Appliance Dell DL1300
Guida dell'utente

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.

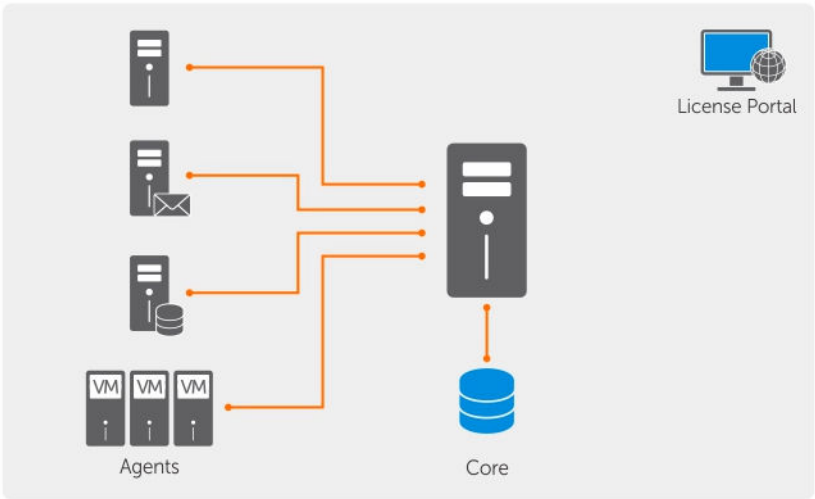


Figura 2. Architettura di distribuzione di Dell DL1300

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

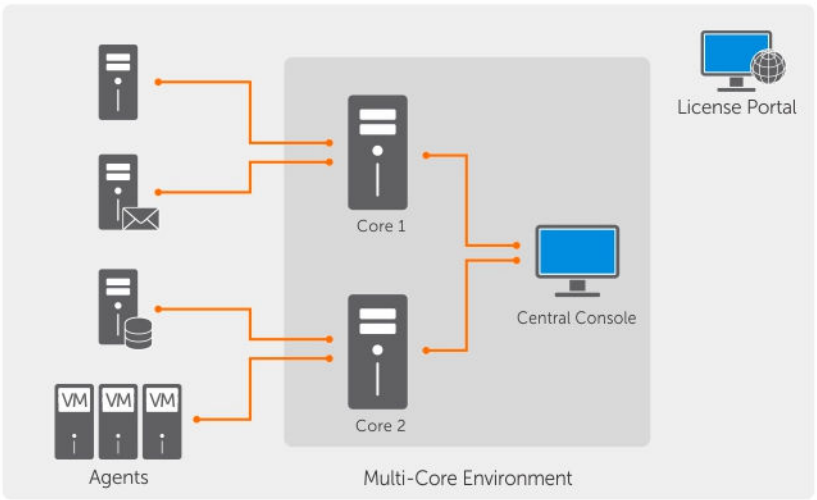


Figura 3. Architettura di distribuzione di più core DL1300

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

Gestione di DL1300

Accesso alla Core Console DL1300

Per accedere alla Core Console DL1300:

1. Aggiornare i siti attendibili nel browser.
2. Configurare i propri browser per accedere in remoto alla Core Console DL1300. Consultare Configurazione dei browser per accedere in remoto alla Core Console.
3. Eseguire una delle operazioni riportate di seguito per accedere alla Core Console DL1300:
   - Accedere in locale al proprio core server DL1300, quindi fare doppio clic sull'icona della **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 visualizzazione** 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**, 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**.

Configurazione dei browser per accedere in remoto alla Core Console

Per accedere alla Core Console da una macchina remota, è necessario modificare le impostazioni del browser.

N.B.: Per modificare le impostazioni del browser, eseguire l'accesso al sistema come amministratore.

N.B.: Google Chrome utilizza le impostazioni di Microsoft Internet Explorer, modificare le impostazioni del browser 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 la **Configurazione di sicurezza avanzata di Internet Explorer**:

1. Aprire **Server Manager**.
2. Selezionare **Configurazione di sicurezza avanzata di Internet Explorer del server locale** visualizzato sulla destra. Accertarsi che sia **Attiva**.

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

1. Aprire Internet Explorer.
2. Dal menu **Strumenti** selezionare **Opzioni Internet**, scheda **Sicurezza**.
3. Fare clic su **Siti attendibili** e quindi fare clic su **Siti**.
4. 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 Core>* per **Siti attendibili**.
5. Fare clic su **Chiudi**, selezionare **Siti attendibili**, quindi fare clic su **Livello personalizzato**.
6. Scorrere lungo il menu fino a **Varie** → **Visualizza contenuto misto** e selezionare **Attiva**.
7. Scorrere alla fine della schermata fino ad **Autenticazione utente** → **Accedi**, quindi selezionare **Accesso automatico con gli attuali nome utente e password**.
8. Fare clic su **OK**, quindi selezionare la scheda **Avanzate**.
9. Scorrere fino a **Elementi multimediali** e selezionare **Riproduci animazioni in pagine Web**.
10. Scorrere lungo l'elenco e individuare **Sicurezza**, selezionare **Abilita autenticazione di Windows integrata**, quindi fare clic su **OK**.

Per modificare le impostazioni del browser Mozilla 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 le macchine locali, immettere il nome host.
   - Per macchine remote, immettere il nome host o l'indirizzo IP, separati da una virgola, del sistema dell'appliance che ospita AppAssure Core; ad esempio, *indirizzo IP*, *nome host*.
4. Riavviare Firefox.

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.

Gestione delle impostazioni del core

Le impostazioni del core vengono utilizzate per definire le varie impostazioni di configurazione e delle prestazioni. La maggior parte delle impostazioni è configurata per l'uso ottimale; tuttavia, è possibile modificare le seguenti impostazioni secondo le proprie esigenze:

- Generali
- Processi notturni
- Coda di trasferimento
- Impostazioni di timeout del client
- Configurazione della cache di deduplicazione
- Impostazioni di connessione al database

Modifica del nome visualizzato del core

N.B.: Si consiglia di selezionare un nome visualizzato definitivo durante la configurazione iniziale dell'appliance. Se si desidera modificarlo in un secondo momento, è necessario eseguire diversi passaggi manuali per accertarsi che il nuovo nome host sia effettivo e l'appliance funzioni correttamente.

Per modificare il nome visualizzato del core:

1. Passare alla Core Console, fare clic su **Configurazione** → **Impostazioni**.
2. Nella sezione **Proprietà generali**, fare clic su **Modifica**.
   Viene visualizzata la finestra di dialogo **Nome visualizzato**.
3. Nella casella di testo **Nome visualizzato**, inserire un nuovo nome da visualizzare per il core.
4. Fare clic su **OK**.

Modifica dell'orario dei processi notturni

L'opzione Processi Notturni pianifica i processi quali roll-up, connettività e troncatura per gli agenti protetti dal Core.

Per regolare l'orario dei processi notturni:

1. Passare alla Core Console e selezionare **Configurazione** → **Impostazioni**.
2. Nella sezione **Processi notturni**, fare clic su **Modifica**.
   Viene visualizzata la finestra di dialogo **Processi notturni**.
3. Nella casella di testo **Orario dei processi notturni**, inserire una nuova ora di inizio.
4. Fare clic su **OK**.

Modifica delle impostazioni delle code di trasferimento

Le impostazioni della coda di trasferimento sono delle impostazioni a livello di core che definiscono il numero massimo di trasferimenti simultanei e tentativi di trasferimento dei dati.

Per modificare le impostazioni di coda di trasferimento:

1. Passare alla Core Console, fare clic su **Configurazione** → **Impostazioni**.
2. Nella sezione **Coda di trasferimento**, fare clic su **Modifica**.
   Viene visualizzata la finestra di dialogo **Coda di trasferimento**.
3. Nella casella di testo **Numero massimo di trasferimenti simultanei**, inserire un valore per aggiornare il numero di trasferimenti simultanei.
   Impostare un numero da 1 a 60. Più piccolo è il numero, minore è il carico sulla rete e su altre risorse di sistema. Man mano che la capacità che viene elaborata aumenta, aumenta anche il carico sul sistema.
4. Nella casella di **Massimo di tentativi**, inserire un valore per aggiornare il numero massimo di tentativi.
5. Fare clic su **OK**.

Regolazione delle impostazioni di timeout del client

Impostazioni del timeout del client specifica il numero di secondi o minuti che il server deve attendere prima che vada in timeout nel tentativo di connessione ad un client.

Per regolare le impostazioni del timeout del client:

1. Passare alla Core Console, quindi fare clic su **Configurazione** → **Impostazioni**.
2. Nella sezione **Configurazione delle impostazioni del timeout del client**, fare clic su **Modifica**.
   Viene visualizzata la finestra di dialogo **Impostazioni del timeout del client**.
3. Nella casella di testo **Timeout connessione**, inserire il numero di minuti e secondi prima che si verifichi il timeout della connessione.
4. Nella casella di testo **Timeout lettura/scrittura**, inserire il numero di minuti e secondi che si desidera attendere prima che si verifichi un timeout durante un evento di lettura/scrittura.
5. Fare clic su **OK**.

Configurazione delle impostazioni della cache di deduplicazione

La deduplicazione a livello globale riduce la quantità di spazio di archiviazione su disco necessaria per il backup dei dati. Il Deduplication Volume Manager (DVM) combina una serie di posizioni di archiviazione in un unico repository. La cache di deduplicazione contiene i riferimenti a blocchi univoci. Per impostazione predefinita, la cache di deduplicazione è di 1,5 GB. Se la quantità di informazioni superflue è così grande che la cache di deduplicazione risulta piena, il repository non può più sfruttare a pieno la deduplicazione nel repository dei dati appena aggiunti. È possibile quindi aumentare le dimensioni della cache di deduplicazione modificando la configurazione della cache di deduplicazione nella Core Console.

Per configurare le impostazioni della cache di deduplicazione:

1. Passare alla Core Console, fare clic su **Configurazione** → **Impostazioni**.
2. Nella sezione **Configurazione della cache di deduplicazione**, fare clic su **Modifica**.
   Viene visualizzata la finestra di dialogo **Configurazione della cache di deduplicazione**.
3. Nella casella di testo **Posizione cache principale**, inserire la posizione aggiornata della cache principale.
4. Nella casella di testo **Posizione cache secondaria**, inserire la posizione aggiornata della cache secondaria.
5. Nella casella di testo **Posizione cache metadati**, inserire la posizione aggiornata della cache dei metadati.

6. Fare clic su **OK**.

   N.B.: È necessario riavviare il servizio Core per rendere effettive le modifiche.

Modifica delle impostazioni del motore

Per modificare le impostazioni del motore:

1. Passare alla Core Console, fare clic su **Configurazione** → **Impostazioni**.
2. Nella sezione **Riesegui configurazione del motore**, fare clic su **Modifica**.

   Viene visualizzata la finestra di dialogo **Riesegui configurazione del motore**.
3. Nella finestra di dialogo **Riesegui configurazione del motore**, specificare l'**indirizzo IP**. Selezionare una delle opzioni riportate di seguito:
   - Per utilizzare l'indirizzo IP preferito dal proprio TCP/IP, fare clic su **Calcolato automaticamente**.
   - Per inserire manualmente un indirizzo IP, fare clic su **Usa un indirizzo IP specifico**.
4. Inserire le informazioni di configurazione come segue:

Casella di testo	Descrizione
Porta preferita	Inserire un numero di porta o accettare l'impostazione predefinita (8007 è la porta predefinita). La porta viene utilizzata per specificare il canale di comunicazione con il motore.
Gruppo amministratori	Inserire un nuovo nome per il gruppo di amministrazione. Il nome predefinito è BUILTIN\Administrators.
Lunghezza I/O asincrono minima	Inserire un valore o scegliere l'impostazione predefinita. Descrive la lunghezza minima asincrona di entrata/uscita. L'impostazione predefinita è 65536.
Dimensione buffer ricezione	Inserire una dimensione in entrata del buffer o accettare l'impostazione predefinita. L'impostazione predefinita è 8192.
Dimensione buffer di invio	Inserire una dimensione di uscita del buffer o accettare l'impostazione predefinita. L'impostazione predefinita è 8192.
Timeout lettura	Inserire un valore di timeout di lettura o scegliere l'impostazione predefinita. L'impostazione predefinita è 00:00:30.
Timeout scrittura	Inserire un valore di timeout di scrittura o scegliere l'impostazione predefinita. L'impostazione predefinita è 00:00:30.

5. Selezionare **Nessun ritardo**.
6. Fare clic su **OK**.

Modifica delle impostazioni di distribuzione

Per modificare le impostazioni di distribuzione:

1. Passare alla Core Console e fare clic sula scheda **Configurazione**, quindi **Impostazioni**.
2. Nel riquadro **Impostazioni di distribuzione**, fare clic su **Modifica**.

   Viene visualizza la finestra di dialogo **Impostazioni di distribuzione**.
3. Nella casella di testo **Nome programma di installazione dell'agente**, inserire il nome del file eseguibile dell'agente. L'impostazione predefinita è AgentWeb. exe.
4. Nella casella di testo **Indirizzo core**, inserire l'indirizzo del core.
5. Nella casella di testo **Timeout di ricezione non riuscita**, inserire il numero di minuti di attesa in assenza di attività prima del timeout.

6. Nella casella di testo **Massimo di installazioni parallele**, inserire un numero massimo di installazioni che possono essere eseguite in parallelo.
7. Selezionare una o entrambe le impostazioni facoltative descritte di seguito:
   - Riavvio automatico dopo l'installazione
   - Protezione dopo distribuzione
8. Fare clic su **OK**.

