Ivanti Patch for Windows® Servers

Leitfaden zum Upgrade

Copyright und Markenhinweise

Informationen zum Dokument und zur Historie

Dokumentnummer: --

Datum	Version	Beschreibung
September 2010	NetChk Protect 7.6	Aktualisierung des Produktbrandings; Hinzufügung von Informationen zu neuen Features und Verbesserungen in 7.6.
März 2011	NetChk Protect 7.8	Hinzufügung von Informationen zu neuen Features und Verbesserungen in 7.8.
Oktober 2011	VMware vCenter Protect 8.0	Aktualisierung des Produktbrandings; Hinzufügung von Informationen zu Tasks für das Upgrade auf 8.0. Entfernen aller Informationen zu Vorversionen von 7.5.
Dezember 2011	VMware vCenter Protect 8.0, Dokumentenversion A	Hinzufügung eines Schritts, in dem die Komprimierung der Datenbank vor dem Beginn des Upgradeprozesses erklärt wird.
September 2012	VMware vCenter Protect 8.0.1	Aktualisierung des Produktnamens und der Version; Aktualisierung der Titelblattgrafik.
Mai 2013	Shavlik Protect 9.0	Aktualisierung der Systemanforderungen. Hinzufügung von Informationen zu neuen Features und Verbesserungen in v9.0.
April 2014	Shavlik Protect 9.1	Aktualisierung der Systemanforderungen. Hinzufügung von Informationen zu neuen Features und Verbesserungen in v9.1.
September 2015	Shavlik Protect 9.2	Aktualisierung der Systemanforderungen. Hinzufügung von Informationen über den neue Funktionen und Verbesserungen in Version 9.2.
April 2017	Ivanti Patch for Windows® Servers 9.3	Rebranding auf Ivanti, Entfernen der Verweise auf AV, Aktualisierung der Systemanforderungen, Hinzufügen neuer Features und Verbesserungen in v9.3.

WILLKOMMEN

Zweck dieses Dokuments

Willkommen bei Ivanti Patch for Windows® Servers 9.3. Dieses Dokument beschreibt das Upgrade von Shavlik Protect 9.1 oder Shavlik Protect 9.2 auf Ivanti Patch for Windows® Servers 9.3.

Neben der Beschreibung des Upgradevorgangs enthält dieses Dokument auch eine Liste der Funktionsunterschiede, die Sie beim Upgrade auf Ivanti Patch for Windows® Servers 9.3 beachten sollten. Ferner werden die Bereiche in der Benutzeroberfläche hervorgehoben, die sich deutlich verändert haben.

Neue Systemanforderungen und Voraussetzungen

Bitte beachten Sie die folgenden neuen Anforderungen und Voraussetzungen für Ivanti Patch for Windows® Servers 9.3.

- Windows Server 2016 und Windows 10 werden nun als Konsolencomputer unterstützt
- Microsoft .NET Framework 4.6.2 oder höher
- Microsoft Visual C++ Redistributable for Visual Studio 2015
- Unterstützung für SQL Server 2005 entfernt. Das neue Minimum ist SQL Server 2008.
- Windows XP und Windows Server 2003 werden auf Agentencomputern nicht mehr unterstützt
- Antivirus wird in diesem Release nicht mehr unterstützt

Alle fehlenden Softwarevoraussetzungen werden während des Upgradeprozesses automatisch installiert. Eine vollständige Liste der Systemanforderungen finden Sie im *Ivanti Patch for Windows® Servers – Installationshandbuch*.

Für das Upgrade geltende Anforderungen an das Benutzerkonto

Damit Sie ein Upgrade für Ihr Benutzerkonto durchführen können, müssen die folgenden Anforderungen erfüllt sein:

- Der Benutzer, der das Datenbank-Upgrade vornimmt, muss Mitglied der Rolle db_owner sein.
- Falls mehrere Konsolen eine Datenbank gemeinsam verwenden und eine zusätzliche Konsole mit einer Datenbank verknüpft wird, für die das Upgrade bereits durchgeführt wurde, muss das verwendete Benutzerkonto ein Mitglied der folgenden Datenbankrollen sein: db_datareader, db_datawriter, STExec und STCatalogupdate. Darüber hinaus muss das für die Hintergrundvorgänge verwendete Dienstkonto ein Mitglied der Rolle db_owner sein. Wenn Ihr Konto Mitglied der Rollen db_securityadmin und db_accessAdmin ist, versucht das Tool für das Datenbank-Upgrade automatisch, die erforderlichen Rollen für Sie zuzuordnen und zu konfigurieren.

VERFAHRENSWEISE BEIM UPGRADE

Übersicht

Dieser Abschnitt beschreibt das Upgrade von Shavlik Protect 9.1 oder Shavlik Protect 9.2 auf Ivanti Patch for Windows® Servers 9.3. Wenn Sie diese Gelegenheit nutzen, um die Konsole auf einen neuen Computer zu verschieben und die Migration mit dem Migrationstool durchführen möchten, lesen Sie dazu die Informationen im *Migrationstool – Benutzerhandbuch*, bevor Sie das Upgrade durchführen.

Bevor Sie das Upgrade durchführen, sollten Sie unbedingt den *Abschnitt Wichtige Änderungen und Verbesserungen* auf der Seite 17 lesen, damit Sie wissen, welche Auswirkungen das Upgrade auf Ihr System hat. Sie sollten sich alle aktuellen benutzerdefinierten Benutzereinstellungen notieren, weil einige davon während des Upgradevorgangs nicht übernommen werden (siehe Seite 14).

Hinweis: Beachten Sie, dass nach Abschluss des Konsolenupgrades alle Agenten, die auf Ihren Zielcomputern installiert sind, automatisch aktualisiert werden, wenn sie das nächste Mal bei der Konsole einchecken.

Durchführen des Upgrades

1. Geben Sie ungenutztem Speicherplatz in der Datenbank frei, die Sie zum Speichern von Scan-und Patchbereitstellungsergebnissen verwendet.

   In SQL Server Management Studio klicken Sie hierzu mit der rechten Maustaste auf die ShavlikScans-Datenbank und wählen dann **Tasks > Verkleinern > Datenbank**.

2. Erstellen Sie mit SQL Server Management Studio eine Sicherung Ihrer aktuellen Datenbank.

   Die Datenbank enthält Ergebnisse aus Programmoperationen und enthält auch Konfigurationsinformationen. Die Sicherung Ihrer Datenbank ist ein wichtiger Schritt.

