aus und klicken Sie anschließend auf **Weiter**.
6. Geben Sie auf der Seite „Details definieren“ einen Namen für die Richtlinie an und wählen Sie den Ordner aus, in dem die Richtlinie abgelegt werden soll.

   Der Name muss unter allen anderen im ausgewählten Ordner befindlichen Richtlinien eindeutig sein.
7. Konfigurieren Sie die richtlinienspezifischen Einstellungen und klicken Sie anschließend auf **Weiter**, bis Sie auf der Seite „Zusammenfassung“ angelangt sind.

   Weitere Informationen über die Einstellungen der Richtlinie erhalten Sie, wenn Sie im ZENworks-Kontrollzentrum auf **Hilfe** > **Aktuelle Seite** klicken.
8. Überprüfen Sie die Informationen auf der Seite „Zusammenfassung“, um sicherzustellen, dass sie korrekt sind. Falls Sie nicht korrekt sind, können Sie auf die Schaltfläche **Zurück** klicken, um die entsprechende Assistentenseite erneut zu besuchen und Änderungen vorzunehmen. Wenn die Informationen korrekt sind, wählen Sie eine der folgenden Optionen aus (falls gewünscht) und klicken Sie anschließend auf **Fertig stellen**.
   - **Als Sandbox erstellen:** Wählen Sie diese Option aus, um die Richtlinie als Sandbox-Version zu erstellen. Benutzer und Geräte haben erst Zugriff auf die Sandbox-Version, wenn Sie sie veröffentlichen. Sie können sie beispielsweise Benutzern und Geräten zuweisen, sie wird jedoch erst angewendet, nachdem Sie sie veröffentlicht haben.
   - **Zusätzliche Eigenschaften definieren:** Wählen Sie diese Option aus, um die Eigenschaftenseiten der Richtlinie anzuzeigen. Auf diesen Seiten können Sie Richtlinieneinstellungen bearbeiten und die Richtlinie Benutzern und Geräten zuweisen.

Zuweisen der Richtlinie zu Geräten

Nachdem Sie eine Festplattenverschlüsselungsrichtlinie erstellt haben, müssen Sie sie Geräten zuweisen.

Die Festplattenverschlüsselungsrichtlinie ist eine Nur-Gerät-Richtlinie. Sie kann Geräten und Geräteordnern zugewiesen werden. Sie kann nicht Gerätegruppen, Benutzern, Benutzergruppen oder Benutzerordnern zugewiesen werden.

Außerdem wird nur die Richtlinie angewendet, die dem Gerät am nächsten ist. Wenn beispielsweise einem Gerät und dem Geräteordner verschiedene Richtlinien zugewiesen wurden, wird die Richtlinie angewendet, die dem Gerät direkt zugewiesen wurde.

WICHTIG: Die Festplattenverschlüsselungsrichtlinie wird auf Windows-Geräten mit UEFI-BIOS nicht unterstützt. Wenn Sie einem Windows-UEFI-Gerät eine Festplattenverschlüsselungsrichtlinie zuweisen, so wird diese Richtlinie auf dem Gerät nicht angewendet.

---

1. Aktivieren Sie im Bereich „Richtlinien“ das Kontrollkästchen neben der Festplattenverschlüsselungsrichtlinie, die zugewiesen werden soll.
2. Klicken Sie auf **Aktion** > **Zu Gerät zuweisen**.
3. Folgen Sie den Eingabeaufforderungen, um die Richtlinie zuzuweisen.

   Klicken Sie auf den einzelnen Seiten des Assistenten auf die Schaltfläche **Hilfe**, um detaillierte Informationen zur jeweiligen Seite anzuzeigen.

   Wenn Sie den Assistenten vollständig ausführen, werden die zugewiesenen Geräte auf der Seite „Beziehungen“ der Richtlinie hinzugefügt. Sie können auf die Richtlinie klicken, um die Zuweisungen anzuzeigen.

