Ivanti Patch for Windows® Servers

Guida di aggiornamento

Copyright e marchi

Informazioni sul documento e cronologia di stampa

Numero documento: N/D

Data	Versione	Descrizione
Settembre 2010	NetChk Protect 7.6	Aggiornato il product branding e aggiunte informazioni sulle nuove funzioni e sui miglioramenti della versione 7.6.
Marzo 2011	NetChk Protect 7.8	Aggiunte informazioni sulle nuove funzioni e sui miglioramenti della versione 7.8.
Ottobre 2011	VMware vCenter Protect 8.0	Aggiornato il product branding e aggiunte informazioni sulle attività di aggiornamento per la versione 8.0. Rimuovere tutte le informazioni in merito alle versioni precedenti alla 7.5.
Dicembre 2011	Vmware vCenter Protect 8.0, Documento Rev A	Aggiunti passaggi esplicativi sulla compressione del database prima di iniziare il processo di aggiornamento.
Settembre 2012	Vmware vCenter Protect 8.0.1	Aggiornato il nome prodotto e la versione, aggiornate le grafiche della copertina.
Maggio 2013	Shavlik Protect 9.0	Aggiornati i requisiti di sistema. Aggiunte informazioni sulle nuove funzioni e sui miglioramenti della versione 9.0.
Aprile 2014	Shavlik Protect 9.1	Aggiornati i requisiti di sistema. Aggiunte informazioni sulle nuove funzioni e sui miglioramenti della versione 9.1.
Settembre 2015	Shavlik Protect 9.2	Aggiornati i requisiti di sistema. Aggiunte informazioni sulle nuove funzioni e sui miglioramenti della versione 9.2.
Aprile 2017	Ivanti Patch for Windows® Servers 9.3	Modifica del marchio in Ivanti, rimozione dei riferimenti a AV, aggiornamento dei requisiti di sistema, aggiunta delle informazioni sulle nuove funzioni e sui miglioramenti della v9.3.

BENVENUTI

Scopo di questa guida

Benvenuti in Ivanti Patch for Windows® Servers 9.3. Questo documento descrive come effettuare l'aggiornamento da Shavlik Protect 9.1 o Shavlik Protect 9.2 a Ivanti Patch for Windows® Servers 9.3.

Oltre a descrivere la procedura di aggiornamento, questo documento elenca una serie di differenze funzionali di cui tenere conto in fase di aggiornamento a Ivanti Patch for Windows® Servers 9.3. Evidenzia inoltre le aree nell'interfaccia utente che hanno subito modifiche sostanziali.

Nuovi requisiti e prerequisiti di sistema

Considerare i seguenti nuovi requisiti e prerequisiti per Ivanti Patch for Windows® Servers 9.3.

- Windows Server 2016 e Windows 10 sono ora supportati come computer della console
- Microsoft .NET Framework 4.6.2 o versione successiva
- Microsoft Visual C++ Redistributable for Visual Studio 2015
- Rimosso il supporto per SQL Server 2005. La nuova versione minima è SQL Server 2008.
- Windows XP e Windows Server 2003 non sono più supportati sui computer degli agenti
- L'Antivirus non è più supportato in questa versione

Tutti i prerequisiti software mancanti verranno installati automaticamente durante il processo di aggiornamento. Consultare la Guida di installazione di *Ivanti Patch for Windows® Servers* per l'elenco completo dei requisiti di sistema.

Requisiti dell'account utente per l'esecuzione di un upgrade

Al fine di eseguire un aggiornamento, l'account utente deve rispettare i seguenti requisiti:

- L'utente che esegue l'aggiornamento del database deve essere membro del ruolo db_owner.
- Se si dispone di più console che condividono un database e se si effettua il collegamento di una console aggiuntiva a un database già aggiornato, l'account utente utilizzato deve essere membro dei seguenti ruoli di database: db_datareader, db_datawriter, STExec e STCatalogupdate. Inoltre, l'account di servizio utilizzato per le operazioni in background deve essere membro del ruolo db_owner. Se il proprio account è membro dei ruoli db_securityadmin e db_accessAdmin, lo strumento di aggiornamento del database cercherà automaticamente di mappare e configurare i ruoli richiesti per l'utente.

PROCEDURA DI AGGIORNAMENTO

Panoramica

Questa sezione descrive come effettuare l'aggiornamento da Shavlik Protect 9.1 o Shavlik Protect 9.2 a Ivanti Patch for Windows® Servers 9.3. Se si sta cogliendo l'opportunità per spostare la console su una nuova macchina e si desidera eseguire la migrazione utilizzando lo Strumento di migrazione, consultare la *Guida per l'utente allo strumento di migrazione* prima di eseguire l'aggiornamento.

Prima di eseguire l'aggiornamento, assicurarsi di leggere la sezione *Modifiche e ottimizzazioni significative* a pagina 17, in modo da essere consapevoli del modo in cui l'aggiornamento influirà sul sistema. Provvedere inoltre ad annotare tutte le impostazioni utente personalizzate correnti, dato che parte di esse non verrà mantenuta durante l'upgrade (vedere pagina 14).

Nota: tenere presente che una volta completato l'aggiornamento della console, qualsiasi agente installato sui propri computer di destinazione verrà aggiornato automaticamente al prossimo check-in con la console.

Esecuzione dell'upgrade

1. Liberare lo spazio inutilizzato nel database usato per archiviare i risultati delle analisi e i risultati di distribuzione delle patch.

   A tal fine, aprire SQL Server Management Studio facendo clic con il pulsante destro del mouse nel database ShavlikScans e selezionare **Attività > Riduci > Database**.

