Novell ZENworks Endpoint Security Management 3.5

18. August 2008

1 Überblick

Die in diesem Dokument beschriebenen Probleme wurden in Novell® ZENworks® Endpoint Security Management 3.5 beobachtet.

- Informationen zur Installation finden Sie im *ZENworks Endpoint Security Management-Installationshandbuch*.
- Bei Fragen zu administrativen Aufgaben sehen Sie bitte im *ZENworks Endpoint Security Management-Administrationshandbuch* nach.

2 Bekannte Probleme

Dieser Abschnitt enthält Informationen zu Problemen, die in ZENworks Endpoint Security Management auftreten können.

2.1 Installation

Dieser Abschnitt enthält Informationen zu den Problemen, die bei der Installation von ZENworks Endpoint Security Management auftreten können.

2.1.1 Windows Server 2008 wird nicht unterstützt.

Die Komponenten des ZENworks Endpoint Security Management-Servers lassen sich aufgrund der neueren IIS-Version nicht unter Microsoft* Windows Server* 2008 installieren.

2.1.2 Installieren der Verwaltungskonsole auf einem Gerät in Active Directory

Das Gerät, auf dem Sie die Verwaltungskonsole installieren, muss ein Mitglied der Active Directory*-Domäne sein, die Sie konfigurieren, oder zumindest eine Verbürgungsbeziehung mit der Domäne aufweisen.

2.1.3 Das Betriebssystem Windows XP mit 64 Bit wird nicht unterstützt.

ZENworks Endpoint Security Management kann auf dem Betriebssystem Windows* XP mit 64 Bit nicht ausgeführt werden. Wir unterstützen allerdings 64-Bit-CPUs auf einem 32-Bit-Betriebssystem. Microsoft Vista* wird zurzeit nicht unterstützt.

2.1.4 Die Verwendung von SQL 2005 und SQL 2008 mit dem ZENworks Endpoint Security Management-Server wird nicht unterstützt.

Informationen über die Verwendung von SQL 2005 und SQL 2008 mit ZENworks Endpoint Security Management finden Sie in TID 3466284 (http://www.novell.com/support/supportcentral/supportcentral.do?id=m1).

2.1.5 SQL Server Express 2005 und SQL Server Express 2008 werden nicht unterstützt.

ZENworks Endpoint Security Management-Server und die Einzelplatz-Verwaltungskonsole werden von SQL Server* Express 2005 und SQL Server Express 2008 nicht unterstützt.

2.1.6 Verwendung von Sonderzeichen im Passwort für das DS_STDSDB_User-Konto

Wenn Sie Sonderzeichen im Passwort für das DS_STDSDB_User-Konto verwenden, werden die Sonderzeichen in den Konfigurationsdateien geändert. So wird beispielsweise @ in den Konfigurationsdateien zu A geändert. Die Kommunikation zwischen Server und Datenbank funktioniert erwartungsgemäß. Wenn Sie jedoch eine Fehlersuche mit OSQL durchführen, müssen Sie die Passwörter der Konfigurationsdatei verwenden, nicht die Passwörter, die Sie mit Sonderzeichen angegeben haben.

2.1.7 Bei Verwendung von SQL Server 2005 müssen Sie sicherstellen, dass die Richtlinie für die Domänensicherheit die Passwortrichtlinie deaktiviert hat, die festlegt: "Kennwort muss Komplexitätsvoraussetzungen entsprechen".

Wenn Sie eine Verbindung mit SQL Server 2005 herstellen, müssen Sie sicherstellen, dass die Richtlinie für die Domänensicherheit die Passwortrichtlinie deaktiviert hat, die gewährleistet, dass das Passwort den Komplexitätsvoraussetzungen entspricht. Nach der Installation können Sie diese Richtlinie erneut aktivieren, da für die in ZENworks Endpoint Security Management für SQL erstellten Konten kein Ablaufdatum gilt.

Diese Richtlinie führt dazu, dass in SQL Server 2005 erstellte SQL-Konten aufgrund der Einschränkung nicht funktionieren. ZENworks Endpoint Security Management kann nur installiert werden, wenn diese Richtlinie deaktiviert wurde. Wenn diese Richtlinie nicht deaktiviert ist, wenn das DS_STDSDB_User-Konto erstellt wird, erhalten Sie eine Meldung, die besagt, dass das für STDSDB eingegebene Passwort falsch ist.

Umgehung des Problems: Sie können die Benutzerkonten mithilfe der Konfigurationsdateien manuell erstellen.

2.2 Anwendungsblockierung

Dieser Abschnitt enthält Informationen zu den Problemen, die bei der Verwendung der Anwendungsblockierung in ZENworks Endpoint Security Management auftreten können.

- „Blockieren einer aktiven Anwendung“ auf Seite 3
- „Blockieren des Netzwerkzugriffs“ auf Seite 3
- „Blockieren einer Anwendung, die eine Netzwerkfreigabe verwendet“ auf Seite 4
- „Blockieren einer Anwendung, die über eine Netzlaufwerksfreigabe gestartet wurde“ auf Seite 4
- „Blockieren von Anwendungen und Sicherheitsmodus“ auf Seite 4

2.2.1 Blockieren einer aktiven Anwendung

Durch Blockieren der Ausführung einer Anwendung wird eine Anwendung, die bereits auf dem Endpunkt geöffnet ist, nicht geschlossen.

