Appliance Dell DL1300
Guida alla distribuzione

Messaggi di N.B., Attenzione e Avvertenza

N.B.: Un messaggio di N.B. indica informazioni importanti che contribuiscono a migliorare l'utilizzo del computer.

ATTENZIONE: Un messaggio di ATTENZIONE indica un danno potenziale all'hardware o la perdita di dati, e spiega come evitare il problema.

AVVERTENZA: Un messaggio di AVVERTENZA indica un rischio di danni materiali, lesioni personali o morte.

2016 - 05

Rev. A01

Sommario

1

Introduzione al computer Dell DL1300

Il Dell DL1300 combina il backup e la replica in un prodotto di protezione dei dati unificato. Fornisce il ripristino affidabile dei dati delle applicazioni dai processi di backup per proteggere le macchine virtuali e quelle fisiche. L'appliance è in grado di gestire fino a terabyte di dati con deduplicazione globale integrata, compressione, crittografia e funzionalità di replica a una specifica infrastruttura di cloud privata o pubblica. Le applicazioni e i dati dei server possono essere ripristinati in pochi minuti per la conservazione dei dati e a scopi di conformità.

Il DL1300 supporta gli ambienti multi-hypervisor su cloud pubblici e privati di VMware vSphere, Oracle VirtualBox e Microsoft Hyper-V.

Tecnologie del core Dell DL1300

L'appliance combina le seguenti tecnologie:

- Live Recovery
- Universal Recovery
- True Global Deduplication
- Crittografia

Live Recovery

Live Recovery è una tecnologia immediata di ripristino per le macchine virtuali o i server. Essa dà accesso quasi continuo a volumi di dati su server virtuali o fisici.

La tecnologia di replica e backup di DL1300 registra copie istantanee simultanee di più macchine virtuali o server, garantendo dati quasi istantanei e protezione del sistema. È possibile riprendere l'uso del server montando il punto di ripristino senza la necessità di attendere un ripristino completo allo stato di archiviazione di produzione.

Universal Recovery

Universal Recovery garantisce una flessibilità illimitata di ripristino delle macchine. È possibile ripristinare i backup da sistemi fisici in macchine virtuali, da macchine virtuali in macchine virtuali, da macchine virtuali in sistemi fisici o da sistemi fisici in sistemi fisici ed effettuare ripristini bare metal in un hardware diverso.

La tecnologia Universal Recovery inoltre accelera spostamenti multipiattaforma tra macchine virtuali. Ad esempio, il passaggio da VMware ad Hyper-V o da Hyper-V a VMware. Si basa su ripristini a livello di applicazione, a livello di elemento e a livello di oggetto (singoli file, cartelle, e-mail, elementi di calendario, database e applicazioni).

True Global Deduplication

True Global Deduplication elimina i dati ridondanti o duplicati eseguendo i backup incrementali a livello di blocco dei computer.

Il layout tipico del disco di un server è composto dal sistema operativo, dalle applicazioni e dai dati. Nella maggior parte degli ambienti, gli amministratori spesso utilizzano una versione comune del sistema operativo del server e del desktop in sistemi multipli per la distribuzione e la gestione efficace. Quando il backup viene eseguito a livello di blocco tra più computer, fornisce una vista più granulare di che cosa è presente nel backup e di cosa non è incluso, a prescindere dall'origine. Questi dati includono il sistema operativo, le applicazioni e i dati dell'applicazione all'interno dell'ambiente.

Figura 1. Diagramma di True Global Deduplication

Crittografia

Il modello DL1300 offre la funzione di crittografia per la protezione dei backup e dei dati memorizzati in caso di accesso e utilizzo non autorizzati, garantendo la privacy dei dati. È possibile accedere ai dati e decrittografarli utilizzando la chiave di crittografia. La crittografia viene eseguita in linea sui dati della copia istantanea, a una velocità di linea senza influire sulle prestazioni.

Funzioni di protezione dei dati di Dell DL1300

Core di Dell DL1300

Il Core è il componente centrale dell'architettura di distribuzione di DL1300. Il Core archivia e gestisce i backup del computer e offre servizi per il backup, il ripristino, la conservazione, la replica, l'archiviazione e la gestione. Il Core è una rete autonoma, un computer indirizzabile che esegue una versione a 64 bit dei sistemi operativi di Microsoft Windows Server 2012 R2 Foundation e Standard. Il dispositivo esegue la compressione, crittografia e deduplicazione in linea dei dati ricevuti dall'agente. Il nucleo archivia quindi i backup di istantanee nel repository, che risiede nel dispositivo. I Core sono combinati per la replica.

Il repository risiede nella memoria interna al Core. Il Core viene gestito mediante l'accesso al seguente URL da un browser Web in cui è abilitato JavaScript:**https://CORENAME:8006/apprecovery/admin**.

Smart Agent Dell DL1300

La funzione Smart Agent è installata sul computer protetto dal core. La funzione Smart Agent tiene traccia dei blocchi modificati sul volume del disco, quindi cattura un'immagine dei blocchi modificati in un intervallo predefinito di protezione. L'approccio permanente delle istantanee incrementali a livello di blocco impedisce la creazione di una copia ripetuta degli stessi dati dal computer protetto al core.

Dopo la configurazione dell'Agente, viene utilizzata una tecnologia intelligente per tenere traccia dei blocchi modificati sui volumi protetti del disco. Quando l'istantanea è pronta per l'invio, è rapidamente trasferita al core utilizzando connessioni intelligenti a thread multipli, connessioni basate su socket.

Processo di copia istantanea

Il processo di protezione di DL1300 inizia quando un'immagine di base viene trasferita da una macchina protetta al Core. In questa fase, una copia completa della macchina viene trasportata su tutta la rete in condizioni di funzionamento normale, seguita da copie istantanee incrementali continue. L'agente DL1300 per Windows utilizza Microsoft Volume Shadow Copy Service (VSS) per bloccare e interrompere il trasferimento dei dati dell'applicazione sul disco per acquisire un backup coerente con il file-system e con l'applicazione. Quando viene creata una copia istantanea, il VSS writer sul server di destinazione impedisce che i contenuti vengano scritti sul disco. Durante il processo di arresto della scrittura dei contenuti sul disco, tutte le operazioni di I/O del disco vengono messe in coda e riprese solo dopo che la copia istantanea è stata completata, mentre le operazioni in corso saranno completate e tutti i file aperti verranno chiusi. Il processo di creazione di una copia shadow non influisce significativamente sulle prestazioni del sistema di produzione.

Il modello DL1300 utilizza Microsoft VSS perché ha un supporto integrato per tutte le tecnologie interne Windows come NTFS, Registry, Active Directory, per scaricare i dati su disco prima della copia istantanea. Inoltre, altre applicazioni aziendali, come ad esempio Microsoft Exchange e SQL, utilizzano il plug-in VSS Writer per ottenere una notifica quando una copia istantanea viene preparata e quando devono scaricare su disco le pagine del database utilizzate per portare il database a uno stato transazionale coerente. I dati catturati vengono rapidamente trasferiti e archiviati sul Core.

Replica - sito di ripristino in caso di calamità o provider di servizi

La replica è il processo di copia di punti di ripristino da un core di AppAssure e la loro trasmissione a un altro core AppAssure in un luogo diverso per il ripristino in caso di calamità. Il processo richiede la presenza di una relazione origine-destinazione accoppiata tra due o più core.

Il core di origine copia i punti di ripristino di macchine virtuali protette selezionate, quindi in modo asincrono e senza soluzione di continuità trasmette i dati incrementali delle copie istantanee al core di destinazione presso un sito remoto per il ripristino in caso di calamità. È possibile configurare la replica in uscita verso un data center di proprietà dell'azienda o verso un sito remoto per il ripristino in caso di calamità (cioè un core di destinazione "autogestito"). Oppure, è possibile configurare la replica in uscita verso un provider di servizi gestito da terze parti (MSP) o verso un provider di servizi cloud che ospita il backup off-site e offre servizi di ripristino in caso di calamità. Quando si esegue la replica verso un core di destinazione di terze parti, è possibile utilizzare flussi di lavoro incorporati che consentono di richiedere connessioni e ricevere notifiche di feedback automatiche.

La replica è gestita a livello di singola macchina protetta. Qualsiasi macchina (o tutte le macchine) protetta o replicata su un core di origine può essere configurata per la replica su un core di destinazione.

La replica è in grado di ottimizzarsi automaticamente in virtù di un algoritmo Read-Match-Write (RMW) univoco che è strettamente associato alla deduplicazione. Con le soluzioni di replica RMW, il servizio di replica dall'origine alla destinazione risponde alle chiavi prima di trasferire i dati dopodiché esegue la replica solo dei dati compressi, crittografati e deduplicati sulla WAN, con una conseguente riduzione pari a 10 volte dei requisiti di larghezza di banda.

La replica inizia con il seeding: il trasferimento iniziale di immagini deduplicate di base e di copie istantanee incrementali delle macchine protette, che può aggiungere fino a centinaia o migliaia di gigabyte di dati. La replica iniziale può essere sottoposta a seeding verso il core di destinazione utilizzando un supporto esterno. Questo in genere si rivela utile in caso di set di dati di grandi dimensioni o siti con collegamenti lenti. I dati all'interno dell'archivio del seeding sono compressi, crittografati e deduplicati. Se la dimensione totale dell'archivio è superiore allo spazio disponibile sul supporto rimovibile, l'archivio può estendersi su più dispositivi in funzione dello spazio disponibile sul supporto. Durante il processo di seeding, i punti di ripristino incrementali vengono replicati sul sito di destinazione. Dopo che il core di destinazione consuma l'archivio del seeding, i punti di ripristino incrementali appena replicati si sincronizzano automaticamente.

Ripristino

Le operazioni di ripristino possono essere eseguite nel sito locale o nel sito remoto replicato. Dopo che la distribuzione è in stato stazionario con protezione locale e replica opzionale, il Core DL1300 consente di eseguire le operazioni di ripristino utilizzando Verified Recovery, Universal Recovery o Live Recovery.

Recovery-as-a-Service (Ripristino come servizio)

I provider di servizi gestiti (Managed Service Providers, MSP) possono sfruttare pienamente DL1300 come piattaforma per fornire il Ripristino come servizio (RaaS). RaaS facilita il ripristino completo nel cloud tramite la replica dei server fisici e virtuali dei clienti. I cloud del provider di servizi vengono utilizzati come macchine virtuali per supportare i test di ripristino o le effettive operazioni di ripristino. I clienti che desiderano eseguire le operazioni di ripristino nel cloud possono configurare la replica sui loro computer protetti sui core locali su un provider di servizi AppAssure. In caso di emergenza, gli MSP possono immediatamente accelerare fino al raggiungimento della velocità operativa le macchine virtuali per il cliente.

Il sistema DL1300 non è multi-tenant. Gli MSP possono utilizzare DL1300 in più siti e creare un ambiente multi-tenant per le loro necessità.

Virtualizzazione e cloud

Il Core DL1300 è pronto per il cloud, cosa che consente di sfruttare la capacità di elaborazione del cloud per il ripristino e l'archiviazione.

DL1300 può esportare qualsiasi computer protetto o replicato in versioni concesse in licenza di VMware o Hyper-V. Con esportazioni continue, la macchina virtuale viene aggiornata in modo incrementale dopo ogni istantanea. Gli aggiornamenti incrementali sono rapidi e forniscono cloni di standby che sono pronti per essere attivati, con un semplice clic. Le esportazioni supportate dalla macchina virtuale sono le seguenti:

- Workstation o server VMware in una cartella
- Esportazione diretta in un host ESXi vSphere o VMware
- Esportazione in Oracle VirtualBox
- Microsoft Hyper-V Server su Windows Server 2008 (x64)

- Microsoft Hyper-V Server su Windows Server 2008 R2
- Microsoft Hyper-V Server su Windows Server 2012 R2

Ora è possibile archiviare i dati del repository sul cloud utilizzando piattaforme quali Microsoft Azure, Amazon S3, Rackspace Cloud Block Storage o altri servizi cloud basati su OpenStack.

Architettura di distribuzione di Dell DL1300

L'architettura di distribuzione di DL1300 è costituita da componenti locali e remoti. I componenti remoti possono essere opzionali per gli ambienti che non richiedono lo sfruttamento di un sito di ripristino in caso di calamità o di un provider di servizi gestito per il ripristino fuori sede. Una distribuzione locale di base è costituita da un server di backup denominato il Core e una o più macchine protette note come gli agenti. Il componente off-site viene attivato tramite replica che fornisce funzionalità complete di ripristino nel sito di ripristino in caso di calamità. Il Core DL1300 utilizza immagini di base e copie istantanee incrementali per la compilazione di punti di ripristino degli agenti protetti.

Inoltre, DL1300 riconosce le applicazioni, perché è in grado di rilevare la presenza di Microsoft Exchange e SQL e dei rispettivi database e file di log. I backup vengono eseguiti utilizzando copie istantanee a livello di blocco con riconoscimento delle applicazioni. DL1300 esegue la troncatura dei log del server di Microsoft Exchange protetto.

Il diagramma seguente illustra una semplice distribuzione di DL1300. Gli agenti DL1300 vengono installati su macchine, come ad esempio un file server, server di posta elettronica, database server, oppure le macchine virtuali vengono collegate a e sono protetti da un singolo Core DL1300, che è composto da un archivio centrale. Il portale delle licenze software Dell gestisce le sottoscrizioni delle licenze, i gruppi e gli utenti per gli agenti e i core nel proprio ambiente. Il portale delle licenze consente agli utenti di effettuare il login, attivare gli account, eseguire il download del software e distribuire gli agenti e i core per ciascuna licenza nel proprio ambiente.

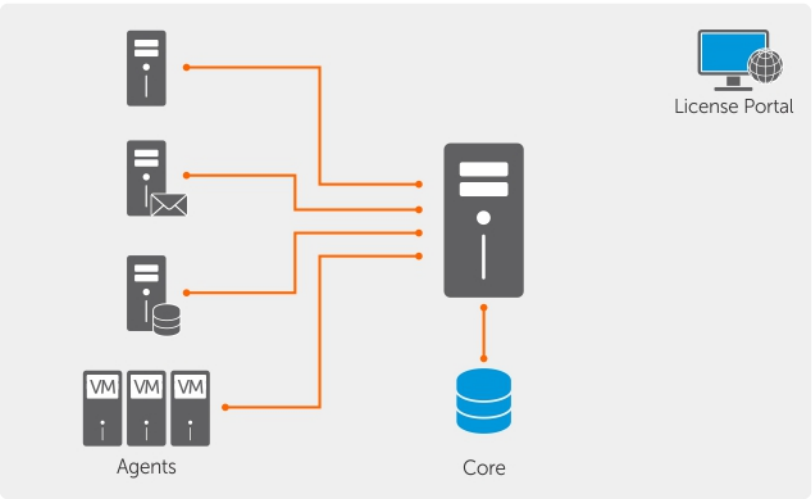

Figura 2. Architettura di distribuzione di Dell DL1300

È inoltre possibile distribuire più core DL1300 come mostrato nel diagramma seguente. Una console centrale gestisce più core.

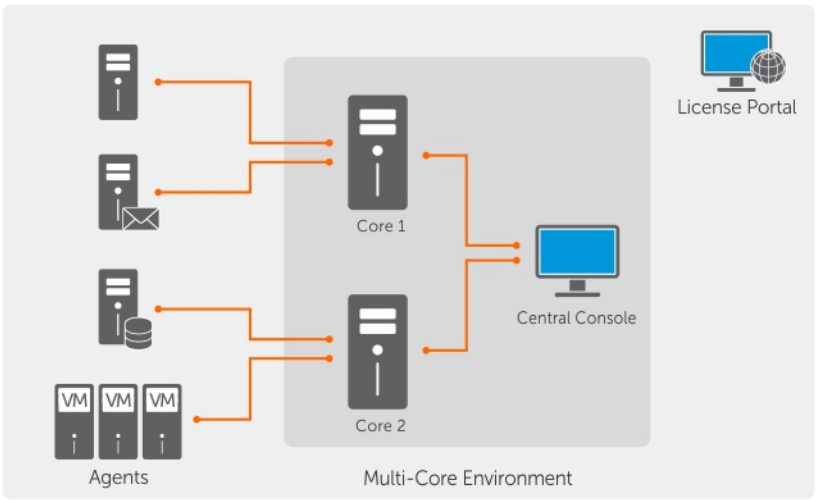

Figura 3. Architettura di distribuzione di più core DL1300

Altre informazioni utili

N.B.: Per tutti i documenti di Dell OpenManage, andare all'indirizzo **Dell.com/openmanagemanuals**.