Modifica delle impostazioni di connessione al database

Per modificare le impostazioni di connessione al database:

1. Passare alla Core Console, fare clic su **Configurazione** → **Impostazioni**.
2. Nella sezione **Impostazioni di connessione al database**, eseguire una delle operazioni riportate di seguito:
   - Per ripristinare la configurazione predefinita, fare clic su **Ripristina impostazioni predefinite**.
   - Per modificare le impostazioni di connessione al database, fare clic su **Modifica**.

   Facendo clic su Modifica, viene visualizzata la finestra di dialogo **Impostazioni di connessione al database**.
3. Inserire le impostazioni per la modifica della connessione al database descritta come segue:

Casella di testo	Descrizione
Nome host	Immettere un nome host per la connessione al database.
Porta	Immettere un numero di porta per la connessione al database.
Nome utente (facoltativo)	Immettere un nome utente per l'accesso e la gestione delle impostazioni di connessione al database. Esso viene utilizzato per specificare le credenziali di accesso per l'accesso alla connessione al database.
Password (facoltativa)	Immettere una password per l'accesso e la gestione delle impostazioni di connessione al database.
Conserva cronologia eventi e processi per, giorni	Immettere il numero di giorni per cui conservare la cronologia eventi e processi per la connessione al database.

4. Fare clic su **Connessione di prova** per verificare le impostazioni.
5. Fare clic su **Salva**.

Gestione degli eventi

Il Core include gruppi predefiniti di eventi, che possono essere utilizzati per notificare agli amministratori eventuali anomalie critiche nel Core o nei processi di backup.

Dalla scheda **Eventi**, è possibile gestire i gruppi di notifica, inviare per e-mail le impostazioni SMTP, le impostazioni del server, i registri con tracciatura abilitata, la configurazione cloud, la riduzione di ripetizione e la conservazione degli eventi.

L'opzione Gruppi di notifica consente di gestire i gruppi di notifica, da cui è possibile:

- Specificare un evento per il quale si desidera generare un avviso per quanto segue:

  - Cluster
  - Connettività
  - Processi
  - Gestione delle licenze
  - Troncatura dei log
  - Archivio
  - Core Service
  - Esportazione
  - Protezione
  - Replica
  - Rollback
- Specificare il tipo di avviso (errore, avvertenza, informativo).
- Specificare la posizione e il destinatario degli avvisi. Le opzioni disponibili sono:
  - Indirizzo di posta elettronica
  - Registri degli eventi Windows
  - Server Syslog
- Specificare una soglia temporale per la ripetizione.
- Specificare il periodo di conservazione di tutti gli eventi.

Configurazione dei gruppi di notifica

Per configurare i gruppi di notifica:

1. Dalla Core Console, selezionare **Configurazione** → **Eventi**.
2. Fare clic su **Aggiungi gruppo**.

   Si apre la finestra di dialogo **Aggiungi gruppo di notifica** e vengono visualizzati due riquadri:
   - **Abilita gli avvisi**
   - **Opzioni di notifica**

Abilitazione degli avvisi

L'abilitazione degli avvisi consente di definire il gruppo di eventi di sistema per cui si desidera registrare, creare rapporti e impostare gli avvisi.

N.B.: Per creare avvisi per tutti gli eventi, selezionare **Tutti gli avvisi**.

- Per creare avvisi specifici per errori, avvertenze e messaggi informativi o una combinazione di questi, selezionare una delle seguenti opzioni:
  - icona triangolare rossa (Errore)
  - icona triangolare gialla (Avvertenza)
  - cerchio blu (Informazioni)
  - freccia curva (Ripristino delle impostazioni predefinite)
- Per creare gli avvisi per eventi specifici fare clic sul simbolo **>** accanto al gruppo scelto, quindi selezionare la casella di controllo per attivare l'avviso.

Configurazione delle opzioni di notifica

1. Nel pannello **Opzioni di notifica**, specificare la modalità di gestione delle notifiche.

   Le opzioni di notifica sono:

Casella di testo	Descrizione
Notifica tramite posta elettronica	Contrassegnare i destinatari della notifica tramite posta elettronica. È possibile inserire più indirizzi di posta elettronica separati, nonché Cc e Ccn, come mostrato di seguito: • **A:** • **Cc:** • **Ccn:**
Notifica tramite registro degli eventi di Windows	Selezionare questa opzione se si desidera che la notifica degli avvisi sia riportata tramite il registro degli eventi di Windows.
Notifica tramite sys logd	Selezionare questa opzione se si desidera che la notifica degli avvisi sia riportata tramite sys logd. Inserire i dettagli del sys logd nelle seguenti caselle di testo: • **Nome host:** • **Porta: 1**
Notifica tramite avvisi Toast	Selezionare questa opzione se si desidera che l'avviso appaia come una finestra pop-up nell'angolo inferiore destro dello schermo.

2. Fare clic su **OK**.

   Viene visualizzato il seguente messaggio: **Il nome del gruppo non può essere modificato dopo la creazione del gruppo di notifica. Utilizzare questo nome?**.

   - Per salvare il nome del gruppo, fare clic su **Sì**.
   - Per modificare il nome del gruppo, fare clic su **No**. Tornare alla finestra **Opzioni di notifica**, aggiornare il nome del gruppo e altre impostazioni di notifica del gruppo e salvare le modifiche apportate.

Configurazione di un server di posta elettronica

N.B.: È necessario configurare le impostazioni di notifica del gruppo, anche abilitando l'opzione **Notifica tramite e-mail**, prima di inviare le e-mail dei messaggi di avviso.

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

1. Dalla Core Console, fare clic su **Configurazione** → **Eventi**.
2. Nel riquadro **Impostazioni di posta elettronica**, fare clic su **Server SMTP**.

   Viene visualizzata la finestra di dialogo **Impostazioni del server SMTP**.
3. Inserire i dettagli del server di posta elettronica come indicato di seguito:

Casella di testo	Descrizione
Server SMTP	Immettere il nome del server di posta elettronica che deve essere utilizzato dal modello di notifica di posta elettronica. La convenzione di denominazione include il nome host, il dominio e il suffisso; ad esempio, **smtp.gmail.com**.

Casella di testo	Descrizione
Da	Immettere un indirizzo di posta elettronica mittente. Esso viene utilizzato per specificare l'indirizzodi posta elettronica mittente per il modello di notifica; ad esempio, **noreply@localhost.com**.
Nome utente	Immettere un nome utente per il server di posta elettronica.
Password	Immettere una password per l'accesso al server di posta elettronica.
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).

4. Fare clic su **Invia e-mail di prova**, eseguire le operazioni riportate di seguito:
   a. Nella finestra di dialogo Invia e-mail di prova, inserire un indirizzo di posta elettronica di destinazione per il messaggio di prova e fare clic su **Invia**.
   b. Se il messaggio di prova non va a buon fine, chiudere la finestra di errore e la finestra **Invia e-mail di prova** e controllare le impostazioni di configurazione del server di posta elettronica. Ripetere il punto 4.
   c. Fare clic su **OK** per confermare.
   d. Verificare che il messaggio di prova sia stato inviato.
   e. Tornare alla finestra di dialogo Impostazioni del server SMTP, fare clic su **Salva** per chiudere la finestra di dialogo e salvare le impostazioni.

Configurazione di un modello di notifica e-mail

Per ricevere notifiche e-mail relative agli eventi è necessario configurare un server di posta elettronica e un modello di notifica e-mail.

N.B.: Per ricevere e-mail dei messaggi di avviso, configurare le impostazioni del gruppo di notifica e attivare l'opzione **Notifica tramite e-mail**.

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

1. Dalla Core Console, fare clic su **Configurazione → Eventi**.
2. Nel riquadro **Impostazioni di posta elettronica**, fare clic su **Modifica**.
   Viene visualizzata la finestra di dialogo **Modifica configurazione della notifica di posta elettronica**.
3. Selezionare **Abilita le notifiche e-mail**, quindi immettere i dettagli per il server e-mail come segue:

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.

4. Fare clic su **Invia e-mail di prova**, eseguire le operazioni riportate di seguito:
   a. Nella finestra di dialogo Invia e-mail di prova, inserire un indirizzo di posta elettronica di destinazione per il messaggio di prova e fare clic su **Invia**.
   b. Se il messaggio di prova non va a buon fine, chiudere la finestra di dialogo di errore e la finestra di dialogo Invia e-mail di prova, fare clic su **OK** per salvare le impostazioni correnti del modello e-mail e modificare le impostazioni del server di posta elettronica, consultare Configurazione di un server di posta elettronica e di un modello di notifica e-mail. Assicurarsi di inserire nuovamente la password dell'account e-mail. Salvare le impostazioni e quindi tornare al punto 4.
   c. Fare clic su **OK** per confermare.
   d. Verificare che il messaggio di prova sia stato inviato.
   e. Tornare alla finestra di dialogo **Modifica configurazione della notifica di posta elettronica**, fare clic su **OK** per chiudere la finestra di dialogo e salvare le impostazioni.

Configurazione della riduzione delle ripetizioni

Per configurare la riduzione di ripetizione:

1. Dalla Core Console, fare clic su **Configurazione** → **Eventi**.
2. Dalla sezione **Riduzione ripetizione**, fare clic su **Modifica**.
   Viene visualizzata la finestra di dialogo **Abilita riduzione della ripetizione** .
3. Selezionare **Abilita riduzione della ripetizione**.
4. Nella casella di testo **Archivia eventi per**, inserire il numero di minuti per archiviare gli eventi per la riduzione della ripetizione.
5. Fare clic su **OK**.

Configurazione della conservazione degli eventi

Per configurare la conservazione degli eventi:

1. Dalla Core Console, fare clic su **Configurazione** → **Impostazioni**.
2. In **Impostazioni di connessione al database**, fare clic su **Modifica**.
   Viene visualizzata la finestra di dialogo**Impostazioni di connessione al database**.
3. Nella casella di testo **Conserva la cronologia eventi e processi per**, inserire il numero di giorni per cui si desidera conservare le informazioni sugli eventi.
   Ad esempio, è possibile selezionare 30 giorni (impostazione predefinita).
4. Fare clic su **Salva**.

Roadmap per la gestione di un repository

Le linee guida per la gestione di un repository coprono attività quali la creazione, la configurazione e visualizzazione di un repository, e includono i seguenti argomenti:

- Creazione di un repository

- Visualizzazione dei dettagli del repository
- Modifica delle impostazioni del repository
- Espansione di un repository esistente
- Aggiunta di una posizione di archiviazione a un repository esistente
- Selezione di un repository
- Eliminazione di un repository
- Ripristino di un repository

N.B.: Si consiglia di utilizzare la scheda **Appliance** per creare o espandere il repository.

Prima di iniziare a utilizzare l'appliance, è necessario impostare il repository nel core server. Un repository archivia i dati protetti. Più specificamente, archivia le istantanee che vengono acquisite dai server protetti nel proprio ambiente.

Configurando il repository è possibile eseguire diverse attività quali specificare dove posizionare l'archiviazione dei dati nel Core server, quante posizioni possono essere aggiunte a ogni repository, il nome del repository, quante operazioni correnti supportano i repository.

Quando si crea un repository, il Core prealloca lo spazio richiesto per l'archiviazione di dati e metadati nella posizione specificata. Per aumentare ulteriormente la dimensione di un repository, è possibile aggiungere nuove posizioni o volumi di archiviazione.

N.B.: L'appliance DL1300 consente di creare un unico repository.

Tutte le versioni di DL1300 supportano l'aggiornamento in-box. La dimensione iniziale del repository disponibile dopo il provisioning dell'archiviazione nell'appliance corrisponde alla versione del sistema. Ad esempio: dopo il provisioning dell'appliance DL1300 da 3 TB+2 VM, la dimensione del repository disponibile è di 3 TB. Lo spazio di archiviazione inutilizzato nel sistema può essere utilizzato per espandere i repository esistenti aggiornando la licenza. Per espandere il repository, consultare Espansione di un repository esistente.

Tabella 1. Dimensioni del repository

Versione	Dimensione iniziale del repository in TB (impostazione predefinita)	Dimensione espandibile del repository in TB
2 TB	2	8
3 TB + 2 VM	3	8
4 TB + 2 VM	4	8

N.B.: Le configurazioni di DL1300 da 4 TB + 2 VM consentono di espandere il repository fino a 18 TB mediante l'acquisto di una licenza appropriata e collegando il contenitore esterno MD 1400.

Creazione di un repository

Per creare un repository:

1. Passare alla Core Console.
2. Fare clic su **Configurazione** → **Repository**.
3. Fare clic su **Aggiungi nuovo**.
   Viene visualizzata la finestra di dialogo **Aggiungi nuovo repository**.

4. Immettere le informazioni come descritto nella seguente tabella.

Casella di testo	Descrizione
Nome repository	Immettere il nome da visualizzare del repository. Per impostazione predefinita, questa casella di testo è costituita dalla parola Repository e un numero di indice che aggiunge in sequenza un numero al nuovo repository a partire da 1. È possibile modificare il nome, a seconda delle necessità. È possibile inserire fino a 150 caratteri.
Operazioni simultanee	Definire il numero di richieste simultanee che si desidera che il repository sia in grado di supportare. Per impostazione predefinita, il valore è 64.
Commenti	Se lo si desidera, inserire una nota descrittiva su questo repository.

5. Per definire il percorso di archiviazione specifico o il volume per il repository, fare clic su **Aggiungi un percorso di archiviazione**.