2. Creare un backup del database corrente utilizzando SQL Server Management Studio.

   Il database contiene risultati dalle operazioni dei programmi e anche informazioni sulla configurazione. Il backup del database è un passaggio importante.

3. Chiudere tutti i programmi in funzione sul computer della console, incluso Shavlik Protect.

4. Scaricare il file eseguibile di Ivanti Patch for Windows® Servers 9.3 nel proprio computer della console utilizzando il seguente collegamento:

   https://www.ivanti.com/it-IT/resources/downloads

5. Avviare il processo di installazione utilizzando uno dei metodi seguenti:

   - Fare doppio clic sul file denominato **IvantiPatchForServers.exe**.
   - Digitare il nome del file in un prompt dei comandi. In questo modo sarà possibile utilizzare una o più opzioni delle righe di comando. Considerare questo metodo se si sta aggiornando un database di grandi dimensioni. L'opzione DBCOMMANDTIMEOUT viene utilizzata per specificare il valore di timeout del comando SQL durante l'installazione. Il valore predefinito è 15 minuti per GB. Il valore di timeout minimo rappresenta il valore maggiore tra 15 minuti per GB e 1800 secondi (30 minuti). È necessario escludere il valore predefinito solo se si prevede che l'upgrade richieda un periodo di tempo eccezionalmente lungo a causa di risorse vincolate. Ad esempio, in presenza di un database da 4 GB, per raddoppiare il valore di timeout

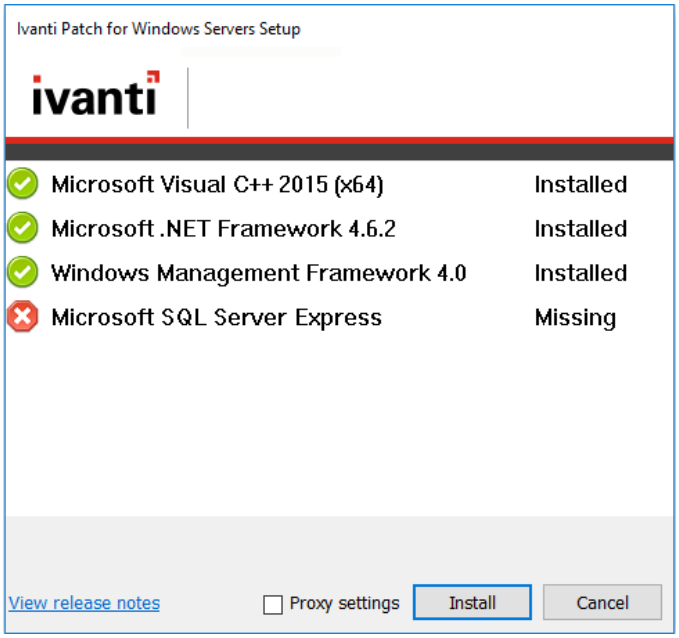
predefinito da 3600 secondi (60 minuti) a 7200 secondi (120 minuti) sarebbe necessario digitare il seguente comando:

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

Nota: se viene visualizzato un messaggio in cui si richiede un riavvio, fare clic su **OK**, la procedura di installazione riprenderà automaticamente dopo il riavvio.

6. Rispondere affermativamente alla finestra di dialogo che richiede se si desidera proseguire l'aggiornamento.

   Se si fa clic su **Sì** e il proprio computer della console risulta privo di uno o più prerequisiti, verrà visualizzata una finestra di dialogo simile alla seguente. Se non manca alcun prerequisito, ignorare il punto seguente e procedere con la finestra di dialogo **Benvenuti.**



7. Fare clic su **Installa** per installare qualsiasi prerequisito mancante.

   La procedura guidata di configurazione potrebbe richiedere un riavvio durante questa fase del processo di installazione. Se è richiesto un riavvio, una volta riavviato il computer verrà visualizzata la finestra di configurazione. Fare nuovamente clic su **Installa** per proseguire l'upgrade.

   Verrà visualizzata la finestra di dialogo Benvenuti.

8. Leggere le informazioni contenute nella finestra di dialogo **Benvenuti**, quindi fare clic su **Avanti**.

   Verrà visualizzato il contratto di licenza. Per poter installare il programma sarà necessario accettare i termini del contratto di licenza.

9. Spuntare la casella di controllo **Accetto i termini del Contratto di licenza**, quindi fare clic su **Avanti**.

   Verrà visualizzata la finestra di dialogo **Cartella di destinazione**.

10. Se si desidera modificare la posizione predefinita del programma, fare clic sul pulsante sfoglia e scegliere una nuova posizione. Qui è inoltre presente l'opzione che consente di installare un'icona del collegamento sul desktop. Al termine, fare clic su **Avanti**.

    Verrà visualizzata la finestra di dialogo **Programma di miglioramento del prodotto**. Leggere la descrizione e decidere se partecipare o meno al programma. Il programma consente a Ivanti di raccogliere informazioni sull'utilizzo del prodotto che verranno utilizzate per migliorare le versioni future.

11. Fare clic su **Avanti**.

    Verrà visualizzata la finestra di dialogo **Pronto per l'installazione**.

12. Per iniziare l'installazione fare clic su **Installa**.

    In prossimità del termine del processo di installazione, verrà visualizzata la finestra di dialogo **Strumento di impostazione del database**.

    Importante! Nella fase seguente NON selezionare **Crea un nuovo database**. Selezionando questa opzione si creerà un nuovo database e i dati esistenti non verranno utilizzati.