N.B.: Verificare sempre la disponibilità di aggiornamenti all'indirizzo **Dell.com/support/manuals** e leggere prima gli aggiornamenti in quanto spesso sostituiscono le informazioni in altri documenti.

N.B.: Per qualsiasi documentazione relativa a Dell OpenManage Server Administrator, vedere **Dell.com/openmanage/manuals**.

La documentazione del prodotto include:

Guida introduttiva	Fornisce una panoramica di impostazione del sistema e le specifiche tecniche. Il presente documento è fornito con il sistema.
Presentazione delle informazioni di sistema	Fornisce informazioni su come configurare l'hardware e installare il software sul dispositivo.
Manuale del proprietario	Fornisce informazioni sulle funzioni del sistema e descrive le modalità per risolvere i problemi del sistema e installare o sostituire i componenti di sistema.
Guida alla distribuzione	Fornisce informazioni sulla distribuzione dell'hardware e la distribuzione iniziale dell'appliance.
Guida dell'utente	Fornisce informazioni sulla configurazione e la gestione del sistema.
Note sulla versione	Fornisce informazioni sui prodotti e una serie di informazioni aggiuntive sull'appliance DL1300
Guida all'interoperabilità	Fornisce informazioni su software e hardware supportati sull'appliance, nonché considerazioni di utilizzo, suggerimenti e regole.
Guida dell'utente di OpenManage	Fornisce informazioni sull'utilizzo di Dell OpenManage Server Administrator per gestire il sistema.

Server
Administrator

2

Installazione di Dell DL1300

Introduzione

L'appliance per backup su disco DL consente:

- Backup più veloci, nonché scenari di ripristino più rapidi rispetto a convenzionali dispositivi su nastro e metodologie di backup
- Funzionalità di deduplicazione opzionale
- Protezione continua dei dati per l'implementazione di data center e server per uffici remoti
- Ricerca rapida e semplice esperienza di distribuzione che riduce il tempo necessario per iniziare a proteggere i dati critici

Configurazioni disponibili

L'appliance DL viene fornita nelle seguenti configurazioni:

Tabella 1. Configurazioni disponibili

Capacità	Configurazione dell'hardware
2 TB	Quattro HDD da 4 TB con spazio di archiviazione da 2 TB utilizzabile
3 TB con 2 VM	Quattro HDD da 4 TB con spazio di archiviazione da 3 TB utilizzabile e spazio per le VM regolabile
4 TB con 2 VM	Quattro HDD da 4 TB con spazio di archiviazione da 4 TB utilizzabile e spazio per le VM regolabile

Ogni configurazione include il seguente hardware e software:

- Sistema Dell DL1300
- Controller RAID Dell PowerEdge (PERC)
- Sotfware Dell AppAssure

Panoramica di installazione

L'installazione del modello DL1300 prevede l'installazione dei servizi del core AppAssure e dell'agente AppAssure 5 sui sistemi che devono essere protetti. Se sono impostati core aggiuntivi allora deve essere installata la console di gestione centrale dei servizi AppAssure 5.
Per installare DL1300 seguire questi passaggi:

1. Procurarsi la chiave di licenza permanente. Dalla Core Console è possibile gestire direttamente le licenze DL1300, modificare la chiave di licenza e contattare il server di licenza. Nella Core Console è inoltre possibile accedere al portale licenze Dell AppAssure dalla pagina Licenze.

N.B.: L'appliance è configurata e viene fornita con una licenza temporanea del software di 30 giorni.

2. Verifica dei prerequisiti di installazione.
3. Impostazione dell'hardware
4. Impostazione del software iniziale (procedura guidata di configurazione dell'appliance AppAssure).
5. Installazione della Core Management Console.

Prerequisiti di installazione

Requisiti di rete

L'appliance richiede il seguente ambiente di rete:

- rete attiva con cavi e connessioni Ethernet disponibili
- un indirizzo IP statico e l'indirizzo IP del server DNS, se non forniti con il Dynamic Host Configuration Protocol (DHCP)
- nome utente e password con privilegi di amministratore

Infrastruttura di rete consigliata

Per ottimizzare le prestazioni Dell consiglia alle aziende di utilizzare gli switch di 1 GbE o superiori insieme alla AppAssure.

Installazione dell'hardware

L'appliance viene fornita con un singolo sistema DL1300. Prima di impostare l'appliance hardware, consultare la *Guida introduttiva* per il sistema fornita con il dispositivo. Disimballare e impostare l'appliance hardware DL1300.

N.B.: Il software è preinstallato sull'appliance. Qualsiasi supporto incluso con il sistema deve essere utilizzato solo in caso di ripristino del sistema.

Per impostare l'hardware DL1300:

1. montare su rack e cablare il sistema DL1300.
2. Accendere il sistema DL1300.

Installazione dell'appliance DL1300 su rack

Se il sistema include un kit di guide, individuare le *Istruzioni di installazione su rack* fornite con il kit per rack. Seguire le istruzioni per installare le guide e il modello DL1300 nel rack.

Utilizzo del sistema senza rack

È possibile utilizzare il sistema senza il server rack. Quando si utilizza il sistema senza rack, accertarsi di seguire queste linee guida:

- Il sistema deve essere posizionato su una superficie stabile e fissa in grado di supportare l'intero sistema.

  N.B.: Il sistema non deve essere collocato in posizione verticale.

- Non posizionare il sistema sul pavimento.
- Non posizionare nulla sulla parte superiore del sistema. Il pannello superiore potrebbe deflettere sotto il peso e causare danni al sistema.
- Garantire spazio sufficiente attorno al sistema per un'adeguata ventilazione.
- Accertarsi che il sistema sia installato nelle condizioni di temperatura consigliate come indicato nella sezione Specifiche tecniche - ambientali del Manuale del proprietario dell'appliance *Dell DL1300* all'indirizzo **Dell.com/support/home**.

ATTENZIONE: La mancata osservanza di queste linee guida potrebbe causare danni al sistema o danno fisico.

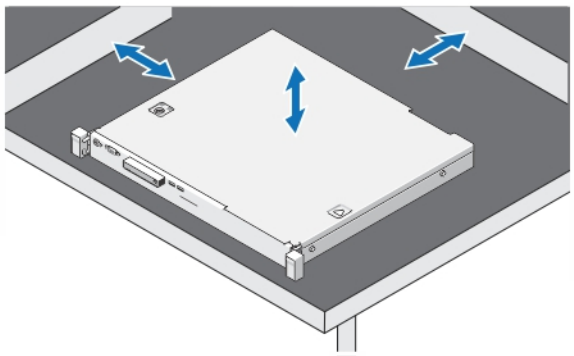

Figura 4. Utilizzo del sistema senza rack

Cablaggio dell'appliance

Individuare la *Guida introduttiva dell'appliance Dell DL1300* fornita con l'appliance e seguire le istruzioni per collegare la tastiera, il mouse, il monitor, l'alimentazione e i cavi di rete per il sistema DL1300.

Collegamento del braccio di gestione dei cavi (opzionale)

Se l'appliance include un braccio di gestione dei cavi (CMA), individuare le *istruzioni di installazione* del CMA fornite con il kit CMA e seguire le istruzioni per installare il CMA.

Accensione dell'appliance DL1300

Dopo il collegamento dell'appliance, accendere il sistema.

N.B.: Si consiglia di collegare il dispositivo a un alimentatore di alimentazione ininterrotta (UPS) per massimi livelli di affidabilità e disponibilità. Per ulteriori informazioni, vedere la sezione *Guida introduttiva a Dell DL1300* all'indirizzo **Dell.com/support/manuals**.

Configurazione iniziale del software

Quando si accende il dispositivo per la prima volta e si modifica la password di sistema, la **Configurazione guidata dell'Appliance AppAssure** si avvia automaticamente.

1. Una volta acceso il sistema, scegliere la lingua del sistema operativo dalle opzioni della lingua di Windows.

Il Contratto di licenza con l'utente finale Microsoft (EULA) viene visualizzato nella pagina **Impostazioni**.

2. Per accettare l'EULA, fare clic sul pulsante **Accetto**.
   Viene visualizzata una pagina per modificare la password dell'amministratore.
3. Fare clic su **OK** sul messaggio che richiede all'utente di modificare la password dell'amministratore.
4. Immettere e confermare la nuova password.
   Un messaggio chiede conferma che la password è stata modificata.
5. Fare clic su **OK**.
6. Dalla schermata **Dell readme.htm**, scorrere verso il basso e fare clic su **Prosegui**.
   Dopo aver immesso la password, viene visualizzata la schermata **Premere Ctrl+Alt+Canc per accedere**.
7. Accedere utilizzando la password dell'amministratore modificata.
   Viene visualizzata la schermata **Selezionare la lingua per l'appliance AppAssure**
8. Selezionare la lingua per il vostro dispositivo dall'elenco delle lingue supportate.
   Viene visualizzata la schermata **EULA**.
9. Per accettare l'EULA, fare clic sul pulsante **Accetta EULA**.

   N.B.: È possibile eseguire la Configurazione guidata dell'appliance AppAssure ulteriormente solo se si accetta l'EULA. In caso contrario, il dispositivo verrà disconnesso immediatamente.

Viene visualizzata la schermata di benvenuto della **Configurazione guidata dell'appliance AppAssure**.

N.B.: La **Configurazione guidata dell'appliance AppAssure** può richiedere fino a 30 secondi per essere visualizzata sulla console del sistema.

Procedura guidata di configurazione dell'appliance AppAssure

ATTENZIONE: Accertarsi di aver completato tutti i passaggi della procedura guidata di configurazione dell'appliance AppAssure prima di eseguire qualsiasi altra attività o modificare le impostazioni sull'appliance. Non apportare eventuali modifiche tramite il Pannello di controllo, utilizzare Microsoft Windows Update, aggiornare il software AppAssure o installare le licenze, fino a quando la procedura guidata è stata completata. Il servizio Windows Update è temporaneamente disabilitato durante il processo di configurazione. L'uscita dalla configurazione guidata dell'appliance AppAssure prima del suo completamento può provocare errori al funzionamento del sistema.

La **Procedura guidata di configurazione dell'appliance AppAssure** guida l'utente attraverso i seguenti passaggi per configurare il software sull'appliance:

- Configurazione dell'interfaccia di rete
- Configurazione delle impostazioni nome host e dominio
- Configurazione delle impostazioni SNMP

Al completamento dell'installazione utilizzando la procedura guidata, la Core Console si avvia automaticamente.

Configurazione dell'interfaccia di rete

Per configurare le interfacce di rete disponibili:

1. nella schermata **Procedura guidata di configurazione iniziale dell'appliance AppAssure**, fare clic su **Avanti**.

La pagina delle **Interfacce di rete** mostra le interfacce di rete disponibili connesse.

2. Selezionare le interfacce di rete che si desidera configurare.

   N.B.: La **Procedura guidata di configurazione dell'appliance AppAssure** configura interfacce di rete come singole porte (non raggruppate). Per migliorare le prestazioni di acquisizione, è possibile creare un canale di acquisizione più grande raggruppando le NIC. Tuttavia, questa operazione deve essere effettuata dopo la configurazione iniziale dell'appliance.

3. Se necessario, collegare altre interfacce di rete e fare clic su **Aggiorna**.

   Le interfacce di rete aggiuntive connesse vengono visualizzate.

4. Fare clic su **Avanti**.

   La pagina **Configura interfaccia di rete selezionata** viene visualizzata.

5. Selezionare il protocollo Internet appropriato per l'interfaccia selezionata.

   È possibile scegliere **IPv4** o **IPv6**.

   I dettagli della rete sono visualizzati a seconda del protocollo Internet che si seleziona.

6. Per assegnare i dettagli del protocollo Internet, effettuare una delle operazioni riportate di seguito:
   - per assegnare automaticamente i dettagli del protocollo Internet selezionato, selezionare **Ottieni automaticamente un indirizzo IPV4**.
   - Per assegnare la connessione di rete manualmente, selezionare **Usa il seguente indirizzo IPv4** e immettere i seguenti dettagli:
     - **Indirizzo IPv4** o **Indirizzo IPv6**
     - **Subnet mask** per IPv4 e **Lunghezza prefisso subnet** per IPv6
     - **Gateway predefinito**
7. Per assegnare i dettagli del server DNS, effettuare una delle operazioni riportate di seguito:
   - per assegnare l'indirizzo del server DNS automaticamente, selezionare **Ottieni indirizzo server DNS automaticamente**.
   - Per assegnare il server DNS manualmente, selezionare **Usa il seguente indirizzo server DNS** e immettere i seguenti dettagli:
     - **Server DNS preferito**
     - **Server DNS alternativo**
8. Fare clic su **Avanti**.

   Viene visualizzata la pagina **Configurazione impostazioni nome host e dominio**.

Per informazioni sui team NIC, vedere Teaming delle schede di rete.

Configurazione delle impostazioni nome host e dominio

È necessario assegnare un nome host per l'appliance. Si consiglia di cambiare il nome dell'host prima di avviare i backup. Per impostazione predefinita, il nome host è il nome di sistema che il sistema operativo assegna.

N.B.: Se si decide di cambiare il nome host, si consiglia di farlo in questa fase. La modifica del nome host dopo aver completato la **Procedura guidata di configurazione dell'appliance AppAssure** richiede diverse operazioni.

Per configurare le impostazioni nome host e dominio:

1. nella pagina **Configurazione impostazioni nome host e dominio**, nella casella di testo **Nuovo nome host** digitare un nome host appropriato.
2. Se non si desidera connettere l'appliance a un dominio, selezionare **No** in **Si desidera che l'appliance si connetta a un dominio?**

N.B.: Se il modello DL1300 è installato con Microsoft Windows Server 2012 Foundation Edition, l'opzione di connettersi a un dominio verrà disattivata.

Per impostazione predefinita è selezionato **Sì**.

3. Se si desidera connettere l'appliance a un dominio, immettere le seguenti informazioni:
   - **Nome dominio**
   - **Nome utente del dominio**

     N.B.: L'utente del dominio deve disporre dei diritti amministrativi locali.
   - **Password utente del dominio**
4. Fare clic su **Avanti**.

   N.B.: La modifica del nome dell'host o del dominio richiede il riavvio della macchina. Dopo il riavvio, la **Procedura guidata di configurazione dell'appliance AppAssure** viene avviata automaticamente. Se l'appliance è collegata a un dominio, dopo il riavvio del computer, è necessario effettuare il login come utente di dominio con privilegi di amministratore per l'appliance.

   Viene visualizzata la pagina **Configura impostazioni SNMP**.

Configurazione delle impostazioni SNMP

SNMP (Simple Network Management Protocol) è un protocollo molto diffuso per la gestione di rete che consente di utilizzare funzionalità di gestione compatibili con SNMP, come per esempio il rilevamento di dispositivi, il monitoraggio e la creazione di eventi. SNMP offre funzionalità di gestione della rete del protocollo TCP/IP.

Per configurare gli avvisi SNMP per l'applicazione:

1. nella pagina **Configurazione delle impostazioni SNMP**, selezionare **Configura SNMP su questa appliance**.

   N.B.: Deselezionare **Configura SNMP su questa appliance** se non si desidera configurare i dettagli e gli avvisi SNMP sull'appliance e andare al passaggio 6.
2. In **Comunità**, immettere uno o più nomi di comunità SNMP.

   Utilizzare le virgole per separare più nomi di comunità.
3. In **Accetta i pacchetti SNMP da questo host**, immettere i nomi degli host con cui l'appliance può comunicare.