   ATTENZIONE: Se il repository AppAssure che si sta creando in questa fase è successivamente rimosso, tutti i file nel percorso di archiviazione del repository verranno eliminati. Se non si definisce una cartella dedicata per l'archiviazione dei file del repository, tali file verranno archiviati nella root; l'eliminazione del repository eliminerà anche l'intero contenuto della root, con conseguente perdita di dati irreversibile.

   N.B.: I repository sono archiviati su dispositivi di archiviazione primari. I dispositivi di archiviazione come Data Domain non sono supportati a causa di limitazioni in termini di prestazioni. Analogamente, i repository non devono essere archiviati su filer NAS che dispongono su livelli sul cloud poiché questi dispositivi tendono ad avere limitazioni di prestazioni quando vengono utilizzati come archiviazione primaria.

   Viene visualizzata la finestra di dialogo **Aggiungi un percorso di archiviazione**.

6. Per specificare lo spazio su disco del proprio sistema come nuovo percorso di archiviazione da aggiungere, inserire le informazioni seguenti:

   - Casella di testo Descrizione

     Percorso dei dati — Immettere il percorso in cui archiviare i dati protetti; ad esempio, digitare **X:\Repository\Data**.

     Per specificare il percorso, utilizzare solo caratteri alfanumerici, il trattino e il punto (solo per separare i nomi host e i domini). Le lettere dalla a alla z non rilevano la distinzione tra maiuscole e minuscole. Non utilizzare spazi. Non sono consentiti altri simboli o caratteri di punteggiatura.

     Percorso dei metadati — Immettere il percorso in cui archiviare i metadati protetti; ad esempio, digitare **X:\Repository\Metadata**.

     Per specificare il percorso, utilizzare solo caratteri alfanumerici, il trattino e il punto (solo per separare i nomi host e i domini). Le lettere dalla a alla z non rilevano la distinzione tra maiuscole e minuscole. Non utilizzare spazi. Non sono consentiti altri simboli o caratteri di punteggiatura.

7. Nel riquadro **Dettagli**, fare clic su **Mostra/Nascondi dettagli** e inserire i dettagli per la posizione di archiviazione nel modo descritto come segue:

Casella di testo	Descrizione
Dimensioni	Impostare la dimensione o la capacità per la posizione di archiviazione. Il valore predefinito è 250 MB. È possibile scegliere tra le seguenti opzioni: • MB • GB • TB **N.B.:** La dimensione specificata non può superare la dimensione del volume. **N.B.:** Se la posizione di archiviazione è un volume New Technology File System (NTFS) che utilizza Windows XP o Windows 7, il limite di dimensioni del file è di 16 TB. Se la posizione di archiviazione è un volume NTFS che utilizza Windows 8 o Windows Server 2012, il limite di dimensioni del file è di 256 TB. **N.B.:** Per convalidare il sistema operativo, Strumentazione gestione Windows (WMI) deve essere installato nella posizione di archiviazione desiderata.
Criterio della cache di scrittura	Il criterio della cache di scrittura controlla in che modo viene utilizzato Windows Cache Manager nel repository e contribuisce a mettere a punto il repository per prestazioni ottimali in diverse configurazioni. Impostare il valore su una delle seguenti opzioni: • Attivato • Disattivato • Sincronizza Se il valore è impostato su Attivato, che è l'impostazione predefinita, Windows controlla il caching. **N.B.:** L'impostazione del criterio della cache di scrittura su Attivato può dare come risultato prestazioni più veloci. Se si sta utilizzando una versione di Windows Server precedente a Server 2012, l'impostazione consigliata è **Disattivato**. Se è impostato su **Disattivato**, AppAssure controlla il caching. Se è impostato su **Sincronizza**, Windows controlla il caching, nonché l'input/output sincrono.
Byte per settore	Specificare il numero di byte che si desidera che ogni settore includa. Il valore predefinito è 512.
Byte medi per record	Specificare il numero medio di byte per record. Il valore predefinito è 8192.

8. Fare clic su **Salva**.
   Viene visualizzata la schermata **Repository** per includere i percorsi di archiviazione appena aggiunti.
9. Ripetere la procedura dal punto 4 al punto 7 per aggiungere ulteriori percorsi di archiviazione per il repository.

10. Fare clic su **Crea** per creare il repository.

    Le informazioni sul **Repository** vengono visualizzate nella scheda **Configurazione**.

Visualizzazione dei dettagli del repository

Per visualizzare i dettagli del repository:

1. Passare alla Core Console.
2. Fare clic su **Configurazione → Repository**.
3. Fare clic sull'icona **Impostazioni** accanto al repository del quale si desidera visualizzare i dettagli.
4. Dalla visualizzazione estesa, è possibile eseguire le seguenti azioni:
   - Aggiungere un percorso di archiviazione
   - Controllare un repository
   - Modificare le impostazioni
   - Eliminare un repository

   Vengono visualizzati anche i dettagli del repository e includono i percorsi di archiviazione e le statistiche. I dettagli sul percorso di archiviazione comprendono il percorso metadati, il percorso dati e le dimensioni. Le informazioni sulle statistiche includono:
   - Deduplicazione - Indicato come il numero di riscontri delle deduplicazioni di blocco, mancati riscontri delle deduplicazioni di blocco e rapporto di compressione di blocco.
   - I/O del record - Costituito dal rapporto (MB/s), rapporto di lettura (MB/s) e rapporto di scrittura (MB/s).
   - Motore di archiviazione - Include il rapporto (MB/s), rapporto di lettura (MB/s) e rapporto di scrittura (MB/s).

Modifica delle impostazioni del repository

Dopo aver aggiunto un repository, è possibile modificare le impostazioni del repository, come ad esempio la descrizione o il massimo delle operazioni simultanee. È anche possibile creare una nuova posizione di archiviazione per il repository.

Per modificare le impostazioni del repository:

1. Passare alla Core Console.
2. Fare clic su **Configurazione → Repository**.
3. Fare clic sull'icona Impostazioni accanto alla colonna Rapporto di compressione sotto il pulsante **Azioni**, quindi **Impostazioni**.

   Viene visualizzata la finestra di dialogo **Impostazioni repository**.
4. Modificare le informazioni di repository descritte come segue:

Campo	Descrizione
Nome repository	Rappresenta il nome visualizzato del repository. Per impostazione predefinita, questa casella di testo è costituita dalla parola Repository e da un numero di indice che corrisponde al numero del repository. **N.B.:** Non è possibile modificare il nome del repository.
Descrizione	Se lo si desidera, inserire una nota descrittiva sul repository.

Campo	Descrizione
Massimo di operazioni simultanee	Definire il numero di richieste simultanee che si desidera che il repository sia in grado di supportare.
Abilitare la deduplicazione	Per disattivare la deduplicazione, deselezionare questa casella. Per abilitare la deduplicazione, selezionare questa casella. **N.B.:** La modifica di questa impostazione è valida solo per i backup eseguiti dopo il completamento dell'impostazione. I dati esistenti o i dati replicati da un altro core o importati da un archivio, conservano i valori della deduplicazione in vigore al momento in cui i dati sono stati acquisiti dalla macchina protetta.
Abilita compressione	Per disattivare la compressione, deselezionare questa casella. Per abilitare la compressione, selezionare questa casella. **N.B.:** Questa impostazione si applica solo ai backup eseguiti dopo la modifica dell'impostazione. I dati esistenti, o i dati replicati da un altro core o importati da un archivio, conservano i valori di compressione in vigore al momento in cui i dati sono stati acquisiti dalla macchina protetta.

5. Fare clic su **Salva**.

Espansione di un repository esistente

È possibile utilizzare lo spazio di archiviazione inutilizzato nell'appliance per espandere un repository esistente. Il tipo di licenza acquistata limita lo spazio di archiviazione che può essere utilizzato dallo spazio di archiviazione inutilizzato per espandere un repository esistente.

Solo l'appliance DL1300 4 TB+2 VM consente di espandere dimensioni di repository di 10 TB collegando il contenitore esterno MD1400.

N.B.: È possibile espandere il repository esistente in incrementi di 1 TB o 2 TB aggiornando la licenza. Per aggiornare la licenza, consultare la sezione Modifica di una chiave di licenza.

Per espandere il repository utilizzando lo spazio di archiviazione inutilizzato e il contenitore esterno collegato:

1. Installare l'MD1400 o aggiornare la licenza di prova. Aprire la Core Console e selezionare la scheda **Appliance**, fare clic su **Attività** → **Provisioning**.
2. Nella schermata **Provisioning**, fare clic su **Esegui provisioning** accanto al controller dell'archiviazione esterna.

   Eseguire questo passaggio solo quando si collega un contenitore esterno.
3. Nella schermata **Provisioning**, fare clic su **Espandi** nella colonna **Azione** accanto all'attività di provisioning appropriata.

   Viene visualizzata la finestra di dialogo **Espandi repository**.
4. Nella finestra di dialogo **Espandi repository**, selezionare il repository che si desidera espandere, quindi fare clic su **Espandi**.

   La posizione del nuovo repository viene aggiunta al repository esistente.

Aggiunta di una posizione di archiviazione a un repository esistente

Aggiunta di una posizione di archiviazione consente di definire la posizione in cui si desidera archiviare il repository o volume.

Per aggiungere una posizione di archiviazione a un repository esistente:

1. Fare clic su **>** accanto alla colonna **Stato** del repository per cui si desidera aggiungere una posizione di archiviazione.
2. Fare clic su **Aggiungi posizione di archiviazione**.

   Viene visualizzata la finestra di dialogo **Aggiungi posizione di archiviazione**.
3. Per aumentare lo spazio su disco del sistema come nuova posizione di archiviazione, immettere le informazioni seguenti:

Casella di testo	Descrizione
Percorso metadati	Immettere la posizione in cui archiviare i metadati protetti.
Percorso dati	Immettere la posizione in cui archiviare i dati protetti.

4. Nella sezione **Dettagli**, fare clic su **Mostra/Nascondi dettagli** e immettere i dettagli per la posizione di archiviazione nel modo seguente:

Casella di testo	Descrizione
Dimensione	Impostare la dimensione i capacità della posizione di archiviazione. La dimensione predefinita è 250 MB. È possibile scegliere tra i seguenti: • MB • GB • TB **N.B.:** La dimensione specificata non può superare la dimensione del volume. **N.B.:** Se la posizione di archiviazione è un volume NTFS che usa Windows XP o Window 7, il limite delle dimensioni del file è 16 TB. Se la posizione di archiviazione è un volume NTFS che usa Windows 8 o Windows Server 2012, il limite delle dimensioni del file è 256 TB. **N.B.:** Per convalidare il sistema operativo, WMI deve essere installato nella posizione di archiviazione desiderata.
Criterio della cache in scrittura	Il criterio della cache in scrittura controlla il modo in cui Windows Cache Manager viene usato nel repository e consente di regolare le prestazioni ottimali di tale repository in diverse configurazioni. Impostare il valore su uno dei seguenti: • Attivato • Disattivato • Sincronizza Se impostato su **Attivato**, il valore predefinito, Windows controlla la memorizzazione nella cache.

Casella di testo	Descrizione
	N.B.: Impostando il criterio della cache in scrittura su **Attivato** può comportare prestazioni più rapide, tuttavia l'impostazione consigliata è **Disattivato**. Se impostato su **Disattivato**, AppAssure controlla la memorizzazione nella cache. Se impostato su **Sincronizza**, Windows controlla la memorizzazione nella cache e la sincronizzazione input/output.
Byte per settore	Specificare il numero di byte che ogni settore deve includere. Il valore predefinito è 512.
Media byte per record	Specificare il numero medio di byte per ciascun record. Il valore predefinito è 8192.

5. Fare clic su **Salva**.
   Viene visualizzata la schermata **Repository** per includere la posizione di archiviazione appena aggiunta.
6. Ripetere i Punti da 4 a 7 per aggiungere più posizioni di archiviazione al repository.
7. Fare clic su **OK**.

Controllo di un repository

L'appliance può eseguire un controllo diagnostico di un volume di repository quando si verificano errori. Gli errori del core potrebbero essere causati, tra le altre ragioni, da un arresto improprio o da un guasto hardware.

N.B.: Questa procedura deve essere eseguita solo per scopi diagnostici.

Per controllare un repository:

1. Nella scheda **Configurazione**, fare clic su **Repository**, selezionare **>** accanto al repository che si desidera controllare.
2. Nel riquadro **Azioni**, fare clic su **Controlla**.
   Viene visualizzata la finestra di dialogo **Controlla repository**.
3. Nella finestra di dialogo **Controlla repository**, fare clic su **Controlla**.

   N.B.: Se la verifica non va a buon fine, ripristinare il repository da un archivio.

Eliminazione di un repository

Per eliminare un repository:

1. Nella scheda **Configurazione**, fare clic su **Repository**, selezionare **>** accanto al repository che si desidera eliminare.
2. Nel riquadro **Azioni**, fare clic su **Elimina**.
3. Nella finestra di dialogo **Elimina repository**, fare clic su **Elimina**.

   ATTENZIONE: Quando un repository viene eliminato, i dati in esso contenuti vengono eliminati e non possono essere recuperati.

Quando si elimina un repository, è necessario poi passare attraverso l'Open Manage System Administrator ed eliminare i dischi virtuali che ospitavano il repository. Dopo l'eliminazione dei dischi virtuali, è possibile eseguire nuovamente il provisioning dei dischi e ricreare il repository.