13. Verificare che risulti selezionato **Utilizzare un database esistente**, quindi fare clic su **Avanti**.

14. Utilizzare le caselle fornite per definire in che modo gli utenti e i servizi avranno accesso al database SQL Server.

    Scegliere un server e un'istanza di database

    - **Nome server:** è possibile specificare un computer oppure un computer e l'istanza di SQL Server in esecuzione su tale computer.
    - **Nome del database:** specificare il nome del database che si desidera utilizzare. Il nome del database predefinito è **Protect**.

    Scegliere come gli utenti interattivi si collegheranno al database

    Specificare le credenziali che si desidera vengano utilizzate dal programma quando un utente esegue un'azione che richiede l'accesso al database.

    - **Autenticazione di Windows integrata:** si tratta dell'opzione raccomandata e predefinita. Ivanti Patch for Windows® Servers utilizzerà le credenziali dell'utente attualmente registrato per connettersi al database SQL Server. Le caselle **Nome utente** e **Password** non saranno disponibili.
    - **Utente Windows specifico:** selezionare questa opzione solo se il database SQL Server si trova su un computer remoto. Questa opzione non avrà alcun effetto se il database si trova sul computer locale (console). (Consultare la sezione *Fornitura di credenziali* nella *Guida amministrativa di Ivanti Patch for Windows®* per ulteriori informazioni sulle credenziali del computer locale.) Tutti gli utenti di Ivanti Patch for Windows® Servers utilizzeranno le credenziali fornite al momento di eseguire azioni che richiedono l'interazione con il database SQL Server remoto.
      Autenticazione SQL: selezionare questa opzione per immettere una combinazione specifica di nome utente e password che verrà utilizzata per accedere all'SQL Server specificato.

Attenzione! Se si forniscono credenziali di autenticazione SQL e non si è implementata la crittografia SSL per le connessioni SQL, le credenziali verranno trasmesse in rete come testo non crittografato.

- **Test connessione database:** per verificare che il programma possa utilizzare le credenziali utente interattive fornite per connettersi al database, fare clic su questo pulsante.

Scegliere come i servizi si collegheranno al database

Specificare le credenziali che si desidera vengano utilizzate dai servizi in background quando si effettua la connessione al database. Si tratta delle credenziali che l'unità di importazione risultati, le operazioni agente e altri servizi utilizzeranno per accedere all'SQL Server e fornire informazioni di stato.

- **Usa credenziali alternative per i servizi della console:**
    - Se il database SQL Server è installato sul computer locale, in genere si ignorerà questa opzione non attivando questa casella di controllo. In questo caso verranno utilizzate le stesse credenziali e la modalità di autenticazione specificate sopra per gli utenti interattivi.
    - In genere si spunterà questa casella di controllo solo se il database SQL Server si trova su un computer remoto. Quando il database si trova su un computer remoto, sarà richiesto un account in grado di autenticarsi al database sul server del database remoto.
- **Metodo di autenticazione:** disponibile solo se è stata attivata l'opzione **Usa credenziali alternative per i servizi della console**.
    - **Autenticazione di Windows integrata:** selezionando questa opzione l'account del computer verrà utilizzato per connettersi all'SQL Server remoto. Il protocollo di autenticazione di rete Kerberos deve essere disponibile al fine di trasmettere le credenziali in tutta sicurezza. Le caselle Nome utente e Password non saranno disponibili.

Nota: se si sceglie l'**Autenticazione di Windows integrata** il programma di installazione cercherà di creare un login di SQL Server per l'account del computer. Se la procedura di creazione account non riesce, consultare la sezione *Note di post-installazione di SQL Server* nella *Guida di installazione di Ivanti Patch for Windows® Servers*, si otterranno istruzioni sulla configurazione manuale di un SQL Server remoto, al fine di accettare le credenziali dell'account del computer. Tale operazione è necessaria dopo il completamento del processo di upgrade di Ivanti Patch for Windows® Servers, ma prima di avviare il programma.

    - **Utente Windows specifico:** selezionare questa opzione per immettere una combinazione specifica di nome utente e password. I servizi in background di Ivanti Patch for Windows® utilizzeranno tali credenziali per connettersi al database di SQL Server. Si tratta di una valida opzione di fallback se per qualche motivo si ha difficoltà a implementare l'autenticazione di Windows integrata.
    - **Autenticazione SQL:** selezionare questa opzione per fornire una combinazione specifica di nome utente e password per i servizi da utilizzare in fase di accesso a SQL Server.

15. Dopo aver fornito tutte le informazioni richieste, fare clic su **Avanti**.

    Nota: se il programma di installazione rileva un problema con una qualsiasi delle credenziali specificate, verrà visualizzato un messaggio di errore. Ciò indica in genere che un account utente specificato non esiste. Effettuare le necessarie correzioni e riprovare.

    La console è collegata al proprio database esistente.

16. Fare clic su **Avanti**.
17. Sulla finestra di dialogo **Installazione completata**, fare clic su **Fine**.
18. Sulla finestra di dialogo **Procedura guidata di configurazione di Ivanti Patch for Windows® Servers completata**, spuntare la casella di controllo **Avvia Ivanti Patch for Windows® Servers**, quindi fare clic su **Fine**.

ATTIVITÀ DI AGGIORNAMENTO ESEGUITE SULLA CONSOLE

Al fine di completare l'aggiornamento, eseguire le attività seguenti sulla console Ivanti Patch for Windows® Servers.

Assegnazione credenziali utilità di pianificazione

Nota: ciò si applica solo in caso di upgrade dalla v9.1 alla v9.3.