   Separare i nomi degli host con virgole, oppure lasciare il campo vuoto per consentire la comunicazione con tutti gli host.
4. Per configurare gli avvisi SNMP, immettere il **Nome della comunità** e le **Destinazioni trap** per gli avvisi SNMP e fare clic su **Aggiungi**.

   Ripetere questo passaggio per aggiungere più indirizzi SNMP.
5. Per rimuovere un indirizzo SNMP configurato, in **Indirizzi SNMP configurati**, selezionare l'indirizzo SNMP appropriato e fare clic su **Rimuovi**.
6. Fare clic su **Avanti**.

   Viene visualizzata la pagina di **Ringraziamento**.
7. Per completare la configurazione, fare clic su **Avanti**.
8. Fare clic su **Esci** nella pagina **Configurazione completata**.

   La Core Console si apre nel browser Web predefinito.

Ripristino e Update Utility

Il Recovery e Update Utility (RUU) è una soluzione all-in-one installer (ad unico installatore) per recuperare e aggiornare il software DL Appliance (DL1000, DL1300, DL4000 e DL4300). Comprende il software AppAssure Core e i component per appliance specifiche.

RUU consiste di versioni aggiornate di Ruoli e funzionalità del server di Windows ASP .NET MVC3, LSI provider, DL Applications, OpenManage Server Administrator e AppAssure Core Software. Inoltre, il Ripristino e Update Utility aggiorna il contenuto del Rapid Appliance Self Recovery (RASR) .

Per scaricare la versione più recente del RUU:

1. Andare al License Portal (portale licenze) sotto la sezione Downloads e scaricare il programma di installazione di RUU o andare al sito**support.dell.com**.
2. Eseguire il programma di installazione di RUU.

   N.B.: Il sistema potrebbe riavviarsi durante il processo di aggiornamento di RUU.

N.B.: Se si utilizza il RUU n. 184 e l'appliance DL dispone di una versione AppAssure Core inferiore (vecchia) rispetto a 5.4.3.106 , viene aggiornato il nucleo di AppAssure Core 5.4.3.106 .

N.B.: Se si esegue l'aggiornamento di RUU n. 184, si vedranno alcune incoerenze nelle esecuzioni future di backup di Windowa già pianificate (tramite RASR) o potrebbero non riuscire a creare una policy di backup Windows. Queste incoerenze si verificano a causa dello spazio limitato della posizione dello storage di backup di Windows.

Altre cause possibili di questi errori includono:

1. Aggiornamento per il Ripristino rapido, soprattutto se viene utilizzata oltre il minimo la cache di deduplicazione.
2. Installazione o aggiornamento del software (ad esempio, Outlook) nell'appliance.
3. Installazione degli aggiornamenti di Windows.
4. Aggiunta/ingrandimento file di dati (come la cache di deduplicazione).
5. Combinazioni dei precedenti.

Rapid Appliance Self Recovery

Rapid Appliance Self Recovery (RASR) è un processo di ripristino bare metal in cui le unità del sistema operativo e le unità dati sono utilizzate per ripristinare le impostazioni di fabbrica.

Creazione della chiave USB RASR

Per creare una chiave USB RASR:

1. passare alla scheda **Appliance**.
2. Utilizzando il pannello di navigazione a sinistra, selezionare **Appliance** → **Backup**.
   Viene visualizzata la finestra **Crea unità USB RASR**.

   N.B.: Inserire una chiave USB da 16 GB o più grande prima di tentare di creare la chiave RASR.
3. Dopo aver inserito una chiave USB da 16 GB o più grande, fare clic su **Crea unità USB RASR ora**.
   Viene visualizzato un messaggio **Controllo dei prerequisiti**.

Dopo che i prerequisiti vengono controllati la finestra **Crea unità USB RASR** mostra la dimensione minima necessaria per creare l'unità USB e l'**Elenco dei possibili percorsi di destinazione**.

4. Selezionare la destinazione e fare clic su **Crea**.
   Viene visualizzata una finestra di dialogo di avviso.
5. Fare clic su **Sì**.
   La chiave di unità USB RASR è stata creata.
6. N.B.: Assicurarsi di utilizzare la funzione Windows di espulsione dell'unità per preparare la chiave USB alla rimozione. In caso contrario, il contenuto della chiave USB può essere danneggiato e la chiave USB non funzionerà come previsto.

   Rimuovere la chiave, etichettarla e conservarla per un utilizzo futuro.

Esecuzione di RASR

N.B.: Dell consiglia di creare una chiave USB RASR dopo aver configurato l'appliance. Per creare una chiave USB RASR, fare riferimento alla sezione Creazione della chiave USB RASR.

Queste operazioni consentono di eseguire il reset ai valori di fabbrica.

.

Per eseguire il RASR:

1. inserire la chiave USB RASR creata.
2. Riavviare l'appliance e selezionare **Boot Manager (F11)**.
3. Nel **Menu principale di Boot Manager**, selezionare **Menu di avvio one-shot del BIOS**.
4. Nel **Menu di avvio di Boot Manager** , selezionare l'unità USB collegata.
5. Selezionare il layout della tastiera.
6. Fare clic su **Risoluzione dei problemi → Rapid Appliance Self Recovery**.
7. Selezionare il sistema operativo (SO) di destinazione.
   RASR viene avviato e viene visualizzata la schermata di introduzione.
8. Fare clic su **Avanti**.
   Viene visualizzata la schermata di controllo dei **Prerequisiti**.

   N.B.: Accertarsi che tutti i prerequisiti hardware e gli altri prerequisiti vengono controllati prima di procedere con il RASR.
9. Fare clic su **Avanti**.
   Nella schermata **Selezione modalità di ripristino** vengono visualizzate tre opzioni:
   - **Ripristina sistema**
   - **Procedura guidata di ripristino Windows**
   - **Ripristina impostazioni di fabbrica**
10. Selezionare l'opzione **Ripristina impostazioni di fabbrica**.
    Questa opzione ripristina il disco del sistema operativo dall'immagine di fabbrica.
11. Fare clic su **Avanti**.
    Il seguente messaggio di avviso viene visualizzato in una finestra di dialogo: `This operation will recover the operating system. All OS disk data will be overwritten.`
12. Fare clic su **Sì**.
    Si avvia il ripristino del disco del sistema operativo ai valori di fabbrica.
13. Dopo il completamento del processo di ripristino delle impostazioni di fabbrica, nella schermata **RASR completato**, fare clic su **Fine**.

3

Configurazione di Dell DL1300

Panoramica della configurazione

La configurazione include attività quali la configurazione dei browser per accedere in remoto alla Core Console di DL1300, la gestione delle licenze e l'impostazione di avvisi e notifiche. Dopo aver completato la configurazione del Core, quindi, è possibile proteggere gli agenti ed eseguire il ripristino.

N.B.: Mentre si utilizza l'Appliance di Backup su disco DL1300, si consiglia di utilizzare la scheda **Appliance** per configurare il Core.

Configurazione del browser per accedere da remoto alla Core Console DL1300

Prima di poter accedere correttamente alla Core Console da un computer remoto, è necessario modificare le impostazioni del browser. Le procedure seguenti descrivono come modificare le impostazioni dei browser Internet Explorer, Mozilla Firefox e Google Chrome.

N.B.: Per modificare le impostazioni del browser, è necessario aver effettuato l'accesso al computer con privilegi di amministratore.

N.B.: Poiché Chrome utilizza le impostazioni di Internet Explorer, è necessario apportare le modifiche per Chrome utilizzando Internet Explorer.

N.B.: Accertarsi che la configurazione di Sicurezza avanzata di Internet Explorer sia attivata quando si accede alla Console Web Core localmente o in remoto. Per attivare Sicurezza avanzata di Internet Explorer, aprire **Server Manager** → **Server locale** → **Sicurezza avanzata di Internet Explorer**. Quando questa opzione viene visualizzata, accertarsi che sia **attiva**.

Configurazione delle impostazioni del browser in Internet Explorer e Chrome

Per configurare le impostazioni del browser in Internet Explorer e Chrome:

1. Dalla schermata **Opzioni Internet**, selezionare la scheda **Sicurezza**.
2. Fare clic su **Siti attendibili** e quindi fare clic su **Siti**.
3. Deselezionare l'opzione **Richiedi verifica server (https:) per tutti i siti della zona**, quindi aggiungere http://*<nome host o indirizzo IP del server dell'appliance che ospita AppAssure 5 Core>* per **Siti attendibili**.
4. Fare clic su **Chiudi**, selezionare **Siti attendibili**, quindi fare clic su **Livello personalizzato**.
5. Scorrere lungo il menu fino a **Varie** → **Visualizza contenuto misto** e selezionare **Attiva**.
6. Scorrere alla fine della schermata fino ad **Autenticazione utente** → **Accedi**, quindi selezionare **Accesso automatico con gli attuali nome utente e password**.
7. Fare clic su **OK**, quindi selezionare la scheda **Avanzate**.
8. Scorrere fino a **Elementi multimediali** e selezionare **Riproduci animazioni in pagine Web**.

9. Scorrere lungo l'elenco e individuare **Sicurezza**, selezionare **Abilita autenticazione di Windows integrata**, quindi fare clic su **OK**.

Impostazioni di configurazione del browser in Firefox

Per modificare le impostazioni del browser in Firefox:

1. Nella barra degli indirizzi di Firefox, digitare **about:config**, quindi fare clic su **Farò attenzione, prometto** se richiesto.
2. Cercare il termine **ntllm**.

   La ricerca deve restituire almeno tre risultati.
3. Fare doppio clic su **network.automatic-ntlm-auth.trusted-uris** e immettere la seguente impostazione in base alle esigenze del computer:
   - Per i computer locali, immettere il nome host.
   - Per i computer remoti, immettere il nome host o l'indirizzo IP, separati da una virgola, del sistema dell'appliance che ospita il Core; ad esempio, *indirizzo IP*, *nome host*.
4. Riavviare Firefox.

Accesso alla Core Console DL1300

Accertarsi di aver aggiornato siti attendibili come descritto nell'argomento Aggiornamento dei siti attendibili in Internet Explorer e configurare il proprio browser come descritto nell'argomento Configurazione del browser per accedere da remoto alla Core Console DL1300 . Dopo aver aggiornato siti attendibili in Internet Explorer e aver configurato i browser, eseguire una delle operazioni riportate di seguito per accedere alla Core Console:

- eseguire l'accesso locale al server del Core, quindi fare doppio clic sull'icona **Core Console**.
- Digitare uno dei seguenti URL nel browser Web:
  - **https://<nome server core>:8006/apprecovery/admin/core**
  - **https://<indirizzo IP server core>:8006/apprecovery/admin/core**

Aggiornamento dei siti attendibili in Internet Explorer

Per aggiornare i siti attendibili in Internet Explorer:

1. Aprire Internet Explorer.
2. Se **File**, **Modifica, Visualizza** e altri menu non vengono visualizzati, premere il tasto <F10 >.
3. Fare clic sulla scheda **Strumenti**, quindi su **Opzioni Internet**.
4. Dalla finestra **Opzioni Internet** , fare clic sulla scheda **Sicurezza**.
5. Fare clic su **Siti attendibili** e quindi fare clic su **Siti**.
6. In **Aggiungi il sito Web all'area**, immettere **https://[Nome visualizzato]**, utilizzando il nuovo nome fornito come nome visualizzato.
7. Fare clic su **Aggiungi**.
8. In **Aggiungi il sito Web all'area**, immettere **about:blank**.
9. Fare clic su **Aggiungi**.
10. Fare clic su **Chiudi**, quindi su **OK**.

Gestione delle licenze

È possibile gestire le licenze di DL1300 direttamente dalla Core Console. Dalla console, è possibile modificare la chiave di licenza e contattare il server di licenza. È inoltre possibile accedere al portale licenze dalla pagina Licenze nella Core Console o è possibile accedere al portale licenze all'indirizzo **https:// licenseportal.com**.

La pagina licenze include le seguenti informazioni:

- Tipo di licenza
- Stato licenza
- Dettagli dell'archivio
- Core master di replica (in entrata)
- Core slave di replica (in uscita)
- Roll-up simultanei
- Criterio di conservazione roll-up
- Chiavi di crittografia
- Esportazioni di standby virtuale
- Controlli della possibilità di montaggio
- Troncature dei log di scambio
- Troncatura dei log di SQL
- Intervallo di istantanee minimo

Come contattare il server del portale licenze

La Core Console contatta il server del portale per aggiornare le modifiche apportate nel portale licenze. La comunicazione con il server del portale viene eseguita automaticamente a intervalli designati; tuttavia, è possibile avviare la comunicazione su richiesta.

Per contattare il server del portale:

1. passare alla Core Console, quindi fare clic su **Configurazione** → **Licenze**.
   Viene visualizzata la pagina **Licenze**.
2. Dall'opzione **Server di licenza**, fare clic su **Contatta ora**.

Modifica di una chiave di licenza

Per modificare una chiave di licenza:

1. passare alla Core Console, selezionare **Configurazione** → **Licenze**.
   Viene visualizzata la pagina **Licenze**.
2. Dalla pagina **Dettagli licenza**, fare clic su **Modifica licenza**.
   Viene visualizzata la finestra di dialogo **Modifica licenza**.
3. Aggiornare la nuova chiave di licenza. Per aggiornare la chiave di licenza:
   - selezionare l'appropriata chiave di licenza utilizzando la scheda **Sfoglia** nella finestra `Carica file di licenza`.

     Per scaricare la licenza appropriata:

     1. andare all'indirizzo **www.rapidrecovery.licenseportal.com**.

2. Dal menu a discesa **Software** nell'angolo in alto a sinistra della pagina, selezionare **Appliance**.

   Tutte le licenze disponibili e le informazioni correlate vengono visualizzate.
3. Nella colonna **Azioni**, fare clic sull'icona download.

   La licenza viene scaricata nel sistema.

- Immettere la chiave di licenza nel campo `Immetti chiave di licenza`.

4. Fare clic su **Continua**.

   La licenza del sistema è aggiornata.

Modifica manuale della lingua di AppAssure

AppAssure consente di modificare la lingua selezionata durante l'esecuzione della Configurazione guidata dell'appliance AppAssure in una delle lingue supportate.
Per modificare la lingua di AppAssure nela lingua desiderata:

1. Avviare l'Editor del registro utilizzando il comando `regedit`.
2. Spostarsi in **HKEY_LOCAL_MACHINE → SOFTWARE → AppRecovery → Core → Localizzazione**.
3. Aprire **LCID**.
4. Selezionare **decimale**.
5. Immettere il valore della lingua richiesto nella casella `Dati valore`, i valori delle lingue supportate sono:

   a. Inglese: 1033
   b. Portoghese brasiliano: 1046
   c. Spagnolo: 1034
   d. Francese: 1036
   e. Tedesco: 1031
   f. Cinese semplificato: 2052
   g. Giapponese: 1041
   h. Coreano: 1042
6. Fare clic con il pulsante destro del mouse e riavviare i servizi nell'ordine dato:

   a. Strumentazione gestione Windows
   b. Web Service SRM
   c. Core AppAssure
7. Cancellare la cache del browser.
8. Chiudere il browser e riavviare la Core Console dall'icona del desktop.

Modifica della lingua del sistema operativo durante l'installazione

In un'installazione di Microsoft Windows in esecuzione, è possibile utilizzare il Pannello di controllo per selezionare i supporti linguistici e configurare le impostazioni internazionali aggiuntive.
Per cambiare lingua del sistema operativo (OS):

N.B.: si consiglia di impostare la lingua del sistema operativo e quella di AppAssure sulla stessa lingua. In caso contrario, alcuni messaggi possono essere visualizzati in lingue diverse.

N.B.: Si consiglia di modificare la lingua del sistema operativo prima di modificare la lingua di AppAssure.

1. Sulla pagina **Start**, digitare `lingua` e assicurarsi che l'ambito della ricerca sia impostato su Impostazioni.
2. Nel pannello **Risultati**, selezionare **Lingua**.
3. Nel pannello **Modifica preferenze lingua**, selezionare **Aggiungi una lingua**.
4. Sfogliare o ricercare la lingua che si desidera installare.