Rimontaggio dei volumi

Le partizioni di archiviazione come repository, archiviazione per le immagini di VM e archiviazione per le immagini di backup di Windows vengono create dopo aver effettuato il provisioning nell'appliance. I percorsi per tali partizioni sono accessibili e visibili per il SO. Tali percorsi sono chiamati punti di montaggio.

Quando si ripristina l'appliance eseguendo un'operazione di ripristino di fabbrica o un'operazione di ripristino di backup di Windows usando RASR, il sistema operativo può perdere i punti di montaggio che erano disponibili prima dell'operazione di ripristino. Se il SO non può recuperare i punti di montaggio assegnati in precedenza, esso ne assegna di casuali. Tali volumi sono accessibili al SO ma non al software AppAssure perché non vi è alcun modo per determinare come sono mappati in punti di montaggio precedenti e quelli nuovi.

Il rimontaggio dei volumi consente di:

- Ripristinare i punti di montaggio e i percorsi ai volumi, in modo che AppAssure Core e gli strumenti dell'appliance possano continuare ad usarli come accadeva prima del ripristino del SO.
- Aggiornare la configurazione dei repository AppAssure Core per garantire che tali repository siano accessibili e possano essere usati per i backup senza interruzioni.

Per rimontare i volumi:

1. Passare alla Core Console.
2. Fare clic su **Appliance** → **Attività**.
3. Fare clic su **Rimonta volumi**.
   I volumi vengono rimontati.

Risoluzione dei volumi esterni

Se un MD1400 sottoposto a provisioning viene spento o disconnesso e poi riacceso, nella Core Console viene visualizzato un evento che indica che l'MD1400 è connesso. Tuttavia nella schermata **Attività** della scheda **Appliance** non compaiono attività che consentano di ripristinarlo. La schermata **Contenitori** riporta l'MD1400 come esterno e i repository nei dischi virtuali esterni sono offline.

Per risolvere i volumi esterni:

1. Dalla Core Console, selezionare la scheda **Appliance** quindi fare clic su **Rimonta volumi**.
   I volumi vengono rimontati.
2. Selezionare la scheda **Configurazione** quindi fare clic su **Repository**.
3. Espandere il repository con l'indicatore di stato rosso selezionando **>** accanto a **Stato**.
4. Per verificare l'integrità del repository, in **Azioni** fare clic su **Controlla**.

Ripristino di un repository

Nel caso in cui l'appliance non riesce ad importare un repository, crea un rapporto dell'errore nella schermata **Attività** con lo stato dell'attività indicato da un cerchio rosso e la descrizione dello stato riporta **Errore, Completato — Eccezione**. Per visualizzare i dettagli dell'errore dalla schermata **Attività**, espandere il dettaglio dell'attività facendo clic su **>** accanto alla colonna **Stato**. **Dettagli stato** riporta che lo stato dell'attività di ripristino è un'eccezione e la colonna **Messaggio d'errore** fornisce ulteriori dettagli relativi alla condizione di errore.

Per ripristinare un repository da uno stato di importazione non riuscita:

1. Passare alla Core Console.

   La schermata **Repository** visualizza il repository non riuscito con un indicatore di stato rosso.
2. Fare clic su **Configurazione** → **Repository**.
3. Espandere il repository non riuscito facendo clic su **>** accanto a **Stato**.
4. Dalla sezione **Azioni**, fare clic su **Controllo**, quindi fare clic su **Sì** per confermare l'esecuzione del controllo.

   L'appliance ripristina il repository.

Ripristino manuale di un repository

Durante il disaster recovery, è stato installato il sistema operativo, scaricata ed eseguita la **Recovery Update Utility**, completata la Configurazione guidata dell'appliance AppAssure e lanciato AppAssure per terminare il processo di ripristino. Tuttavia, breadcrumb incompleti impediscono che il processo **Rimonta Volume** esegua il montaggio dei volumi.

Per ripristinare un repository manualmente:

1. Avviare **Gestione computer**, quindi selezionare **Gestione archiviazione** → **Gestione disco**.
2. Aggiungere una lettera di unità al volume denominato **DL_REPO_xxxx**.
3. Verificare il volume **DL_REPO_xxxx**; annotare la lettera dell'unità, il percorso del file e assicurarsi che un file AppRecoveryCoreConfigurationBackup esista già.
4. Dalla Core Console AppAssure, selezionare la scheda **Configurazione**, quindi selezionare **Ripristina**.
5. Nella casella di testo**Inserisci percorso directory locale**, inserire la lettera dell'unità e il percorso del file nel repository, quindi selezionare l'opzione **Ripristina repository**.
6. Fare clic su **Ripristina**.

   AppAssure ripristina il repository, ma lo stato del repository è rosso.
7. Espandere le informazioni del repository e copiare il percorso dei metadati.
8. Per creare la cartella del punto di montaggio, aprire una finestra PowerShell e digitare il seguente comando:

   md "<percorso metadati>"

   N.B.: Accertarsi di rimuovere la parte \File_x del percorso dei metadati e racchiudere il percorso dei metadati tra virgolette.
9. Da **Gestione computer** → **Gestione archiviazione** → **Gestione disco**, aggiungere il percorso di montaggio al volume.

   N.B.: Accertarsi di rimuovere la parte \File_x del percorso dei metadati.
10. Rimuovere la lettera di unità.
11. Aggiungere le lettere di unità a tutti i volumi DL_VMRSRV_x.
12. Dalla schermata Core Console AppAssure → **Configurazione** → **Ripristino**, fare clic su **Correggi percorso**, quindi fare clic su **Salva**.

    Il repository è tornato online e mostra uno stato verde.

    N.B.: È necessario ripetere la procedura dal punto 9 al punto 12 per ciascun volume **DL_REPO_xxxx**.

Gestione della sicurezza

Il modello DL1300 fornisce potenti crittografie in modo da rendere inaccessibili i backup delle macchine protette. Solo l'utente in possesso della chiave di crittografia può accedere e decrittografare i dati. La crittografia non influisce sulle prestazioni. I concetti e le considerazioni sulla sicurezza delle chiavi sono:

- La crittografia viene eseguita utilizzando AES a 256 bit in modalità CBC (Cipher Block Chaining) che è conforme alla SHA-3.
- La deduplicazione avviene all'interno di un dominio di crittografia per garantire la privacy.
- La crittografia viene eseguita senza impatto sulle prestazioni.
- È possibile aggiungere, rimuovere, importare, esportare, modificare ed eliminare una chiave di crittografia configurata sul Core.

Aggiunta di una chiave di crittografia

Per aggiungere una chiave di crittografia:

1. Nella Core Console, fare clic su **Configurazione** → **Sicurezza**.
2. Dal menu a discesa **Azioni**, fare clic su **Aggiungi chiave di crittografia**.

   Viene visualizzata la finestra di dialogo **Crea chiave di crittografia**.
3. Nella finestra di dialogo **Crea chiave di crittografia**, inserire i dettagli della chiave descritta come indicato di seguito.

Casella di testo	Descrizione
Nome	Immettere un nome per la chiave di crittografia.
Descrizione	Inserire una descrizione della chiave di crittografia, che viene utilizzata per fornire maggiori dettagli della 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.

4. Fare clic su **OK**.

   ATTENZIONE: Si consiglia di proteggere la passphrase. In caso di smarrimento della passphrase, non è possibile recuperare i dati.

Modifica di una chiave di crittografia

Per modificare una chiave di crittografia:

1. Dalla Core Console, fare clic su **Configurazione** → **Sicurezza**.

   Viene visualizzata la schermata **Chiavi di crittografia**.
2. Fare clic su **>** accanto al nome della chiave di crittografia che si desidera modificare, quindi fare clic su **Modifica**.

   Viene visualizzata la finestra di dialogo **Modifica chiave di crittografia**.
3. Nella finestra di dialogo **Modifica chiave di crittografia**, modificare il nome o modificare la descrizione della chiave di crittografia.
4. Fare clic su **OK**.

Modifica della passphrase di una chiave di crittografia

Per modificare una passphrase di una chiave di crittografia:

1. Dalla Core Console, fare clic su **Configurazione** → **Sicurezza**.
2. Fare clic su **>** accanto al nome della chiave di crittografia che si desidera modificare, quindi fare clic su **Modifica passphrase**.

   Viene visualizzata la finestra di dialogo **Modifica passphrase**.
3. Nella finestra di dialogo **Modifica la passphrase**, inserire la nuova passphrase per la crittografia, quindi inserire nuovamente la passphrase per confermare i dati inseriti.
4. Fare clic su **OK**.

   ATTENZIONE: Si consiglia di custodire la passphrase. In caso di smarrimento della passphrase, non sarà possibile accedere ai dati nel sistema.

Importazione di una chiave di crittografia

Per importare una chiave di crittografia:

1. Dalla Core Console, fare clic su **Configurazione** → **Sicurezza**.
2. Dal menu a discesa **Azioni**, fare clic su **Importa**.

   Viene visualizzata la finestra di dialogo **Importa chiave**.
3. Nella finestra di dialogo **Importa chiave**, fare clic su **Sfoglia** per individuare la chiave di crittografia che si desidera importare, quindi fare clic su **Apri**.
4. Fare clic su **OK**.

Esportazione di una chiave di crittografia

Per esportare una chiave di crittografia:

1. Dalla Core Console, fare clic su **Configurazione** → **Sicurezza**.
2. Dal menu a discesa Configurazione, per la chiave di crittografia che si desidera esportare, selezionare **Esporta**.

   Viene visualizzata la finestra di dialogo **Esporta chiave**.
3. Nella finestra di dialogo **Esporta chiave**, fare clic su **Salva file** per salvare e archiviare le chiavi di crittografia in una posizione sicura.
4. Fare clic su **OK**.

Rimozione di una chiave di crittografia

Per rimuovere una chiave di crittografia:

1. Dalla Core Console, fare clic su **Configurazione** → **Sicurezza**.
2. Per visualizzare la chiave di crittografia che si desidera rimuovere, dal menu a discesa Configurazione selezionare **Rimuovi**.

   Viene visualizzata la finestra di dialogo **Rimuovi chiave**.
3. Per rimuovere la chiave di crittografia, nella finestra di dialogo **Rimuovi chiave** fare clic su **OK**.

   N.B.: La rimozione di una chiave di crittografia comporta la decrittografia dei dati.

Gestione degli account cloud

L'appliance DL consente di eseguire il backup dei dati attraverso la creazione di un archivio di backup dei punti di ripristino sul cloud. Con l'appliance DL, è possibile creare, modificare e gestire l'account cloud tramite il provider di archiviazione cloud. È possibile archiviare i dati sul cloud tramite Microsoft Azure, Amazon S3, Rackspace Cloud Block Storage o altri servizi cloud basati su OpenStack. Consultare i seguenti argomenti per gestire gli account cloud:

- Aggiunta di un account cloud
- Modifica di un account cloud
- Configurazione delle impostazioni di account cloud
- Rimuovere un account cloud

Aggiunta di un account cloud

Prima di poter esportare i dati archiviati in un cloud, aggiungere l'account per il proprio provider di servizi cloud nella Core Console.

Per aggiungere un account cloud:

1. Nella Core Console, fare clic sulla scheda **Strumenti**.
2. Nel menu a sinistra, fare clic su **Cloud**.
3. Nella pagina **Cloud**, fare clic su **Aggiungi nuovo account**.
   Si apre la finestra di dialogo **Aggiungi nuovo account**.
4. Selezionare un provider di servizi cloud compatibile dall'elenco a discesa **Tipo cloud**.
5. Immettere i dettagli descritti nella tabella riportata di seguito in base al tipo di cloud selezionato nel punto 4.

Tabella 2. Aggiunta di un account cloud

Tipo di cloud	Casella di testo	Descrizione
Microsoft Azure	Nome account archiviazione	Inserire il nome dell'account di archiviazione di Windows Azure.
	Chiave di accesso	Inserire la chiave di accesso per l'account.
	Nome da visualizzare	Creare un nome da visualizzare per questo account in AppAssure; ad esempio, Windows Azure 1.
Amazon S3	Chiave di accesso	Inserire la chiave di accesso per l'account cloud di Amazon.
	Chiave segreta	Inserire la chiave segreta per questo account.
	Nome da visualizzare	Creare un nome da visualizzare per questo account in AppAssure; ad esempio, Amazon 1.

Tipo di cloud	Casella di testo	Descrizione
Powered by OpenStack	Nome utente	Inserire il nome utente per l'account cloud basato su OpenStack.
	Chiave API	Inserire la chiave API per l'account dell'utente.
	Nome da visualizzare	Creare un nome da visualizzare per questo account in AppAssure; ad esempio, OpenStack 1.
	ID detentore	Inserire l'ID detentore per questo account.
	URL di autenticazione	Inserire l'URL di autenticazione per questo account.
Rackspace Cloud Block Storage	Nome utente	Inserire il nome utente per l'account cloud di Rackspace.
	Chiave API	Inserire la chiave API per questo account.
	Nome da visualizzare	Creare un nome da visualizzare per questo account in AppAssure; ad esempio, Rackspace 1.

6. Fare clic su **Aggiungi**.
   La finestra di dialogo si chiude e l'account viene visualizzato sulla pagina **Cloud** della Core Console.

Modifica di un account cloud

Eseguire i seguenti passaggi per modificare un account nel cloud:

1. Nella Core Console, fare clic sulla scheda **Strumenti**.
2. Nel menu a sinistra, fare clic su **Cloud**.
3. Accanto all'account cloud che si desidera modificare, fare clic sul menu a discesa, quindi fare clic su **Modifica**.
   Si apre la finestra **Modifica account**.
4. Modificare i dettagli come necessario, quindi fare clic su **Salva**.