Una credenziale utilità di pianificazione corrispondente al proprio account utente corrente è ora richiesta per eseguire le attività pianificate della console. In presenza di attività pianificate sulla console con la credenziale utilità di pianificazione non impostata, si riceverà un messaggio all'avvio in cui verrà richiesto di impostare la credenziale. Tale verifica avviene a ogni avvio di Ivanti Patch for Windows®, al fine di assicurare il costante funzionamento delle attività pianificate.

Revisione delle attività pianificate

Le attività pianificate vengono monitorate e gestite da due aree separate. Esaminare entrambe le gestioni attività pianificate per verificare che le proprie attività esistenti siano state importate correttamente.

- La **Gestione attività console pianificate** fornisce una posizione in cui visualizzare le attività attualmente pianificate sulla console, come le analisi patch, le analisi asset, le distribuzioni di patch sul computer della console, l'esecuzione di script e i report pianificati.
- La **Gestione attività remote pianificate** fornisce una posizione in cui visualizzare le attività di alimentazione e le attività di distribuzione patch attualmente pianificate sui propri computer di destinazione remoti.

Aggiornamento della licenza (solo console offline)

Se la propria console è offline (non dispone di una connessione a Internet), al fine di poter visualizzare e utilizzare le nuove funzioni in Ivanti Patch for Windows® Servers 9.3 sarà necessario aggiornare manualmente la propria licenza. Per informazioni sull'attivazione di una console disconnessa, consultare il sistema di Guida online alla pagina **Avvio rapido > Configurazione > Primo sguardo al programma > Attivazione del programma**.

Se la console è online, la licenza verrà aggiornata automaticamente durante il processo di aggiornamento.

Revisione dei modelli di analisi delle patch e dei gruppi di patch

Vi sono tre problematiche da considerare in queste aree, in modo particolare per i clienti che effettuano l'upgrade dalla v9.1 alla v9.3.

- **Modelli di analisi delle patch:** la scheda **Filtro** sulla finestra di dialogo **Modello di analisi delle patch** è stata aggiornata per consentire una maggiore precisione durante l'analisi. Mentre la procedura di upgrade convertirà automaticamente i propri modelli di analisi delle patch esistenti al nuovo stile, sarà necessario esaminare i modelli per verificare le modifiche.

- **Gruppi di patch:** i gruppi di patch non vengono più definiti utilizzando una finestra di dialogo separata, ma vengono creati e gestiti all'interno di Visualizzazione patch. Mentre la procedura di upgrade convertirà automaticamente i propri gruppi di patch esistenti alla nuova convenzione, sarà necessario esaminare i gruppi per verificare le modifiche. I propri gruppi di patch potrebbero risultare più piccoli dopo l'upgrade, dato che Ivanti ha interrotto il supporto per molte patch datate.

- **Gruppi di patch modificati e generati in automatico:** al fine di preservare il comportamento dei modelli di analisi delle patch, uno o più dei propri gruppi di patch esistenti può essere modificato durante il processo di upgrade e uno o più dei nuovi gruppi di patch può essere generato automaticamente.

    - **Gruppi di patch modificati:** se si fa riferimento a un gruppo di patch all'interno della sezione **Impostazioni filtro patch** del proprio modello di analisi delle patch 9.1 e **Analizza selezionati** risulta abilitato, qualsiasi patch che non rispetta i criteri definiti dai filtri del modello di analisi verrà rimossa dal gruppo. Ecco perché: in Protect 9.1, i filtri dei modelli di analisi possono mascherare il fatto che il proprio gruppo di patch può contenere tipi di patch che non si è mai scelto intenzionalmente di analizzare o distribuire. In Ivanti Patch for Windows® Servers 9.3, quando il gruppo di patch viene utilizzato come baseline, i filtri dei modelli di analisi non verranno applicati, rivelando potenziali imprecisioni nei gruppi di patch. Se il processo di upgrade rileva tale situazione, modificherà automaticamente il gruppo di patch, al fine di preservare l'interazione prevista tra il modello di analisi e il gruppo di patch.

      Esempio:

      Ipotizziamo che il proprio gruppo di patch 9.1 contenga un mix di patch di Protezione, Non di protezione e di Distribuzione software. Nel modello di analisi che fa riferimento a questo gruppo di patch, la sezione **Impostazioni filtro patch** viene impostata su **Analizza selezionati**, mentre la sezione **Proprietà patch** viene impostata in modo da rilevare solo le patch di Protezione. In questa configurazione, il filtro **Proprietà patch** verrà rispettato e verranno rilevate solo le patch di Protezione (nonostante il gruppo di patch contenga patch Non di protezione e di Distribuzione software).

      Dopo l'upgrade alla versione 9.3, il modello di analisi definirà il gruppo di patch come filtro di baseline e tutti gli altri filtri dei modelli di analisi verranno ignorati. Se il gruppo di patch non viene modificato, le patch Non di protezione e di Distribuzione software verranno ora rilevate (e distribuite, se si spunta la casella di controllo **Distribuisci automaticamente le patch dopo l'analisi** al momento di eseguire un'analisi). Il processo di upgrade riconoscerà la discrepanza e rimuoverà le patch Non di protezione e di Distribuzione software dal gruppo di patch.

      Nota: proseguendo, prestare attenzione al fine di gestire correttamente i gruppi di patch, in modo da non aggiungere patch o tipi di patch non necessari o indesiderati.