2.2.2 Blockieren des Netzwerkzugriffs

Das Blockieren des Netzwerkzugriffs auf eine Anwendung unterbricht nicht den Zugriff auf eine Anwendung, die aktives Daten-Streaming an den Endpunkt durchführt.

2.2.3 Blockieren einer Anwendung, die eine Netzwerkfreigabe verwendet

Das Blockieren des Netzwerkzugriffs auf eine Anwendung unterbricht nicht den Zugriff auf eine Anwendung, die Daten über eine Netzwerkfreigabe erhält.

2.2.4 Blockieren einer Anwendung, die über eine Netzlaufwerksfreigabe gestartet wurde

Wenn die Ausführung einer Anwendung blockiert ist, wird diese dennoch gestartet, wenn der Start über eine Netzlaufwerksfreigabe erfolgt, bei der der Lesezugriff für das System blockiert wurde.

2.2.5 Blockieren von Anwendungen und Sicherheitsmodus

Die Netzwerk-Anwendungssteuerung funktioniert nicht, wenn das Gerät mit Networking im Sicherheitsmodus gebootet wird.

2.3 Client Self Defense

Dieser Abschnitt enthält Informationen zu den Problemen, die bei der Verwendung von Client Self Defense in ZEN Endpoint Security Management auftreten können.

- „Client Self Defense erfordert ein Passwort zur Deinstallation“ auf Seite 4
- „GPO-Sicherheitsrichtlinien und Software von Drittanbietern können CPU-Spitzenauslastungen (Spikes) verursachen“ auf Seite 4

2.3.1 Client Self Defense erfordert ein Passwort zur Deinstallation

Damit Client Self Defense vollständig funktionieren kann, muss ein Passwort für die Deinstallation implementiert werden.

2.3.2 GPO-Sicherheitsrichtlinien und Software von Drittanbietern können CPU-Spitzenauslastungen (Spikes) verursachen

Es besteht die Möglichkeit, dass eine Interaktion mit GPO-Sicherheitsrichtlinien oder Software von Drittanbietern, die den Zugriff auf die Registrierung, Dateien und Ordner, WMI und Prozess- oder Serviceinformationen steuert, CPU-Spitzenauslastungen (Spikes) verursacht. GPO-Sicherheitsrichtlinien, die verhindern, dass der ZENworks Endpoint Security Management-Client die Registrierungsschlüssel, die das Produkt benötigt, liest und zurücksetzt, können CPU-Spitzenauslastungen (Spikes) verursachen. Antivirus- und SpyWare-Software erfordern eventuell die uneingeschränkte Ausführbarkeit von `STEngine.exe` und `STUser.exe`.

2.4 Steuern der Kommunikations-Hardware

Dieser Abschnitt enthält Informationen zu den Problemen, die bei der Verwendung von ZENworks Endpoint Security Management zur Steuerung der Kommunikations-Hardware auftreten können.

- „Unterstützte Geräte“ auf Seite 5
- „Geräteunterstützung feststellen“ auf Seite 5

2.4.1 Unterstützte Geräte

Die meisten Widcom-basierten Bluetooth*-Lösungen werden unterstützt. Folgende Geräte werden unterstützt:

- Geräte, die den Microsoft-Standard Typ GUID {e0cbf06cL-cd8b-4647-bb8a263b43f0f974} verwenden
- Geräte, die das Dell* USB Bluetooth-Module; den Dell Typ GUID {7240100F-6512-4548-8418-9EBB5C6A1A94} verwenden
- Geräte, die das HP*/Compaq* Bluetooth-Modul verwenden; HP Typ GUID {95C7A0A0L-3094-11D7-A202-00508B9D7D5A}verwenden

2.4.2 Geräteunterstützung feststellen

1. Öffnen Sie Regedit.
2. Navigieren Sie zu `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class`.
3. Suchen Sie nach den gelisteten Typen der GUID-Schlüssel (gelistet inAbschnitt 2.4.1, „Unterstützte Geräte“, auf Seite 5).Der Microsoft-Schlüssel muss mehr als einen Unterschlüssel haben, um gültig zu sein.

2.5 Datenverschlüsselung und Leistung

Dieser Abschnitt enthält Informationen zu den Leistungsproblemen, die bei der Verwendung von Datenverschlüsselung in ZENworks Endpoint Security Management auftreten können.

2.5.1 Verwenden von Datenverschlüsselung in Windows 2000 SP4 und Windows XP SP1

ZENworks Endpoint Security Management wird auf Windows XP SP2 durch erforderliche Filter-Manager-Unterstützung unterstützt. ZENworks Endpoint Security Management kann auf Windows 2000 SP4 und XP SP1 installiert werden. Wenn diese Betriebssysteme jedoch eine Verschlüsselungsrichtlinie erhalten, werden die Anfragen zur Verschlüsselung ignoriert und eine Warnmeldung wird an den Administrator gesendet.

2.5.2 Verwenden des ZENworks File Decryption Utility

Das ZENworks File Decryption Utility wird verwendet, um passwortgeschützte Daten aus dem Ordner `Freigegebene Dateien` auf verschlüsselte Wechseldatenträger zu extrahieren. Dieses einfache Tool kann der Benutzer an andere senden (obwohl es nicht auf dem Wechseldatenträger gespeichert werden kann), damit eine andere Person auf die Dateien im Ordner `Freigegebene Dateien` zugreifen kann.