3. Schließen Sie alle Programme, die auf dem Konsolencomputer ausgeführt werden – auch Shavlik Protect.

4. Laden Sie die ausführbare Datei für Ivanti Patch for Windows® Servers 9.3 auf Ihren Konsolencomputer herunter. Nutzen Sie dazu den folgenden Link:

   https://www.ivanti.com/de-DE/resources/downloads

5. Beginnen Sie den Installationsvorgang auf eine der folgenden Weisen:

   - Doppelklicken Sie auf den Dateinamen **IvantiPatchForServers.exe**.
   - Geben Sie den Namen der Datei in einer Eingabeaufforderung ein. Damit können Sie mehrere Befehlszeilenoptionen verwenden. Dieses Methode ist beim Upgrade einer sehr großen Datenbank zu bevorzugen. Die Option DBCOMMANDTIMEOUT wird verwendet, um den Timeout-Wert des SQL-Befehls während der Installation anzugeben. Der Standardwert ist 15 Minuten pro GB. Der Mindestwert für das Timeout ist der größere Wert von entweder 15 Minuten pro GB oder 1800 Sekunden (30 Minuten). Sie sollten den Standardwert nur dann überschreiben, wenn Sie erwarten, dass das Upgrade aufgrund von eingeschränkten Ressourcen außergewöhnlich lange dauern wird. Zum Beispiel: Wenn Ihnen eine 4-GB-Datenbank vorliegt, müssen Sie den folgenden Befehl eingeben, um den Standardwert für das

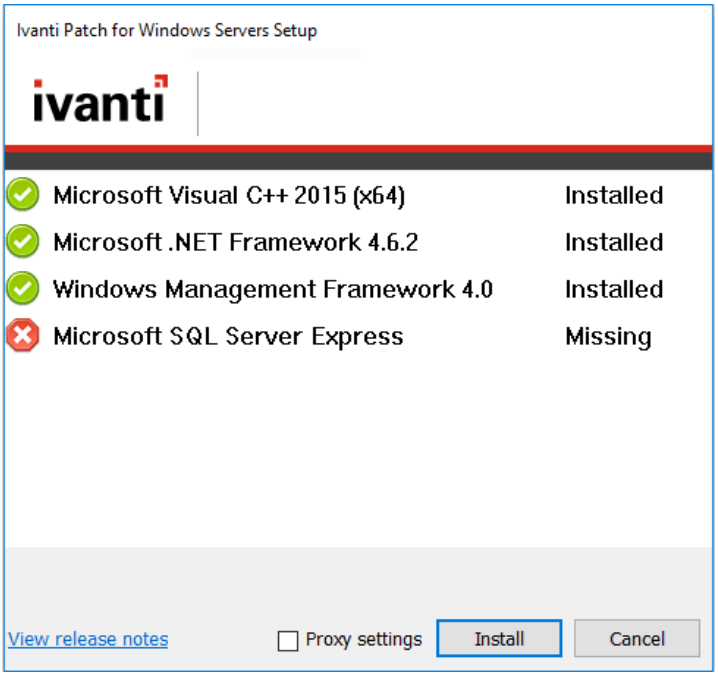
Timeout-von 3600 Sekunden (60 Minuten) auf 7200 Sekunden (120 Minuten) zu verdoppeln:

```
IvantiPatchForServers /wi:"DBCOMMANDTIMEOUT =7200"
```

Hinweis: Falls eine Meldung darauf hinweist, dass ein Neustart erforderlich ist, klicken Sie auf **OK**. Der Installationsvorgang wird dann automatisch nach dem Neustart fortgesetzt.

6. Der Installationsvorgang wird dann automatisch nach dem Neustart fortgesetzt.

   Beantworten Sie im anschließend angezeigten Dialogfeld die Frage, ob Sie mit dem Upgrade fortfahren wollen. Wenn alle Voraussetzungen erfüllt sind, überspringen Sie den folgenden Schritt und fahren mit dem **Begrüßungsbildschirm fort**.



7. Klicken Sie auf die Schaltfläche **Installieren**, um alle fehlenden Voraussetzungen zu installieren.

   Möglicherweise muss der Einrichtungsassistent während dieses Teils des Installationsprozesses einen Neustart durchführen. Falls ein Neustart erforderlich ist, wird nach dem Neustart des Computers das Dialogfeld „Einrichten" angezeigt. Klicken Sie einfach erneut auf **Installieren** , um mit dem Upgrade fortzufahren.

   Das Dialogfeld Willkommen wird angezeigt.

8. Lesen Sie die Informationen im Dialogfeld **Willkommen**, und klicken Sie dann auf **Weiter**.

   Die Lizenzvereinbarung wird angezeigt. Sie müssen die Bedingungen dieser Lizenzvereinbarung akzeptieren, damit Sie das Programm installieren können.

9. Aktivieren Sie das Kontrollkästchen **Ich akzeptiere die Bedingungen der Lizenzvereinbarung**, und klicken Sie dann auf **Weiter**.

   Das Dialogfeld **Zielordner** wird angezeigt.

10. Wenn Sie den Standardspeicherort des Programms ändern möchten, klicken Sie auf die Schaltfläche zum Durchsuchen (... Sie haben an dieser Stelle ferner die Option, einen Shortcut auf dem Desktop zu erstellen. Wenn Sie fertig sind, klicken Sie auf **Weiter**.

    Das Dialogfeld **Produktverbesserungsprogramm** wird angezeigt. Lesen Sie die Beschreibung und entscheiden Sie, ob Sie an dem Programm teilnehmen möchten. Das Programm versetzt Ivanti in die Lage, Nutzungsdaten zu sammeln, die zur Verbesserung zukünftiger Versionen des Produkts beitragen werden.

11. Klicken Sie auf **Weiter**.

    Das Dialogfeld **Bereit zur Installation** wird angezeigt.

12. Um die Installation zu starten, klicken Sie auf **Installieren**.

    Gegen Ende des Installationsvorgangs wird das Dialogfeld **Datenbank-Setuptool** angezeigt.

    Wichtig! Wählen Sie im nächsten Schritt KEINESFALLS **Neue Datenbank erstellen** aus, denn sonst wird eine neue Datenbank erstellt und Ihre vorhandenen Daten werden nicht verwendet.Wenn Sie so vorgehen, wird eine neue Datenbank erstellt und Ihre vorhandenen Daten werden nicht verwendet.

13. Vergewissern Sie sich, dass **Eine vorhandene Datenbank verwenden** ausgewählt ist und klicken Sie dann auf **Weiter**.

14. Geben Sie mithilfe der verfügbaren Felder an, wie Benutzer und Dienste auf die SQL Server-Datenbank zugreifen werden.

    Wählen Sie einen Datenbankserver und eine Instanz aus.