    - **Gruppi di patch generati in automatico:** una copia di un gruppo di patch esistenti verrà generata automaticamente dal processo di upgrade nel caso in cui vengano rispettate tutte le condizioni seguenti:

- Se si fa riferimento al gruppo di patch all'interno della sezione **Impostazioni filtro patch** di un modello di analisi delle patch e **Analizza selezionati** risulta abilitato, e
- Se un criterio agente o un secondo modello di analisi contenente definizioni dei filtri diverse fa riferimento al gruppo di patch, e
- Se il gruppo di patch deve essere modificato dal processo di upgrade per mantenere la compatibilità (vedere sopra)

In questa situazione, una copia del gruppo di patch verrà generata e quindi modificata come descritto sopra. Il nome del nuovo gruppo di patch sarà ***<nome gruppo di patch> -generated for <nome modello di analisi>**. I modelli di analisi che fanno riferimento al gruppo di patch verranno aggiornati in modo da utilizzare il nuovo nome del gruppo di patch. Il gruppo di patch originale verrà mantenuto, in modo da preservare i riferimenti a esso da parte dei propri criteri agente o di altri modelli di analisi.

È necessario esaminare le modifiche e, se desiderato, rinominare il gruppo di patch con generazione automatica utilizzando un nome più semplice o comprensibile.

Assegnazione di alias alla console

Questa attività è necessaria in caso di applicazione di una o più delle seguenti condizioni:

- Il computer della console è stato assegnato a un nuovo dominio
- Alla console è stato assegnato un nuovo nome comune o indirizzo IP
- Gli agenti sono stati installati manualmente e utilizzano un indirizzo IP per comunicare con la console

In presenza di tali condizioni è necessario utilizzare lo strumento **Editor dell'alias della console** per identificare i nomi o gli indirizzi della console precedente come alias attendibili. In caso contrario, quando un agente effettua il check-in con la console Ivanti Patch for Windows® Servers console o quando un computer senza agente tenta di inviare messaggi di stato di distribuzione patch alla console, non sarà in grado di verificare l'attendibilità del computer contattato.

1. Selezionare **Strumenti > Editor dell'alias della console**.

   Verrà visualizzata la finestra di dialogo **Editor dell'alias della console**. Contiene i nomi e gli indirizzi IP attualmente utilizzati per identificare il computer della console.

2. Digitare i nomi e/o gli indirizzi IP che si desidera utilizzare come alias per il computer della console.

   È possibile specificare gli indirizzi IP utilizzando un formato IPv4 o IPv6.

3. Fare clic su **Aggiorna**.

4. Fare clic su **Continua** o **Annulla**.

   Facendo clic su **Continua**, sia il servizio console sia il programma Ivanti Patch for Windows® Servers verranno riavviati automaticamente; ciò risulta necessario al fine di aggiornare l'elenco di alias della console. Facendo clic su **Annulla**, l'elenco alias della console non verrà aggiornato.

IMPORTANTE! Gli agenti non riconosceranno un nuovo alias fino a quando non avranno effettuato il check-in con la console riavviata. Il check-in deve essere inizializzato da un agente manualmente utilizzando il programma client agente o mediante un check-in pianificato; un comando di check-in emesso dalla console per un agente non aggiornerà il certificato della console.

Sincronizzazione dei server di distribuzione

È necessario aggiornare i server di distribuzione con le patch e/o i motori di analisi e i file XML delle definizioni più recenti contenuti sulla console. Ciò risulta particolarmente importante se i propri agenti utilizzano server di distribuzione per scaricare tali file. I server di distribuzione devono essere sincronizzati con i file aggiornati della console **prima** che gli agenti eseguano il relativo check-in.

Per sincronizzare i propri server di distribuzione:

1. Selezionare **Guida > Aggiorna file** per assicurarsi che la console contenga tutti i file più recenti.
2. Selezionare **Strumenti > Opzioni > Server di distribuzione**.
3. Nella casella **Aggiungi sincronizzazione pianificata** contenuta nel riquadro superiore, selezionare il componente che si desidera sincronizzare.
4. Nel riquadro superiore, selezionare quale server di distribuzione si desidera sincronizzare con la console.
5. Fare clic su **Aggiungi sincronizzazione pianificata**.
6. Specificare quando si desidera che avvenga la sincronizzazione, quindi fare clic su **Salva**.
7. Nel riquadro **Sincronizzazione automatica pianificata**, selezionare la voce di sincronizzazione pianificata.
8. Fare clic su **Esegui adesso**.

Non vi saranno problemi in caso di esecuzione del check-in degli agenti prima del termine della sincronizzazione dei server di distribuzione. Gli agenti verranno aggiornati alla prossima esecuzione di un'attività pianificata o al prossimo aggiornamento dei relativi file binari da parte degli agenti.

Valutazione dell'attivazione della funzione Patch predittiva

Questa funzione è diventata disponibile nella v9.2, pertanto risulta nuova in caso di upgrade dalla v9.1. Consente a Ivanti Patch for Windows® Servers di scaricare automaticamente le patch che con tutta probabilità verranno distribuite nel prossimo futuro. Se si utilizzano server di distribuzione, è possibile sincronizzare Patch predittiva con i propri server di distribuzione in modo che possano ricevere copie delle patch scaricate. L'opzione Patch predittiva si attiva nella scheda **Strumenti > Opzioni > Download** e viene sincronizzata con i propri server di distribuzione spuntando l'opzione **Sincronizza con patch predittiva** sulla finestra di dialogo **Server di distribuzione**. Consultare la sezione Guida per i dettagli completi.

Ristabilimento della sicurezza tra le console di rollup dei dati

Nota: ciò si applica solo in caso di upgrade dalla v9.1 alla v9.3.L'associazione di sicurezza stabilita nella v9.2 continuerà a funzionare nella v9.3.