Das Programm befindet sich auf der Produkt-DVD oder auf der Novell ZENworks Endpoint Security Management Website (ftp://ftp.novell.com/outgoing/STDECRYPT-NOVELL-Release-3.5.zip).

Weitere Informationen finden Sie unter "Verwendung des ZENworks File Decryption Utility" im *ZENworks Endpoint Security Management-Administrationshandbuch*.

2.5.3 Kopieren von Ordnern auf einen Wechseldatenträger mit aktivierter Verschlüsselung

Das Kopieren von Ordnern, die viele Dateien und Ordner enthalten, auf einen Wechseldatenträger mit aktivierter Verschlüsselung nimmt längere Zeit in Anspruch. In unseren Tests dauerte beispielsweise das Kopieren eines Ordners mit 38 MB zwischen fünf und sechs Minuten.

2.5.4 Anwendungen, die direkt auf einen verschlüsselten Wechseldatenträger speichern, können zu Leistungsproblemen führen

Eine potenzielle Leistungsbeeinträchtigung des Computers liegt vor, wenn Anwendungen direkt auf einen verschlüsselten Wechseldatenträger speichern (abhängig von der von der Anwendung verwendeten Schreibgröße für die Datei).

2.5.5 Auswahl von Safe Harbor-Bereichen im System-Volume.

Eine potenzielle Leistungsbeeinträchtigung des Computers liegt vor, wenn auf dem System-Volume Safe Harbor-Bereiche ausgewählt werden.

2.5.6 Verschlüsseln des Ordners "Eigene Dateien"

Bei Verschlüsselung des Ordners `Eigene Dateien` erhält nur der aktive Benutzer Zugriff zur Entschlüsselung der Dateien in seinem jeweiligen Ordner `Meine Dokumente` (nicht im gleichnamigen Ordner anderer Personen).

2.5.7 Kopieren mehrerer Dateien von einem Laufwerk mit Verschlüsselung für Wechseldatenträger auf ein eingebautes Laufwerk mit Safe Harbor-Verschlüsselung

Das Kopieren mehrerer Dateien von einem Laufwerk mit Verschlüsselung für Wechseldatenträger auf ein eingebautes Laufwerk mit Safe Harbor-Verschlüsselung kann geraume Zeit in Anspruch nehmen.

2.5.8 Zur Aktivierung der Safe Harbor-Funktion ist zweimaliges erneutes Booten erforderlich

Zweimaliges erneutes Booten ist erforderlich, wenn die Verschlüsselung in einer Richtlinie erstmals aktiviert wird und wenn entweder die Safe Harbor-Verschlüsselung oder die Verschlüsselung für Wechseldatenträger aktiviert wird (wenn die Aktivierung getrennt von der

Verschlüsselungsaktivierung erfolgt). Beispielsweise ist zweimaliges erneutes Booten erforderlich, wenn eine Verschlüsselungsrichtlinie erstmals angewendet wird: Beim ersten erneuten Booten werden die Treiber initialisiert und beim zweiten werden etwaige Safe Harbor-Bereiche in die Verschlüsselung einbezogen. Wenn nach der Anwendung der Richtlinie weitere Safe Harbor-Bereiche ausgewählt werden, ist nur ein einmaliges erneutes Booten erforderlich, um den betreffenden Safe Harbor-Bereich in die Richtlinie aufzunehmen.

2.6 Verwenden des Assistenten für neue Directory Services

Dieser Abschnitt enthält allgemeine Informationen zur Konfiguration von Directory Services mit dem Assistenten für neue Directory Services

Spezifische Informationen zur Konfiguration von ZENworks Endpoint Security Management für Novell eDirectory™ oder Microsoft Active Directory* finden Sie unter Abschnitt 2.7, „Konfigurieren des Directory Service für Novell eDirectory“, auf Seite 7 bzw. Abschnitt 2.8, „Konfigurieren des Directory Service für Microsoft Active Directory“, auf Seite 8.

2.6.1 Verwenden der Schaltfläche "Zurück" im Assistenten für neue Directory Services

Bei Verwendung der Schaltfläche *Zurück* im Konfigurationsassistenten für neue Directory Services gehen zurzeit Daten verloren und die Synchronisierung kann nicht ordnungsgemäß ausgeführt werden. Wenn Sie einen Fehler gemacht haben, sollten Sie wieder ganz von vorne beginnen.

2.7 Konfigurieren des Directory Service für Novell eDirectory

Dieser Abschnitt enthält Informationen zur Konfiguration von Directory Services für Novell eDirectory unter Verwendung des Assistenten für neue Directory Services Weitere Informationen finden Sie unter “Konfigurieren des Directory Service für Novell eDirectory” im *ZENworks Endpoint Security Management-Administrationshandbuch*.