    - **Servername:** Sie können einen Computer angeben oder Sie können einen Computer und die auf diesem Computer ausgeführte SQL Server-Instanz angeben.
    - **Datenbankname:** Geben Sie den Datenbanknamen an, den Sie verwenden möchten. Der Standard-Datenbankname lautet **Protect**.

    Wählen Sie, wie interaktive Benutzer die Verbindung zur Datenbank herstellen.

    Geben Sie die Anmeldeinformationen an, die das Programm verwenden soll, wenn ein Benutzer eine Aktion ausführt, die Zugriff auf die Datenbank erfordert.

    - **Integrierte Windows-Authentifizierung:** Dies ist die empfohlene Standardoption. Ivanti Patch for Windows® Servers verwendet die Anmeldeinformationen des derzeit angemeldeten Benutzers, um die Verbindung zur SQL Server-Datenbank herzustellen. Die Felder **Benutzername** und **Kennwort** sind dann nicht verfügbar.
    - **Bestimmter Windows-Benutzer:** Wählen Sie diese Option nur, wenn sich die SQL Server-Datenbank auf einem Remotecomputer befindet. Diese Option hat keinerlei Auswirkungen, wenn sich die Datenbank auf dem lokalen (Konsolen-)Computer befindet. (Weitere Informationen zu Anmeldeinformationen des lokalen Computers finden Sie unter *Angeben von Anmeldeinformationen* im *Ivanti Patch for Windows ®* Servers – *Administrationshandbuch*.) Alle Ivanti Patch for Windows® Servers-Benutzer werden die angegebenen Anmeldeinformationen verwenden, wenn sie

Aktionen durchführen, die eine Interaktion mit der remoten SQL Server-Datenbank erfordern.
SQL-Authentifizierung: Wählen Sie diese Option, wenn Sie eine spezifische Kombination von Benutzername und Kennwort für die Windows-Anmeldung bei diesem spezifischen SQL Server verwenden möchten.

Vorsicht! Wenn Sie Anmeldeinformationen für die SQL-Authentifizierung angeben und für SQL-Verbindungen keine SSL-Verschlüsselung implementiert ist, werden die Anmeldeinformationen im Klartext über das Netzwerk weitergegeben.

- **Datenbankverbindung testen:** Um sicherzustellen, dass das Programm mit den angegebenen Informationen für die interaktive Benutzeranmeldung den Kontakt zur Datenbank herstellen kann, klicken Sie auf diese Schaltfläche.

Wählen Sie, wie Dienste die Verbindung zur Datenbank herstellen.

Geben Sie die Anmeldeinformationen an, die von den Hintergrunddiensten zum Herstellen einer Verbindung zur Datenbank verwendet werden sollen. Dies sind die Anmeldeinformationen, die vom Ergebnisimportprogramm, von Vorgängen mit Agents und anderen Diensten zur Anmeldung beim SQL Server und zur Weitergabe des Status verwendet werden.

- **Alternative Anmeldeinformationen für Konsolendienste verwenden:**
    - Wenn die SQL Server-Datenbank auf dem lokalen Computer installiert ist, werden Sie diese Option in der Regel ignorieren, indem Sie dieses Kontrollkästchen nicht aktivieren. In diesem Fall werden dieselben Anmeldeinformationen und derselbe Authentifizierungsmodus verwendet, den Sie oben für interaktive Benutzer angegeben haben.
    - Dieses Kontrollkästchen sollte normalerweise nur dann aktiviert werden, wenn sich die SQL Server-Datenbank auf einem Remotecomputer befindet. Wenn sich die Datenbank auf einem Remotecomputer befindet, benötigen Sie ein Konto, mit dem die Authentifizierung gegenüber der Datenbank auf dem remoten Datenbankserver möglich ist.
- **Authentifizierungsmethode:** Nur verfügbar, wenn **Alternative Anmeldeinformationen für Konsolendienste verwenden** aktiviert wurde.
    - **Integrierte Windows-Authentifizierung:** Die Auswahl dieser Option bedeutet, dass das Computerkonto zum Herstellen der Verbindung zum remoten SQL Server verwendet wird. Damit die Anmeldeinformationen sicher übertragen werden können, muss das Netzwerk-Authentifizierungsprotokoll Kerberos verfügbar sein. The User name and Password boxes will be unavailable.

Hinweis: Wenn Sie die **Integrierte Windows-Authentifizierung** wählen, versucht das Installationsprogramm, eine SQL Server-Anmeldung für das Computerkonto zu erstellen. Sollte der Prozess zur Kontoerstellung fehlschlagen, lesen Sie unter *Nach der Installation von SQL Server – Hinweise* in der *Ivanti Patch for Windows® Servers – Installationsanleitung* nach, wie ein remoter SQL Server manuell so konfiguriert wird, dass er die Anmeldeinformationen eines Computerkontos akzeptiert. Dieser Konfigurationsschritt sollte nach Abschluss des Ivanti Patch for Windows® Servers-Upgradeprozesses, aber vor dem ersten Programmstart durchgeführt werden.

- **Bestimmter Windows-Benutzer:** Diese Option wählen Sie, um eine spezifische Kombination von Benutzernamen und Kennwort anzugeben. Die Hintergrunddienste von Ivanti Patch for Windows® Servers verwenden diese Anmeldeinformationen zum Herstellen einer Verbindung zur SQL Server-Datenbank. Dies ist eine gute Ausweichoption, wenn aus irgendeinem Grund Schwierigkeiten bei der Implementierung der integrierten Windows-Authentifizierung auftreten sollten.
- **SQL-Authentifizierung:** Wählen Sie diese Option aus, wenn Sie eine spezifische Kombination von Benutzername und Kennwort vorgeben wollen, die von Diensten zur Anmeldung bei SQL Server verwendet werden soll.

15. Klicken Sie nach der Eingabe aller erforderlichen Informationen auf **Weiter**.

    Hinweis: Wenn das Installationsprogramm bei beliebigen Anmeldeinformationen, die Sie angegeben, ein Problem erkennt, wird eine Fehlermeldung angezeigt. Zumeist ist dies ein Hinweis darauf, dass das von Ihnen angegebene Benutzerkonto nicht existiert. Nehmen Sie entsprechende Korrekturen vor und versuchen Sie es erneut.

    Die Konsole wird mit Ihrer vorhandenen Datenbank verknüpft.

16. Klicken Sie auf **Weiter**.
17. Klicken Sie im Dialogfeld **Installation abgeschlossen** auf **Fertig stellen**.
18. Aktivieren Sie im Dialogfeld **Ivanti Patch for Windows® Servers Setup Wizard wurde abgeschlossen** das Kontrollkästchen **Ivanti Patch for Windows® Servers starten** und klicken Sie dann auf **Fertig stellen**.