Se si utilizzano più console ed è stata stabilita una configurazione di rollup dei dati, è necessario ristabilire l'associazione di sicurezza tra la console centrale e ciascuna console remota.

IMPORTANTE! All'inizio del processo di aggiornamento, non avrà luogo alcuna attività di rollup dei dati fino a che non viene aggiornata la console centrale e la console remota e non viene ristabilita l'associazione di sicurezza tra le due console. Pertanto, si consiglia caldamente di aggiornare entrambe le console insieme e nello stesso momento quando si prevede una scarsa attività di rollup dei dati.

Sulla console centrale

1. Aggiornare la console centrale.
2. Selezionare **Strumenti > Opzioni > Rollup dei dati** e verificare che la casella di controllo **Accetta e importa risultati da un mittente di rollup** sia attivata.

Su ciascuna console remota

1. Aggiornare ciascuna console remota.
2. Selezionare **Strumenti > Opzioni > Rollup dei dati**.
3. Verificare i valori Indirizzo IP/Nome host e porta utilizzati dalla console di rollup.
4. Fare clic su **Registra**.

Per ulteriori informazioni sul rollup dei dati, nel sistema della guida online vedere **Amministrazione > Gestione di più console > Configurazione di rollup dei dati**.

Scansione delle proprie macchine virtuali

Nota: ciò si applica solo in caso di upgrade dalla v9.1 alla v9.3.

Se si dispone di macchine virtuali definite in un gruppo di computer o nella scheda **Macchine virtuali ospitate** o **Macchine virtuali workstation**, dopo aver eseguito l'upgrade è necessario inizializzare un'analisi di tali computer dalla pagina home o dall'interno del gruppo di computer. Ciò risulta necessario al fine di ristabilire le identità dei computer con Ivanti Patch for Windows® Servers. Se non si esegue l'analisi, i campi **Server virtuale** e **Percorso** potrebbero non essere visualizzati in Visualizzazione computer e le distribuzioni a tali computer potrebbero non riuscire.

Verifica delle impostazioni utente personalizzate

Le seguenti impostazioni utente personalizzate non vengono preservate durante l'upgrade.

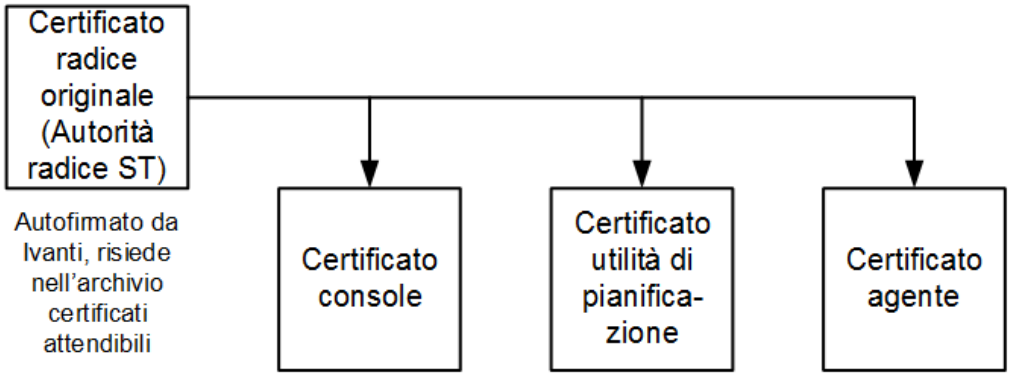
- Scheda Strumenti > Opzioni > Visualizzazione:
  - Elemento recente (giorni)
  - Elementi antecedenti
  - Mostra solo gli elementi creati da me
  - Mostra newsfeed principale
  - Mostra elementi informativi nei risultati di analisi delle patch
  - Mostra service pack in Visualizza -> Patch
- Scheda Strumenti > Opzioni > Notifiche e avvisi:
  - Avvisa prima di pianificare distribuzioni
  - Chiudi Aggiorna file quando terminato
  - Avvisa se la sincronizzazione di Cloud Protect non è abilitata su questa console
  - Avvisa prima di aprire 7 o più bollettini
- Scheda Strumenti > Opzioni > Patch:
  - Pool thread globale

    Questa è una novità di v9.3 e si applica a tutte le funzionalità nel prodotto. Nella v9.2 il pool di thread è stato definito sul modello Analisi asset, ma viene rimosso durante l'upgrade. Il nuovo valore predefinito può risultare diverso da quanto specificato sulla vecchia opzione del pool di thread.
- Scheda Strumenti > Opzioni > Registrazione:
  - Analisi diagnostica delle patch
- Monitoraggio distribuzione:
  - Velocità di aggiornamento
  - Giorni da mostrare
  - Mostra operazioni non riuscite
  - Mostra in corso
  - Mostra operazioni completate correttamente
- Finestra di dialogo Report
  - Ordina per ID IAVA
- Scheda Bollettini dell'hypervisor ESXi
  - Mostra solo i più recenti
- Cronologia eventi
  - Limita risultati ai precedenti (giorni)
- Visualizzazione risultati di ITScripts
  - Risultati dal

È necessario sapere che la v9.3 utilizza una struttura diversa dei certificati

Le posizioni e le relazioni dei certificati varieranno quando si effettua l'upgrade da Shavlik Protect 9.1 o 9.2 a Ivanti Patch for Windows® Servers 9.3. Nella v9.1 e nella v9.2, i certificati delle utilità di pianificazione e degli agenti venivano emessi dal certificato della console. Nella v9.3, il certificato della console, il certificato delle utilità di pianificazione e il certificato degli agenti vengono tutti emessi dal certificato radice autofirmato.