- „Port 389 oder 636 mit Novell eDirectory verwenden“ auf Seite 7
- „Verwendung von Directory Services für Windows mit ZENworks Endpoint Security Management und eDirectory“ auf Seite 8
- „Den Benutzern können benutzerbasierte, nicht jedoch computerbasierte Richtlinien bereitgestellt werden.“ auf Seite 8
- „Clients werden aufgefordert, sich für das erste Check-In beim Server anzumelden“ auf Seite 8
- „Bei Verwendung von ZENworks Configuration Management in Verbindung mit eDirectory und DLU fordert der ZENworks Endpoint Security Management-Client zur Eingabe eines Passworts auf.“ auf Seite 8
- „Das Verschieben von Benutzern im eDirectory-Tree verursacht Probleme“ auf Seite 8

2.7.1 Port 389 oder 636 mit Novell eDirectory verwenden

Während der Konfiguration des Directory Service für eDirectory müssen Sie Port 389 oder 636 verwenden, wenn Sie eine Verschlüsselung mit TLS/SSL nutzen.

2.7.2 Verwendung von Directory Services für Windows mit ZENworks Endpoint Security Management und eDirectory

Zurzeit kann ZENworks Endpoint Security Management in Verbindung mit eDirectory nicht zusammen mit Directory Services für Windows verwendet werden.

2.7.3 Den Benutzern können benutzerbasierte, nicht jedoch computerbasierte Richtlinien bereitgestellt werden.

Wenn Sie während der Installation des ZENworks Security-Client Novell eDirectory als Directory Service verwenden, müssen Sie die Option für die benutzerbasierte Richtlinie verwenden.

2.7.4 Clients werden aufgefordert, sich für das erste Check-In beim Server anzumelden

Die Clients werden aufgefordert, sich für das erste Check-In beim ZENworks Endpoint Security Management-Server anzumelden. Die Benutzer müssen Benutzernamen und Passwort, nicht jedoch den Kontext angeben.

2.7.5 Bei Verwendung von ZENworks Configuration Management in Verbindung mit eDirectory und DLU fordert der ZENworks Endpoint Security Management-Client zur Eingabe eines Passworts auf.

Wenn Sie ZENworks Configuration Management in Verbindung mit Novell eDirectory und DLU bei Aktivierung des temporären Benutzers verwenden, werden die Clients bei jeder Anmeldung bei ihrem Windows-Gerät zur Eingabe von Anmeldedaten aus dem ZENworks Endpoint Security Management-Server aufgefordert. Dies liegt daran, dass sich die eindeutigen Nummern (wie die SID in Windows) bei jedem Bootvorgang ändern.

2.7.6 Das Verschieben von Benutzern im eDirectory-Tree verursacht Probleme

Zurzeit ist der ZENworks Endpoint Security Management-Server nicht in der Lage, einem Benutzer zu folgen, wenn dieser im eDirectory-Baum verschoben wird.

Umgehung des Problems: Konfigurieren Sie einen neuen Benutzer in ZENworks Endpoint Security Management.

2.8 Konfigurieren des Directory Service für Microsoft Active Directory

Dieser Abschnitt enthält Informationen zur Konfiguration des Directory Service für Microsoft Active Directory unter Verwendung des Assistenten für neue Directory Services Weitere Informationen finden Sie unter “Konfigurieren des Directory Service für Microsoft Active Directory”.

- „Konfigurationsanforderungen für den Domänencontroller für Active Directory“ auf Seite 9
- „Vergewissern sie sich vor der Konfiguration, dass Sie bei der Domäne angemeldet sind“ auf Seite 9

2.8.1 Konfigurationsanforderungen für den Domänencontroller für Active Directory

Für die Konfigurationen des Domänencontrollers für Active Directory ist Windows Server 2000 mit SP4 oder Windows Server 2003 erforderlich.

2.8.2 Vergewissern sie sich vor der Konfiguration, dass Sie bei der Domäne angemeldet sind

Um den Verzeichnisdienst für Active Directory konfigurieren zu können, müssen Sie sich zuerst bei der Domäne anmelden.

2.9 Sicherstellen der Endpunktsicherheit

Dieser Abschnitt enthält Informationen zu den Problemen, die bei der Verwendung von Antivirus- und Spyware-Regeln in ZENworks Endpoint Security Management auftreten können.

2.9.1 Verwenden der Antivirus- und Spyware-Regeln

Einige der bei ZENworks Endpoint Security Management vorinstallierten Antivirus- und Spyware-Regeln müssen eventuell für eine spezifische oder benutzerdefinierte Version der Antivirus- oder Spyware-Software modifiziert werden.

2.10 Firewalls

Dieser Abschnitt enthält Informationen zu den Problemen, die bei der Verwendung einer Firewall und ZENworks Endpoint Security Management auftreten können.

- „Verwenden dynamisch zugewiesener Ports“ auf Seite 9
- „Verwenden von FTP-Sitzungen“ auf Seite 9

2.10.1 Verwenden dynamisch zugewiesener Ports

In den meisten Einstellungen erlaubt die ZENworks-Firewall keine eingehenden Verbindungen an dynamisch zugewiesene Ports. Wenn eine Anwendung eine eingehende Verbindung erfordert, muss der Port statisch sein und bei der Firewall muss die Einstellung *Offen* erstellt werden, um die eingehende Verbindung zuzulassen. Wenn die eingehende Verbindung von einem bekannten Remote-Gerät stammt, kann ACL verwendet werden.