AUF DER KONSOLE DURCHGEFÜHRTE UPGRADETASKS

Um das Upgrade abzuschließen, müssen folgende Aufgaben auf jederIvanti Patch for Windows® Servers-Konsole ausgeführt werden.

Zuweisen von Scheduler-Anmeldeinform-ationen

Hinweis: Dies gilt nur beim Upgrade von v9.1 auf v9.3.

Jetzt werden zur Ausführung von Konsolentasks Scheduler-Anmeldeinformationen benötigt, die Ihrem aktuellen Benutzerkonto entsprechen. Falls auf der Konsole geplante Tasks vorliegen und die Scheduler-Anmeldeinformationen nicht festgelegt wurden, wird zur Startzeit der Tasks eine Meldung angezeigt, die zur Einrichtung der Anmeldeinformationen auffordert. Diese Prüfung erfolgt jedes Mal, wenn Ivanti Patch for Windows® Servers gestartet wird. So wird sichergestellt, dass die geplanten Tasks weiterhin ausgeführt werden.

Überprüfen der geplanten Tasks

Geplante Tasks werden in zwei getrennten Bereichen überwacht und verwaltet. Sie müssen beide Bereiche der geplanten Tasks überprüfen, und sicherstellen, dass die vorhandenen Tasks ordnungsgemäß übertragen wurden.

- **Verwaltung für geplante Konsolentasks** ist die zentrale Stelle zur Anzeige der derzeit auf der Konsole geplanten Tasks, wie z.
- **Verwaltung für geplante Remotetasks** ist die zentrale Stelle zur Anzeige von Energietasks und Patchbereitstellungstasks, die derzeit auf remoten Zielcomputern geplant sind.

Aktualisieren der Lizenz (nur bei Offline-Konsolen)

Wenn Ihre Konsole offline ist (wenn sie keine Internetverbindung hat), müssen Sie Ihre Lizenz manuell aktualisieren, um die neuen Funktionen in Ivanti Patch for Windows® Servers 9.3 nutzen zu können. Informationen zum Aktivieren einer Offline-Konsole finden Sie im Online-Hilfesystem **Schnellstart > Setup > Der erste Blick auf das Programm > Aktivieren des Programms**.

Ist die Konsole online, wird die Lizenz während des Upgrades automatisch aktualisiert.

Überprüfen Ihrer Patchscanvorlagen und Patchgruppen

In diesen Bereichen sind drei Punkte zu berücksichtigen, vor allem für diejenigen Kunden, die ein Upgrade von v9.1 auf v9.3 durchführen.

- **Patchscanvorlagen:** Die Registerkarte **Filterung** des Dialogfelds **Patchscanvorlage** wurde aktualisiert und ermöglicht jetzt präziseres Scannen. Auch wenn beim Upgradevorgang automatisch vorhandene Patchscanvorlagen in den neuen Stil konvertiert werden, sollten Sie Ihre Vorlagen doch überprüfen, um die Änderungen zu bestätigen.
- **Patchgruppen:** Patchgruppen werden nicht mehr mit einem separaten Dialogfeld definiert, sondern werden jetzt aus der Patchansicht heraus

erstellt und verwaltet. Auch wenn beim Upgradevorgang automatisch vorhandene Patchgruppen in den neuen Stil konvertiert werden, sollten Sie Ihre Gruppen doch überprüfen, um die Änderungen zu bestätigen. Ihre Patchgruppen können nach dem Upgrade kleiner sein, da Ivanti viele alte Patches nicht weiter unterstützt.

- **Geänderte und automatisch generierte Patchgruppen:** Um das Verhalten Ihrer Patchscan-Vorlagen zu erhalten, könnten eine oder mehrere Ihrer vorhandenen Patchgruppen während des Upgradeprozesses geändert und eine oder mehrere neue Patchgruppen automatisch generiert worden sein.
    - **Geänderte Patchgruppen:** Wenn Sie im Abschnitt **Patchfiltereinstellungen** in Ihrer 9.1-Patchscanvorlage auf eine dieser Patchgruppen verweisen und **Ausgewählte scannen** aktiviert ist, werden alle Patches aus der Gruppe entfernt, die nicht den durch die Patchscanfilter definierten Kriterien entsprechen. Der Grund dafür ist: In Protect 9.1 können die Scanvorlagenfilter die Tatsache verdecken, dass Ihre Patchgruppe Patchtypen enthalten kann, die Sie eigentlich nie scannen oder implementieren wollten. Wenn in Ivanti Patch for Windows® Servers 9.3 die Patchgruppe als Baseline verwendet wird, werden die Scanvorlagenfilter nicht angewendet, was Ungenauigkeiten bei Ihren Patchgruppen aufdecken kann. Wird vom Upgradeprozess eine solche Situation erkannt, ändert er die Patchgruppe automatisch, um die beabsichtigte Interaktion zwischen Scanvorlage und Patchgruppe beizubehalten.

      Beispiel:

      Angenommen, Ihre 9.1-Patchgruppe enthält eine Kombination aus Sicherheitspatches, Softwareverteilungspatches und nicht sicherheitsrelevanten Patches. In der Scanvorlage, die auf diese Patchgruppe verweist, ist der Abschnitt **Patchfiltereinstellungen** auf **Ausgewählte scannen** eingestellt, und der Abschnitt **Patcheigenschaften** ist so eingestellt, dass nur Sicherheitspatches erkannt werden. Bei dieser Konfiguration wird der Filter **Patcheigenschaften** berücksichtigt, und es werden nur Sicherheitspatches erkannt (trotz der Tatsache, dass die Patchgruppe nicht sicherheitsrelevante und Softwareverteilungspatches enthält).

      Nach dem Upgrade auf 9.3 definiert die Scanvorlage die Patchgruppe als Baseline-Filter, und alle anderen Scanvorlagenfilter werden ignoriert. Wenn die Patchgruppe nicht geändert wird, werden nicht sicherheitsrelevante und Softwareverteilungspatches jetzt erkannt (und bereitgestellt, wenn Sie das Kontrollkästchen **Automatische Bereitstellung von Patches nach dem Scan** bei der Ausführung von Scans aktivieren). Der Upgradeprozess erkennt das und entfernt die nicht sicherheitsrelevanten und Softwareverteilungspatches aus der Patchgruppe.

      Hinweis: Achten Sie im weiteren Verlauf darauf, Ihre Patchgruppen ordnungsgemäß zu verwalten. Vermeiden Sie es,

unnötige oder unerwünschte Patches oder Patchtypen hinzuzufügen.