   Ad esempio, selezionare **Catalano**, quindi selezionare **Aggiungi**. Catalano è stato aggiunto come una delle lingue.
5. Nel pannello Modifica preferenze lingua, selezionare **Opzioni** accanto alla lingua che si è aggiunta.
6. Se un supporto linguistico è disponibile per la lingua, selezionare `Scarica e installa il supporto linguistico`.
7. Quando il supporto linguistico è installato, la lingua è visualizzata come lingua disponibile da utilizzare per la visualizzazione di Windows.
8. Per far diventare questa lingua la lingua di visualizzazione, disporla come prima voce dell'elenco delle lingue.
9. Disconnettersi e accedere nuovamente a Windows per rendere effettive le modifiche.

Crittografia dei dati di istantanea dell'agente

Tramite il Core è possibile crittografare i dati di istantanea dell'agente all'interno del repository, Invece di crittografare l'intero repository, DL1300 consente di specificare una chiave di crittografia durante la protezione di un agente in un repository che permette al tasto di essere riutilizzato per diversi agenti.

Per crittografare i dati di istantanea di un agente:

1. Dal Core, fare clic su **Configurazione** → **Gestione** → **Sicurezza**.
2. Fare clic su **Azioni**, quindi fare clic su **Aggiungi chiave di crittografia**.

   Viene visualizzata la pagina **Crea chiave di crittografia**.
3. Completare le seguenti informazioni:

Campo	Descrizione
Nome	Immettere un nome per la chiave di crittografia.
Commento	Inserire un commento per la chiave di crittografia. Esso viene utilizzato per fornire dettagli circa la chiave di crittografia.
Passphrase	Immettere una passphrase. Essa viene utilizzata per il controllo degli accessi.
Conferma passphrase	Inserire nuovamente la passphrase. Essa viene utilizzata per confermare l'immissione della passphrase.

N.B.: Si consiglia di registrare la passphrase di crittografia, dato che perdere la passphrase rende i dati inaccessibili. Per ulteriori informazioni, fare riferimento al capitolo Gestione della sicurezza nella *Guida dell'utente dell'appliance Dell DL1300*.

Configurazione di un server di posta elettronica e di un modello di notifica e-mail.

Se si desidera ricevere notifiche tramite e-mail sugli eventi, configurare un server di posta elettronica e un modello di notifica e-mail.

N.B.: Inoltre, è necessario configurare le impostazioni di notifica di gruppo, abilitando l'opzione **Notifica tramite e-mail** prima che vengano inviati messaggi e-mail di avviso. Per ulteriori informazioni su come specificare gli eventi per ricevere avvisi tramite e-mail, vedere Configurazione dei gruppi di notifica per gli eventi di sistema nella *Guidaa dell'utente dell'appliance Dell DL1300* su **Dell.com/support/home**.

Per configurare un server di posta elettronica e un modello di notifica e-mail, attenersi alla procedura descritta di seguito:

1. Dal Core, selezionare la scheda **Configurazione**.
2. Dall'opzione **Gestisci**, fare clic su **Eventi**.
3. Nel riquadro **Impostazioni del server SMTP** , fare clic su **Modifica**.
   Viene visualizzata la finestra di dialogo **Modifica configurazione della notifica di posta elettronica**.
4. Selezionare **Abilita le notifiche e-mail**, quindi immettere i dettagli per il server e-mail descritto come segue:

Casella di testo	Descrizione
Server SMTP	Immettere il nome del server di posta elettronica che deve essere utilizzato dal modello di notifica e-mail. La convenzione di denominazione include il nome host, il dominio e il suffisso; ad esempio, **smtp.gmail.com**.
Porta	Immettere un numero di porta. Esso viene utilizzato per identificare la porta per il server di posta elettronica, ad esempio, la porta 587 per Gmail. Il valore predefinito è 25.
Timeout (secondi)	Per specificare per quanto tempo provare una connessione prima del time out, immettere un valore intero. Esso viene utilizzato per stabilire il tempo in secondi durante il tentativo di connessione al server di posta elettronica prima che un timeout si verifichi. L'impostazione predefinita è 30 secondi.
TLS	Selezionare questa opzione se il server di posta elettronica utilizza una connessione protetta, ad esempio Transport Layer Security (TLS) o Secure Sockets Layer (SSL).
Nome utente	Immettere un nome utente per il server di posta elettronica.
Password	Immettere una password per l'accesso al server di posta elettronica.
Da	Immettere un indirizzo e-mail mittente. Esso viene utilizzato per specificare l'indirizzo e-mail mittente per il modello di notifica e-mail; ad esempio, **noreply@localhost.com**.

Casella di testo	Descrizione
Oggetto del messaggio di posta elettronica	Immettere un oggetto per il modello di posta elettronica. Esso viene utilizzato per definire l'argomento del modello di notifica e-mail; ad esempio, `<hostname> - <level> <name>`.
E-mail	Immettere le informazioni per il corpo del modello che descrive l'evento, quando si è verificato e la gravità.

5. Fare clic su **Invia e-mail di prova** e verificare i risultati.
6. Quando si è soddisfatti con i risultati dei test, fare clic su **OK**.

4

Preparazione per proteggere i server

Panoramica

Per proteggere i dati utilizzando DL1300, è necessario aggiungere le workstation e i server per la protezione nella Core Console; ad esempio, il server Exchange, SQL Server, il server Linux, e così via.

Nella Core Console è possibile individuare il computer in cui è installato un agente e specificare quali volumi proteggere, ad esempio uno spazio di archiviazione Microsoft Windows. È possibile definire le pianificazioni di protezione, aggiungere ulteriori misure di sicurezza, ad esempio la crittografia, e molto altro ancora. Per ulteriori informazioni su come accedere alla Core Console per proteggere le workstation e i server, vedere Protezione dei computer.

Protezione dei computer

Dopo la configurazione dell'appliance e del Core, verificare che sia possibile connettersi alle macchine che si prevede di sottoporre a backup.

Per proteggere una macchina:

1. passare alla Core Console e selezionare la scheda **Macchine**.
2. Nel menu a discesa **Azioni**, fare clic su **Proteggi macchina**.
   Viene visualizzata la finestra di dialogo **Connetti**.
3. Nella finestra di dialogo **Connetti**, immettere le informazioni relative alla macchina alla quale si desidera connettersi come descritto nella tabella riportata di seguito.

Host	Il nome host o l'indirizzo IP della macchina che si desidera proteggere.
Porta	Il numero di porta su cui il Core comunica con l'agente sulla macchina.
Nome utente	Il nome utente utilizzato per collegarsi a questa macchina, ad esempio amministratore.
Password	La password utilizzata per la connessione a questo computer.

4. Fare clic su **Connetti**.
5. Se si riceve un messaggio di errore, l'appliance non riesce a connettersi alla macchina per eseguirne il backup. Per risolvere il problema:
   a. Verificare la connettività di rete.
   b. Controllare le impostazioni firewall.
   c. Verificare che i servizi di AppAssure e RPC siano in esecuzione.
   d. Verificare le ricerche del servizio nome del dominio (se applicabile).

Verifica della connettività di rete

Per verificare la connettività di rete, effettuare le seguenti operazioni:

1. sul sistema del client a cui si desidera connettersi, aprire un'interfaccia della riga di comando.
2. Eseguire il comando **ipconfig** e prendere nota dell'indirizzo IP del client.
3. Aprire un'interfaccia della linea di comando sull'appliance.
4. Eseguire il comando **ping <indirizzo IP del client>**.
5. A seconda del risultato, effettuare una delle operazioni riportate di seguito:
   - se il client non rispondere al ping, verificare la connettività e le impostazioni di rete del server.
   - Se il cliente risponde, verificare che le impostazioni del firewall consentano l'esecuzione dei componenti di DL1300.

Controllo delle impostazioni del firewall

Se il client è collegato correttamente alla rete, ma non si vede dalla Core Console, verificare il firewall per garantire che le necessarie comunicazioni in entrata e in uscita siano consentite.

Per verificare le impostazioni del firewall sul Core e su eventuali client dei quali esegue il backup:

1. sull'appliance DL1300, fare clic su **Start → Pannello di controllo.**
2. Nel **Pannello di controllo**, fare clic su **Sistema e sicurezza**, in **Windows Firewall** fare clic su **Controlla stato firewall**.
3. Fare clic su **Impostazioni avanzate**.
4. Nella schermata **Windows Firewall con protezione avanzata**, fare clic su **Regole in entrata**.
5. Verificare che per il Core e per le porte venga visualizzato **Sì** nella colonna **Abilitato**.
6. Se la regola non è abilitata, fare clic con il pulsante destro del mouse sul Core e selezionare **Abilita regola**.
7. Fare clic su **Regole in uscita** ed eseguire le stesse verifiche relative al Core.

Controllo risoluzione DNS.

Se la macchina per la quale si sta tentando di eseguire il backup utilizza DNS, verificare che le ricerche DNS forward e reverse siano corrette.

Per garantire che le ricerche reverse siano corrette:

1. sull'appliance, passare agli host **C:\Windows\system32\drivers\etc**.
2. Immettere l'indirizzo IP di ciascun client che esegue il backup su DL1300.

Teaming delle schede di rete

Per impostazione predefinita, le schede di rete (NIC) sull'appliance DL1300 non sono collegate, cosa che incide sulle prestazioni del sistema. Si consiglia di raggruppare le schede NIC in una singola interfaccia. Il teaming delle schede NIC richiede:

- Reinstallazione di Broadcom Advanced Control Suite
- Creazione del team NIC

Reinstallazione di Broadcom Advanced Configuration Suite

Per reinstallare Broadcom Advanced Configuration Suite:

1. andare in C:\Install\BroadcomAdvanced e fare doppio clic su **setup**.
   Viene visualizzata l'**Installazione guidata InstallShield**.
2. Fare clic su **Avanti**.
3. Fare clic su **Modifica, Aggiungi o Rimuovi**.
   Viene visualizzata la finestra **Installazione personalizzata**.
4. Fare clic su **CIM provider**, quindi selezionare **Questa funzione verrà installata sul disco rigido locale**.
5. Fare clic su **BASP**, quindi selezionare **Questa funzione verrà installata sul disco rigido locale**.
6. Fare clic su **Avanti**.
7. Fare clic su **Installa**.
8. Fare clic su **Fine**.

Creazione del team NIC

N.B.: Si consiglia di **non** utilizzare l'interfaccia nativa Teaming in Windows Server 2012. L'algoritmo Teaming è ottimizzato per il traffico in uscita e non per quello in entrata. Questa soluzione offre prestazioni scarse con un carico di lavoro di backup, anche con un numero maggiore di porte di rete all'interno del team.

Per creare il team NIC:

1. Andare a **Start → Ricerca → Broadcom Advanced Control Suite.**

   N.B.: Quando si utilizza Broadcom Advanced Control Suite, selezionare solo le schede di rete Broadcom.
2. In **Broadcom Advanced Control Suite**, selezionare **Team → Vai a visualizzazione Team.**
3. Nel campo **Elenco host** sul lato sinistro, fare clic con il pulsante destro del mouse sul nome host dell'appliance DL1300 e selezionare **Crea team**.
   Viene visualizzata la finestra **Procedura guidata di creazione del team Broadcom**.
4. Fare clic su **Avanti**.
5. Immettere un nome per il team e fare clic su **Avanti**.
6. Selezionare il **Tipo di team** e fare clic su **Avanti**.
7. Selezionare una scheda che si desidera faccia parte del team e fare clic su **Aggiungi**.
8. Ripetere la procedura per tutte le altre schede che fanno parte del team.
9. Quando tutte le schede sono selezionate per il team, fare clic su **Avanti**.
10. Selezionare una scheda NIC in standby se si desidera aggiungere una scheda NIC che possa essere utilizzata come impostazione predefinita, se la creazione del team non riesce.
11. Selezionare se si desidera configurare **LiveLink**, quindi fare clic su **Avanti**.
12. Selezionare **Ignora gestione VLAN** e fare clic su **Avanti**.
13. Selezionare **Conferma modifiche al sistema** e fare clic su **Fine**.
14. Fare clic su **Sì** quando si riceve l'avviso che la connessione di rete è interrotta.

    N.B.: La creazione del team NIC potrebbe richiedere circa 5 minuti.

Regolazione flussi simultanei

Per impostazione predefinita, AppAssure è configurato in modo da consentire tre flussi simultanei verso l'appliance. Si consiglia di fare in modo che il numero di flussi sia pari al numero di macchine (agenti) per le quali si sta eseguendo il backup più uno. Ad esempio, se si sta eseguendo il backup di sei agenti, il **Numero massimo di trasferimenti simultanei** deve essere impostato su 7.

Per modificare il numero di flussi simultanei:

1. selezionare la scheda **Configurazione** e quindi fare clic su **Impostazioni**.
2. Selezionare cambia in **Coda trasferimento**.
3. Modificare **Numero massimo di trasferimenti simultanei** in un numero che sia pari almeno al numero di client per i quali si sta eseguendo il backup più uno.

Installazione degli agenti sui client

Ogni client per il quale è stato eseguito il backup tramite l'appliance AppAssure deve avere l'agente AppAssure installato. La Core Console di AppAssure consente di distribuire gli agenti sulle macchine. La distribuzione degli agenti sulle macchine richiede impostazioni di pre-configurazione che consentano di selezionare un singolo tipo di agente per il quale eseguire il push verso i client. Questo metodo funziona bene se tutti i client eseguono lo stesso sistema operativo. Tuttavia, se esistono diverse versioni di sistemi operativi, può risultare più semplice l'installazione degli agenti sulle macchine.

È inoltre possibile distribuire il software dell'agente alla macchina dell'agente durante il processo di protezione di una macchina. Questa opzione è disponibile per le macchine sulle quali il software dell'agente non è già installato. Per ulteriori informazioni su come distribuire il software dell'agente proteggendo una macchina, consultare la *Guida dell'utente appliance Dell DL1300* all'indirizzo **Dell.com/support/home**.

Installazione degli agenti in remoto (push)

Per installare gli agenti in remoto (push):

1. se nel client è in esecuzione una versione del sistema operativo che è precedente a Windows Server 2012, verificare che il client abbia il Microsoft.NET 4 Framework installato:
   a. sul client, avviare il **Windows Server Manager**.
   b. Fare clic su **Servizi di → configurazione.**
   c. Accertarsi che Microsoft .NET Framework sia visualizzato nell'elenco dei servizi.
      Se non è installato, è possibile ottenere una copia da installare da **microsoft.com**.
2. Verificare o modificare il percorso dei pacchetti di installazione dell'agente:
   a. nella Core Console AppAssure, fare clic sulla scheda **Configurazione**, quindi fare clic su **Impostazioni** nel riquadro a sinistra.
   b. Nell'area **Distribuisci impostazioni**, fare clic su **Modifica**.
   c. Completare le seguenti informazioni sulla posizione dell'agente:

Campo	Descrizione
Nome file di installazione dell'agente	Specifica il percorso esatto per la\il **folder\file** dell'agente.

Campo	Descrizione
Indirizzo core	Specifica l'indirizzo IP dell'appliance in cui è in esecuzione il Core AppAssure. **N.B.:** Per impostazione predefinita, **Indirizzo core** è vuoto. Nel campo **Indirizzo core** non è necessario un indirizzo IP in quanto i file di installazione sono installati sull'appliance.

d. Fare clic su **OK**.

3. Fare clic sulla scheda **Strumenti**, quindi fare clic su **Distribuzione di massa** nel riquadro a sinistra.

   N.B.: Se il cliente ha già un agente installato, il programma di installazione verificherà la versione dell'agente. Se l'agente per il quale si sta tentando il push è più recente della versione installata, il programma di installazione propone di aggiornare l'agente. Se l'host ha la versione corrente dell'agente installata, allora la distribuzione di massa avvierà la protezione tra il Core AppAssure e l'agente.

4. Nell'elenco dei client, selezionare tutti i client e fare clic su **Verifica** per garantire che la macchina sia attiva e l'agente possa essere distribuito.
5. Quando colonna **Messaggio** conferma che la macchina è pronta, fare clic su **Distribuisci**.
6. Per monitorare lo stato della distribuzione, selezionare la scheda **Eventi**.