2.10.2 Verwenden von FTP-Sitzungen

Die Standard-Firewall-Einstellung *Alle adaptiv (Stateful)* lässt eine aktive FTP-Sitzung nicht zu. Sie müssen stattdessen passives FTP verwenden. Eine gute Erklärung zum Unterschied von aktivem und passivem FTP finden Sie auf der Slacksite-Website (http://slacksite.com/other/ftp.html).

2.11 Lokalisierung

Dieser Abschnitt enthält Informationen zu den Lokalisierungsproblemen in ZENworks Endpoint Security Management.

- Unter "Berichterstellung" in der Endpunktüberwachung gibt es unübersetzte Elemente und Beschreibungen.

- Es gibt unübersetzte Strings im Dialogfeld "Berichte" unter *Endpunktüberwachung: Berichterstellung*.
- In der Baumansicht unter der Registerkarte *Berichterstellung* liegt unübersetzter Text vor.
- Bei Auswahl des Installationstyps im Installationsprogramm für den Management Service ist ein Optionsfeld nicht vollständig zu sehen.
- In der Verwaltungskonsole sind Berichte nicht vollständig zu sehen.
- Der Standardinstallationspfad des Richtlinienverteilungsservice enthält chinesische Zeichen.
- Beim Abbrechen der Installation des ZENworks Security-Client ist eine Registerkarte nicht übersetzt.
- Die Beschreibung der Anwendungsereignisprotokolle für `STEngine` ist auf Chinesisch traditionell und Chinesisch vereinfacht nicht vorhanden.
- Die Eingabeaufforderung für das Deinstallationspasswort ist in englischer Sprache.

2.12 Verwaltungskonsole

Dieser Abschnitt enthält Informationen zu Problemen, die bei der Verwendung der Verwaltungskonsole in ZENworks Endpoint Security Management auftreten können.

- „Verwenden der Verwaltungskonsole in Active Directory“ auf Seite 10
- „Anzeige der Fehlermeldungen“ auf Seite 10
- „Potenzielle Ausnahme in Verbindung mit der Verknüpfung einer bestehenden Integritätsregel“ auf Seite 10
- „Auf Netzwerkgeräte, die als Dualgeräte installiert werden, wird die Richtlinie möglicherweise nicht angewendet“ auf Seite 11
- „Die Optionen und Steuerelemente für Berechtigungen stehen in der Verwaltungskonsole nicht zur Verfügung“ auf Seite 11

2.12.1 Verwenden der Verwaltungskonsole in Active Directory

Wenn Sie Microsoft Active Directory als Directory Service verwenden, müssen Sie bei der Domäne angemeldet sein, um die Verwaltungskonsole verwenden zu können.

2.12.2 Anzeige der Fehlermeldungen

Bei Anklicken einer Fehlermeldung in der Verwaltungskonsole wird nicht jedes Mal der richtige Bildschirm angezeigt. Die Einschränkung tritt bei Bildschirmen mit mehreren Registerkarten auf.

2.12.3 Potenzielle Ausnahme in Verbindung mit der Verknüpfung einer bestehenden Integritätsregel

Eine potenzielle Ausnahme kann in Verbindung mit der Verknüpfung einer bestehenden Integritätsregel auftreten, wenn Sie vor der Veröffentlichung der Richtlinie nicht alle Auslöser, Ereignisse, Firewalls usw. überprüfen. Die Richtlinie kann nicht ausgeführt werden und folgender Fehler wird angezeigt:

```
“Senforce.PolicyEditor.Bll.FatalErorException:component_value table in
unknown state” “at
Senforce.PolicyEditor.UI.Forms.PolicyForm.SavePolicy()” “at
Senforce.PolicyEditor.UI.Forms.MainForm.PublishPolicy()”
```

Umgehung des Problems: Vergewissern Sie sich, dass alle Optionen konfiguriert wurden, und klicken Sie auf jeder Seite der Verwaltungskonsole auf *Richtlinie speichern*, bevor Sie zur nächsten Seite übergehen.

2.12.4 Auf Netzwerkgeräte, die als Dualgeräte installiert werden, wird die Richtlinie möglicherweise nicht angewendet

Netzwerkgeräte, die als Dualgeräte installiert werden (z. B. Modem und Wireless (802.11)), werden im Registrierungseintrag `HKLM\\Software\Microsoft\Windows NT\\Network Cards` möglicherweise nicht ordnungsgemäß angezeigt und es wird keine Richtlinie auf sie angewendet (Firewall oder Adaptersteuerung).

2.12.5 Die Optionen und Steuerelemente für Berechtigungen stehen in der Verwaltungskonsole nicht zur Verfügung

Die Optionen und Steuerelemente für Berechtigungen funktionieren zurzeit nicht ordnungsgemäß, weshalb sie entfernt wurden. Das Entfernen der Berechtigungen eines Benutzers für die Verwaltungskonsole wird nicht aktiv, bis die Verwaltungskonsolensitzung des Benutzers beendet wird.

Umgehung des Problems: Steuern Sie die Berechtigungen, indem Sie ein Passwort festlegen, das den Benutzerzugriff auf den Computer steuert, auf dem die Verwaltungskonsole ausgeführt wird.

2.13 Netzwerkumgebungen

Dieser Abschnitt enthält Informationen zu Problemen, die bei der Verwendung von ZENworks Endpoint Security Management zur Verwaltung von Netzwerken auftreten können.