Informationen zu den Vorgängen nach dem Zuweisen einer Richtlinie zu einem Gerät

Nachdem Sie einem Gerät eine Richtlinie zugewiesen haben, unterscheiden sich die Richtliniendurchsetzung und der Workflow zur Festplattenverschlüsselung geringfügig, wenn Sie die Preboot-Authentifizierung verwenden. Im Folgenden werden die Konzepte für die Festplattenverschlüsselung und Preboot-Authentifizierung beschrieben, die Sie verstehen müssen, wenn Sie eine Festplattenverschlüsselungsrichtlinie auf ein Gerät anwenden.

Festplattenverschlüsselung

ZENworks Full Disk Encryption bietet softwarebasierte Verschlüsselung für Standard-, Solid State- und selbstverschlüsselte Festplatten.

Mit Full Disk Encryption steht Ihnen eine sektorbasierte Verschlüsselung der gesamten Festplatte oder ausgewählter Volumes (Partitionen) zur Verfügung. Alle Dateien in einem Volume werden verschlüsselt, einschließlich etwaiger temporärer Dateien, Auslagerungsdateien oder Betriebssystemdateien. Da alle Dateien verschlüsselt werden, ist beim Booten des Computers von einem externen Medium wie CD-ROM, Diskette oder USB-Laufwerk kein Zugriff auf die Daten möglich.

Alle 3,5- oder 2,5-Zoll-Festplatten mit dem IDE-, SATA- oder PATA- Schnittstellenstandard sind kompatibel.

Sie können den Branchenstandard-Verschlüsselungsalgorithmus (AES, Blowfish, DES oder DESX) und die Schlüssellänge auswählen, die die Anforderungen Ihrer Organisation am besten erfüllt. Wenn die Gerätefirmware für UEFI konfiguriert ist, werden der AES-Algorithmus und die Schlüssellänge 256 automatisch verwendet.

HINWEIS: Das Kryptografiemodul, das in ZENworks Full Disk Encryption zum Verschlüsseln von standardmäßigen Festplatten verwendet wird, ist *nicht* nach dem Federal Information Processing Standard (FIPS) 140-2 zertifiziert. Das Kryptografiemodul implementiert jedoch die Standards, die der Zertifizierung nach FIPS 140-2 Level 1 entsprechen.

Authentifizierung vor dem Booten

ZENworks Full Disk Encryption schützt die Daten eines Geräts, wenn das Gerät ausgeschaltet wurde bzw. sich im Ruhezustand befindet. Sobald sich ein Benutzer erfolgreich beim Windows-Betriebssystem angemeldet hat, sind die verschlüsselten Volumes nicht mehr geschützt und der Benutzer kann ungehindert auf die Daten zugreifen. Für eine höhere Anmeldesicherheit können Sie die Preboot-Authentifizierung (PBA) von ZENworks verwenden.

Bei der ZENworks-PBA handelt es sich um eine Linux-basierte Komponente. Wenn die Festplattenverschlüsselungsrichtlinie auf ein Gerät angewendet wird, wird eine 500-MB-Partition mit einem Linux-Kernel und der ZENworks-PBA auf der Festplatte erstellt.

Während des normalen Betriebs bootet das Gerät in die Linux-Partition und lädt die ZENworks-PBA. Sobald der Benutzer den entsprechenden Berechtigungsnachweis (Benutzer-ID/Passwort oder Smartcard) bereitstellt, wird die PBA terminiert und das Windows-Betriebssystem bootet und gestattet den Zugriff auf die verschlüsselten Daten auf den zuvor verborgenen und unzugänglichen Windows-Laufwerken.

Die Linux-Partition ist gehärtet, bietet also einen höheren Schutz, und die ZENworks-PBA ist mit MD5-Prüfsummen und starker Verschlüsselung für Authentifizierungsschlüssel vor Änderungen geschützt.

ZENworks-Preboot-Authentifizierung wird dringend empfohlen. Wenn Sie ZENworks-PBA nicht verwenden, sind verschlüsselte Daten nur durch die Windows-Authentifizierung geschützt.