   Dopo che l'agente viene distribuito, un backup del client viene avviato automaticamente.

Distribuzione del software dell'agente quando si protegge una macchina

È possibile scaricare e distribuire gli agenti durante il processo di aggiunta di un agente per la protezione.

N.B.: Non è necessario eseguire questa procedura se è già stato installato il software dell'agente su una macchina che si desidera proteggere.

Per distribuire agenti durante il processo di aggiunta di un agente per la protezione:

1. passare a **Proteggi computer** → **Connetti**, dopo aver immesso le impostazioni di connessione appropriate nella finestra di dialogo.
2. Fare clic su **Connetti**.

   Viene visualizzata la finestra di dialogo **Distribuzione agente**.
3. Fare clic su **Sì** per distribuire il software dell'agente in remoto alla macchina.

   Viene visualizzata la finestra di dialogo **Distribuzione agente**.
4. Immettere login e impostazioni di protezione come indicato di seguito:
   - **Nome host**: consente di specificare il nome host o l'indirizzo IP della macchina che si desidera proteggere.
   - **Porta**: consente di specificare il numero di porta su cui il Core comunica con l'agente sulla macchina. Il valore predefinito è 8006.
   - **Nome utente**: consente di specificare il nome utente utilizzato per collegarsi a questa macchina, ad esempio amministratore.
   - **Password**: consente di specificare la password utilizzata per la connessione a questo computer.
   - **Nome visualizzato**: consente di specificare un nome per la macchina virtuale che viene visualizzato sulla Core Console. Il nome visualizzato potrebbe essere lo stesso valore del nome dell'host.
   - **Proteggi computer dopo l'installazione**: selezionando questa opzione si consente a DL1300 di scattare copie istantanee dei dati dopo aver aggiunto la macchina per la protezione. Per

impostazione predefinita questa opzione è sempre attivata. Se si deseleziona questa opzione, è quindi necessario forzare manualmente una copia istantanea quando si è pronti per avviare la protezione dei dati. Per ulteriori informazioni su come forzare manualmente una copia istantanea, consultare l'argomento Forzare una copia istantanea nella Guida per l'utente Appliance *Dell DL1300* all'indirizzo **Dell.com/support/home**.

- **Archivio**: selezionare l'archivio in cui memorizzare i dati da questo agente.

  N.B.: È possibile memorizzare i dati provenienti da più agenti in un unico archivio.

- **Chiave di crittografia**: consente di specificare se la crittografia deve essere applicata ai dati per ogni volume presente su questa macchina che deve essere memorizzato nell'archivio.

  N.B.: È possibile definire le impostazioni per la crittografia per un archivio nella scheda **Configurazione** nella Core Console.

5. Fare clic su **Distribuisci**.

   La finestra di dialogo **Distribuzione agente** viene chiusa. È possibile che si verifichi un ritardo prima di vedere l'agente selezionato visualizzato nell'elenco di macchine virtuali protette.

Installazione di agenti Microsoft Windows sul client

Per installare gli agenti:

1. verificare che sul client sia installato 4 Microsoft .NET Framework:
   a. sul client, avviare il **Windows Server Manager**.
   b. Fare clic su **Servizi di → configurazione.**
   c. Accertarsi che Microsoft .NET Framework sia presente nell'elenco dei servizi.

      Se non è installato, è possibile ottenere una copia da **microsoft.com**.
2. Installare l'agente:
   a. sull'appliance AppAssure, condividere la directory C:\install\AppAssure con i client dei quali si intende eseguire il backup.
   b. Sul sistema client, mappare un'unità C:\install\AppAssure sull'appliance AppAssure.
   c. Sul sistema client, aprire la directory C:\install\AppAssure e fare doppio clic sul corretto agente del sistema client per iniziare l'installazione.

Aggiunta di un agente utilizzando il portale di licenze

N.B.: È necessario disporre dei privilegi amministrativi per scaricare e aggiungere agenti.

Per aggiungere un agente:

1. Sulla pagina iniziale del **Portale licenze AppAssure 5**, selezionare un gruppo, quindi fare clic su **Scarica agente**.

   Viene visualizzata la finestra di dialogo **Scarica agente**.
2. Fare clic su **Scarica**, situato accanto al programma di installazione della versione che si desidera scaricare.

   È possibile scegliere tra le seguenti opzioni:

   - Programma di installazione di Windows 32 bit
   - Programma di installazione di Windows 64 bit
   - Programma di installazione di Red Hat Enterprise Linux 6.3 e 6.4 32 bit

- Programma di installazione di Red Hat Enterprise Linux 6.3 e 6.4 64 bit
- Programma di installazione di CentOS 6.3 e 6.4 32 bit
- Programma di installazione di CentOS 6.3 e 6.4 64 bit
- Programma di installazione di Ubuntu LTS 12.04 e 13.04 32 bit
- Programma di installazione di Ubuntu LTS 12.04 e 13.04 64 bit
- Programma di installazione di SUSE Linux Enterprise Server 11 SP2, SP3 32 bit
- Programma di installazione di SUSE Linux Enterprise Server 11 SP2, SP3 64 bit
- Microsoft Hyper-V Server 2012

N.B.: Dell supporta le versioni precedenti di Linux e ha testato le versioni rilasciate del kernel.

N.B.: Gli agenti installati su Hyper-V Server 2012 Microsoft funzionano in modalità edizione base di Windows Server 2012.

Il file di download dell'**agente**.

3. Fare clic su **Esegui** nella finestra di dialogo **Installazione**.

   N.B.: Per informazioni sull'aggiunta di agenti utilizzando la macchina core, vedere Distribuzione di un agente (installazione push) nella *Guida per l'utente dell'appliance DL1300* all'indirizzo **Dell.com/support/home**.

Installazione degli agenti sui computer Linux

Scaricare il programma di installazione per la distribuzione specifico a 32 bit o 64 bit su ogni server Linux che si desidera proteggere utilizzando il Core. È possibile scaricare il programma di installazione dal portale delle licenze a **https://licenseportal.com**. Per ulteriori informazioni, vedere Aggiunta di un agente utilizzando il portale di licenze.

N.B.: La sicurezza legata alla protezione di un computer si basa sul PAM (Pluggable Authentication Module) in Linux. Dopo essersi è autenticato mediante **libpam**, un utente è autorizzato a proteggere il computer, se si trova in uno dei seguenti gruppi:

- sudo
- admin
- appassure
- wheel

Per ulteriori informazioni sulla protezione di un computer, consultare la sezione "Protezione di un computer" nella *Guida dell'utente dell'appliance Dell DL1300* su **Dell.com/support/home**.

Le istruzioni di installazione variano a seconda della distribuzione di Linux che si sta utilizzando. Per ulteriori informazioni sull'installazione dell'agente Linux sulla propria distribuzione, consultare le seguenti risorse:

- Installazione dell'agente su Ubuntu
- Installazione dell'agente su Red Hat Enterprise Linux e CentOS
- Installazione dell'agente su SUSE Linux Enterprise Server

N.B.: L'installazione dell'agente Linux sovrascrive tutte le regole del firewall che non sono state applicate tramite UFW, YaST2, o **system-config-firewall**.

Se sono state aggiunte manualmente le regole del firewall, allora è necessario aggiungere manualmente le porte AppAssure dopo l'installazione. Un backup di regole esistenti verrà scritto su **/var/lib/appassure fwl/backup"**.

È necessario aggiungere eccezioni del firewall per tutti i server su cui è in esecuzione l'agente per le porte TCP 8006 e 8009 per il Core per accedere agli agenti.

Posizione dei file dell'agente Linux

I file dell'agente Linux si trovano nelle seguenti directory per tutte le distribuzioni:

Componente	Posizione/Percorso
mono	/opt/appassure/mono
agent	/opt/appassure/aagent
aamount	/opt/appassure/amount
aavdisk e aavdctl	/usr/bin
file di configurazione per aavdisk	/etc/appassure/aavdisk.conf
wrapper per aamount e agente	• /usr/bin/aamount • /usr/bin/aagent
esecuzione automatica di script per aavdisk e agent	• /etc/init.d/appassure-agent • /etc/init.d/appassure-vdisk

Dipendenze dell'agente

Le seguenti sono le dipendenze necessarie e vengono installate come parte del del pacchetto del programma di installazione dell'agente:

Per Ubuntu:	Dipendenza
appassure-vss richiede	`dkms, gcc, make, linux-headers-‘uname-r‘`
appassure-aavdisk richiede	`libc6 (>=2.7-18), libblkid1, libpam0g, libpcre3`
appassure-mono richiede	`libc6 (>=2.7-18)`

Per Red Hat Enterprise Linux e CentOS	Dipendenza
nbd-dkms richiede	`dkms, gcc, make, kernel-headers-‘uname-r‘ kernel-devel-‘uname-r‘`
appassure-vss richiede	`dkms, gcc, make, kernel-headers-‘uname-r‘ kernel-devel-‘uname-r‘`
appassure-aavdisk richiede	`nbd-dkms, libblkid, pam, pcre`
appassure-mono richiede	`glibc >=2.11`

Per SUSE Linux Enterprise Server	Dipendenza
nbd-dkms richiede	`dkms, gcc, make, kernel-syms`
appassure-vss richiede	`dkms, kernel-syms, gcc, make`
appassure-aavdisk richiede	`libblkid1, pam, pcre`
appassure-mono richiede	`glibc >= 2.11`

Installazione dell'agente su Ubuntu

N.B.: Prima di eseguire questa procedura, accertarsi di aver scaricato il pacchetto di installazione specifico per Ubuntu in **/home/system directory**.

Per installare l'agente su Ubuntu:

1. aprire una sessione terminale con accesso utente root.
2. Per rendere il programma di installazione dell'agente eseguibile, digitare il comando riportato di seguito:

   `chmod +x appassure-installer_ubuntu_amd64_5.x.x.xxxxx.sh` , quindi premere il tasto <Invio>.

   Il file diventa eseguibile.

   N.B.: Per gli ambienti a 32 bit, il programma di installazione è denominato **appassureinstaller_ubuntu_i386_5.x.x.xxxxx.sh**
3. Per estrarre ed eseguire l'installazione dell'agente, digitare il comando riportato di seguito:

   `/appassure-installer_ubuntu_amd64_5.x.x.xxxxx.sh`, quindi premere il tasto <Invio>.

   L'agente Linux inizia l'estrazione e il processo di installazione. Tutti i pacchetti o i file mancanti di cui l'agente necessita vengono scaricati e installati automaticamente come parte dello script.

   N.B.: Per informazioni sui file richiesti dall'agente, vedere Dipendenze dell'agente.

Al termine del processo di installazione, l'agente Ubuntu è installato sulla macchina. Per ulteriori informazioni sulla protezione della macchina mediante core, consultare l'argomento "Proteggere le workstation e i server" nella *Guida dell'utente dell'appliance Dell DL1300* all'indirizzo **Dell.com/support/home**.

Installazione dell'agente su Red Hat Enterprise Linux e CentOS

N.B.: Prima di eseguire questa procedura, accertarsi di aver scaricato il pacchetto di installazione Red Hat o CentOS in **/home/system directory**. I seguenti passaggi sono gli stessi per entrambi gli ambienti a 32 bit e a 64 bit.

Per installare un agente su Red Hat Enterprise Linux e CentOS:

1. aprire una sessione terminale con accesso utente root.
2. Per rendere il programma di installazione dell'agente eseguibile, digitare il comando riportato di seguito:

   `chmod +x appassure-installer__rhel_amd64_5.x.x.xxxxx.sh`, quindi premere il tasto <Invio>.

   N.B.: Per gli ambienti a 32 bit, il programma di installazione è denominato `appassureinstaller__ rhel_i386_5.x.x.xxxxx.sh`.

   Il file diventa eseguibile.
3. Per estrarre ed eseguire l'installazione dell'agente, digitare il comando riportato di seguito:

   `/appassure-installer_rhel_amd64_5.x.x.xxxxx.sh`, quindi premere il tasto <Invio>.

   L'agente di Linux inizia il processo di estrazione e di installazione. Tutti i pacchetti o i file mancanti di cui l'agente necessita vengono scaricati e installati automaticamente come parte dello script.

   Per informazioni sui file richiesti dall'agente, vedere Dipendenze dell'agente.

Dopo che il programma di installazione viene completato, l'agente sarà in esecuzione sulla macchina. Per ulteriori informazioni sulla protezione della macchina con il Core, consultare l'argomento "Proteggere le workstation e i server" nella *Guida dell'utente appliance Dell DL1300* all'indirizzo **Dell.com/support/home**.

Installazione dell'agente su SUSE Linux Enterprise Server

N.B.: Prima di eseguire questa procedura, accertarsi di aver scaricato il pacchetto di installazione SUSE Linux Enterprise Server (SLES) in **/home/system directory**. I seguenti passaggi sono gli stessi per entrambi gli ambienti a 32 bit e a 64 bit.

Per installare l'agente su SLES:

1. Aprire una sessione terminale con accesso root.
2. Per rendere il programma di installazione dell'agente DL1300 eseguibile, digitare il comando riportato di seguito:

   `chmod +x appassure-installer_sles_amd64_5.x.x.xxxxx.sh`, quindi premere il tasto <INVIO>.

N.B.: Per gli ambienti a 32 bit, il programma di installazione è denominato `appassureinstaller__ sles_i386_5.x.x.xxxxx.sh`

Il file diventa eseguibile.

3. Per estrarre ed eseguire l'installazione dell'agente DL1300, digitare il comando riportato di seguito: `/appassure-installer_sles_amd64_5.x.x.xxxxx.sh`, quindi premere il tasto <Invio>.

   L'agente Linux inizia l'estrazione e il processo di installazione. Tutti i pacchetti o i file mancanti richiesti dall'agente vengono scaricati e installati automaticamente come parte dello script.

   Per informazioni sui file richiesti dall'agente, vedere Dipendenze dell'agente.

4. Quando viene richiesto di installare nuovi pacchetti, digitare `y`, quindi premere <Invio>.

   Il sistema termina il processo di installazione.

Dopo che il programma di installazione viene completato, l'agente è in esecuzione sul computer. Per ulteriori informazioni sulla protezione di questo computer con il Core, consultare la sezione "Protezione workstation e server" nella *Guida dell'utente dell'appliance Dell DL1300* su **Dell.com/support/home**.

5

Casi di utilizzo comuni

Questa sezione illustra i casi di utilizzo più comuni per la serie DL1300 e fornisce una panoramica di alto livello delle informazioni e procedure necessarie per ogni scenario. Quando è necessario, vengono forniti i riferimenti a informazioni supplementari.

Protezione dei computer

La tecnologia di replica e backup AppAssure fornisce funzionalità avanzate di protezione delle macchine virtuali (VM) o server consentendo al contempo un'applicazione flessibile e il ripristino dei dati. Quando una macchina è protetta, copie istantanee complete e incrementali dei dati sono acquisite e archiviate nell'archivio del Core. Il processo di protezione AppAssure sfrutta due tecnologie chiave - Copie istantanee e l'agente Smart Dell DL1300 che sono descritte di seguito.

Copie istantanee

L'agente AppAssure per Windows utilizza Microsoft Volume Shadow Copy Service (VSS) per bloccare e interrompere le attività dei dati delle applicazioni su disco per acquisire un backup coerente con il file-system e con l'applicazione. Quando una copia istantanea viene creata, il VSS writer sul server di destinazione impedisce che i contenuti vengano scritti sul disco. Durante il processo di arresto della scrittura dei contenuti su disco, tutte le operazioni di I/O del disco vengono messe in coda e riprese solo dopo che la copia istantanea è stata completata, mentre le operazioni già in transito saranno completate e tutti i file aperti saranno chiusi. Per ulteriori informazioni, vedere l'argomento Processo di copia istantanea.