2.13.1 Verwenden adapterspezifischer Netzwerkumgebungen

Adapterspezifische Netzwerkumgebungen, die ungültig werden, können dazu führen, dass ein Client weiterhin zwischen dem der Umgebung zugewiesenen Standort und Unbekannt wechselt. Um dies zu vermeiden, stellen Sie den Adaptertyp der Netzwerkumgebung auf einen Adapter, der an dem Standort aktiviert ist, ein.

2.14 Berichte

Dieser Abschnitt enthält Informationen zur Verwendung von Berichten in ZENworks Endpoint Security Management.

- In Adherence Reports sind Daten falsch oder fehlen.
- In Richtlinienberichten fehlen Daten.

2.15 Speichergeräte

Dieser Abschnitt enthält Informationen zu Problemen, die bei der Verwendung von ZENworks Endpoint Security Management zur Verwaltung von Speichergeräten auftreten können.

- „Steuerung von USB-Geräten“ auf Seite 12

- „Steuerung von CD/DVD-Geräten“ auf Seite 12
- „Einstellungen für die Speichergerätesteuerung können in der Verwaltungskonsole nicht nach Standort gespeichert werden“ auf Seite 12

2.15.1 Steuerung von USB-Geräten

Nicht alle USB-Festplattenlaufwerke haben eine Seriennummer. Einige Seriennummern von Festplattenlaufwerken sind abhängig von der Kombination von Anschluss und Laufwerk und einige sind nicht eindeutig. Die meisten Thumb-Laufwerke haben scheinbar eine eindeutige Seriennummer.

2.15.2 Steuerung von CD/DVD-Geräten

Wenn ein CD/DVD-Brenner nach der Installation des ZENworks Sicherheits-Client hinzugefügt wird, werden Richtlinien, die dem Gerät einen Nur-Lesen-Modus zuschreiben, nicht durchgesetzt, wenn Sie Brennsoftware von Dritten, wie Roxio* oder Nero*, verwenden.

2.15.3 Einstellungen für die Speichergerätesteuerung können in der Verwaltungskonsole nicht nach Standort gespeichert werden

Wenn Sie Einstellungen für die Speichergerätesteuerung auf der Registerkarte *Standorte* konfigurieren, können Sie Ihre Einstellungen nicht speichern. Wenden Sie sich an den zuständigen Supportmitarbeiter, um einen Patch und Anweisungen zur Behebung des Problems anzufordern. Dieses Problem tritt nicht auf, wenn die Einstellungen für die Speichergerätesteuerung auf der Registerkarte *Allgemeine Richtlinieneinstellungen* festgelegt werden.

2.16 Deinstallation

Dieser Abschnitt enthält Informationen zu den Problemen, die bei der Deinstallation von ZENworks Endpoint Security Management auftreten können.

2.16.1 Deinstallation von ZENworks Endpoint Security Management mit aktivierter Safe Harbor-Funktion

Bei aktivierter Safe Harbor-Funktion und Deinstallation mithilfe einer Richtlinie werden Sie bei der Deinstallation aufgefordert, Dateien auf einer eingebauten Festplatte zu deinstallieren Nach dem Klicken auf *OK* erhalten Sie möglicherweise die Meldung `Remove Directory Failed` (Fehler beim Entfernen des Verzeichnisses). Diese Meldung lässt sich nicht ausblenden.

Umgehung des Problems: Sie müssen das Gerät neu booten und das Deinstallationsprogramm erneut ausführen.

2.17 Upgrades

Dieser Abschnitt enthält Informationen zu den Problemen, die auftreten können, wenn Sie eine Aufrüstung von einer früheren Version von ZENworks Endpoint Security Management durchführen.

- „Wenden Sie sich vor der Durchführung der Aufrüstung an den Kundensupport“ auf Seite 13
- „Kein Support für Serveraufrüstungen“ auf Seite 13
- „Frühere Versionen des Richtlinieneditors der Senforce Endpoint Security Suite werden in Version 3.5 nicht unterstützt.“ auf Seite 13

2.17.1 Wenden Sie sich vor der Durchführung der Aufrüstung an den Kundensupport

Sie sollten sich bei allen Aufrüstungen an den für Sie zuständigen Support-Mitarbeiter um Unterstützung wenden.

2.17.2 Kein Support für Serveraufrüstungen

Aufgrund von Korrekturen und neuen Funktionen in dieser Version wird die Aufrüstung des ZENworks Endpoint Security-Servers nicht unterstützt. Wenden Sie sich an den für Sie zuständigen Support-Mitarbeiter, um Unterstützung bei der Aufrüstung Ihres Systems zu erhalten. Der Support-Mitarbeiter kann Ihnen dabei helfen, Sicherheitsrichtlinien aus Ihrer früheren Version beizubehalten.

2.17.3 Frühere Versionen des Richtlinieneditors der Senforce Endpoint Security Suite werden in Version 3.5 nicht unterstützt.

Frühere Versionen des Richtlinieneditors der Senforce® Endpoint Security Suite können bei einer Installation von ZENworks Endpoint Security Management 3.5 Server nicht ausgeführt werden.