   N.B.: Non è possibile modificare il tipo di cloud.

Configurazione delle impostazioni dell'account cloud

Le impostazioni di configurazione del cloud consentono di determinare il numero di volte per cui AppAssure può tentare di connettersi all'account cloud dell'utente, e l'intervallo di tempo impiegato in un tentativo prima che vada in timeout.
Per configurare le impostazioni di connessione per l'account cloud dell'utente:

1. Nella Core Console, fare clic sulla scheda **Configurazione**.
2. Nel menu a sinistra, fare clic su **Impostazioni**.

3. Sulla pagina **Impostazioni**, scorrere in basso fino a **Configurazione cloud**.
4. Fare clic sul menu a discesa accanto all'account cloud che si desidera configurare e successivamente effettuare una delle seguenti operazioni:
   - Fare clic su **Modifica**.
     Viene visualizzata la finestra di dialogo **Configurazione cloud**.
     1. Utilizzare le frecce SU e GIÙ per modificare una delle seguenti opzioni:
        - **Timeout richiesta:** visualizzato in minuti e secondi, determina la quantità di tempo che AppAssure deve impiegare in un unico tentativo di connessione all'account cloud quando vi è un ritardo. I tentativi di connessione cesseranno allo scadere della quantità di tempo immessa.
        - **Numero di tentativi:** determina il numero di tentativi che AppAssure deve effettuare prima di determinare che l'account cloud non può essere raggiunto.
        - **Dimensione buffer di scrittura:** determina la dimensione del buffer riservato per la scrittura dei dati archiviati sul cloud.
        - **Dimensione buffer di lettura:** determina la dimensione dei blocchi riservati per la lettura dei dati archiviati dal cloud.
     2. Fare clic su **Avanti**.
   - Fare clic su **Ripristina**. Ripristina la configurazione alle seguenti impostazioni predefinite:
     - **Timeout richiesta:** 01:30 (minuti e secondi)
     - **Numero di tentativi:** 3 (tentativi)

Rimozione di un account cloud

È possibile rimuovere un account cloud, interrompere il servizio cloud, o interromperne l'utilizzo per un core specifico.
Per rimuovere un account cloud:

1. Nella Core Console, fare clic sulla scheda **Strumenti**.
2. Nel menu a sinistra, fare clic su **Cloud**.
3. Accanto all'account cloud che si desidera modificare, fare clic sul menu a discesa, quindi fare clic su **Rimuovi**.
4. Nella finestra **Rimuovi account**, fare clic su **Sì** per confermare la rimozione dell'account.
5. Se l'account cloud è attualmente in uso, una seconda finestra chiede se si desidera ancora rimuoverlo. Fare clic su **Sì** per confermare.

   N.B.: La rimozione di un account attualmente in uso provoca un errore di tutti i processi di archiviazione programmati per questo account.

Monitoraggio di DL1300

È possibile monitorare lo stato dei sottosistemi dell'appliance DL1300 tramite la pagina **Stato generale** nella scheda **Appliance**. La pagina **Stato generale** visualizza un indicatore di stato accanto a ciascun sottosistema, insieme ad una descrizione dello stato di salute del sottosistema.

La pagina Stato generale fornisce inoltre i link agli strumenti di analisi dei dettagli di ciascun sottosistema, che può essere utile per risolvere problemi su avvisi o errori. Il link **Amministratore di sistema**, disponibile per i sottosistemi Appliance Hardware e Storage Hardware, chiede all'utente di accedere all'applicazione Amministratore di sistema utilizzata per la gestione dell'hardware. Per ulteriori informazioni

sull'applicazione Amministratore di sistema, consultare la *Guida dell'utente per amministratore di OpenManage Server* all'indirizzo **dell.com/support/manuals**.

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**.

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.

Aggiornamento dell'appliance

Per aggiornare l'appliance:

1. Scaricare l'utilità di ripristino e aggiornamento **Recovery and Update Utility** da **dell.com/support** nell'appliance DL1300.
2. Copiare l'utility sul desktop dell'appliance ed estrarre i file.
3. Fare doppio clic sull'icona **avviaRUU**.
4. Quando richiesto, fare clic su **Sì** per confermare che nessuno dei processi elencati è in esecuzione.
5. Quando viene visualizzata la schermata della **Recovery and Update Utility**, fare clic su **Start**.
6. Quando viene richiesto di riavviare, fare clic su **OK**.

   Le versioni aggiornate di ruoli e funzioni dei server Windows, ASP .NET MVC3, LSI Provider, applicazioni DL, OpenManage Server Administrator e software AppAssure Core sono installate come parte della Recovery and Update Utility. Inoltre, essa aggiorna anche il contenuto del Rapid Appliance Self Recovery (RASR).

   N.B.: Come parte del processo di aggiornamento del software AppAssure Core, l'utilità di ripristino e aggiornamento invia una notifica della versione di AppAssure attualmente installata e chiede all'utente di confermare se desidera aggiornare il software Core alla versione che è inclusa nell'utilità. I downgrade del software AppAssure Core non sono supportati.
7. Se richiesto, riavviare il sistema.
8. Dopo che tutti i servizi e le applicazioni sono stati installati, fare clic su **Prosegui**.

   Viene avviata la Core Console.

Riparazione dell'appliance

Per riparare l'appliance:

1. Scaricare l'utilità di ripristino e aggiornamento **Recovery and Update Utility** da **dell.com/support** nell'appliance.
2. Copiare l'utility sul desktop dell'appliance ed estrarre i file.
3. Fare doppio clic sull'icona **avviaRUU**.
4. Quando richiesto, fare clic su **Sì** per confermare che nessuno dei processi elencati è in esecuzione.
5. Quando viene visualizzata la schermata della Recovery and Update Utility, fare clic su **Start**.
6. Quando viene richiesto di riavviare, fare clic su **OK**.

   Le versioni aggiornate di ruoli e funzioni dei server Windows, ASP .NET MVC3, LSI Provider, applicazioni DL, OpenManage Server Administrator e software AppAssure Core sono installate come parte della Recovery and Update Utility.
7. Se la versione inclusa nell'utilità è uguale alla versione installata, la Recovery and Update Utility richiede di confermare che si desidera eseguire un'installazione di riparazione. Questo passo può essere saltato se non è necessaria un'installazione di riparazione di AppAssure Core.
8. Se la versione inclusa nell'utilità è superiore alla versione installata, la Recovery and Update Utility richiede di confermare che si desidera aggiornare il software AppAssure Core.

   N.B.: I downgrade del software AppAssure Core non sono supportati.
9. Se richiesto, riavviare il sistema.
10. Dopo che tutti i servizi e le applicazioni sono stati installati, fare clic su **Prosegui**.

Se il sistema deve essere configurato nuovamente dopo la riparazione verrà avviata la Configurazione guidata dell'appliance AppAssure, altrimenti verrà avviata la Core Console.

3

Gestione dell'appliance

La Core Console contiene una scheda **Appliance**, che è possibile utilizzare per eseguire il provisioning dello spazio, il monitoraggio dello stato dell'appliance e l'accesso agli strumenti di gestione.

Monitoraggio dello stato dell'appliance

È possibile monitorare lo stato dei sottosistemi dell'Appliance tramite la pagina **Stato generale** nella scheda **Appliance**. La pagina **Stato generale** visualizza un indicatore di stato accanto a ciascun sottosistema, insieme ad una descrizione dello stato di salute del sottosistema.

La pagina Stato generale fornisce anche i collegamenti agli strumenti che analizzano i dettagli di ciascun sottosistema, che possono essere utili per la risoluzione di avvisi o errori. Il collegamento **Amministratore di sistema**, disponibile per i sottosistemi Appliance Hardware e Storage Hardware, richiede all'utente di accedere all'applicazione Amministratore di sistema utilizzata per la gestione dell'hardware. Per ulteriori informazioni sull'applicazione Amministratore di sistema, consultare la *Guida dell'utente di OpenManage Server Administrator* su **dell.com/support/home**. Il collegamento **Stato provisioning**, disponibile per il sottosistema Storage Provisioning, apre la schermata **Attività** che visualizza lo stato di provisioning del sottosistema. Se lo spazio di archiviazione è disponibile per il provisioning, viene visualizzato un collegamento a **Esegui provisioning** in **Azioni** accanto all'attività provisioning.

Provisioning dell'archiviazione

L'appliance configura l'archiviazione interna disponibile per:

- Repository AppAssure

  N.B.: Il processo di creazione dei repository è manuale. La creazione di un repository da parte di AppAssure non avverrà automaticamente nella directory root. Per ulteriori informazioni, consultare la *Dell1300 Appliance Deployment Guide* (Guida alla distribuzione dell'appliance Dell1300).
- Standby virtuale dei computer protetti

N.B.: Il provisioning dello spazio per le VM in standby virtuale può essere eseguito solo in sistemi DL1300 3 TB+2 VM e DL1300 4 TB+2 VM.

Durante il provisioning dei sistemi VM DL1300, è possibile allocare qualsiasi percentuale dello spazio di archiviazione disponibile dopo la creazione di un repository per l'hosting delle VM. La capacità stimata della VM per la versione DL1300 3 TB+2 VM e DL1300 4 TB+2 VM è 2,7 TB. Utilizzando lo Storage Resource Management (SRM), è possibile allocare qualsiasi percentuale di tale spazio per l'hosting delle macchine virtuali. Utilizzando la funzione Live Recovery di AppAssure, è possibile utilizzare queste macchine virtuali per sostituire rapidamente qualsiasi server danneggiato che l'appliance protegge.

Quando si seleziona la scheda **Appliance**, il software AppAssure Appliance individua lo spazio di archiviazione disponibile per tutti i controller supportati nel sistema e verifica che l'hardware soddisfi i requisiti.

Per completare il provisioning del disco per tutte le unità di archiviazione disponibili:

1. Nella scheda **Appliance**, fare clic su **Attività** → **Provisioning**.
   La schermata **Provisioning** visualizza la capacità stimata per il provisioning. Questa capacità viene utilizzata per creare un repository AppAssure.

   ATTENZIONE: Prima di procedere, verificare di aver seguito i punti da 2 a 4 in questa procedura.
2. Aprire la finestra **Provisioning dell'archiviazione** facendo clic su **Esegui provisioning** nella colonna Azione accanto al sistema di archiviazione per cui si vuole eseguire il provisioning.
3. Nella sezione **Riserva di archiviazione opzionale**, selezionare la casella di controllo accanto a **Allocare una porzione di archiviazione in corso di provisioning per le macchine virtuali in standby o per altre finalità** e specificare una percentuale di archiviazione da allocare.
4. Fare clic su **Esegui provisioning**.
   Vengono creati il repository e la partizione in standby della VM.

Provisioning delle unità di archiviazione selezionate

Per eseguire il provisioning dell'archiviazione selezionata:

1. Nella scheda **Appliance**, fare clic su **Attività** → **Provisioning**.
   La schermata **Provisioning** mostra la capacità stimata per il provisioning. Questa capacità viene utilizzata per creare un nuovo repository di AppAssure.
2. Per eseguire il provisioning solo di una porzione dello spazio disponibile, fare clic su **Esegui provisioning** in **Azioni** accanto allo spazio di archiviazione di cui si desidera eseguire il provisioning.
   - Per creare un nuovo repository, selezionare **Crea un nuovo repository**, e fornire un nome per il repository.
     Come impostazione predefinita, Repository 1 appare come nome del repository. È possibile scegliere di sovrascrivere il nome.
   - Per aggiungere capacità a un repository esistente, selezionare **Espandi il repository esistente**, quindi selezionare il repository dall'elenco **Repository esistenti**.

   N.B.: Per aggiungere capacità, si consiglia di espandere un repository esistente invece di aggiungere un repository. I repository separati non sfruttano la capacità in maniera efficiente poiché la deduplicazione non può avvenire su repository separati.
3. In **Riserva di archiviazione opzionale**, selezionare **Allocare una porzione di archiviazione in corso di provisioning per le macchine virtuali in standby o per altre finalità**, quindi specificare la percentuale di archiviazione da allocare per le macchine virtuali.
4. Fare clic su **Esegui provisioning**.
   Il provisioning del disco viene avviato e viene visualizzato lo stato della creazione del repository di AppAssure nell'area **Stato** della schermata **Attività**. Lo **Stato** visualizza **Provisioning effettuato**.
5. Per visualizzare i dettagli dopo il completamento del provisioning del disco, fare clic su **>** accanto all'indicatore di stato.
   La pagina **Attività** si espande e mostra i dettagli di stato, repository e disco virtuale (se allocato).

Eliminare l'allocazione dello spazio di un disco virtuale

Prima di iniziare questa procedura, specificare quale disco virtuale si desidera eliminare. Dalla Core Console, selezionare la scheda **Appliance**, fare clic su **Attività**, quindi espandere il repository che contiene i dischi virtuali per visualizzare i dettagli del disco virtuale.
Per eliminare l'allocazione dello spazio di un disco virtuale:

1. Dall'applicazione OpenManage Server Administrator, espandere **Archiviazione**.
2. Espandere il controller che ospita il disco virtuale, quindi selezionare **Dischi virtuali**.
3. Selezionare il disco virtuale che si desidera rimuovere, quindi selezionare **Elimina** dal menu a discesa **Attività**.
4. Dopo aver confermato l'eliminazione, lo spazio viene visualizzato nella schermata **Attività** della scheda **Appliance** della Core Console come disponibile per il provisioning.