- **Automatisch generierte Patchgruppen:** Der Upgradeprozess erzeugt automatische eine Kopie einer vorhandenen Patchgruppe, wenn alle der folgenden Bedingungen erfüllt sind:
  - Wenn im Abschnitt **Patchfiltereinstellungen** einer Patchvorlage auf die Patchgruppe verwiesen wird und **Ausgewählte scannen** aktiviert ist, und
  - Wenn von einer Agentrichtlinie oder einer weiteren Scanvorlage mit anderen Filterdefinitionen auf die Patchgruppe verwiesen wird, und
  - Wenn die Patchgruppe vom Upgradeprozess aus Kompatibilitätsgründen geändert werden muss (siehe oben)

  In diesem Fall wird eine Kopie der Patchgruppe erstellt, die dann wie oben beschrieben geändert wird. Der Name der neuen Patchgruppe lautet ***<Patchgruppenname> -generated for <Scanvorlagenname>**. Die Scanvorlagen, die auf die Patchgruppe verweisen, werden dahingehend aktualisiert, dass sie den neuen Patchgruppennamen verwenden. Die ursprüngliche Patchgruppe wird beibehalten, damit Verweise darauf durch Ihre Agentrichtlinien oder andere Scanvorlagen weiter unterstützt werden.

  Sie sollten die Änderungen überprüfen und, falls gewünscht, den Namen der automatisch generierte Patchgruppe in einen aussagekräftigeren Namen umbenennen.

Zuweisen von Aliasen zur Konsole

Dieser Task muss ausgeführt werden, wenn mindestens eine der folgenden Bedingungen zutrifft:

- Sie haben den Konsolencomputer einer neuen Domäne zugewiesen.
- Sie haben der Konsole einen neuen allgemeinen Namen oder eine neue IP-Adresse zugewiesen.
- Sie haben Agents manuell installiert, und die Agents verwenden zur Kommunikation mit der Konsole eine IP-Adresse.

Unter diesen Bedingungen müssen Sie das Tool **Konsolen-Aliaseditor** zur Identifizierung der alten Konsolennamen oder Adressen einsetzen, die beide als vertrauenswürdige Aliase dienen. Falls Sie das nicht tun und ein Agent mit dem Ivanti Patch for Windows® Servers-Konsole eincheckt oder ein agentenloser Computer versucht, Statusmeldungen der Patchbereitstellung an die Konsole zu senden, ist es nicht möglich zu überprüfen, ob der kontaktierte Computer ein vertrauenswürdiger Computer ist.

1. Wählen Sie **Tools > Konsolen-Aliaseditor** aus.

   Das Dialogfeld **Konsolen-Aliaseditor** wird angezeigt. Es enthält die Namen und IP-Adressen, die derzeit zur Identifizierung des Konsolencomputers verwendet werden.

2. Geben Sie die Namen und/oder die IP-Adressen ein, die Sie als Alias für den Konsolencomputer verwenden möchten.

   IP-Adressen können entweder im IPv4-Format oder im IPv6-Format angegeben werden.

3. Klicken Sie auf **Aktualisieren**.

4. Klicken Sie entweder auf **Weiter** oder auf **Abbrechen**.

   Wenn Sie auf **Weiter** klicken, werden sowohl der Konsolendienst als auch das Programm Ivanti Patch for Windows® Servers automatisch neu gestartet. Das ist notwendig, um die Liste der Konsolenaliase zu aktualisieren. Wenn Sie auf **Abbrechen** klicken, wird die Liste der Konsolenaliase nicht aktualisiert.

WICHTIG! Die Agents erkennen einen neuen Alias erst, nachdem sie bei der neu gestarteten Konsole einchecken. Das Einchecken muss von einem Agent entweder manuell mit dem Agentclientprogramm initiiert werden oder über ein geplantes Einchecken; ein von der Konsole ausgegebener Eincheckbefehl für einen Agent wird das Konsolenzertifikat nicht aktualisieren.

Synchronisieren von Verteilungsservern

Sie müssen Ihre Verteilungsserver mit den neuesten Patches und/oder Scanmodulen und XML-Definitionsdateien aktualisieren, die auf der Konsole vorliegen. Dies ist insbesondere dann wichtig, wenn Ihre Agents für den Download dieser Dateien auf Verteilungsserver zurückgreifen. Die Verteilungsserver müssen mit den aktualisierten Konsolendateien synchronisiert werden, **bevor** die Agents einchecken.

So synchronisieren Sie Ihre Verteilungsserver:

1. Wählen Sie **Hilfe > Dateien aktualisieren** aus, um sicherzustellen, dass die Konsole die neuesten Dateien aufweist.

2. Wählen Sie **Tools > Optionen > Verteilungsserver**.

3. Wählen Sie im oberen Bereich im Feld **Geplante Synchronisierung hinzufügen** die Komponente aus, die synchronisiert werden soll.

4. Wählen Sie im oberen Bereich den Verteilungsserver aus, den Sie mit der Konsole synchronisieren möchten.

5. Klicken Sie auf **Geplante Synchronisierung hinzufügen**.

6. Geben Sie an, wann die Synchronisierung erfolgen soll und klicken Sie dann auf **Speichern**.

7. Wählen Sie im Bereich **Geplante automatische Synchronisierung** den Eintrag für die geplante Synchronisierung aus.

8. Klicken Sie auf **Jetzt ausführen**.

Sollten die Agents einchecken, bevor Sie die Synchronisierung der Verteilungsserver abgeschlossen haben, ist das kein Problem. Die Agents werden aktualisiert, sobald das nächste Mal ein geplanter Task ausgeführt wird oder der Agent seine Binärdateien aktualisiert.

Erwägen der Aktivierung der Funktion „Prädiktiver Patch“

Diese Funktion wurde erstmals in v9.2 verfügbar und ist daher neu für Sie, wenn Sie ein Upgrade von v9.1 durchführen. Damit kann Ivanti Patch for Windows® Servers Patches automatisch herunterladen, die wahrscheinlich in naher Zukunft bereitgestellt werden. Wenn Sie Verteilungsserver verwenden, können Sie „Prädiktiver Patch“ mit Ihrem Verteilungsserver synchronisieren, sodass die Server Kopien der heruntergeladenen Patches erhalten. Die Option „Prädiktiver Patch“ wird auf der Registerkarte **Tools > Optionen> Downloads** aktiviert. Sie wird mit Ihrem Verteilungsserver synchronisiert, indem Sie die Option **Mit prädiktivem Patch synchronisieren** Option im Dialogfeld **Verteilungsserver** aktivieren. Weitere Einzelheiten finden Sie im Hilfesystem.

Wiederherstellung der Sicherheit zwischen den Datenrollup-Konsolen

Hinweis: Dies gilt nur beim Upgrade von v9.1 auf v9.3. Die in v9.2 eingerichtete Sicherheitszuweisung funktioniert weiterhin auch in v9.3.