Weitere Informationen zur Preboot-Authentifizierung von ZENworks finden Sie im Handbuch *ZENworks Full Disk Encryption PBA Reference* (ZENworks: Referenz für die PBA zur vollständigen Festplattenverschlüsselung).

Weitere Informationen

Weitere Informationen zur vollständigen Festplattenverschlüsselung von ZENworks finden Sie in den folgenden Handbüchern:

- *ZENworks: Referenz für die Richtlinie zur vollständigen Festplattenverschlüsselung*
- *ZENworks: Referenz für den Agenten zur vollständigen Festplattenverschlüsselung*
- *ZENworks: Referenz für die PBA zur vollständigen Festplattenverschlüsselung*
- *ZENworks: Referenz für die Notfallwiederherstellung der vollständigen Festplattenverschlüsselung*

12 Patch Management

Mit Patch Management können Sie Softwarepatches automatisch und konsistent anwenden, um Schwachstellen und Probleme zu minimieren.

Patch Management bleibt auf dem aktuellen Stand mit neuesten Patches und Fehlerbehebungen durch regelmäßige Internet-Kommunikation mit dem ZENworks Patch Subscription Service. Wenn Sie den täglichen Download der neuesten Daten zu Schwachstellen und Patches nach der 60-tägigen Testzeit weiter nutzen möchten, müssen Sie ein kostenpflichtiges Abonnement für Patch Management erwerben.

Wenn ein neuer Patch vom Abonnementservice verfügbar ist, lädt ein ZENworks-Server die entsprechenden Informationen herunter. Sie können den Patch auf Geräten bereitstellen oder ignorieren.

Nachdem die Patches auf den ZENworks-Server heruntergeladen und eine Patch-Absuche durchgeführt wurde, können Sie in der Patch-Verwaltung feststellen, welche Geräte in Ihrer Zone anfällig sind. Sie können jedoch nicht ohne Weiteres feststellen, welche Schwachstelle durch einen Patch behoben wird. Dazu müssen Sie das Fenster „Patch-Details“ anzeigen oder die CVE-ID kennen, anhand derer Sie eine Suche durchführen können. Im Rahmen der Sicherheitsfunktion bietet Ihnen ZENworks jetzt jedoch eine neue Sicherheitsansicht, mit der die Einrichtung und Verfolgung der Sicherheit in Ihrer Zone vereinfacht wird. Mit der auf Schwachstellen basierenden Ansicht und dem Ansatz zur Fehlerbehebung können Sie sich schnell einen Überblick über den Sicherheitsstatus Ihrer Geräte verschaffen. Sie können Patches anhand von CVE-Informationen ermitteln und dann die Schwachstellen auf anfälligen Geräten beheben, indem Sie die relevante Patch-Behebungsrichtlinie oder das entsprechende Bundle anwenden. Schwachstellen können in ZENworks durch folgende Vorgehensweise ermittelt werden:

1. Der Administrator erstellt ein CVE-Abonnement und führt es aus, um Daten aus dem NVD-Repository zu importieren.
2. Der Administrator erstellt ein Patch-Abonnement und führt es aus, um Daten aus dem Repository für Patch-Inhalte zu importieren.

   Nachdem das CVE- und das Patch-Abonnement ausgeführt wurden, werden die CVEs und Patches in den konfigurierten ZENworks-Server importiert.
3. Anhand der CVE-ID, die der Patch-Signatur zugeordnet ist, weist ZENworks die Patches den CVEs zu.

   Wenn bei der Geräteaktualisierung eine Patch-Absuche auf Geräten durchgeführt wird, werden die anfälligen Geräte ermittelt. Benutzer können abhängig von ihren Anforderungen auch einen Zeitplan für die Patch-Absuche konfigurieren oder die Schnellaufgabe „Patch-Absuche starten“ manuell ausführen.
4. Die entsprechenden Patches werden dann auf den anfälligen Geräten bereitgestellt, entweder über Patch-Richtlinien oder über Fehlerbehebungs-Bundles.

Sobald alle Patches des CVE auf dem Gerät installiert sind, ist das Gerät nicht mehr anfällig.