Risoluzione delle attività non riuscite

AppAssure riporta le attività di verifica, provisioning e di recupero non riuscite con un evento sulla home page della Core Console e anche sulla schermata **Attività** della scheda **Appliance**.

Per sapere come risolvere un'attività non riuscita, selezionare la scheda **Appliance** quindi fare clic su **Attività**. Espandere l'attività non riuscita facendo clic su **>** accanto a **Stato** e rivedere i messaggi di errore e l'operazione consigliata.

4

Protezione di workstation e server

Informazioni sulla protezione di workstation e server

Per proteggere i dati utilizzando DL1300, aggiungere le workstation e i server che si desidera proteggere nella Core Console; ad esempio, il server Exchange, SQL Server o il server Linux.

N.B.: In questo capitolo, la parola *macchina* si riferisce anche al software AppAssure Agent installato nella macchina.

Nella Core Console, è possibile individuare la macchina su cui è installato un software AppAssure Agent e specificare quali volumi proteggere, definire le pianificaizoni di protezione, aggiungere ulteriori misure di sicurezza, ad esempio la crittografia, e altro ancora. Per ulteriori informazioni su come accedere alla Core Console per la protezione delle workstation e dei server, consultare Protezione di una macchina.

Distribuzione di un agente (installazione push)

Il DL1300 permette la distribuzione del programma di installazione dell'agente AppAssure su singole macchine Windows per la protezione. Completare i passaggi seguenti per portare il programma di installazione a un agente. Per distribuire gli agenti su più macchine contemporaneamente, consultare Distribuzione in più macchine.

N.B.: Gli agenti devono essere configurati con un criterio di sicurezza che rende possibile l'installazione in modalità remota.

Per distribuire un agente:

1. Dall'area di navigazione sinistra della Core Console, fare clic su **Macchine protette**.
2. Fare clic su **Azioni** → **Distribuisci agente**.
   Viene visualizzata la finestra di dialogo **Distribuisci agente**.
3. Nella finestra di dialogo **Distribuisci agente**, inserire le impostazioni di accesso come descritto nella tabella riportata di seguito.

Casella di testo	Descrizione
Macchina	Inserire il nome host o l'indirizzo IP della macchina che si desidera distribuire.
Nome utente	Inserire il nome utente per collegarsi alla macchina (ad esempio, amministratore).
Password	Inserire la password per collegarsi alla macchina.
Riavvio automatico dopo l'installazione	Selezionare questa opzione per specificare se il Core deve avviarsi al completamento della distribuzione e installazione del programma di installazione dell'agente AppAssure.

4. Fare clic su **Verifica** per verificare le credenziali specificate.
   La finestra di dialogo **Distribuisci agente** visualizza un messaggio che indica che la verifica è in corso.

5. Fare clic su **Interrompi** se si desidera annullare il processo di verifica.

   Al termine del processo di verifica, viene visualizzato un messaggio che indica che la verifica è stata completata.
6. Fare clic su **Distribuisci**.

   Viene visualizzato un messaggio che indica che la distribuzione è stata avviata. È possibile visualizzare lo stato nella scheda **Eventi**.
7. Fare clic su **Mostra dettagli** per visualizzare ulteriori informazioni sullo stato di distribuzione dell'agente.
8. Fare clic su **OK**.

Protezione di una macchina

Questo argomento descrive il modo in cui iniziare a proteggere i dati in una macchina specificata dall'utente.

N.B.: Per essere protetta, la macchina deve avere il software AppAssure Agent installato. È possibile scegliere di installare tale software prima di seguire questa procedura, oppure è possibile distribuire il software all'agente quando si definisce la modalità di protezione nella finestra di dialogo **Connessione**. Per installare il software AppAssure Agent durante il processo di impostazione della protezione di una macchina, consultare Distribuzione del software dell'agente durante la protezione di un agente.

Quando si aggiunge la protezione, è necessario specificare il nome o l'indirizzo IP della macchina da proteggere e dei volumi da proteggere in tale macchina, come anche definire la pianificazione di protezione per ciascun volume.

Per proteggere più macchine contemporaneamente, consultare Protezione di più macchine.

Per proteggere una macchina:

1. Riavviare la macchina in cui è installato il software AppAssure Agent, se non lo si è ancora fatto.
2. Dalla Core Console nella macchina core, fare clic su **Proteggi** → **Proteggi macchina** sulla barra dei pulsanti.

   Viene visualizzata la **Protezione guidata della macchina**.
3. Nella pagina **Introduzione**, selezionare le opzioni di installazione appropriate:
   - Se non è necessario definire un repository o stabilire la crittografia, selezionare **Tipica**.
   - Se non si desidera visualizzare la pagina **Introduzione** per la **Protezione guidata della macchina** in futuro, selezionare l'opzione **Ignora la pagina Introduzione alla prossima apertura della procedura guidata**.
4. Fare clic su **Avanti**.
5. Nella pagina **Connessione**, immettere le informazioni sulla macchina a cui si desidera effettuare la connessione nel modo descritto nella tabella seguente.

Casella di testo	Descrizione
Host	Nome host o indirizzo IP della macchina che si desidera proteggere.
Porta	Numero di porta tramite cui il Core AppAssure comunica con l'agente sulla macchina. Il numero della porta predefinita è 8006.
Nome utente	Nome utente utilizzato per connettersi a questa macchina, ad esempio amministratore.

Casella di testo	Descrizione
Password	Password utilizzata per connettersi a questa macchina.

6. Fare clic su **Avanti**. Se viene visualizzata la pagina **Protezione** accanto alla **Protezione guidata della macchina**, passare al punto 7.

   N.B.: Se viene visualizzata la pagina **Installa agente** accanto alla **Protezione guidata della macchina**, significa che il software dell'agente non è stato ancora installato nella macchina designata. Fare clic su **Avanti** per installare il software dell'agente. Tale software deve essere installato nella macchina da proteggere, che dovrà essere riavviata prima di poter effettuare il backup nel Core. Affinché il programma di installazione riavvii la macchina dell'agente, selezionare l'opzione **Dopo l'installazione, riavviare la macchina automaticamente (scelta consigliata)** prima di selezionare **Avanti**.

7. In questo campo di testo viene visualizzato il nome host o indirizzo IP specificato nella finestra di dialogo **Connetti**. Facoltativamente, immettere un nuovo nome per la macchina da visualizzare nella Core Console.
8. Selezionare la pianificazione di protezione appropriata:
   - Per usare la pianificazione di protezione predefinita, nell'opzione **Impostazioni di pianificazione**, selezionare **Protezione predefinita (istantanee di 3 ore di tutti i volumi)**. Con una pianificazione di protezione predefinita, il Core effettuerà istantanee della macchina dell'agente ogni 3 ore. Tali istantanee possono essere effettuate ogni ora (minimo). Per modificare le impostazioni di protezione in qualsiasi momento dopo aver chiuso la procedura guidata, inclusa la selezione dei volumi da proteggere, andare alla scheda Riepilogo della macchina specifica dell'agente.
   - Per definire una pianificazione di protezione diversa, nell'opzione **Impostazioni di pianificazione** selezionare **Protezione personalizzata**.
9. Selezionare una delle seguenti:
   - Se è stata selezionata la configurazione Tipica dalla **Protezione guidata della macchina** ed è stata specificata la protezione predefinita, fare clic su **Fine** per confermare le scelte, chiudere la procedura guidata e proteggere la macchina specificata.
   - La prima volta in cui viene aggiunta la protezione per una macchina, un'immagine di base (cioè un'istantanea di tutti i dati nei volumi protetti) viene trasferita al repository nell'AppAssure Core in base alla pianificazione definita dall'utente, salvo specificato di sospendere inizialmente la protezione.
   - Se è stata selezionata una configurazione Tipica per la **Protezione guidata della macchina** ed è stata specificata la protezione personalizzata, fare clic su **Avanti** per impostare una pianificazione di protezione personalizzata. Per dettagli su come definire una pianificazione di protezione personalizzata, consultare Creazione di pianificazioni di protezione personalizzate.
   - Se è stata selezionata la configurazione Avanzata per la **Protezione guidata della macchina** e la protezione predefinita, fare clic su **Avanti** e passare al punto 12 per visualizzare le opzioni di repository e crittografia.
   - Se è stata selezionata la configurazione Avanzata per la **Protezione guidata della macchina** ed è stata specificata la protezione personalizzata, fare clic su **Avanti** e passare al punto 10 per scegliere quali volumi proteggere.
10. Nella pagina **Protezione volumi**, selezionare i volumi nella macchina dell'agente da proteggere. Se sono elencati volumi che non si desidera proteggere, fare clic nella colonna Seleziona per annullare la selezione. Successivamente, fare clic su **Avanti**.

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

11. Nella pagina **Pianificazione di protezione**, definire una pianificazione di protezione personalizzata.
12. Nella pagina **Repository** selezionare **Usa un repository esistente**.
13. Fare clic su **Avanti**.

    Viene visualizzata la pagina **Crittografia**.

14. In alternativa, per abilitare la crittografia, nella pagina **Crittografia** selezionare **Abilita crittografia**.

    I campi di **Chiave di crittografia** vengono visualizzati nella pagina **Crittografia**.

    N.B.: Se si abilita la crittografia, essa verrà applicata ai dati di tutti i volumi protetti per questa macchina dell'agente. È possibile modificare le impostazioni in un secondo momento dalla scheda **Configurazione** nella Core Console.

    ATTENZIONE: AppAssure utilizza la crittografia AES a 256 bit in modalità Cipher Block Chaining (CBC) con chiavi a 256 bit. Sebbene l'utilizzo della crittografia sia facoltativo, Dell consiglia vivamente di stabilire una chiave di crittografia e di proteggere la passphrase definita. Archiviare la passphrase in un percorso sicuro in quanto è essenziale per il ripristino dei dati. Senza una passphrase, infatti, il ripristino dei dati non è eseguibile.

15. Immettere le informazioni come indicato nella tabella seguente per aggiungere una chiave di crittografia al Core.

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

16. Fare clic su **Fine** per salvare e applicare le impostazioni.

    La prima volta in cui viene aggiunta la protezione per una macchina, un'immagine di base (cioè un'istantanea di tutti i dati nei volumi protetti) viene trasferita al repository nel Core in base alla pianificazione definita dall'utente, salvo specificato di sospendere inizialmente la protezione.

Sospensione e ripresa della protezione

Quando si sospende la protezione, si interrompono temporaneamente tutti i trasferimenti di dati dalla macchina corrente.

Per sospendere la protezione:

1. Nella Core Console, fare clic sul menu a discesa **Macchine protette** nell'area di navigazione a sinistra.
2. Selezionare **Sospendi protezione** della macchina della quale si desidera sospendere la protezione.

   Viene visualizzata la finestra di dialogo **Sospendi protezione**.
3. Selezionare una delle seguenti opzioni e fare clic su **OK**.
   - Se si desidera sospendere la protezione fino a quando non si desidera riprenderla, selezionare **Sospendi fino a ripresa**.
   - Se si desidera sospendere la protezione per un periodo specificato, selezionare **Sospendi per** , quindi nei campi giorni, ore e minuti digitare o selezionare il periodo di sospensione appropriato in base alle esigenze.

   N.B.: Per riprendere la protezione selezionare **Riprendi protezione** dal menu a discesa **Macchine protette**.

Distribuzione del software dell'agente quando si protegge un agente

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. Fare clic su **Macchine protette** nel riquadro di navigazione sinistro.
2. Fare clic su **Azioni** → **Distribuisci agente**.
   Viene visualizzata la finestra di dialogo **Distribuisci agente**.
3. Immettere impostazioni di accesso e protezione come indicato di seguito:
   - **Nome host** - Specifica il nome host o l'indirizzo IP della macchina che si desidera proteggere.
   - **Nome utente** - Specifica il nome utente utilizzato per connettersi a questa macchina, ad esempio amministratore.
   - **Password** - Specifica la password utilizzata per connettersi a questo computer.
   - **Proteggi macchina dopo l'installazione** - Selezionando questa opzione si consente ad AppAssure di eseguire un'istantanea di base dei dati dopo aver aggiunto la macchina per la protezione. Questa opzione è selezionata per impostazione predefinita. Se si deseleziona questa opzione, è quindi necessario forzare manualmente un'istantanea quando si è pronti per avviare la protezione dei dati.
   - **Nome visualizzato** - Specifica un nome per la macchina che viene visualizzato nella Core Console. Il nome visualizzato potrebbe essere lo stesso valore del nome dell'host.
   - **Porta** - Specifica il numero di porta tramite cui il Core comunica con l'agente sulla macchina. Il valore predefinito è 8006.
   - **Repository** - Selezionare il repository in cui archiviare i dati da questo agente.

     N.B.: È possibile archiviare i dati provenienti da più agenti in un unico repository.
   - **Chiave di crittografia** - Specifica se la crittografia deve essere applicata ai dati per ogni volume presente su questa macchina che deve essere archiviato nel repository.

     N.B.: È possibile definire le impostazioni di crittografia per un repository nella scheda **Configurazione** nella Core Console.
4. 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 protette.

Informazioni sulle pianificazioni di protezione

Una pianificazione di protezione definisce quando i backup vengono trasferiti da macchine dell'agente all'AppAssure Core.

Le pianificazioni di protezione vengono inizialmente definite usando la **Protezione guidata della macchina** o la **Protezione guidata di più macchine**. È poi possibile modificare la pianificazione esistente in qualsiasi momento dalla scheda Riepilogo di una macchina dell'agente specifica.