Wenn Sie mehrere Konsolen verwenden und eine Datenrollup-Konfiguration eingerichtet ist, müssen Sie die Sicherheitszuordnung zwischen der zentralen Konsole und jeder einzelnen Remotekonsole wiederherstellen.

WICHTIG! Sobald Sie den Upgradevorgang beginnen, finden solange keine Rollup-Aktivitäten mehr statt, bis das Upgrade sowohl für die zentrale Konsole als auch für die Remotekonsole durchgeführt und die Sicherheitszuordnungen zwischen beiden Konsolen wieder hergestellt wurden. Aus diesem Grund wird dringend empfohlen, dass Sie das Upgrade für Ihre Konsolen parallel und zu einem Zeitpunkt durchführen, wenn Sie nur sehr wenige Datenrollup-Aktivitäten erwarten.

Auf der zentralen Konsole

1. Führen Sie das Upgrade für die zentrale Konsole durch.
2. Wählen Sie **Tools > Optionen > Datenrollup** und vergewissern Sie sich, dass das Kontrollkästchen **Ergebnisse von einem Rollup-Absender akzeptieren** aktiviert ist.

Auf allen Remotekonsolen

1. Führen Sie das Upgrade auf allen Remotekonsolen durch.
2. Wählen Sie **Tools > Optionen > Datenrollup**.
3. Überprüfen Sie die Werte für IP-Adresse/Hostnamen und Port der Rollup-Konsole.
4. Klicken Sie auf **Registrieren**.

Weitere Informationen finden Sie im Online-Hilfesystem, siehe **Administration > Verwalten von mehreren Konsolen > Datenrollup-Konfiguration**.

Scannen von virtuellen Maschinen

Hinweis: Dies gilt nur beim Upgrade von v9.1 auf v9.3.

Sind in Ihrer Computergruppe virtuelle Maschinen definiert – entweder auf der Registerkarte **Gehostete virtuelle Maschinen** oder auf der Registerkarte **Workstation virtuelle Maschinen** – müssen Sie nach dem Upgrade entweder von der Startseite aus oder aus der Computergruppe heraus einen Scan dieser Maschinen initiieren. Das ist notwendig, um die Computeridentitäten bei Ivanti Patch for Windows® Servers wieder neu aufzubauen. Falls Sie den Scan nicht durchführen, werden die Felder **Virtueller Server** und **Pfad** in der Computeransicht möglicherweise nicht angezeigt, und Bereitstellungen für diese Maschinen können fehlschlagen.

Überprüfen der benutzerdefinierten Benutzereinstellungen

Folgende individuelle Benutzereinstellungen werden während des Upgradevorgangs nicht beibehalten.

- Tools > Optionen > Registerkarte „Anzeige“:
  - Aktuelles Element (Tage)
  - Archivierte Elemente
  - Nur von mir erstellte Elemente anzeigen
  - Primären Newsfeed anzeigen
  - 'Zur Information' in Patchscanergebnissen anzeigen
  - Service Packs in Ansicht > Patches anzeigen
- Tools > Einstellungen > Registerkarte „Benachrichtigungen und Warnungen“:
  - Vor dem Planen von Bereitstellungen warnen
  - 'Dateien aktualisieren' nach Abschluss schließen
  - Warnung bei nicht aktivierter Protect Cloud-Synchronisierung auf dieser Konsole
  - Vor dem Öffnen von 7 oder mehr Bulletins eine Warnung anzeigen
- Registerkarte Tools > Optionen> Patch:
  - Globales Threadpool

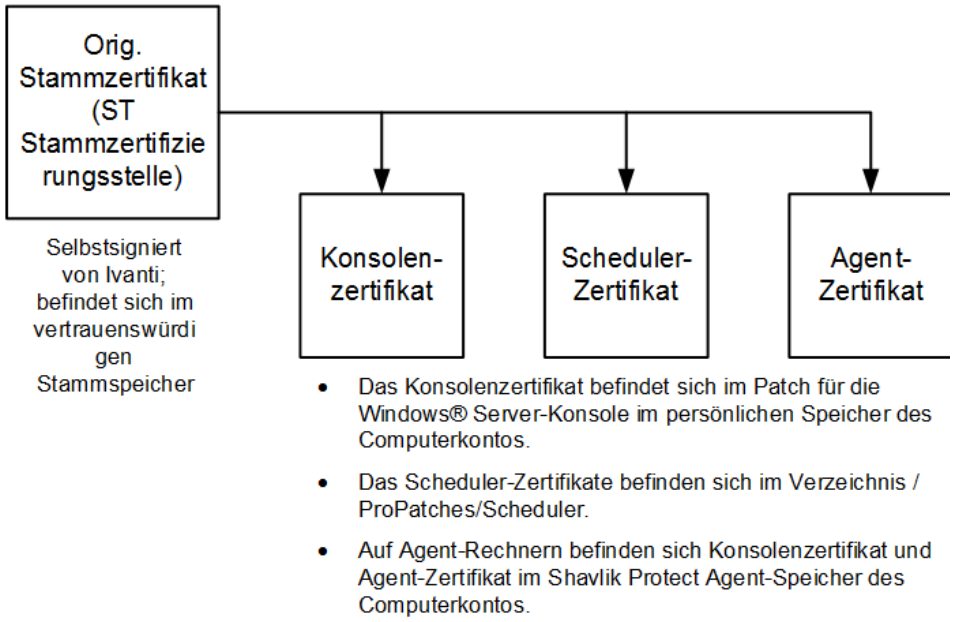
    Dies ist neu in v9.3 und gilt für alle Funktionen des Produktes. In v9.2 wurde das Threadpool in der Assetscanvorlage definiert, was jedoch während des Upgrades entfernt wurde. Der neue Standardwert kann anders sein als der bei der alten Threadpool-Option angegebene.
- Tools > Optionen > Registerkarte „Protokollierung“:
  - Diagnosepatch-Scan
- Bereitstellungsverfolgung:
  - Aktualisierungsgeschwindigkeit
  - Anzuzeigende Tage
  - Fehler anzeigen:
  - In Bearbeitung anzeigen:
  - Erfolgreich abgeschlossene anzeigen:
- Das Dialogfeld „Berichte“
  - Nach IAVA-Kennung sortieren

- Registerkarte „ESXi Hypervisor-Bulletins“:
  - Nur neueste anzeigen
- Ereignisverlauf
  - Ergebnisse auf vorherige (Tage) begrenzen
- ITScripts-Ergebnisansicht
  - Ergebnisse seit

Beachten Sie, dass V9.3 andere Zertifikatstruktur einsetzt

Speicherorte und Beziehungen der Zertifikate ändern sich, wenn Sie ein Upgrade von von Shavlik Protect 9.1 oder Shavlik Protect 9.2 auf Ivanti Patch for Windows® Servers 9.3 durchführen. In v9.1 und v9.2 wurden die Scheduler- und Agent-Zertifikate vom Konsolenzertifikat ausgestellt. In v9.3 werden Konsolen-, Scheduler- und Agent-Zertifikat vom selbstsignierten Stammzertifikat ausgestellt.