In den folgenden Abschnitten wird erläutert, wie Sie die CVE- und die Patch-Verwaltung verwenden, um Schwachstellen und Probleme zu identifizieren, die durch veraltete Software oder Software ohne Patches auftreten können.

Erstellen und Konfigurieren des CVE-Abonnements

Um ZENworks zu ermöglichen, CVE-Daten aus der National Vulnerability Database (NVD) zu importieren, müssen Sie zunächst das CVE-Abonnement erstellen und ausführen.

Erstellen des CVE-Abonnements

So erstellen Sie das CVE-Abonnement:

1. Melden Sie sich beim ZENworks-Kontrollzentrum an und klicken Sie auf **Abonnieren und freigeben**.
2. Klicken Sie in der Liste „Abonnements“ auf **Neu** > **Abonnement**.
3. Wählen Sie auf der Seite „Abonnementtyp auswählen“ das CVE-Abonnement aus und klicken Sie auf **Weiter**.
4. Geben Sie auf der Seite „Details definieren“ die folgenden Details an:
   - **Name des Abonnements:** Eindeutiger Name des Abonnements.
   - **Ordner:** Geben Sie den Namen des Ordners ein oder navigieren Sie zu dem Ordner, in dem dieses Abonnement erstellt werden soll. Das Abonnement wird standardmäßig im Ordner „/Subscriptions“ erstellt.
   - **Beschreibung:** Eine kurze Beschreibung des Abonnements. Diese Beschreibung wird auf der Seite „Zusammenfassung“ des Abonnements angezeigt.
5. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite „CVE-Abonnement-Server auswählen“ den Primärserver aus, auf dem der CVE-Abonnementdienst ausgeführt wird. Die CVE-Daten aus dem NVD-Repository werden auf diesen Server heruntergeladen.
7. Wählen Sie die Häufigkeit, mit der die CVE-Daten aus dem NVD-Repository heruntergeladen werden sollen. Standardmäßig werden die CVE-Daten täglich um 23:00 Uhr heruntergeladen.

   Das CVE-Abonnement sollte vor dem Patch-Abonnement ausgeführt werden, damit das Patch-Abonnement die CVE-Patch-Zuordnung vornehmen kann. Wenn das CVE-Abonnement nach dem Patch-Abonnement ausgeführt wird, erfolgt die Zuordnung erst bei der nächsten Ausführung des Patch-Abonnements, die möglicherweise am nächsten Tag stattfindet.

8 Klicken Sie auf **Weiter**, um die Seite „Zusammenfassung“ anzuzeigen.

9 Überprüfen Sie die Informationen. Wenn Änderungen erforderlich sind, können Sie diese über die Schaltfläche **Zurück** vornehmen.

10 (Bedingt) Aktivieren Sie das Kontrollkästchen **Zusätzliche Eigenschaften definieren**, um nach Fertigstellung des Assistenten die Seite „Zusammenfassung“ des Abonnements anzuzeigen.

Auf den verschiedenen Registerkarten der Seite „Zusammenfassung“ können Sie die Abonnementinformationen bearbeiten.

11 (Bedingt) Aktivieren Sie das Kontrollkästchen **Abonnement jetzt ausführen**, um den Abonnementdienst direkt im Anschluss an die Erstellung des Abonnements auszuführen. Sie können das Abonnement auch zu einem späteren Zeitpunkt ausführen, indem Sie zur Seite **Abonnieren und freigeben** navigieren und auf das CVE-Abonnement klicken.

12 Klicken Sie auf **Fertig stellen**, um das Abonnement zu erstellen.

Konfigurieren des CVE-Abonnements

Wenn Sie beim Erstellen des CVE-Abonnements nicht die Option ausgewählt haben, mit der der Abonnementdienst direkt im Anschluss an die Erstellung des CVE-Abonnements gestartet wird, können Sie das Abonnement starten und auch Änderungen daran vornehmen, indem Sie das CVE-Abonnementobjekt auswählen.