AppAssure fornisce una pianificazione di protezione predefinita, con due periodi di protezione definiti. Il primo periodo è per i giorni della settimana (dal lunedì al venerdì), con un unico periodo di tempo definito (dalle 12:00 AM alle 11:59 PM). L'intervallo predefinito (il periodo di tempo tra le istantanee) è di 3 ore. Il secondo periodo è per i fine settimana (sabato e domenica). L'intervallo predefinito per il secondo periodo è di 3 ore.

Quando la protezione viene abilitata per la prima volta, viene attivata la pianificazione. In questo modo, usando le impostazioni predefinite, indipendentemente dall'ora del giorno il primo backup viene eseguito ogni 3 ore.

Il primo trasferimento di backup salvato nel Core è chiamato istantanea dell'immagine di base. Tutti i dati presenti in tutti i volumi specificati (inclusi sistema operativo, applicazioni e impostazioni) vengono salvati nel Core. Successivamente, le istantanee incrementali (backup di dimensioni inferiori costituiti solo dai dati cambiati nell'agente dall'ultimo backup) vengono salvate nel Core regolarmente in base all'intervallo definito.

È possibile creare una pianificazione personalizzata per modificare la frequenza dei backup. Ad esempio, è possibile modificare l'intervallo per il periodo del giorno della settimana a 60 minuti, avendo quindi istantanee ogni ora. Oppure è possibile aumentare l'intervallo durante il fine settimana da 60 minuti a 180 minuti, avendo quindi istantanee ogni tre ore quando il traffico è ridotto.

Altre opzioni nella pagina **Pianificazione di protezione guidata** includono l'impostazione di un'ora di protezione quotidiana. In questo modo viene eseguito un backup quotidiano nel periodo definito (l'impostazione predefinita è 12:00 PM).

L'opzione di sospendere inizialmente la protezione impedisce l'esecuzione di un'immagine di base (e, di fatto, impedisce tutti i backup) finché si riprende espressamente la protezione. Quando l'utente decide di iniziare a proteggere le proprie macchine in base alla pianificazione di protezione stabilita, deve riprendere espressamente la protezione.

Creazione di pianificazioni personalizzate

1. Nella pagina **Pianificazione di protezione** di **Proteggi macchina** o **Protezione guidata di più macchine**, per modificare l'intervallo di pianificazione di qualsiasi periodo, seguire le istruzioni riportate di seguito:
   a. Selezionare **Periodi**.

      Vengono visualizzati i periodi esistenti che possono essere modificati. I campi modificabili sono l'ora di inizio, l'ora di fine e l'intervallo (in minuti) per ciascun periodo.
   b. Fare clic nel campo intervallo e digitare un intervallo appropriato in minuti.

      Ad esempio, evidenziare l'intervallo esistente e sostituirlo con il valore **60** per eseguire un'istantanea ogni 60 minuti in questo periodo.
2. Per creare un periodo di punta e non di punta per i giorni feriali, modificare l'intervallo di tempo del periodo feriale in modo da non includere un periodo di 24 ore, impostare un intervallo ottimale per i picchi, selezionare **Esegui istantanee per il restante tempo** e impostare un intervallo non di punta, effettuando le operazioni riportate di seguito:
   a. Selezionare **Periodi**.

      Vengono visualizzati i periodi esistenti che possono essere modificati.
   b. Fare clic nella casella **Da** per modificare l'ora di inizio per il periodo.

      Viene visualizzata la finestra di dialogo **Scegli orario**.
   c. Selezionare con lo slider le ore e i minuti per il tempo di inizio desiderato, quindi fare clic su **Fine**. Per specificare l'ora corrente, fare clic su **Ora**.
   d. Fare clic nella casella **A** per modificare l'ora di fine per il periodo.

      Viene visualizzata la finestra di dialogo **Scegli orario**.
   e. Selezionare con lo slider le ore e i minuti per il tempo di inizio desiderato, quindi fare clic su **Fine**. Per specificare l'ora corrente, fare clic su **Ora**.
3. Per impostare un unico momento della giornata per un singolo backup giornaliero, selezionare **Orario di protezione giornaliero** quindi inserire l'orario nel formato HH:MM AM.

4. Per definire la pianificazione senza effettuare backup iniziali, selezionare **Sospendi inizialmente protezione**.

   La sospensione della protezione dalla procedura guidata rimane tale fino ad esplicita ripresa della protezione. Una volta ripresa la protezione, i backup verranno eseguiti in base alla pianificazione stabilita.
5. Fare clic su **Fine** o **Avanti**.

Modifica delle pianificazioni di protezione

È possibile modificare le pianificazioni di protezione per volumi specifici su una macchina.

Per modificare le pianificazioni di protezione:

1. Nella Core Console, selezionare la macchina con una pianificazione di protezione definita che si desidera modificare.

   Viene visualizzata la scheda Riepilogo per la macchina.
2. Selezionare i volumi della macchina protetta che si desidera modificare, quindi fare clic su **Impostare una pianificazione**. Per selezionare tutti i volumi in una sola volta, fare clic sulla casella di controllo nella riga dell'intestazione.

   Inizialmente, tutti i volumi condividono la stessa pianificazione di protezione. In genere, è buona norma proteggere, come minimo, il volume di sistema riservato e il volume con il sistema operativo (in genere l'unità C).

   Viene visualizzata la finestra di dialogo **Pianificazione di protezione**.
3. Nella finestra di dialogo **Pianificazione di protezione**, se in precedenza è stato creato un modello di pianificazione di protezione e si desidera applicarlo a questo agente, selezionare il modello dall'elenco a discesa, quindi andare al punto 9.
4. Se si desidera salvare la nuova pianificazione di protezione come un modello, inserire un nome per il modello nella casella di testo.
5. Se si desidera rimuovere un determinato periodo di tempo dalla pianificazione, deselezionare le caselle di controllo accanto a ciascuna opzione di periodo di tempo. Le opzioni includono quanto segue:
   - **Lun - Ven** Questo intervallo di tempo indica una tipica settimana di lavoro di cinque giorni.
   - **Sab - Dom** Questo intervallo di tempo indica un tipico fine settimana.
6. Se gli orari di inizio e di fine dei giorni della settimana sono dalle 12:00 alle 23:59, allora esiste un singolo periodo. Per modificare l'ora di inizio o di fine di un periodo definito, effettuare le operazioni riportate di seguito:
   a. Selezionare il periodo di tempo appropriato.
   b. Fare clic sulla casella **Ora di inizio** per modificare l'ora di inizio per questo periodo.
   c. Trascinare i cursori delle ore e dei minuti come appropriato per l'ora di inizio desiderata, quindi fare clic su **Fine**. Per specificare l'ora corrente, fare clic su **Ora**.
   d. Fare clic sulla casella **Ora di fine** per modificare l'ora di fine per questo periodo.

      Viene visualizzata la finestra di dialogo **Scegli l'ora**.
   e. Trascinare i cursori delle ore e dei minuti come appropriato per l'ora di inizio desiderata, quindi fare clic su **Fine**. Per specificare l'ora corrente, fare clic su **Ora**.
   f. Modificare l'intervallo in base alle proprie esigenze. Ad esempio, se si definisce un periodo di picco, modificare l'intervallo da 60 minuti a 20 minuti per acquisire istantanee tre volte su base oraria.
7. Se è stato definito un periodo diverso da dalle 12:00 alle 23:59 nel punto 6, e si desidera che vengano eseguiti i backup negli intervalli di tempo rimanenti, è necessario aggiungere ulteriori periodi per definire la protezione effettuando le operazioni riportate di seguito:

a. Fare clic su **+ Aggiungi periodo**.

   Nella categoria appropriata (giorni della settimana o fine settimana), viene visualizzato un nuovo periodo di tempo. Se il primo periodo è iniziato dopo le 12:00, allora AppAssure avvia automaticamente questo periodo alle 12:00. Secondo l'esempio di cui sopra, questo secondo periodo inizia alle 12:00. Potrebbe essere necessario regolare ore o minuti per gli orari di inizio e di fine.

b. Trascinare i cursori delle ore e dei minuti come appropriato per l'ora di inizio e di fine desiderata, in base alle proprie esigenze.

c. Modificare l'intervallo in base alle proprie esigenze. Ad esempio, se si definisce un periodo non di picco, modificare l'intervallo da 60 minuti a 120 minuti per acquisire istantanee ogni due ore.

8. Se necessario, continuare a creare ulteriori periodi, impostando le ore di inizio e fine e gli intervalli in base alle proprie esigenze.

   N.B.: Se si desidera rimuovere un periodo che è stato aggiunto, fare clic sulla **X** all'estrema destra di tale periodo. Se si rimuove un periodo per errore, è possibile fare clic su **Annulla**.

9. Quando la pianificazione di protezione soddisfa i propri requisiti, fare clic su **Applica**.

   La finestra di dialogo **Pianificazione di protezione** viene chiusa.

Configurazione delle impostazioni della macchina protetta

Dopo aver aggiunto le protezioni per le macchine in AppAssure, è possibile modificare le impostazioni di base della configurazione della macchina (come il nome e il nome host), le impostazioni di protezione (modifica del programma di protezione per i volumi sulla macchina, aggiunta o rimozione di volumi, o sospensione protezione) e altro ancora.

Visualizzazione e modifica delle impostazioni di configurazione

Per visualizzare e modificare le impostazioni di configurazione:

1. Dalla Core Console, passare alla macchina che si desidera modificare.
2. Fare clic su **Configurazione** → **Impostazioni**.
3. Fare clic su **Modifica** per modificare le impostazioni della macchina come descritto nella tabella riportata di seguito.

Casella di testo	Descrizione
Nome visualizzato	Immettere un nome da visualizzare per la macchina. Un nome per la macchina da visualizzare nella Core Console. Per impostazione predefinita, questo è il nome host della macchina. È possibile modificare il nome visualizzato in qualcosa di più intuitivo, se necessario.
Nome host	Immettere un nome host per la macchina.
Porta	Immettere un numero di porta per la macchina. Il core utilizza la porta predefinita 8006 per comunicare con la macchina.

Casella di testo	Descrizione
Chiave di crittografia	Modificare la chiave di crittografia, se necessario. Specifica se la crittografia viene applicata ai dati per ogni volume sulla macchina archiviato nel repository.
Repository	Selezionare un repository per i punti di ripristino. Visualizza il repository nel Core in cui archiviare i dati da questa macchina. N.B.: Questa impostazione può essere modificata solo se non vi sono punti di ripristino o manca il repository precedente.

Visualizzazione delle informazioni di sistema di una macchina

La Core Console visualizza tutte le macchine che sono protette.

Per visualizzare le informazioni di sistema di una macchina:

1. Nell'area di navigazione a sinistra della Core Console, in **Macchine protette**, selezionare la macchina per visualizzare informazioni dettagliate di sistema.
2. Fare clic sulla scheda **Strumenti**.

   Viene visualizzata la scheda Informazioni di sistema che elenca:

   - Nome host
   - Versione del SO
   - Architettura del SO
   - Memoria (fisica)
   - Nome visualizzato
   - Nome completo del dominio
   - Tipo di macchina virtuale (se applicabile)

   Le informazioni dettagliate sui volumi contenuti in questa macchina includono:

   - Nome
   - ID dispositivo
   - File system
   - Capacità (incluse primaria, formattata e utilizzata)

   Altre informazioni visualizzate sulla macchina sono:

   - Processori
   - Schede di rete
   - Indirizzi IP associati a questa macchina

Visualizzazione delle informazioni sulla licenza

È possibile visualizzare le informazioni sullo stato attuale della licenza per il software AppAssure Agent installato su una macchina.

Per visualizzare le informazioni sulla licenza:

1. Nel riquadro di navigazione, selezionare la macchina che si desidera visualizzare.
2. Fare clic su **Configurazione** → **Licenze**.

   La schermata **Stato** visualizza i dettagli relativi alle licenze dei prodotti.

Modifica delle impostazioni di trasferimento

È possibile modificare le impostazioni per gestire i processi di trasferimento dei dati per una macchina protetta. Le impostazioni di trasferimento descritte in questa sezione sono impostazioni a livello di agente. Per influenzare il trasferimento a livello di core, consultare Modifica delle impostazioni delle code di trasferimento.

ATTENZIONE: La modifica delle impostazioni di trasferimento potrebbe avere effetti notevoli sul vostro ambiente AppAssure. Prima di modificare i valori delle impostazioni di trasferimento, fare riferimento alla Guida di configurazione per l'esecuzione di trasferimenti nella knowledge base di Dell AppAssure.

Ci sono tre tipi di trasferimenti in DL1300:

Istantanee	Il trasferimento che esegue il backup dei dati sulla macchina protetta.
Esportazione delle macchine virtuali	Un tipo di trasferimento che crea una macchina virtuale con tutte le informazioni di backup e i parametri come specificati dalla pianificazione definita per la protezione della macchina.
Ripristino	Un processo che ripristina le informazioni di backup su una macchina protetta.

Il trasferimento di dati in DL1300 implica la trasmissione di un volume di dati su una rete da macchine AppAssure Agent al Core. In caso di replica, il trasferimento si verifica anche dal Core di origine o di origine al Core di destinazione.