Smart Agent Dell DL1300

Lo Smart Agent è installato sui computer che sono protetti dal Core DL1300. La funzione Smart Agent tiene traccia dei blocchi modificati sul volume del disco, quindi scatta un'immagine dei blocchi modificati in un intervallo predefinito di protezione. L'approccio senza limiti nel tempo delle copie istantanee del livello incrementale dei blocchi impedisce la copia ripetuta degli stessi dati dalla macchina protetta al Core. Quando la copia istantanea è pronta per l'invio, è rapidamente trasferita al Core utilizzando connessioni intelligenti multi-threaded, basate su socket. Per ulteriori informazioni, vedere l'argomento Smart Agent Dell DL1300.

Distribuzione degli Smart Agent

È necessario installare il programma di installazione dell'agente AppAssure su ogni computer nell'ambiente protetto dal Core DL1300.

N.B.: Queste procedure sono un riepilogo. Per informazioni dettagliate o istruzioni specifiche per gli agenti Linux, fare riferimento alla *Guida dell'utente dell'appliance Dell DL1300*.

Passaggio 1: Procedura per ottenere il software agente

Il software Smart Agent può essere ottenuto attenendosi a uno dei metodi seguenti:

- **Scaricamento da AppAssure Core** - Accedere alla Core Console e scaricare il software sul computer agente. Selezionare **Scarica** dalla scheda **Strumenti**, quindi scaricare il programma di installazione Web per il componente agente.
- **Scaricamento dal portale di licenza AppAssure** - Se è stata effettuata la registrazione del software nel portale di licenza software Dell, è possibile accedere al portale e scaricare la licenza software per il computer agente.
- **Distribuzione del software agente durante la protezione di un computer** - È possibile distribuire il software agente sul computer che si desidera proteggere utilizzando la **Protezione guidata di un computer**.
- **Utilizzo della funzione Distribuzione di massa** - Se il Core è installato, è possibile distribuire il software agente in più computer con la funzionalità **Distribuzione di massa**, a cui si accede dalla scheda **Strumenti** della Core Console.

Fase 2: Installazione del software dell'agente

Avviare il programma di installazione come descritto di seguito per installare il software su ogni computer che si desidera proteggere nel Core. Per installare il software dell'agente su macchine Windows:

1. dalla macchina che si desidera proteggere, fare doppio clic sul file di installazione dell'agente.
2. Nella pagina **Introduzione**, fare clic su **Avanti** per continuare con l'installazione.
3. Nella pagina **Contratto di licenza**, fare clic su **Accetto i termini del contratto di licenza**, quindi fare clic su **Avanti**.

   N.B.: Il file d'installazione dell'agente verifica l'esistenza dei file prerequisito. Se i file prerequisito non sono presenti, il file di installazione dell'agente identifica i file necessari e visualizza i risultati di conseguenza; ad esempio, Microsoft System CLR Types per SQL Server 2008 R2 (x64).
4. Fare clic su **Installa prerequisiti**.
5. Una volta completata l'installazione dei file prerequisito, fare clic su **Avanti**.
6. Nella pagina **Opzioni di installazione**, verificare le opzioni di installazione. Se necessario, modificarle come descritto di seguito:
   a. nel campo di testo **Cartella di destinazione**, verificare la cartella di destinazione per l'installazione. Se si desidera modificare il percorso, effettuare le operazioni riportate di seguito:
      - fare clic sull'icona della cartella
      - Nella finestra di dialogo **Sfoglia alla destinazione**, selezionare una nuova posizione. Fare clic su **OK**.
   b. Nel campo di testo **Numero di porta**, immettere un numero di porta da utilizzare per la comunicazione tra l'agente e il Core.

      N.B.: Il valore predefinito è 8006. Se si modifica il numero di porta, prenderne nota nel caso in cui si renda necessaria la regolazione delle impostazioni di configurazione in un secondo momento.
7. Verificare la presenza di opzioni di installazione, fare clic su **Installa**. Al termine dell'installazione, viene visualizzata la pagina **Completata**.
8. Selezionare una delle seguenti opzioni, quindi fare clic su **Fine**: Sì, riavvia il computer ora.No, riavvia il computer in seguito.

N.B.: È necessario riavviare il sistema prima di utilizzare il software dell'agente.

Configurazione dei processi di protezione

Quando si aggiunge la protezione, è necessario definire le informazioni di connessione, come ad esempio l'indirizzo IP e la porta, e fornire le credenziali per la macchina che si desidera proteggere. In alternativa, è possibile fornire un nome di visualizzazione da visualizzare nella Core Console invece dell'indirizzo IP. Sarà inoltre necessario definire la pianificazione di protezione per la macchina.

N.B.: Queste procedure sono un riepilogo. Per informazioni dettagliate, fare riferimento alla *GuidaDL1300 dell'utente all'appliance Dell DL1300* all'indirizzo **Dell.com/support/home**.

Protezione di un computer

Questo argomento descrive come iniziare a proteggere i dati su un computer specificato.

N.B.: Sul computer è necessario che sia installato il software agente AppAssure in modo che esso sia protetto. È possibile scegliere di installare il software agente prima di questa procedura, oppure è possibile distribuire il software per l'agente nel momento in cui si specifica la protezione nella finestra di dialogo **Connessione**. Per installare il software agente durante il processo di protezione di un computer, vedere l'argomento "Distribuzione del software agente durante la protezione di un agente" nella *Guida dell'utente dell'Aplliance Dell DL1300*.

Quando si aggiunge la protezione, è necessario specificare il nome o l'indirizzo IP del computer da proteggere e i volumi sul computer in questione da proteggere, oltre a definire la pianificazione di protezione per ciascun volume.

Per proteggere più computer allo stesso tempo, vedere l'argomento "Protezione di più computer" nella *Guida dell'utente dell'appliance Dell DL1300*.

Per proteggere una macchina:

1. Riavviare il computer su cui il software agente AppAssure è installato, se non si è ancora eseguita tale operazione.
2. Dalla Core Console sul computer principale, fare clic su **Proteggi** → **Proteggi computer** sulla barra dei pulsanti.

   Viene visualizzata la **Protezione guidata computer**.
3. Sulla pagina **Introduzione**, selezionare le appropriate opzioni di installazione:
   - Se non è necessario specificare un repository o stabilire la crittografia, selezionare **Tipica**.
   - Se non si desidera vedere la pagina **Introduzione** per la **Protezione guidata computer** in futuro, selezionare l'opzione **Ignora la pagina di Introduzione all'apertura successiva della procedura guidata**.
4. Fare clic su **Avanti**.
5. Sulla pagina **Connessione**, immettere le informazioni relative al computer al quale si desidera connettersi come descritto nella tabella riportata di seguito.

Casella di testo	Descrizione
Host	Il nome host o l'indirizzo IP della macchina che si desidera proteggere.
Porta	Il numero di porta su cui l'AppAssure Core comunica con l'agente sul computer. Il numero di porta predefinito è 8006.

Casella di testo	Descrizione
Nome utente	Il nome utente utilizzato per collegarsi a questa macchina, ad esempio amministratore.
Password	La password utilizzata per la connessione a questo computer.

6. Fare clic su **Avanti**. Se la pagina **Protezione** viene visualizzata successivamente nella **Protezione guidata computer**, andare al Passaggio 7.

   N.B.: Se la pagina **Installazione dell'agente** viene visualizzata successivamente nella **Protezione guidata computer**, ciò indica che il software agente non è ancora installato sul computer indicato. Fare clic su **Avanti** per installare il software agente. Il software agente deve essere installato sul computer che si desidera proteggere e riavviato, prima di poter eseguire il backup sul Core. Per fare in modo che il programma di installazione riavvii il computer agente, selezionare l'opzione **Dopo l'installazione riavviare il computer automaticamente (consigliata)**prima di fare clic su **Avanti**.

7. Il nome host o l'indirizzo IP specificato nella finestra di dialogo **Connessione** viene visualizzato in questo campo di testo. Se lo si desidera, immettere un nuovo nome per il computer da visualizzare nella Core Console.
8. Selezionare la pianificazione appropriata di protezione:
   - Per utilizzare la pianificazione di protezione predefinita, nell'opzione **Impostazioni di pianificazione**, selezionare **Protezione predefinita (istantanee ogni 3 ore di tutti i volumi)**. Con una pianificazione di protezione predefinita, il Core eseguirà istantanee del computer agente una volta ogni 3 ore. Le istantanee del computer agente possono essere eseguite una volta ogni ora (minimo). Per modificare le impostazioni di protezione in qualsiasi momento dopo la chiusura della procedura guidata, tra cui la scelta dei volumi da proteggere, passare alla scheda Riepilogo per lo specifico computer agente.
   - Per definire una diversa pianificazione di protezione, nell'opzione **Impostazioni di pianificazione**, selezionare **Protezione personalizzata**.
9. Selezionare una delle seguenti:
   - Se è stata selezionata una configurazione tipica dalla **Protezione guidata computer** e specificata una protezione predefinita, fare clic su **Fine** per confermare le proprie scelte, chiudere la procedura guidata e proteggere il computer specificato.
   - La prima volta che si aggiunge la protezione per un computer, un'immagine di base (cioè, un'istantanea di tutti i dati all'interno dei volumi protetti) sarà in grado di trasferire al repository sul Core seguendo la pianificazione definita, a meno che non sia stato specificato di sospendere inizialmente la protezione.
   - Se è stata selezionata una configurazione tipica per la **Protezione guidata computer** e specificata una protezione personalizzata, fare clic su **Avanti** per impostare una pianificazione di protezione personalizzata. Per ulteriori informazioni sulla definizione di una pianificazione di protezione personalizzata, fare riferimento alla sezione Creazione di pianificazioni di protezione personalizzata.
   - Se è stata selezionata la configurazione avanzata per la **Protezione guidata computer** e selezionata la protezione predefinita, fare clic su **Avanti** e procedere al Passaggio 12 per vedere le opzioni di repository e crittografia.
   - Se è stata selezionata la configurazione avanzata per la **Protezione guidata computer** e specificata una protezione personalizzata, fare clic su **Avanti** e procedere al Passaggio 10 per scegliere quali volumi proteggere.
10. Nella pagina **Protezione dei volumi**, selezionare i volumi sul computer agente che si desidera proteggere. Se sono elencati volumi che non si desidera includere nella protezione, fare clic su nella colonna di controllo per cancellare la selezione. Quindi fare clic su **Avanti**.

N.B.: Si consiglia di proteggere il volume di sistema riservato e il volume con il sistema operativo (in genere l'unità C).

11. Sulla pagina **Pianificazione di protezione** specificare una pianificazione di protezione personalizzata.
12. Sulla pagina **Repository**, selezionare **Usa un repository esistente**.
13. Fare clic su **Avanti**.
    Viene visualizzata la pagina **Crittografia**.
14. In alternativa, per abilitare la crittografia, selezionare **Abilita crittografia**.
    I campi **Chiave di crittografia** vengono visualizzati sulla pagina **Crittografia**.

    N.B.: Se si attiva la crittografia, sarà applicata ai dati per tutti i volumi protetti per questo computer agente. È possibile modificare le impostazioni in seguito dalla scheda Configurazione nella Core Console di AppAssure 5.

    ATTENZIONE: Viene utilizzata una crittografia AES a 256 bit nella modalità CBC (Cipher Block Chaining) con chiavi a 256 bit. Mentre l'utilizzo della crittografia è opzionale, è altamente consigliabile impostare una chiave di crittografia, e di proteggere la passphrase specificata. Memorizzare la password in una posizione sicura, dato che è fondamentale per il ripristino dei dati. Senza una passphrase, il ripristino dei dati non è possibile.
15. Immettere le informazioni come descritto nella seguente tabella per aggiungere una chiave di crittografia per il Core.

Casella di testo	Descrizione
Nome	Immettere un nome per la chiave di crittografia.
Descrizione	Immettere una descrizione per fornire ulteriori dettagli relativi a una chiave di crittografia.
Passphrase	Immettere la passphrase utilizzata per controllare l'accesso.
Conferma passphrase	Inserire nuovamente la passphrase appena immessa.

16. Fare clic su **Fine** per salvare e applicare le impostazioni.
    La prima volta che si aggiunge una protezione per un computer, un'immagine di base (cioè, un'istantanea di tutti i dati all'interno dei volumi protetti) sarà in grado di trasferire al repository sull'AppAssure Core seguendo la pianificazione definita, a meno che non sia stato specificato di sospendere inizialmente la protezione.

Recupero dei dati

Con DL1300, i dati vengono protetti sia sulle macchine che utilizzano Windows sia su quelle che utilizzano Linux. I backup delle macchine protette vengono salvati nel Core come punti di ripristino che possono essere utilizzati per il ripristino dei dati. Interi volumi possono essere ripristinati, sostituiti da un punto di ripristino verso le macchine di destinazione. Per ripristinare i dati dai punti di ripristino può essere utilizzato uno qualsiasi dei seguenti metodi:

- Ripristino di file e cartelle
- Ripristino dei volumi di dati, utilizzando Live Recovery
- Ripristino bare-metal, utilizzando Universal Recovery

Ripristino di file o directory

È possibile utilizzare Esplora risorse di Windows per copiare e incollare directory e file da un punto di ripristino montato su qualsiasi macchina Windows. Ciò può essere utile quando si desidera distribuire solo una parte di un punto di ripristino ai propri utenti. Quando si esegue la copia delle directory e dei file, le autorizzazioni di accesso dell'utente che sta eseguendo l'operazione di copia, vengono utilizzate e applicate ai file e directory incollati.
Per ripristinare un file o directory tramite Esplora risorse di Windows:

1. montare il punto di ripristino che contiene i dati che si desidera ripristinare. Per ulteriori informazioni, consultare l'argomento Montaggio di un punto di ripristino per una macchina Windows nella Guida dell'utente Appliance *Dell DL1300*.
2. In Esplora risorse di Windows, navigare al punto di ripristino montato e selezionare i file e le directory che si desidera ripristinare. Fare clic con il pulsante destro del mouse e selezionare **Copia**.
3. In Esplora risorse di Windows, andare alla posizione della macchina in cui si desidera ripristinare i dati. Fare clic con il pulsante destro del mouse e selezionare **Incolla**.

Ripristino dei volumi

Dalla Core Console è possibile ripristinare interi volumi da un punto di ripristino di un volume non di sistema, sostituendo i volumi sul computer di destinazione.

N.B.: La procedura riportata di seguito è una panoramica semplificata del processo di ripristino. Per informazioni dettagliate o per le procedure su ulteriori opzioni di ripristino, vedere l'argomento "Ripristino dei volumi da un punto di ripristino" nel *Manuale dell'utente dell'appliance Dell DL1300*.

Per ripristinare i volumi da un punto di ripristino:

1. Nella Core Console fare clic sulla scheda **Ripristina**.

   Viene visualizzato il **Ripristino guidato computer**.
2. Dalla pagina **Computer protetti**, selezionare il computer protetto per il quale si desidera ripristinare i dati, quindi fare clic su **Avanti**.

   N.B.: È necessario che il software agente sia installato sul computer protetto e che tale computer disponga di punti di ripristino dai quali si eseguirà l'operazione di ripristino.

   Viene visualizzata la pagina **Punti di ripristino**.
3. Dall'elenco dei punti di ripristino, cercare la copia istantanea che si desidera ripristinare sul computer agente.

   N.B.: Se necessario, utilizzare i pulsanti di navigazione nella parte inferiore della pagina per visualizzare ulteriori punti di ripristino. O se si desidera limitare la quantità di punti di ripristino visualizzati nella pagina Punti di ripristino della procedura guidata, è possibile filtrare per volumi (se definiti) o data di creazione del punto di ripristino.
4. Fare clic su qualsiasi punto di ripristino per selezionarlo, quindi fare clic su **Avanti**.

   Viene visualizzata la pagina **Destinazione**.
5. Sulla pagina **Destinazione**, scegliere il computer sul quale si desidera ripristinare i dati come segue:
   - Se si desidera ripristinare i dati dal punto di ripristino selezionato sullo stesso computer agente (ad esempio, Computer1) e se i volumi che si desidera ripristinare non includono il volume di sistema, scegliere **Ripristina su un computer protetto (solo volumi non di sistema)**, verificare che il computer di destinazione (Computer1) sia selezionato, quindi fare clic su **Avanti**. Viene visualizzata la pagina Mapping dei volumi. Procedere al Passaggio 6.