1 Klicken Sie im linken Bereich von ZCC auf **Abonnieren und freigeben**.

2 Klicken Sie auf der Seite „Abonnements“ auf das Objekt „CVE-Abonnement“. Die Details zum CVE-Abonnement werden angezeigt:

Der Bereich „Allgemein“ enthält folgende Informationen:

- Name: Zeigt den Namen des Abonnements an.
- Typ: Zeigt den Typ des Abonnements an.
- Erstellt von: Zeigt den Namen des Benutzers an, der das Abonnement erstellt hat.
- GUID: Zeigt den GUID (Global Unique Identifier) des Abonnements an, eine nach dem Zufallsprinzip generierte Zeichenkette, die einen eindeutigen Bezeichner für das Abonnement bereitstellt.
- Beschreibung: Zeigt eine Beschreibung des Abonnements an, sofern bei der Erstellung des Abonnements eine Beschreibung angegeben wurde. Die Beschreibung wird nur im ZENworks-Kontrollzentrum angezeigt. Klicken Sie auf Bearbeiten, um die Beschreibung zu ändern.
- Aktiviert: Zeigt an, ob das Abonnement aktiviert ist oder nicht.
- Abonnement-Protokolle: Zeigt die mit der letzten Ausführung des Abonnements verknüpften Meldungen an. Klicken Sie auf den Link „Protokoll anzeigen“, um die Abonnementprotokolle anzuzeigen.

Der Bereich „Abonnement“ zeigt eine Zusammenfassung des CVE-Abonnements. Es können folgende Details angezeigt werden:

- URL für CVE-NVD-Feeds: Die URL des NVD-Repositorys, aus dem die CVE-Feeds importiert werden. Mit dem Link „Bearbeiten“ können Sie die URL ändern.

WICHTIG: Ändern Sie die URL NICHT, es sei denn, Sie werden vom Micro Focus-Kundenservice dazu aufgefordert.

- CVE-Abonnement-Server: Server, der sich mit dem NVD-Repository synchronisiert sowie CVE-Daten herunterlädt und in der ZENworks-Datenbank speichert.
- Letzte Reproduktion: Datum und Uhrzeit der letzten Synchronisierung des Abonnementservers mit dem NVD-Repository. Die folgenden Optionen stehen zur Auswahl:
  - Jetzt ausführen: Synchronisierung wird sofort ausgeführt, ohne bis zu dem im Zeitplan festgelegten Zeitpunkt zu warten. Bei der ersten Synchronisierung erfolgt die vollständige Ausführung, mit der alle CVE-Daten heruntergeladen werden. Liegt die letzte Ausführung weniger als 8 Tage zurück, werden jedoch nur die Änderungen seit der letzten Ausführung heruntergeladen.
  - Manuell importieren: Laden Sie die Daten aus dem NVD-Repository im JSON-Dateiformat herunter und laden Sie dann die JSON-ZIP-Datei auf den Server hoch. Dieser Schritt muss nur bei einem Problem mit dem Abonnementdienst ausgeführt werden. Um die Datei manuell heraufzuladen, navigieren Sie zu https://nvd.nist.gov/vuln/data-feeds und wählen die ZIP-Datei für das Jahr aus, für das Sie die Daten herunterladen möchten. Sie können auch eine ZIP-Datei mit dem Feed-Namen **CVE-Modified** auswählen, um nur die geänderten CVE-Daten herunterzuladen.
- Vollständige Ausführung: Falls noch keine CVE-Daten heruntergeladen wurden oder die letzte Ausführung mehr als 8 Tage zurückliegt, laden Sie mit dieser Funktion alle Daten aus dem NVD-Repository herunter.
- Status: Status der letzten Synchronisierung mit dem NVD-Repository.
- Planungsintervall: Das Intervall, in dem die Synchronisierung mit dem NVD-Server durchgeführt wird. Sie können die Synchronisierung wahlweise täglich zu einer bestimmten Uhrzeit oder auch im Stundenabstand ausführen.