Dopo l'upgrade a Ivanti Patch for Windows® Servers 9.3



- Il certificato console risiede sulla console Patch for Windows ® Servers nell'archivio personale dell'account del computer.
- I certificati dell'utilità di pianificazione risiedono nella directory /ProPatches/ Scheduler.
- Sui computer agente, il certificato della console e il certificato agente risiedono nell'archivio Shavlik Protect Agent dell'account del computer.

Dopo aver completato il processo di upgrade, Ivanti Patch for Windows® Servers 9.3 inizierà il proprio processo dietro le scene per la gestione dei certificati.

- Il certificato della console esistente verrà rimosso dall'archivio Autorità intermedia. Ciò si verifica entro il primo o il secondo giorno di attività, in base alle proprie attività di manutenzione.
- Un nuovo certificato di utilità di pianificazione verrà emesso dal certificato radice ogni volta in cui viene installato Ivanti Scheduler o viene eseguita una distribuzione senza agenti usando Ivanti Scheduler. Il vecchio certificato di utilità di pianificazione (quello emesso originariamente dal certificato della console 9.2) verrà eliminato.
- Un nuovo certificato agente verrà emesso automaticamente dal certificato radice ogni volta in cui viene installato un nuovo agente o quando è necessario emettere nuovamente il certificato di un agente esistente.L'agente memorizzerà il certificato agente nel relativo archivio locale e sposterà il certificato della console dall'archivio Trusted Root sul computer dell'agente all'archivio Personale. Il vecchio certificato agente (quello emesso originariamente dalla console 9.2) verrà eliminato.

Parte della procedura di upgrade degli agenti coinvolge l'attesa del check-in degli agenti, in modo che ricevano un nuovo certificato agente. Tale procedura potrà richiedere alcuni giorni o alcune settimane, in base a una serie di fattori, ma avverrà sempre in background. L'unica attività riservata all'utente potrà prevedere il monitoraggio del registro Cronologia eventi per rilevare l'eventuale presenza di problemi che ne richiedono l'intervento.

In caso di utilizzo di un agente sulla console

Se si dispone di un agente installato sulla console Ivanti Patch for Windows®, reinstallare manualmente tale agente. Ciò dovrebbe avvenire al fine di assicurarsi che l'agente della console venga aggiornato correttamente con il nuovo certificato agente. Non è richiesta alcuna azione per gli agenti installati sui computer di destinazione.

MODIFICHE E MIGLIORAMENTI SIGNIFICATIVI A IVANTI PATCH FOR WINDOWS® SERVERS 9.3

Nel sistema di guida online sono riportati i dettagli completi relativi a ciascuno dei seguenti argomenti:

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

Funzionalità API

La funzionalità API è destinata agli utenti avanzati che dispongono di una conoscenza lavorativa di PowerShell e desiderano eseguire attività oltre quelle disponibili mediante l'interfaccia utente Ivanti Patch for Windows® Servers. È possibile utilizzare la funzionalità API per:

- Interagire con vari sistemi del proprio ambiente
- Eseguire lo script di eventi complessi contenenti dipendenze
- Eseguire azioni in gruppo o input di elenchi di processo da altri sistemi
- Pianificare in modo programmatico le distribuzioni di patch o inizializzare download di patch

Per i dettagli su come utilizzare la funzionalità API, consultare la *Guida di avvio rapido API*.

Percorsi delle cartelle nel riquadro di navigazione

Un'altra nuova funzionalità offre la possibilità di creare una struttura gerarchica per i propri gruppi di computer, modelli di analisi delle patch e modelli di distribuzione patch. Se si creano molti gruppi o modelli, è necessario considerare la possibilità di organizzarli in cartelle logiche. In questo modo sarà possibile individuare e gestire rapidamente i propri gruppi e modelli. Y

È possibile creare tutte le cartelle e le cartelle secondarie necessarie all'interno del riquadro di navigazione. Ad esempio, è possibile scegliere di organizzare i propri gruppi in base ai tipi di computer che contengono, alla posizione, ecc.

Una volta creati, è possibile trascinare e rilasciare gli elementi da una cartella all'altra. È inoltre possibile fare clic con il pulsante destro del mouse su qualsiasi livello della gerarchia ed eseguire un'operazione su tutti gli elementi a o sotto quel livello.

Distribuzioni in fasi

Sono ora disponibili quattro punti pianificabili discreti nel processo di analisi e distribuzione patch. Ciò fornisce un controllo molto superiore sull'intero processo. È possibile:

- Eseguire solo l'analisi
- Eseguire un'analisi e poi suddividere in fasi le patch mancanti sul computer di destinazione a un momento specifico senza installare le patch
- Eseguire un'analisi, suddividere in fasi le patch mancanti e quindi installare le patch al momento desiderato

Manutenzione snapshot pianificate

Questa nuova funzionalità consente di pianificare un'attività singola o ricorrente che rimuoverà le vecchie snapshot delle macchine virtuali dal server. Precedentemente, l'unico modo in cui era possibile rimuovere le vecchie istantanee era in tempo reale, durante un'attività di distribuzione. Per accedere a questa funzionalità, selezionare **Strumenti > Opzioni > Manutenzione snapshot** e aggiungere un'attività.

Capacità di utilizzare una CA di terze parti

È possibile utilizzare un'autorità di certificazione (CA) attendibile dalla propria infrastruttura PKI al fine di emettere un certificato radice di sostituzione per Ivanti Patch for Windows® Servers. Ciò non rappresenta una necessità, ma se si utilizza uno strumento di protezione che considera il certificato radice autofirmato predefinito come un rischio di livello medio, risulta ora disponibile un processo con cui generare un certificato di sostituzione. Per ulteriori informazioni, nel sistema della guida online vedere **Amministrazione > Utilità > Generazione di un certificato da una CA di 3ª parte**.