- Se si desidera ripristinare i dati dal punto di ripristino selezionato su un altro computer protetto (ad esempio, per sostituire il contenuto di Computer2 con i dati di Computer1), scegliere **Ripristina su un computer protetto (solo volumi non di sistema)**, selezionare il computer di destinazione (ad esempio, Computer2) dall'elenco, quindi fare clic su **Avanti**. Viene visualizzata la pagina Mapping dei volumi. Procedere al Passaggio 6.
- Se si desidera eseguire il ripristino da un punto di ripristino su un volume di sistema (ad esempio, l'unità C del computer agente chiamato Computer1), è necessario eseguire una BMR.

6. Sulla pagina Mapping dei volumi, per ciascun volume nel punto di ripristino che si desidera ripristinare, selezionare il volume di destinazione appropriato. Se non si desidera ripristinare un volume, nella colonna Volumi di destinazione selezionare **Non ripristinare**.
7. Selezionare **Mostra opzioni avanzate**, quindi procedere come segue:
   - Per il ripristino di computer Windows, se si desidera utilizzare Live Recovery, selezionare **Live Recovery**.

     Utilizzando la tecnologia istantanea di ripristino Live Recovery di AppAssure 5, è possibile recuperare o ripristinare immediatamente i dati su computer fisici o virtuali da punti di ripristino archiviati di computer Windows, inclusi gli spazi di archiviazione Microsoft Windows. Live Recovery non è disponibile per i computer Linux.
   - Se si desidera forzare lo smontaggio, scegliere **Forza smontaggio**.

     Se non si forza uno smontaggio prima del ripristino dei dati, il ripristino potrebbe non riuscire con un errore del volume in uso.

     Il computer agente, quando viene avviato dal CD di avvio, visualizza l'interfaccia della Universal Recovery Console (URC). Questo ambiente è utilizzato per ripristinare l'unità di sistema o i volumi selezionati direttamente dal Core. Annotare l'indirizzo IP e le credenziali della chiave di autenticazione nell'URC, che si aggiornano ogni volta che si effettua l'avvio dal CD di avvio.
8. Se i volumi che si desidera ripristinare contengono i database di SQL o Microsoft Exchange, sulla pagina **Smonta i database** viene richiesto di smontarli. In alternativa, se si desidera reinstallare questi database al termine del ripristino, selezionare **Reinstalla automaticamente tutti i database dopo il ripristino del punto di ripristino**. Fare clic su **Fine**.
9. Fare clic su **OK** per confermare il messaggio di stato che il processo di ripristino è stato avviato.
10. Per monitorare l'avanzamento del processo di ripristino, sulla Core Console fare clic su **Eventi**.

Bare Metal Recovery (Ripristino bare metal)

Utilizzando AppAssure è possibile eseguire un ripristino bare metal (BMR) per macchine Windows o Linux. BMR è un processo che consente di ripristinare la configurazione completa del software per un sistema specifico. È utilizzato il termine "bare metal" perché l'operazione di ripristino non soltanto consente di ripristinare i dati dal server, ma di riformattare anche il disco rigido e reinstallare il sistema operativo e tutte le applicazioni software. Per eseguire un ripristino BMR, è possibile specificare un punto di ripristino da un computer protetto, quindi eseguire il rollback sulla macchina fisica o virtuale designata. Le altre circostanze in cui è possibile scegliere di eseguire un ripristino bare metal includono l'aggiornamento dell'hardware o la sostituzione del server.

L'esecuzione di un ripristino BMR è possibile per computer fisici o macchine virtuali. Come ulteriore vantaggio, AppAssure consente di eseguire un BMR se l'hardware è simile o differente.

Prerequisiti per l'esecuzione di un Bare Metal Restore (Ripristino bare metal) per un computer Windows

Prima di iniziare il processo di esecuzione di un ripristino bare metal per un computer Windows, è necessario assicurarsi che le condizioni e i criteri seguenti siano rispettati:

- **Backup del computer che si desidera ripristinare** - è necessario disporre di un Core AppAssure funzionante contenente i punti di ripristino del server protetto che si desidera ripristinare.
- **Hardware per il ripristino (nuovo o vecchio, simile o differerente)** - Il computer di destinazione deve soddisfare i requisiti di installazione dell'agente.
- **Supporti di memorizzazione e software per immagini**- è necessario disporre di un CD o DVD vuoto, di software per la masterizzazione su disco o software per creare un'immagine ISO. Se vengono gestiti computer in remoto utilizzando software di rete virtuale (virtual network computing), ad esempio UltraVNC, è necessario disporre di VNC Viewer.
- **Driver di archiviazione e driver di schede di rete compatibili**- se il ripristino viene eseguito su hardware diverso, è necessario disporre di driver di archiviazione e driver di schede di rete compatibili con Windows 7 PE (32 bit) per il computer di destinazione, tra cui RAID, AHCI e driver per chipset per il sistema operativo di destinazione, in base alle proprie esigenze.
- **Spazio di archiviazione e partizioni, in base alle necessità**: assicurarsi che ci sia abbastanza spazio sul disco rigido per creare le partizioni di destinazione sul computer di destinazione per contenere i volumi di origine. Una partizione di destinazione deve essere grande almeno quanto l'iniziale partizione di origine.
- **Partizioni compatibili**: i sistemi operativi Windows 8 e Windows Server 2012 che vengono avviati da partizioni FAT32 EFI sono disponibili per la protezione o il ripristino, nonché i volumi Resilient File System (ReFS). Le partizioni basate su UEFI sono trattate come semplici volumi FAT32. I trasferimenti incrementali sono completamente supportati e protetti. AppAssure 5 fornisce supporto ai sistemi UEFI per BMR inclusi i dischi GPT di partizionamento automatico.

Roadmap per l'esecuzione di un Bare Metal Restore (Ripristino bare metal) per un computer Windows

N.B.: Di seguito vengono indicati i passaggi base utilizzati nel processo di Bare Metal Restore (BMR). Per informazioni dettagliate su ciascun passaggio, consultare la *Guida dell'utente dell'appliance Dell DL1300*.

Per eseguire un BMR per un computer Windows:

1. Creare un CD di avvio.
2. Masterizzare l'immagine su disco.
3. Avviare il server di destinazione dal CD di avvio
4. Connettersi al disco di ripristino.
5. Eseguire la mappatura dei volumi.
6. Avviare il ripristino.
7. Monitorare lo stato di avanzamento.

Replica dei punti di ripristino

La replica è il processo di copia dei punti di ripristino e di trasferimento di essi in una posizione secondaria ai fini del ripristino di emergenza. Il processo richiede la presenza di una relazione associata origine-destinazione tra due core. Il core di origine copia i punti di ripristino degli agenti protetti e quindi in modo asincrono e continuo li trasmette al core di destinazione presso un sito remoto per il ripristino di emergenza. La posizione fuori sede può essere un data center di proprietà dell'azienda (core autogestito) o la posizione di un provider di servizi (MSP) gestito da terze parti o un ambiente cloud. Quando si esegue la replica su un MSP, è possibile utilizzare flussi di lavoro incorporati che consentono di richiedere connessioni e ricevere notifiche di feedback automatico. Possibili scenari del processo di replica includono:

- **Replica su una posizione locale**— Il core di destinazione è situato in un data center a livello locale o posizione in sede e la replica è mantenuta in qualsiasi momento. In questa configurazione, la perdita del Core non impedirebbe il ripristino.
- **Replica su una posizione fuori sede** — Il core di destinazione è situato presso una struttura fuori sede per il ripristino in caso di perdita.
- **Replica reciproca**— Due data center in due diverse posizioni contengono ognuno un core e stanno proteggendo gli agenti offrendo backup fuori sede per il ripristino di emergenza per ognuno di essi. In questo scenario, ciascun core replica gli agenti sul core che si trova in un altro data center.
- **Replica ospitata e in cloud**— I partner MSP di AppAssure gestiscono più core di destinazione in un data center o un cloud pubblico. Su ognuno di questi core, il partner MSP consente a uno o più dei loro clienti di replicare i punti di ripristino da un core di origine sul sito del cliente nel core di destinazione del MSP previo pagamento di una tariffa.

Impostazione dell'ambiente

Se la larghezza di banda tra il core di origine e di destinazione non può contenere il trasferimento dei punti di ripristino archiviati, la replica inizia con il seeding del core di destinazione con le immagini di base e i punti di ripristino dai server selezionati protetti sul core di origine. Il processo di seeding può essere eseguito in qualsiasi momento, come parte del trasferimento iniziale dei dati in modo che sia possibile utilizzarlo come base per una replica pianificata regolarmente oppure, in caso di ripristino della replica per un computer replicato in precedenza, la cui replica era stata sospesa o eliminata. In questo caso, l'opzione Genera una catena di punti di ripristino (RP) consentirebbe di copiare punti di ripristino non ancora replicati su un'unità seed.

Durante la preparazione per la replica, è necessario considerare i seguenti fattori:

- **Velocità di variazione**: la velocità di variazione è la velocità con cui viene raccolta la quantità di dati protetti. La velocità dipende dalla quantità di dati che cambia sui volumi protetti e dall'intervallo di protezione dei volumi. Se un insieme di blocchi cambia sul volume, riducendo l'intervallo di protezione si riduce la velocità di variazione.
- **Larghezza di banda**: la larghezza di banda è la velocità di trasferimento disponibile tra il core di origine e di destinazione. È fondamentale che la larghezza di banda sia superiore alla velocità di variazione per la replica in modo da stare al passo con i punti di ripristino creati dalle istantanee. A causa della quantità di dati trasmessi da un core all'altro, potrebbe essere richiesto che più flussi paralleli realizzino alte velocità fino alla velocità di una connessione 1 GB Ethernet.

  N.B.: La larghezza specificata dall'ISP è la larghezza di banda totale disponibile. La larghezza di banda in uscita è condivisa da tutti i dispositivi sulla rete. Assicurarsi che vi sia sufficiente larghezza di banda libera per la replica, in modo da ospitare la velocità di variazione.
- **Numero di agenti**: è importante prendere in considerazione il numero degli agenti protetti per core di origine e il numero che si intende replicare sulla destinazione. DL1300 consente di eseguire la replica sulla base di un singolo server protetto, in modo da poter scegliere di replicare determinati server. Se tutti i server protetti devono essere replicati, questo influenza drasticamente la velocità di variazione, in particolare se la larghezza di banda tra il core di l'origine e di destinazione è insufficiente per la quantità e la dimensione dei punti di ripristino in corso di replica.

  A seconda della configurazione di rete, la replica può essere una procedura che richiede molto tempo.

  La massima velocità di variazione per i tipi di connessione WAN è illustrata nella tabella di seguito con esempi della larghezza di banda necessaria per gigabyte per una ragionevole velocità di variazione.

Tabella 2. Massima velocità di variazione per i tipi di connessione WAN.

Banda larga	Larghezza di banda	Max velocità di variazione
DSL	768 Kbps e superiore	330 MB per ora
Cavo	1 Mbps e superiore	429 MB per ora
T1	1,5 Mbps e superiore	644 MB per ora
Fibra	20 Mbps e superiore	8,38 GB per ora

Per ottenere risultati ottimali, è necessario rispettare le raccomandazioni elencate nella tabella precedente. Se il collegamento non funziona durante il trasferimento dei dati, la replica riprende dal punto precedente di errore del trasferimento al ripristino della funzionalità di collegamento.

Procedura per la configurazione di una replica

N.B.: Le informazioni riportate di seguito vengono presentate come una panoramica di alto livello delle operazioni necessarie per eseguire la replica. Per le procedure complete, consultare la *Guida dell'utente dell'appliance Dell DL1300* su **dell.com/support/home**.

Per replicare i dati utilizzando AppAssure, è necessario configurare i core di origine e destinazione per la replica. Una volta configurata la replica, quindi, è possibile replicare i dati dell'agente, monitorare e gestire le attività di replica, quindi eseguire il ripristino. L'esecuzione di una replica in AppAssure prevede l'esecuzione delle seguenti operazioni:

- **Configurare la replica auto-gestita** - Per ulteriori informazioni sulla replica di un core di destinazione autogestito, vedere l'argomento "Replica su un core di destinazione auto-gestito" nella *Guida dell'utente dell'appliance Dell DL1300* su **Dell.com/support/home**.
- **Configurare la replica di terze parti** - Per ulteriori informazioni sulla replica su un core di destinazione di terze parti, vedere l'argomento "Processo di replica su un core di destinazione di terze parti" nella *Guida dell'utente dell'appliance Dell DL1300* su **Dell.com/support/home**.
- **Replicare un agente esistente** - Per ulteriori informazioni sulla replica di un agente che è già protetto dal core di origine, vedere l'argomento "Aggiunta di un computer alla replica esistente" nella *Guida dell'utente dell'appliance Dell DL1300* at **Dell.com/support/home**.
- **Consumare l'unità seed** - Per ulteriori informazioni sul consumo dei dati dell'unità seed nel core di destinazione, vedere l'argomento "Consumo dell'unità seed su un core di destinazione" nella *Guida dell'utente dell'appliance Dell DL1300* at **Dell.com/support/home**.
- **Impostare la priorità di replica per un agente** - Per ulteriori informazioni sulle priorità della replica per gli agenti, vedere l'argomento "Impostazione della priorità di replica per un agente" nella *Guida dell'utente dell'appliance Dell DL1300* su **Dell.com/support/home**.
- **Impostare una pianificazione di replica per un agente** - Per ulteriori informazioni sull'impostazione di una pianificazione di replica, vedere l'argomento "Pianificazione di replica" nella *Guida dell'utente dell'appliance Dell DL1300* su **Dell.com/support/home**.
- **Monitorare le repliche in base alle necessità** - Per ulteriori informazioni sul monitoraggio della replica, vedere l'argomento "Monitoraggio della replica" nella *Guida dell'utente dell'appliance Dell DL1300* su **Dell.com/support/home**.
- **Gestire le impostazioni di replica in base alle necessità** - Per ulteriori informazioni sulla gestione delle impostazioni di replica, vedere l'argomento "Gestione delle impostazioni di replica" nella *Guida dell'utente dell'appliance Dell DL1300* su **Dell.com/support/home**.

- **Ripristinare i dati replicati in caso di emergenza o perdita dei dati** - Per ulteriori informazioni sul ripristino dei dati replicati, vedere l'argomento "Ripristino dei dati replicati" nella *Guida dell'utente dell'appliance Dell DL1300* su **Dell.com/support/home**.

Utilizzo di standby virtuali

AppAssure supporta sia l'esportazione in una sola volta sia l'esportazione continua (per il supporto di standby virtuali) delle informazioni di backup di Windows ad una macchina virtuale. L'esportazione dei dati su una macchina virtuale in standby fornisce una copia dei dati ad alta disponibilità. Se una macchina protetta si guasta, è possibile avviare la macchina virtuale per eseguire il recupero.

Quando si esporta verso una macchina virtuale, tutti i dati di backup da un punto di ripristino, nonché i parametri definiti per la pianificazione di protezione per la macchina verranno esportati. È inoltre possibile creare uno "standby virtuale" attraverso la creazione di una protezione continua dei dati esportati dalla propria macchina protetta verso una macchina virtuale.

N.B.: Solo la configurazione 3 TB con 2 macchine virtuali e 4 TB con 2 macchine virtuali di DL1300 supporta l'esportazione in una sola volta e l'esportazione continua su macchine virtuali in standby virtuale.

Esecuzione di un'esportazione Hyper-V unica

Per eseguire l'esportazione Hyper-V unica:

1. Nella Core Console, spostarsi sul computer che si desidera esportare.
2. Nella scheda Riepilogo, fare clic su **Azioni** → **Esporta** → **Una volta**.
   L'**Esportazione guidata** viene visualizzata sulla pagina **Computer protetti**.
3. Selezionare un computer per l'esportazione, quindi fare clic su **Avanti**.
4. Sulla pagina **Punti di ripristino**, selezionare il punto di ripristino che si desidera esportare, quindi fare clic su **Avanti**.