Aktivieren der Patchverwaltung

1. Klicken Sie im ZENworks-Kontrollzentrum auf **Konfiguration**.
2. Klicken Sie in der Kontrollleiste „Lizenzen“ auf **ZENworks 2020 Patch Management**.
3. Wählen Sie **Produkt aktivieren** und füllen Sie die Felder aus:

   Seriennummer des Produktabonnements: Die Seriennummer, die Sie beim Kauf der Abonnementlizenz erhalten haben. Wenn Sie keine Abonnementlizenz gekauft haben, können Sie den Testevaluierungscode eingeben. Nach Ablauf des 60-tägigen Evaluierungszeitraums ist für Patch Management eine Abonnementlizenz erforderlich, um sicherzustellen, dass Sie weiterhin Patches vom Abonnementdienst erhalten. Eine Abonnementlizenz können Sie auf der ZENworks Patch Management-Produkt-Website (http://www.novell.com/products/zenworks/patchmanagement) erwerben.
4. Klicken Sie auf **Apply** (Anwenden).

Aktivieren der Patchverwaltung im ZENworks Agent

Damit der ZENworks Agent Patchverwaltungsvorgänge auf einem Gerät durchführen kann, muss die Patchverwaltungsfunktion des Agent aktiviert werden. Die Patchverwaltungsfunktion wird standardmäßig aktiviert, sobald ZENworks Patch Management aktiviert wird (mit Voll- oder Evaluierungslizenz).

Überprüfen Sie, ob die Patchverwaltungsfunktion des Agent nach wie vor aktiviert ist. Eine Anleitung dazu finden Sie in „Konfigurieren der ZENworks-Agent-Funktionen“, auf Seite 41.

Starten des Patch-Abonnementdiensts

Bevor Sie Patches empfangen können, müssen Sie den Abonnementdienst auf einem unserer ZENworks-Server starten und die Option für das tägliche Herunterladen von Patches aktivieren.

Wenn ein neuer Patch vom Abonnementdienst verfügbar ist, wird er automatisch von einem ZENworks-Server heruntergeladen. Auf der Seite „Patches“ (der Registerkarte **Sicherheit**) wird der neue Patch zusammen mit einer Beschreibung und der betrieblichen Auswirkung angezeigt. Sie können den Patch auf Geräten bereitstellen oder ignorieren.

Patch Management bleibt auf dem aktuellen Stand mit neuesten Patches und Fehlerbehebungen durch regelmäßige Internet-Kommunikation mit dem ZENworks Patch Subscription Service. Nach der anfänglichen 60-tägigen Evaluierungsphase erfordert Patch Management ein kostenpflichtiges Abonnement, um den täglichen Download der neuesten Daten zu Schwachstellen und Patches fortzusetzen.

Wenn es mehrere ZENworks-Server in Ihrer Verwaltungszone gibt, können Sie einen beliebigen als Patchverwaltungsserver auswählen. Der als Patch Management-Server ausgewählte Server sollte über eine optimale Internetkonnektivität verfügen, da er täglich neue Patches und Aktualisierungen herunterlädt.

So starten Sie den Abonnementdienst:

1. Klicken Sie im ZENworks-Kontrollzentrum auf die Registerkarte **Konfiguration**.
2. Klicken Sie unter „Verwaltungszoneneinstellungen“ auf **Sicherheit** und dann auf **Patch Subscription Service Information** (Informationen für den Patch-Abonnementdienst).
3. Wählen Sie in der Liste **Startet den Abonnementdienst** den ZENworks-Server aus, der den Abonnementdienst ausführen soll, und klicken Sie dann auf **Dienst starten**.

   Sobald der Abonnementdienst ausgeführt wird, wird auf der Schaltfläche **Dienst starten** der Text **Dienst wird ausgeführt** angezeigt.
4. Wählen Sie aus der Liste **Intervall der Abonnement-Kommunikation (täglich um)** die Zeit aus, zu der täglich die Patches heruntergeladen werden sollen.
5. Klicken Sie auf **OK**.