2.17.4 Bei der Aufrüstung einer Senforce 3.2-Richtlinie geht die Passwortüberschreibung verloren

Bei der Aufrüstung einer vorhandenen Senforce Endpoint Security Suite 3.2-Richtlinie auf eine Richtlinie der Version 3.5 geht die Passwortüberschreibung verloren. Wenn eine Richtlinie der Version 3.2 über eine Passwortüberschreibung verfügt, muss diese in die Richtlinie der Version 3.5 erneut eingegeben werden. Dies ist standardmäßig festgelegt.

2.17.5 Aufrüsten des ZENworks Security-Client auf verwalteten Geräten

Zur manuellen Aufrüstung des ZENworks Security-Client auf verwalteten Geräten ist der Schalter `-stupgrade` wie im folgenden Beispiel zu verwenden:

```
setup.exe /V"STUPGRADE=1"
```

Wenn Sie den ZENworks Security-Client mit einer ZENworks Endpoint Security Management-Richtlinie aufrüsten, wird dieser Schalter nicht benötigt.

2.17.6 Keine Unterstützung für Client-Aufrüstungen aus Senforce-Client-Builds

Die Aufrüstung eines Senforce Endpoint Security-Client auf einen Novell ZENworks Endpoint Security-Client ist nicht möglich.

2.18 VPN-Verbindungen

Dieser Abschnitt enthält Informationen zu Problemen, die bei der Verwendung von ZENworks Endpoint Security Management zur Verwaltung von VPN-Verbindungen auftreten können.

2.18.1 Konfigurieren der VPN-Einstellungen

ZENworks Endpoint Security Management unterstützt bei der Konfigurierung der VPN-Einstellungen keine Split-Tunnel.

2.19 Wi-Fi-Konnektivität

Dieser Abschnitt enthält Informationen zu Problemen, die bei der Verwendung von ZENworks Endpoint Security Management zur Verwaltung von Wi-Fi-Verbindungen auftreten können.

- „Anzeige benutzerdefinierter Meldungen zu Wi-Fi-Übertragungen und zur Deaktivierung von Adapter Bridging für Benutzer“ auf Seite 14
- „Vewenden von WPA-Zugriffspunkten“ auf Seite 14
- „Steuerung von Mobiltelefonen“ auf Seite 14
- „Wi-Fi-Einstellungen können in der Verwaltungskonsole nicht nach Standort gespeichert werden“ auf Seite 14
- „Nicht unterstützte Wi-Fi-Geräte“ auf Seite 15

2.19.1 Anzeige benutzerdefinierter Meldungen zu Wi-Fi-Übertragungen und zur Deaktivierung von Adapter Bridging für Benutzer

Die Meldungen "Deaktivieren Sie Wi-Fi-Übertragung" und "Deaktivieren Sie Adapter Bridging" werden nur angezeigt, wenn der Benutzer versucht, die Durchsetzung zu umgehen. Sie werden ohne Warnmeldung durchgesetzt.

2.19.2 Vewenden von WPA-Zugriffspunkten

WPA-Zugriffspunkte können zur Filterung identifiziert werden (wir unterscheiden nicht zwischen WPA und WPA2). ZENworks Endpoint Security Management verteilt nur WEP-Schlüssel.

2.19.3 Steuerung von Mobiltelefonen

Möglicherweise können Sie Wireless-Verbindungen, die über Mobiltelefone hergestellt wurden, nicht über die Wi-Fi-Steuerfunktionen in der Verwaltungskonsole steuern. Diese Geräte werden im Allgemeinen vom Betriebssystem als Modems behandelt und benötigen deswegen entsprechende Richtlinienänderungen, um gesteuert werden zu können (z.B. Deaktivieren der Modems bei Verkabelung durch Scripting).

2.19.4 Wi-Fi-Einstellungen können in der Verwaltungskonsole nicht nach Standort gespeichert werden

Wenn Sie Wi-Fi-Einstellungen auf der Registerkarte *Standorte* konfigurieren, können Sie Ihre Einstellungen nicht speichern. Wenden Sie sich an den zuständigen Supportmitarbeiter, um einen Patch und Anweisungen zur Behebung des Problems anzufordern. Dieses Problem tritt nicht auf, wenn die Wi-Fi-Einstellungen auf der Registerkarte *Allgemeine Richtlinieneinstellungen* festgelegt werden.

2.19.5 Nicht unterstützte Wi-Fi-Geräte

Bestimmte veraltete drahtlose Adapter funktionieren nicht richtig, wenn Sie über ZENworks Endpoint Security Management verwaltet werden. Dazu gehören folgende Geräte:

- Orinoco* 8470-WD Gold
- 3Com* 3CRWE62092B
- Dell True Mobile 1180
- Proxim* Orinoco 802.11bg combo card

2.20 ZENworks Endpoint Security-Client

Dieser Abschnitt enthält Informationen zu Problemen, die bei der Verwendung des ZENworks Endpoint Security-Client auf verwalteten Geräten auftreten können.

- „In der Windows-Taskleiste werden zwei Symbole für den ZENworks Endpoint Security-Client angezeigt“ auf Seite 15
- „Nach der Installation des ZENworks Security-Client wird der Benutzer aufgefordert, sich beim Client anzumelden.“ auf Seite 15

2.20.1 In der Windows-Taskleiste werden zwei Symbole für den ZENworks Endpoint Security-Client angezeigt

Wenn Sie Ihren ZENworks Endpoint Security Client-Rechner booten, sehen Sie eventuell zwei ZENworks Endpoint Security-Client-Symbole in der Windows-Taskleiste. Richten Sie den Mauszeiger auf eines der Symbole; das Symbol wird dann ausgeblendet.