Definizione di impostazioni per l'esecuzione di un'esportazione Hyper-V

Per definire le impostazioni per l'esecuzione di un'esportazione Hyper-V:

1. Dalla finestra di dialogo Hyper-V, fare clic su **Utilizza macchina locale** per eseguire l'esportazione Hyper-V in un computer locale con il ruolo Hyper-V assegnato.
2. Fare clic sull' opzione **Host remoto** per indicare che il server Hyper-V è situato su un computer remoto. Se è stata selezionata l'opzione host remoto, immettere i parametri per l'host remoto come descritto di seguito:

Casella di testo	Descrizione
Nome host	Immettere l'indirizzo IP o il nome host per il server Hyper-V. Esso rappresenta l'indirizzo IP o il nome host del server remoto Hyper-V.
Porta	Immettere un numero di porta per la macchina. Rappresenta la porta attraverso la quale il core comunica con questa macchina.
Nome utente	Immettere il nome utente per l'utente con privilegi di amministratore per la workstation con il server Hyper-V. Esso viene utilizzato per specificare le credenziali di accesso per la macchina virtuale.

Casella di testo	Descrizione
Password	Immettere la password per l'account utente con privilegi di amministratore sulla workstation con Hyper-V server. Esso viene utilizzato per specificare le credenziali di accesso per la macchina virtuale.

3. Fare clic su **Avanti**.
4. Sulla pagina **Opzioni di macchine virtuali** nella casella di testo **Posizione della macchina VM**, immettere il percorso o posizione per la macchina virtuale. Ad esempio, D:\export. La posizione della macchina virtuale deve disporre di spazio sufficiente per contenere i metadati della VM e le unità virtuali necessarie per la macchina virtuale.
5. Immettere il nome della macchina virtuale nella casella di testo **Nome della macchina virtuale**.

   Il nome che si immette viene visualizzato nell'elenco delle macchine virtuali nella console di gestione di Hyper-V.
6. Fare clic su una delle seguenti opzioni:
   - **Usa la stessa quantità di RAM** della macchina di origine per identificare che la RAM utilizzata è identica tra la macchina virtuale e quella di origine.
   - **Utilizza una specifica quantità di RAM** per specificare la quantità di memoria della macchina virtuale dopo l'esportazione; ad esempio, 4096 MB (consigliato)
7. Per specificare il formato del disco, accanto a **Formato disco**, fare clic su una delle seguenti opzioni:
   - **VHDX**
   - **VHD**

   N.B.: L'esportazione Hyper-V supporta formati di disco VHDx se sul computer di destinazione è in esecuzione Windows 8 (Windows Server 2012) o superiore. Se il VHDX non è supportato per l'ambiente in uso, l'opzione è disabilitata.
8. Sulla pagina **Volumi**, selezionare i volumi da esportare. Affinché la macchina virtuale rappresenti un efficace backup del computer protetto includere l'unità di avvio del computer protetto. Esempio C:\.

   I volumi selezionati non devono essere superiori a 2040 GB per VHD. Se i volumi selezionati sono più grandi del 2040 GB, e il formato VHD è selezionato, viene visualizzato un messaggio di errore.
9. Nella pagina **Riepilogo**, fare clic su **Fine** per completare la procedura guidata e avviare l'esportazione.

Esecuzione di un'esportazione continua Hyper-V (standby virtuale)

N.B.: Solo le configurazioni 3 TB con 2 macchine virtuali e 4 TB con 2 macchine virtuali di DL1300 supportano l'esportazione in una sola volta e l'esportazione continua su macchine virtuali in standby virtuale.

Per eseguire un'esportazione continua Hyper-V (standby virtuale):

1. nella Core Console, nella scheda **Standby virtuale**, fare clic su **Aggiungi** per avviare la **Procedura guidata di esportazione**. Sulla pagina **Macchine protette** della **Procedura guidata di esportazione**.
2. Selezionare la macchina che si desidera esportare e quindi fare clic su **Avanti**.
3. Nella scheda **Riepilogo**, fare clic su **Esporta → standby virtuale**.
4. Dalla finestra di dialogo Hyper-V, fare clic su **Utilizza macchina locale** per eseguire l'esportazione Hyper-V in un computer locale con il ruolo Hyper-V assegnato.
5. Fare clic sull' opzione **Host remoto** per indicare che il server Hyper-V è situato su un computer remoto. Se è stata selezionata l'opzione host remoto, immettere i parametri per l'host remoto come descritto di seguito:

Casella di testo	Descrizione
Nome host	Immettere l'indirizzo IP o il nome host del server Hyper-V. Rappresenta l'indirizzo IP o il nome host del server remoto Hyper-V.
Porta	Immettere un numero di porta per la macchina. Rappresenta la porta attraverso la quale il core comunica con questa macchina.
Nome utente	Immettere il nome utente per l'utente con privilegi di amministratore per la workstation con il server Hyper-V. Esso viene utilizzato per specificare le credenziali di accesso per la macchina virtuale.
Password	Immettere la password per l'account utente con privilegi di amministratore sulla workstation con Hyper-V server. Esso viene utilizzato per specificare le credenziali di accesso per la macchina virtuale.

6. Sulla pagina **Opzioni macchine virtuali** nella casella di testo **Posizione macchina virtuale**, immettere il percorso o la posizione della macchina virtuale. Ad esempio D:\export. La collocazione della macchina virtuale deve disporre di spazio sufficiente per contenere i metadati della macchina virtuale e le unità virtuali necessarie per la macchina virtuale.
7. Immettere il nome della macchina virtuale nella casella di testo **Nome della macchina virtuale**.

   Il nome che si immette viene visualizzato nell'elenco delle macchine virtuali nella console di gestione di Hyper-V.
8. Fare clic su una delle seguenti opzioni:
   - **Usa la stessa quantità di RAM** della macchina di origine per identificare che la RAM utilizzata è identica tra la macchina virtuale e quella di origine.
   - **Usa una quantità specifica di RAM** per specificare la quantità di memoria di cui dispone la macchina virtuale dopo l'esportazione; ad esempio, 4096 MB (consigliato).
9. Per specificare la generazione, fare clic su una delle seguenti opzioni:
   - Generation 1 (consigliato)
   - Generation 2
10. Per specificare il formato del disco, accanto a **Formato disco**, fare clic su una delle seguenti opzioni:
    - **VHDX** (impostazione predefinita)
    - **VHD**

    N.B.: L'esportazione Hyper-V supporta formati di dischi VHDx se sul computer di destinazione è in esecuzione Windows 8 (Windows Server 2012) o superiore. Se il VHDx non è supportato per l'ambiente in uso, l'opzione è disabilitata. Nella pagina Schede di rete selezionare la scheda virtuale da collegare ad uno switch.
11. Sulla pagina **Volumi**, selezionare i volumi da esportare. Affinché la macchina virtuale costituisca un backup efficace della macchina protetta includere l'unità di avvio della macchina protetta. Esempio C:\.

    I volumi selezionati non devono essere superiori a 2040 GB per VHD. Se i volumi selezionati sono più grandi del 2040 GB, e il formato VHD è selezionato, viene visualizzato un messaggio di errore.
12. Nella pagina **Riepilogo**, fare clic su **Fine** per completare la procedura guidata e per avviare l'esportazione.

    N.B.: È possibile monitorare lo stato e l'avanzamento dell'esportazione, controllando la scheda **Standby virtuale** o **Eventi**

Gestione dei punti di ripristino

Le copie istantanee periodiche di backup di tutti i server protetti si accumulano sul Core nel tempo. I criteri di conservazione sono utilizzati per conservare le copie istantanee di backup per periodi di tempo più lunghi e per favorire la gestione di tali copie istantanee di backup. Il criterio di conservazione viene applicato da un processo notturno di rollup che permette di stabilire da quanto tempo sono presenti i backup ed eliminare quelli obsoleti.

Archiviazione dei dati

I criteri di conservazione applicano i periodi per cui i backup vengono archiviati su supporti a breve termine (veloci e costosi). A volte alcuni requisiti tecnici e commerciali comportano una conservazione prolungata di questi backup, ma l'utilizzo di dispositivi di archiviazione veloci è proibitivo in termini di costi. Pertanto, questo requisito genera la necessità di un'archiviazione a lungo termine (lenta e conveniente). Le aziende utilizzano spesso l'archiviazione a lungo termine per l'archiviazione di dati conformi e non conformi. La funzione archivio in AppAssure viene utilizzata per supportare la conservazione prolungata dei dati conformi e non conformi. Questa funzione viene utilizzata anche per il seeding dei dati di replica a un core remoto di replica.

Creazione di un archivio

Per creare un archivio:

1. Nella Core Console, fare clic su **Strumenti** → **Crea archivio** → .
   Viene visualizzata la finestra di dialogo **Aggiunta guidata archivio**.
2. Nella pagina di creazione dell'Aggiunta guidata archivio, selezionare una delle opzioni di seguito riportate dall'elenco a discesa Tipo di posizione:
   - Locale
   - Rete
   - Cloud
3. Immettere i dettagli per l'archivio come descritto nella tabella riportata di seguito in base al tipo di posizione selezionata nel Passaggio 3.

Tabella 3. Creazione di un archivio

Opzione	Casella di testo	Descrizione
Locale	Posizione dell'output	Immettere la posizione per l'output. Essa viene utilizzata per definire il percorso della posizione in cui si desidera che risieda l'archivio; ad esempio, d:\work\archive.
Rete	Posizione dell'output	Immettere la posizione per l'output. Essa viene utilizzata per definire il percorso della posizione in cui si desidera che risieda l'archivio; ad esempio, \\servername\sharename.

Opzione	Casella di testo	Descrizione
	Nome utente	Immettere un nome utente. Esso viene utilizzato per stabilire credenziali di accesso per la condivisione di rete.
	Password	Immettere una password per il percorso di rete. Essa viene utilizzata per stabilire credenziali di accesso per la condivisione di rete.
Cloud	Account	Selezionare un account dall'elenco a discesa. **N.B.:** Per selezionare un account per il cloud, è prima necessario aggiungerlo alla Core Console. Vedere l'argomento "Aggiunta di un account cloud" nella *Guida dell'utente dell'appliance Dell DL1300*.
	Contenitore	Selezionare un contenitore associato all'account dal menu a discesa.
	Nome cartella	Immettere un nome per la cartella in cui salvare i dati archiviati. Il nome predefinito è AppAssure-5-Archive-[DATA ULTIMA MODIFICA]-[ORA ULTIMA MODIFICA]

4. Fare clic su **Avanti**.
5. Nella pagina Computer della procedura guidata, selezionare quale o quali computer protetti contengono i punti di ripristino che si desidera archiviare.
6. Fare clic su **Avanti**.
7. Nella pagina **Opzioni** immettere le informazioni descritte nella tabella riportata di seguito.

Casella di testo	Descrizione
Dimensione massima	Gli archivi di dati di grandi dimensioni possono essere suddivisi in più segmenti. Selezionare la quantità massima di spazio che si desidera riservare per la creazione dell'archivio, eseguendo una delle operazioni riportate di seguito: • Selezionare Intera destinazione per riservare tutto lo spazio disponibile nel percorso fornito nella destinazione indicata nel Passaggio 4 (ad esempio, se il percorso è D:\work\archive, viene riservato tutto lo spazio disponibile sull'unità D:).

Casella di testo	Descrizione
	• Selezionare la casella di testo vuota, utilizzare freccia SU e freccia GIÙ per immettere una quantità, quindi selezionare un'unità di misura dall'elenco a discesa per personalizzare lo spazio massimo che si desidera riservare. **N.B.:** Gli archivi cloud di Amazon vengono automaticamente suddivisi in segmenti di 50 GB. Gli archivi cloud di Windows Azure divengono automaticamente suddivisi in segmenti di 200 GB.
Azione di riciclo	Selezionare una delle seguenti opzioni di azione di riciclo: • **Non riutilizzare**: non sovrascrive o cancella tutti i dati archiviati dalla posizione. Se il percorso non è vuoto, la scrittura dell'archivio non riesce. • **Sostituisci questo Core**: sovrascrive qualsiasi dato archiviato preesistente relativo al core in oggetto ma lascia intatti i dati per altri core • **Cancella completamente**: cancella tutti i dati archiviati dalla directory prima di eseguire l'operazione di scrittura del nuovo archivio. • **Incrementale**: consente di aggiungere i punti di ripristino a un archivio esistente. Mette a confronto i punti di ripristino in modo da evitare la duplicazione dei dati già presenti nell'archivio.
Commento	Immettere eventuali informazioni aggiuntive che è necessario acquisire per l'archivio. Il commento verrà visualizzato se si importa l'archivio più tardi.
Utilizzo del formato compatibile	Selezionare questa opzione per archiviare i dati in un formato che è compatibile con le versioni precedenti di core. **N.B.:** Il nuovo formato offre prestazioni migliori; tuttavia non è compatibile con l'aggiunta di core precedenti.

8. Fare clic su **Avanti**.
9. Sulla pagina dell'intervallo date, immettere la data di inizio e la data di scadenza dei punti di ripristino da archiviare.
   - Per immettere un'ora, fare clic sull'ora indicata (impostazione predefinita, 8:00) per visualizzare le barre di scorrimento che consentono di selezionare ore e minuti.
   - Per immettere una data, fare clic sulla casella di testo per mostrare il calendario, quindi fare clic sul giorno preferito.
10. Fare clic su **Fine**.

Archiviazione in un cloud

È possibile archiviare i dati in un cloud caricandoli su una vasta gamma di provider di cloud direttamente dalla Core Console. Cloud compatibili includono Windows Azure, Amazon, Rackspace e qualsiasi provider basato su OpenStack.

Per esportare un archivio in un cloud:

- Aggiungere l'account di cloud alla Core Console. Per ulteriori informazioni, vedere l'argomento "Aggiunta di un account di cloud' nella *Guida dell'utente dell'appliance Dell DL1300* su **Dell.com/support/home**.
- Archiviare i dati ed esportarli in un account di cloud. Per ulteriori informazioni, vedere l'argomento "Creare un archivio" nella *Guida dell'utente dell'appliance Dell DL1300* su **Dell.com/support/home**.

- Recuperare i dati archiviati importandoli dalla sede del cloud. Per ulteriori informazioni, vedere l'argomento "Importare un archivio" nella *Guida dell'utente dell'appliance Dell DL1300* su **Dell.com/support/home**.

6

Come ottenere assistenza

Ricerca di documentazione e aggiornamenti software

Collegamenti diretti ad AppAssure e alla documentazione e agli aggiornamenti del software di appliance DL1300 sono disponibili nella Core Console.

Documentazione

Per accedere al collegamento alla documentazione:

1. sulla Core Console, fare clic sulla scheda **Appliance**.
2. Nel riquadro a sinistra, andare al collegamento **Documentazione → appliance**.

Aggiornamenti software

Per accedere al collegamento per gli aggiornamenti software:

1. sulla Core Console, fare clic sulla scheda **Appliance**.
2. Nel riquadro a sinistra, andare al collegamento **Aggiornamenti software → appliance**.

Come contattare Dell

N.B.: Se non si dispone di una connessione Internet attiva, è possibile trovare i recapiti sulla fattura di acquisto, sulla distinta di imballaggio, sulla fattura o sul catalogo dei prodotti Dell.

Dell fornisce diverse opzioni di supporto e assistenza telefonica e in linea. Se non si dispone di una connessione Internet attiva, è possibile trovare le informazioni di contatto su fatture di acquisto, distinte di imballaggio, scontrini o sul catalogo dei prodotti Dell. La disponibilità varia a seconda del Paese e del prodotto, e alcuni servizi potrebbero non essere disponibili nella regione di riferimento. Per contattare Dell in merito a problemi relativi a vendite, assistenza tecnica o assistenza clienti, visitare il sito **software.dell.com/support**.

Feedback sulla documentazione

Fare clic sul collegamento **Feedback** in qualsiasi pagina della documentazione Dell, compilare il modulo e fare clic su **Invia** per inviare il feedback.