Nach dem Upgrade auf Ivanti Patch for Windows® Servers 9.3



Nachdem Sie den Upgradevorgang abgeschlossen haben, startet Ivanti Patch for Windows® Servers 9.3 seinen eigenen Prozess zur Verwaltung der Zertifikate hinter den Kulissen.

- Das vorhandene Konsolenzertifikat wird aus dem Speicher für die Zwischenzertifizierungsstelle entfernt. Dies erfolgt innerhalb der ersten ein oder zwei Einsatztage, abhängig von Ihren Wartungsaktivitäten.
- Ein neues Zertifikat für den Scheduler wird jedes Mal vom Stammzertifikat erstellt, wenn der Ivanti Scheduler installiert oder eine agentenlose Bereitstellung mithilfe des Schedulers ausgeführt wird. Das alte Scheduler-Zertifikat (das ursprünglich vom 9.2-Konsolenzertifikat ausgestellte Original) wird gelöscht.
- Ein neues Zertifikat für den Agenten wird jedes Mal vom Stammzertifikat erstellt, wenn ein neuer Agent installiert wird oder das Zertifikat eines vorhandenen Agenten erneuert werden muss. Der Agent speichert das Agent-Zertifikat in seinem lokalen Speicher und

das Konsolenzertifikat wird aus dem vertrauenswürdigen Stammspeicher auf dem Agentencomputer in den privaten Speicher verschoben. Das alte Agent-Zertifikat (das ursprünglich vom 9.2-Konsolenzertifikat ausgestellte Original) wird gelöscht.

Zum Agent-Upgradeprozess gehört auch darauf zu warten, bis sich Ihre Agenten einchecken, damit sie ein neues Agent-Zertifikat erhalten. Die Dauer hängt von einer Reihe von Faktoren ab, doch wird der gesamte Prozess im Hintergrund abgewickelt. Einzig die Überwachung des Ereignisverlaufsprotokolls liegt bei Ihnen, um zu prüfen, ob Probleme auftreten, um die Sie sich kümmern müssen.

Wenn Sie einen Agent auf der Konsole verwenden

Wenn Sie einen Agenten auf der Ivanti Patch for Windows® Servers-Konsole installiert haben, müssen Sie diesen Agenten manuell neu installieren. Das ist notwendig, um sicherzustellen, dass der Konsolenagent ordnungsgemäß mit dem neuen Agent-Zertifikat aktualisiert wird. Bei Agenten, die auf Zielcomputern installiert sind, ist keine Aktion erforderlich.

WESENTLICHE ÄNDERUNGEN UND VERBESSERUNGEN IN IVANTI PATCH FOR WINDOWS® SERVERS 9.3

Ausführliche Details zu den folgenden Themen finden Sie im Online-Hilfesystem:

https://help.ivanti.com/sh/help/de_DE/PWS/93/PWS.htm

API-Funktion

Die API-Funktion wurde für erfahrene Benutzer entwickelt, die über praktische Erfahrung mit PowerShell verfügen und zusätzliche Tasks durchführen möchten, die in der normalen Benutzeroberfläche von Ivanti Patch for Windows® Servers nicht verfügbar sind. Sie können die API-Funktion für Folgendes einsetzen:

- Interaktion mit verschiedenen Systemen in Ihrer Umgebung
- Skript-Erstellung für eine Abfolge von komplexen Ereignissen, die Abhängigkeiten enthalten
- Durchführen von Massenvorgängen oder Verarbeitung von Listeneingaben aus anderen Systemen
- Programmgesteuerte Staffelung von Patchimplementierungen oder Initiieren von Patchdownloads

Ausführliche Informationen zum Verwenden der API-Funktion finden Sie in der *API Schnellstart-Direkthilfe*.

Ordnerpfade im Navigationsbereich

Ein weiteres neues Feature ist die Möglichkeit, eine hierarchische Struktur für Ihre Computergruppen, Patchscanvorlagen und Patch-Bereitstellungsvorlagen zu erstellen. Wenn Sie viele Gruppen oder Vorlagen erstellen, kann es ratsam sein, sie auf logische Ordner zu verteilen. Auf diese Weise können Sie Ihre Gruppen und Vorlagen schneller auffinden und leichter verwalten. Y

Im Navigationsfenster können Sie beliebig viele Ordner und Unterordner erstellen. Sie können Ihre Gruppen zum Beispiel nach dem Typ der enthaltenen Computer oder nach dem Standort organisieren.

Nachdem sie angelegt wurden, können Sie per Drag & Drop Elemente aus einem Ordner in einen anderen verschieben. Sie können auch mit der rechten Maustaste auf eine beliebige Ebene der Hierarchie klicken und einen Vorgang für alle Elemente auf oder unterhalb dieser Ebene durchführen.

Gestaffelte Bereitstellungen

Es gibt jetzt vier separate, planbare Punkte im Patchscan- und Bereitstellungsprozess. Das erlaubt Ihnen eine wesentlich bessere Kontrolle über den gesamten Prozess. Sie haben folgende Möglichkeiten:

- Nur einen Scan durchführen
- Durchführen eines Scan und dann Ausführen des Staging für die fehlenden Patches auf dem Zielcomputer zu einem bestimmten Zeitpunkt, ohne die Patches zu installieren
- Durchführen eines Scans, Ausführen des Staging für die fehlenden Patches und Installieren der Patches zu einem Zeitpunkt Ihrer Wahl

Geplante Snapshot-Wartung

Mit dieser neuen Funktion können Sie einen einmaligen oder wiederkehrenden Task planem, um alte VM-Snapshots auf dem Server zu entfernen. Bisher konnten alte Snapshots nur in Echtzeit und während eines Bereitstellungstasks gelöscht werden. Um auf diese Funktion zuzugreifen, wählen Sie **Tools > Optionen > Snapshot-Wartung** und fügen einen Task hinzu.