Erstellen von Patch-Richtlinien

Bevor Sie Patches auf Geräten bereitstellen können, muss der ZENworks Agent die Aufgabe zur Ermittlung anwendbarer Aktualisierungen (Discover Applicable Updates, DAU) ausführen. Mithilfe der DAU-Aufgabe kann der ZENworks Agent den Status („Gepatcht“, „Nicht gepatcht“ oder „Nicht zutreffend“) der einzelnen Patches abhängig von den Geräten Ihres Netzwerks erkennen.

Der Patch-Erkennungszyklus wird jeden Tag auf dem ZENworks-Server ausgeführt, auf dem für jedes verwaltete Gerät (Server und Arbeitsstationen) eine Aufgabe zur Ermittlung anwendbarer Aktualisierungen (DAU) geplant ist. Sie können auch eine DAU-Aufgabe von einem einzelnen Agenten aus starten. Die Ergebnisse der Patch-Erkennung werden im Abschnitt „Patches“ unter der Registerkarte **Sicherheit** oder der Registerkarte **Geräte** des ZENworks-Servers angezeigt. Die Ergebnisse sind auch dann verfügbar, wenn die Verbindung einer Arbeitsstation zum Netzwerk getrennt ist.

Stellen Sie die Patches wahlweise mit Patch-Richtlinien oder mit der Funktion „Behebung bereitstellen“ bereit. Die Patch-Richtlinien automatisieren die Patch-Bereitstellung und werden daher empfohlen. Mithilfe von Regeln in den Patch-Richtlinien beschränken Sie das Caching und die Bereitstellung ausschließlich auf die Patches, die für die Geräte tatsächlich erforderlich sind.

Die folgenden Schritte setzen voraus, dass mindestens ein Patch vom Abonnementdienst zur Verfügung steht.

1. Navigieren Sie im ZENworks-Kontrollzentrum zu **Sicherheit** > **Patch-Richtlinien**.
2. Klicken Sie auf der Seite „Patch-Richtlinien“ auf **Neu**.
3. Befolgen Sie die Anweisungen zum Erstellen einer Patch-Richtlinie.

   Mit der Schaltfläche **Hilfe** auf den einzelnen Seiten erhalten Sie jeweils ausführliche Informationen zur betreffenden Seite.
4. Klicken Sie auf die erstellte Patch-Richtlinie und wechseln Sie zur Seite **Beziehungen**.
5. Klicken Sie im Bereich „Gerätezuweisungen“ auf **Hinzufügen** und weisen Sie der Richtlinie mindestens ein Gerät zu.
6. Klicken Sie auf **Veröffentlichen**. Die erforderlichen Patches werden gemäß der Konfiguration der Patch-Richtlinie an die Geräte verteilt und dort angewendet.

WICHTIG: Wenden Sie die Patches zunächst probehalber auf ein Testgerät an, bevor Sie sie auf die Geräte in der gesamten Zone anwenden. Die Patches werden auf allen als „Testgerät“ konfigurierten Geräten automatisch über die Sandbox angewendet; Schritt 6 (Veröffentlichen der Richtlinie) wird dabei übersprungen.

Alternativ können Sie schon beim Erstellen der Patch-Richtlinie die Option **Patches nach erfolgreicher Testdurchsetzung automatisch genehmigen** konfigurieren. Mit dieser Option in der Richtlinienkonfiguration wird die Richtlinie automatisch auf allen Geräten veröffentlicht, die dieser Richtlinie zugewiesen sind, sobald die Anwendung auf 100 Prozent der Testgeräte erfolgreich abgeschlossen wurde, wobei die Veröffentlichung (Schritt 6 oben) wiederum entfällt.

Weitere Informationen

Weitere Informationen über die Verfolgung von Software-Schwachstellen auf Geräten mithilfe von CVE-Daten, damit Sie anschließend auf diese Schwachstellen durch Anwendung des entsprechenden Patches reagieren können, finden Sie in der *ZENworks-CVE-Referenz*.

Weitere Informationen zum Konfigurieren von Patch Management, zur Automatisierung der Patch-Verteilung in der Verwaltungszone mithilfe von Patch-Richtlinien sowie zur Funktion „Behebung bereitstellen“ finden Sie in der *Referenz zu ZENworks Patch Management*.