Gestione attività remote pianificate

Sono state introdotte svariate modifiche alla Gestione attività remote pianificate.

- Ora vi si accede facendo clic con il pulsante destro del mouse su un computer nella Visualizzazione computer o nella Visualizzazione analisi, per poi selezionare **Visualizza attività pianificate**.
- Le informazioni in merito alle attività di alimentazione e di distribuzione patch vengono ora presentate in un formato simile alla Gestione attività console pianificate.
- Ora vengono visualizzate le attività pianificate sul computer remoto usando l'Utilità di pianificazione Ivanti o Microsoft.

Nuove skin

Sulla finestra di dialogo **Opzioni visualizzazione** è ora presente una nuova opzione che consente di specificare il tema cromatico che si desidera utilizzare per l'interfaccia di Ivanti Patch for Windows® Servers. Oltre alla scelta di un colore piacevole alla vista, è inoltre possibile considerare una skin che fornisca molto contrasto, in particolare negli ambienti RDP con una larghezza di banda ridotta.

Nuove capacità di filtro colonne

È ora possibile applicare filtri a una o più intestazioni delle colonne nella griglia. A tal fine, passare il mouse sopra l'intestazione di una colonna, quindi fare clic sull'icona filtro situata nell'angolo in alto a destra. Ad esempio:

Utilizzare il menu filtro per selezionare quali dei valori attualmente contenuti nella colonna debba essere visualizzato.

Metodo di download manuale

Una nuova colonna **Metodo download** indica se una patch possa essere scaricata automaticamente o debba essere scaricata manualmente. Se il valore in questa colonna è **Automatico**, ciò significa che Ivanti Patch for Windows® Servers può scaricare la patch automaticamente. Se il valore è **Acquisisci dal vendor** o qualche altro valore, ciò significa che è necessario scaricare manualmente la patch per poi spostarla nella directory di download patch. Una volta presente, la patch può essere distribuita usando la normale procedura di deployment.Se viene utilizzata la distribuzione automatica e una patch richiede un download manuale, il processo di distribuzione automatica non funzionerà.

Possono essere molti i motivi per i quali non è possibile scaricare automaticamente una patch. Ad esempio, si potrebbe disporre di una patch creata da un programma software proprietario, oppure aver ricevuto patch per un programma che non è più ufficialmente supportato dal vendor.

Informazioni sulla configurazione della distribuzione

La finestra di dialogo **Configurazione distribuzione** mostra informazioni sui requisiti relativi allo spazio su disco in fase di distribuzione delle patch.

Opzioni consolidate di programma

Tutte le opzioni di programma vengono ora consolidate in un'unica posizione. Per visualizzare le opzioni, selezionare **Strumenti > Opzioni**. Il menu **Strumenti > Operazioni** è stato rimosso.

Filtro gruppo di patch

Visualizzazione patch contiene un nuovo filtro gruppo di patch. La casella di controllo **Mostra le patch (sopra) attualmente incluse nel Gruppo di patch selezionato** consente di scegliere se le patch contenute nel gruppo patch selezionato debbano essere visualizzate nell'elenco Visualizzazione patch.

Modifiche all'interfaccia utente di Monitoraggio distribuzione

Monitoraggio distribuzione è stato riprogettato per fornire maggiori dettagli in merito alle attività di distribuzione patch attualmente in corso. Ora è inoltre possibile utilizzare Monitoraggio distribuzione per annullare una distribuzione; il processo di preparazione della distribuzione deve essere completato ma la distribuzione effettuata non può essere iniziata.

Esporta pacchetto di download

Ora è possibile esportare i collegamenti di download per le patch selezionate in un file CSV (Valori separati da virgola). Ciò risulta particolarmente utile per una console che si trova in un ambiente disconnesso. Il file CSV può essere utilizzato da un computer connesso per scaricare le patch, che possono quindi essere copiate nella directory patch della console disconnessa.

Nota: uno script File Downloader PowerShell è disponibile per assistere nel processo di download del file.

Nuovi report IAVA

Sono ora disponibili due nuovi report IAVA: Conformità computer (IAVA) e Non conformità computer (IAVA). Questi due report contengono informazioni aggiuntive richieste dal governo degli Stati Uniti al momento di inviare i dati di report.

Pool thread globale

La Gestione thread si è spostata dal livello di modello al pool nell'intero sistema ed è ora definita sulla finestra di dialogo **Strumenti > Opzioni > Patch**. Per impostazione predefinita, il programma utilizzerà 8 thread per core della CPU, ma è comunque possibile regolare il valore in base alle esigenze. Tale valore singolo specifica il numero totale di thread utilizzabili durante un'analisi patch o una distribuzione, un'analisi asset o un'analisi dello stato di alimentazione.

Capacità di ricerca ampliate

Le capacità di ricerca del prodotto sono state ampliate a più aree. Ora è possibile eseguire ricerche:

- Sulla scheda **Macchine virtuali ospitate** di un gruppo di computer.
- Facendo clic con il pulsante destro del mouse su qualsiasi gruppo di computer nel riquadro di navigazione e selezionando **Cerca gruppi di computer**. Ciò consente di individuare computer e gruppi specifici tra tutti i propri gruppi di computer.
- Utilizzando la nuova casella Cerca nel riquadro centrale di Visualizzazione analisi e Visualizzazione computer.