Möglichkeit zur Nutzung einer Drittanbieter-Zertifizierungsstelle

Sie haben die Möglichkeit, eine vertrauenswürdige Zertifizierungsstelle (CA) aus Ihrer eigenen PKI-Infrastruktur einzusetzen, um ein Ersatz-Stammzertifikat für Ivanti Patch for Windows® Servers herauszugeben. Dies ist keine Notwendigkeit. Wenn Sie aber ein Sicherheitstool nutzen, das das standardmäßig selbstsignierte Stammzertifikat als ein mittleres Sicherheitsrisiko ansieht, steht jetzt ein Prozess zur Verfügung, mit dem ein Ersatzzertifikat generiert werden kann. Weitere Informationen finden Sie im Online-Hilfesystem, siehe **Administration > Dienstprogramme > Generieren eines Zertifikats von einer Drittanbieter-CA**.

Verwaltung für geplante Remotetasks

Mehrere Änderungen wurden an der Verwaltung für geplante Remotetasks vofgenommen.

- Der Zugriff erfolgt jetzt durch einen Rechtsklick auf einen Computer in der Computeransicht oder der Scanansicht und anschließende Auswahl von **Geplante Tasks anzeigen**.
- Informationen zu Energietasks und Patchbereitstellungstasks werden jetzt in einem Format dargestellt, das der Verwaltung für geplante Konsolentasks ähnelt.
- Jetzt werden Tasks angezeigt, die auf dem Remotecomputer entweder mit dem Ivanti Scheduler oder dem Microsoft Task Scheduler geplant wurden.

Neue Designs

Im Dialogfeld **Anzeigeoptionen** steht jetzt eine neue Option zur Verfügung, mit der Sie das Farbschema für die Benutzeroberfläche für Ivanti Patch for Windows® Servers angeben können. Sie können nicht nur die für Ihre Augen angenehmste Farbe auswählen, sondern auch Designs mit höherem Kontrast wählen, was besonders bei RDP-Umgebungen mit geringer Bandbreite hilfreich ist.

Neue Möglichkeiten bei Spaltenfiltern

Filter können jetzt auf eine oder mehrere Spaltenüberschriften im Raster angewendet werden. Bewegen Sie dazu den Mauszeiger über eine Spaltenüberschrift und klicken Sie dann auf das Filtersymbol, das sich in der rechten oberen Ecke befindet. Beispiel:

Im Filtermenü können Sie auswählen, welche der derzeit in der Spalte enthaltenen Werte angezeigt werden sollen.

Manuelle Download-Methode

Eine neue Spalte **Download-Methode** gibt an, ob ein Patch automatisch oder nur manuell heruntergeladen werden kann. Wenn der Wert in dieser Spalte **Automatisch** ist, bedeutet da, dass Ivanti Patch for Windows® Servers den Patch automatisch herunterladen kann. Ist der Wert **Vom Anbieter erwerben** oder ein anderen Wert, bedeutet dies, dass Sie selbst den Patch manuell herunterladen und ihn dann in das Patch-Downloadverzeichnis verschieben müssen. Nachdem der Patch dort ist, kann er mit dem normalen Bereitstellungsprozess bereitgestellt werden. Wenn die automatische Bereitstellung genutzt wird und ein Patch manuell heruntergeladen werden muss, funktioniert der automatische Bereitstellungsprozess nicht.

Ein Reihe von Gründen können dafür verantwortlich sein, dass ein Patch nicht automatisch heruntergeladen werden kann. Beispielsweise haben Sie einen Patch, der für ein proprietäres Softwareprogramm erstellt wurde, oder Sie erhalten Patches für ein Programm, das nicht mehr offiziell vom Hersteller unterstützt wird.

Informationen zur Bereitstellungskonfiguration

Das Dialogfeld **Bereitstellungskonfiguration** enthält jetzt Informationen über den Speicherplatzbedarf bei der Bereitstellung von Patches.

Konsolidierte Programmoptionen

Alle Programmoptionen sind jetzt an einer Stelle konsolidiert. Zur Anzeige der Optionen wählen Sie **Tools > Optionen**. Das Menü **Tools > Vorgänge** wurde entfernt.

Patchgruppenfilter

Die Patchansicht enthält einen neuen Patchgruppenfilter. Das Kontrollkästchen **Patches anzeigen, die derzeit in der ausgewählten Patchgruppe enthalten sind** ermöglicht es Ihnen auszuwählen, ob Patches in der ausgewählten Patchgruppe in der Liste Patchgruppe enthalten angezeigt werden sollen.

Änderungen an der Benutzeroberfläche von Bereitstellungsverfolgung

Die Bereitstellungsverfolgung wurde neu gestaltet, um mehr Details zu den Patchbereitstellungstasks zu liefern, die gerade ausgeführt werden. Außerdem könen Sie jetzt eine Bereitstellung aus der Bereitstellungsverfolgung heraus abbrechen. Der Vorbereitungsvorgang muss abgeschlossen sein, doch die eigentliche Bereitstellung darf noch nicht gestartet sein.

Downloadpaket exportieren

Sie können jetzt die Download-Links für ausgewählte Patches in eine CSV-Datei exportieren. Dies ist besonders bei eine Konsole in einer Offline-Umgebung nützlich. Die CSV-Datei kann von einem Computer, der online ist, dazu genutzt werden, die Patches herunterzuladen. Dann können die Patches in das Patchverzeichnis des Offline-Computers kopiert werden.

Hinweis: Ein File Skript-Downloader PowerShell-Skript kann Ihnen beim Dateidownloadvorgang helfen.

Neue IAVA-Berichte

Jetzt sind zwei neue IAVA-Berichte verfügbar: „Computercompliance (IAVA)“ und „Keine Computercompliance (IAVA)“. Diese beiden Berichte enthalten zusätzliche Informationen, die von der US- Regierung bei der Übergabe von Berichtsdaten verlangt werden.

Globales Threadpool

Die Threadverwaltung hat sich von der Vorlagenebene in ein systemübergreifendes Pool verschoben und wird jetzt im Dialogfeld **Tools > Optionen > Patch** definiert. Gemäß Voreinstellung nutzt das Programm 8 Threads pro CPU-Kern. Diesen Wert können Sie jedoch nach Bedarf einstellen. Dieser Einzelwert gibt die Gesamtzahl der Threads an, die während eines Patchscans oder einer Bereitstellung, eines Assetscans oder eines Energiestatusscans genutzt werden können.

Erweiterte Suchfunktionen

Die Suchfunktionen des Produkts wurden auf weitere Bereiche ausgedehnt. Sie können jetzt Suchen durchführen:

- Auf der Registerkarte **Gehostete virtuelle Maschinen** einer Computergruppe.
- Durch Klicken mit der rechten Maustaste auf eine beliebige Computergruppe im Navigationsfenster und Auswahl von **Computergruppen durchsuchen**. Dadurch können Sie bestimmte Computer und Gruppen über alle Computergruppen hinweg lokalisieren.
- Mithilfe des neuen Suchfelds im mittleren Bereich in der Scanansicht und der Computeransicht.