2.20.2 Nach der Installation des ZENworks Security-Client wird der Benutzer aufgefordert, sich beim Client anzumelden.

Die Benutzer werden möglicherweise zur Eingabe eines Berechtigungsnachweises (Benutzername bzw. kurzer oder vollständiger LDAP-Kontext) aufgefordert, um sich beim ZENworks Endpoint Security Management-Server anzumelden. Dies geschieht nur einmal und nur nach der Installation des ZENworks Security-Client. Die Gründe für dieses Problem sind folgende:

- Der Backend-Server befindet sich auf Novell eDirectory.
- Der Benutzer meldet sich lokal auf dem Rechner an und nicht über die Domäne.
- Der Benutzer meldet sich über NetWare®, nicht über Microsoft Windows an.
- Der Administrator hat beim Einrichten der Authentifizierungsverzeichnisse in der Infrastruktur den Suchkontext nicht korrekt eingerichtet, so dass die Container des Benutzers oder Rechners nicht mit eingeschlossen sind.
- Die SID des Rechners oder des Benutzers ist nicht mehr gültig und es muss eine neue erstellt werden.
- Sie vewenden Directory Services für Windows, anstatt direkt mit eDirectory oder Active Directory zu kommunizieren.
- Der ZENworks Configuration Management-Client verwendet die Funktion für dynamische lokale Benutzer (Dynamic Local User; DLU) mit Aktivierung des temporären Benutzers.

Hinweis: Wenn mehrere eDirectory-Benutzer sich mit demselben lokalen Administrator-Benutzerkonto anmelden, erhalten alle Benutzer dieselbe Richtlinie. Jeder eDirectory-Benutzer muss sein eigenes lokales Benutzerkonto besitzen.

3 Konventionen in der Dokumentation

In dieser Dokumentation trennt das Größer-als-Zeichen (>) Aktionen innerhalb eines Schritts und Elemente in einem Querverweispfad voneinander.

Ein Markensymbol (® , ™ usw.) kennzeichnet eine Marke von Novell; ein Sternchen (*) kennzeichnet eine Drittanbieter-Marke

4 Rechtliche Hinweise

Novell, Inc. übernimmt für Inhalt oder Verwendung dieser Dokumentation keine Haftung und schließt insbesondere jede ausdrückliche oder implizite Garantie für Marktfähigkeit oder Eignung für einen bestimmten Zweck aus. Novell, Inc. behält sich das Recht vor, dieses Dokument jederzeit teilweise oder vollständig zu ändern, ohne dass für Novell, Inc. die Verpflichtung entsteht, Personen oder Organisationen davon in Kenntnis zu setzen.

Novell, Inc. gibt ebenfalls keine Erklärungen oder Garantien in Bezug auf Novell-Software und schließt insbesondere jede ausdrückliche oder implizite Garantie für handelsübliche Qualität oder Eignung für einen bestimmten Zweck aus. Außerdem behält sich Novell, Inc. das Recht vor, Novell-Software jederzeit ganz oder teilweise zu ändern, ohne dass für Novell, Inc. die Verpflichtung entsteht, Personen oder Organisationen von diesen Änderungen in Kenntnis zu setzen.

Alle im Zusammenhang mit dieser Vereinbarung zur Verfügung gestellten Produkte oder technischen Informationen unterliegen möglicherweise den US-Gesetzen zur Exportkontrolle sowie den Handelsgesetzen anderer Länder. Sie stimmen zu, alle Gesetze zur Exportkontrolle einzuhalten und alle für den Export, Reexport oder Import von Lieferungen erforderlichen Lizenzen oder Klassifikationen zu erwerben. Sie erklären sich damit einverstanden, nicht an juristische Personen, die in der aktuellen US-Exportausschlussliste enthalten sind, oder an in den US-Exportgesetzen aufgeführte terroristische Länder oder Länder, die einem Embargo unterliegen, zu exportieren oder zu reexportieren. Sie stimmen zu, keine Lieferungen für verbotene nukleare oder chemisch-biologische Waffen oder Waffen im Zusammenhang mit Flugkörpern zu verwenden. Weitere Informationen zum Exportieren von Novell-Software finden Sie auf der Webseite Novell International Trade Services (http://www.novell.com/info/exports/). Novell übernimmt keine Verantwortung für das Nichteinholen notwendiger Exportgenehmigungen.

Novell, Inc. besitzt Rechte auf geistiges Eigentum für die Technologie, die in dem in diesem Dokument beschriebenen Produkt integriert ist. Diese Rechte auf geistiges Eigentum umfassen möglicherweise insbesondere ein oder mehrere Patente in den USA, die auf der Webseite Novell Legal Patents (http://www.novell.com/company/legal/patents/) aufgeführt sind, sowie ein oder mehrere andere Patente oder laufende Patentanträge in den USA und in anderen Ländern.

Hinweise zu Novell-Marken finden Sie in der Novell Trademark and Service Mark-Liste (http://www.novell.com/company/legal/trademarks/tmlist.html).

Die Rechte für alle Marken von Drittanbietern liegen bei den jeweiligen Eigentümern.