Il trasferimento di dati può essere ottimizzato per il sistema attraverso alcune impostazioni delle opzioni per le prestazioni. Queste impostazioni controllano l'utilizzo della larghezza di banda di dati durante il processo di esecuzione di backup delle macchine agente, l'esecuzione di esportazione delle macchine virtuali, o l'esecuzione di un rollback. Alcuni fattori che influiscono sulle prestazioni di trasferimento dei dati sono:

- Numero di trasferimenti dei dati agente simultanei
- Numero di flussi di dati simultanei
- Quantità di modifica dei dati su disco
- Larghezza di banda della rete disponibile
- Prestazioni del sottosistema del disco di repository
- Quantità di memoria disponibile per il buffer dei dati

È possibile regolare le opzioni di prestazioni al fine di meglio soddisfare le proprie esigenze aziendali e ottimizzare le prestazioni in base all'ambiente.

Per modificare le impostazioni di trasferimento:

1. Nella Core Console, passare alla macchina che si desidera modificare.
2. Fare clic sulla scheda **Configurazione**, quindi fare clic su **Impostazioni di trasferimento**.
   Viene visualizzata la pagina delle attuali **Impostazioni di trasferimento**.
3. Nella pagina **Impostazioni di trasferimento**, fare clic su **Modifica**.
   Viene visualizzata la finestra di dialogo **Impostazioni di trasferimento**.
4. Immettere le opzioni di **Impostazioni di trasferimento** per la macchina come descritto nella seguente tabella.

Casella di testo	Descrizione
Priorità	Imposta la priorità di trasferimento tra macchine protette. Consente di assegnare priorità rispetto ad altre macchine protette. Selezionare un numero compreso tra 1 e 10, dove 1 indica la priorità più elevata. L'impostazione predefinita stabilisce una priorità di 5. **N.B.:** La priorità viene applicata ai trasferimenti che sono in coda.
Massimo di flussi simultanei	Imposta il numero massimo di collegamenti TCP che vengono inviati al Core per essere elaborati in parallelo per ciascun agente. **N.B.:** Dell consiglia l'impostazione di questo valore su 8. Se si riscontrano pacchetti ignorati, provare ad aumentare questa impostazione.
Massimo di scritture simultanee	Impostare il numero massimo di azioni di scrittura su disco simultanee per connessione dell'agente. **N.B.:** Dell consiglia di impostare questo valore con lo stesso valore selezionato per il Massimo di flussi simultanei. Se si riscontrano perdite di pacchetti, impostare questo valore leggermente inferiore. Se, ad esempio, Massimo di flussi simultanei è impostato su 8, impostare questa opzione su 7.
Massimo di tentativi	Impostare il numero massimo di tentativi per ogni macchina protetta, se alcune delle operazioni non vengono completate.
Dimensione massima dei segmenti	Specifica la massima quantità di dati, in byte, che un computer può ricevere in un singolo segmento TCP. L'impostazione predefinita è 4194304. **ATTENZIONE: Non modificare questa opzione dall'impostazione predefinita.**
Lunghezza massima della coda dei trasferimenti	Specifica il numero di comandi che possono essere inviati contemporaneamente. È possibile regolare questa opzione su un numero più alto se il sistema ha un numero elevato di operazioni di input/output simultanee.
Letture in sospeso per flusso	Specifica quante operazioni di lettura in coda verranno memorizzate sul back-end. Questa impostazione contribuisce a controllare la messa in coda degli agenti. **N.B.:** Dell consiglia l'impostazione di questo valore a 24.
Writer esclusi	Selezionare un writer se si desidera escluderlo. Dal momento che i writer che compaiono nell'elenco sono specifici per la macchina che si sta configurando, potrebbe non essere possibile vedere tutti i writer elencati. Alcuni writer visibili includono: • Writer di ASR • Writer di BITS • Writer di COM+ REGDB • Writer dei contatori delle prestazioni • Writer del registro

Casella di testo	Descrizione
	• Writer di ottimizzazione di Shadow Copy • SQLServerWriter • Writer di sistema • Writer di pianificaizone delle attività • Writer di archiviazione dei metadati VSS • Writer di WMI
Porta del server per trasferimento dati	Imposta la porta per i trasferimenti. L'impostazione predefinita è 8009.
Timeout di trasferimento	Specifica in minuti e secondi la quantità di tempo da concedere a un pacchetto per diventare statico senza trasferimento.
Timeout istantanea	Specifica in minuti e secondi il tempo massimo di attesa per acquisire un'istantanea.
Timeout di lettura in rete	Specifica in minuti e secondi il tempo massimo di attesa per una connessione in lettura. Se la lettura in rete non viene eseguita in questo periodo di tempo, l'operazione viene ripetuta.
Timeout di scrittura in rete	Specifica in secondi il tempo massimo di attesa per una connessione in scrittura. Se la scrittura in rete non viene eseguita in questo periodo di tempo, l'operazione viene ripetuta.

5. Fare clic su **OK**.

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** → **Archivio** → **Crea**.
   Viene visualizzata la finestra di dialogo **Aggiunta guidata dell'archivio**.
2. Nella pagina **Crea** dell'**Aggiunta guidata dell'archivio**, selezionare una delle seguenti opzioni 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 punto 3.

Tabella 3. Creazione di un archivio

Opzione	Casella di testo	Descrizione
Locale	Percorso di output	Immettere il percorso per l'output. Questo viene utilizzato per definire la posizione in cui deve trovarsi l'archivio, per esempio d:\work\archive.
Rete	Percorso di output	Immettere il percorso per l'output. Questo viene utilizzato per definire la posizione in cui deve trovarsi l'archivio, per esempio \\servername \sharename.
	Nome utente	Immettere un nome utente. Questo viene utilizzato per stabilire le credenziali di accesso alla condivisione di rete.
	Password	Immettere una password per il percorso di rete. Questa viene utilizzata per stabilire le credenziali di accesso alla condivisione di rete.
Cloud	Account	Selezionare un account dall'elenco a discesa. **N.B.:** Per selezionare un account cloud, è necessario prima aggiungerlo alla Core Console. Consultare Aggiunta di un account cloud.
	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 CREAZIONE]- [ORA CREAZIONE]

4. Fare clic su **Avanti**.
5. Nella pagina **Macchine** della procedura guidata, selezionare quale macchina o quali macchine protette contengono i punti di ripristino da archiviare.

6. Fare clic su **Avanti**.
7. Nella pagina **Opzioni**, immettere le informazioni descritte nella tabella seguente.

Casella di testo	Descrizione
Dimensione massima	Gli archivi di dati di grandi dimensioni possono essere suddivisi in più segmenti. Selezionare la quantità di spazio massima che si desidera riservare per creare l'archivio effettuando una delle seguenti operazioni: • Selezionare Intera destinazione per riservare tutto lo spazio disponibile nel percorso della destinazione fornita al punto 4 (per esempio, se la posizione è D:\work\archive, viene riservato tutto lo spazio disponibile nell'unità D:). • Selezionare la casella di testo vuota, usare le frecce SU e GIÙ per immettere una quantità, quindi selezionare un'unità di misura dall'elenco a discesa per personalizzare lo spazio massimo da riservare. **N.B.:** Gli archivi cloud di Amazon vengono automaticamente suddivisi in segmenti da 50 GB. Gli archivi cloud di Windows Azure vengono automaticamente suddivisi in segmenti da 200 GB.
Azione riciclo	Selezionare una delle seguenti opzioni di azione riciclo: • **Non riutilizzare**: non sovrascrive o cancella gli eventuali dati archiviati esistenti dalla posizione. Se la posizione non è vuota, la scrittura dell'archivio non viene eseguita. • **Sostituisci questo Core**: sovrascrive gli eventuali dati archiviati preesistenti relativi a questo core, ma lascia intatti i dati degli altri core. • **Cancella completamente**: cancella tutti i dati archiviati dalla directory prima di scrivere il nuovo archivio. • **Incrementale**: consente di aggiungere punti di ripristino ad un archivio esistente. Esso confronta i punti di ripristino per evitare di duplicare i dati già esistenti nell'archivio.
Commento	Immettere eventuali informazioni aggiuntive necessarie da acquisire per l'archivio. Il commento verrà visualizzato anche alla successiva importazione dell'archivio.
Usa formato compatibile	Selezionare questa opzione per archiviare i dati in un formato che è compatibile con le versioni di core precedenti. **N.B.:** Il nuovo formato offre prestazioni migliori, tuttavia non è compatibile con i core precedenti.

8. Fare clic su **Avanti**.
9. Nella pagina Intervallo date, immettere data di inizio e di scadenza dei punti di ripristino da archiviare.
   - Per immettere un orario, fare clic sull'ora mostrata (predefinita 8:00 AM) per visualizzare le barre di scorrimento per selezionare ore e minuti.
   - Per immettere una data, fare clic sulla casella di testo per mostrare il calendario, quindi fare clic sul giorno desiderato.
10. Fare clic su **Fine**.

Importazione di un archivio

Per importare un archivio:

1. Nella Core Console, fare clic su **Strumenti** → **Archivio** → **Importazione**.
2. Per **Tipo di posizione**, selezionare una delle seguenti opzioni dall'elenco a discesa:
   - 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 punto 3.

Tabella 4. Importazione 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`ea.
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.
	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 cloud, è prima necessario aggiungerlo alla Core Console. Vedere l'argomento Aggiunta di un account cloud.

Opzione	Casella di testo	Descrizione
	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 **Controlla file** per convalidare l'esistenza dell'archivio da importare.
   Viene visualizzata la finestra di dialogo **Ripristina**.
5. Nella finestra di dialogo **Ripristina**, verificare il nome del core di origine.
6. Selezionare gli agenti da importare dall'archivio.
7. Selezionare il repository.
8. Fare clic su **Ripristina** per importare l'archivio.

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 cloud alla Core Console. Per ulteriori informazioni, consultare Aggiunta di un account cloud.
- Archiviazione ed esportazione dei dati in un account cloud.
- Recuperare i dati archiviati tramite importazione dalla posizione cloud.

Gestione della connettività di SQL

Tutte le versioni di DL1300 hanno attivata la funzionalità di SQL che consente di pianificare ed eseguire i controlli di connettività di SQL e le troncature dei log di SQL.

N.B.: Per impostazione predefinita, ogni appliance DL1300 dispone di una licenza di prova che viene attivata durante la configurazione iniziale dell'appliance. La funzionalità SQL non è attiva per le licenze di prova. Per attivare le funzionalità di SQL, sarà necessario attivare la licenza acquistata.

La configurazione di connettività di SQL abilita il Core a connettere i file di registro e il database SQL in un'istantanea di un server SQL utilizzando un'istanza locale di Microsoft SQL Server. Il test di connettività consente al core di controllare la coerenza dei database SQL e garantisce che tutti i file di dati (file MDF e LDF) siano disponibili nell'istantanea di backup. I controlli di connettività possono essere eseguiti su richiesta per punti di ripristino specifici o come parte di un processo notturno.

La connettività richiede un'istanza locale di Microsoft SQL Server sulla macchina AppAssure Core. Questa istanza deve essere una versione dotata di licenza completa di SQL Server acquistata da Microsoft o da un rivenditore autorizzato. Microsoft non consente l'utilizzo delle licenze passive di SQL.

La connettività supporta SQL Server 2005, 2008, 2008 R2, 2012 e 2014. All'account utilizzato per eseguire il test deve essere concesso il ruolo sysadmin nell'istanza di SQL Server.

Il formato di archiviazione su disco dell'SQL Server è lo stesso sia in ambienti a 64 bit che a 32 bit e la connettività funziona su entrambe le versioni. Un database che è scollegato da un'istanza del server che è in esecuzione in un ambiente può essere connesso a un'istanza del server che viene eseguita in un altro ambiente.

ATTENZIONE: La versione di SQL Server nel Core deve essere uguale o più recente della versione di SQL Server in tutti gli agenti con SQL Server installato.

Configurazione delle impostazioni di connettività di SQL

Prima di eseguire i controlli di connettività sui database SQL protetti, selezionare un'istanza locale del Server SQL sulla macchina Core che verrà utilizzata per eseguire i controlli sulla macchina agente.

N.B.: La connettività richiede un'istanza locale di Microsoft SQL Server sulla macchina AppAssure Core. Questa istanza deve essere una versione dotata di licenza completa di SQL Server acquistata da Microsoft o da un rivenditore autorizzato. Microsoft non consente l'utilizzo delle licenze passive di SQL.

Per configurare le impostazioni di connettività di SQL:

1. Passare alla Core Console. Fare clic sulla scheda.
2. Fare clic su **Configurazione** → **Impostazioni**.
3. Nel riquadro Processi notturni, fare clic su **Modifica**.
   Viene visualizzata la finestra di dialogo **Processo notturno**.
4. Selezionare **Processo di controllo di connettività**, quindi fare clic su **Impostazioni**.
5. Usare i menu a discesa per selezionare l'istanza del Server SQL installata sul Core tre le seguenti opzioni:
   È possibile scegliere tra le seguenti opzioni:
   - **SQL Server 2005**
   - **SQL Server 2008**
   - **SQL Server 2008 R2**
   - **SQL Server 2012**
   - **SQL Server 2014**
6. Selezionare il tipo di credenziali.
   È possibile scegliere tra le seguenti opzioni:
   - **Windows**
   - **SQL**
7. Specificare le credenziali con privilegi di amministrazione per le istanze Windows o del Server SQL, descritte come segue:

Casella di testo	Descrizione
Nome utente	Immettere un nome utente per le autorizzazioni di accesso al server SQL.
Password	Immettere una password per la connettività di SQL. Viene utilizzata per controllare l'attività di accesso.

8. Fare clic su **Connessione di prova**.

   N.B.: Se sono state inserite credenziali errate, viene visualizzato un messaggio che informa che il test delle credenziali non è riuscito. Correggere le informazioni sulle credenziali ed eseguire nuovamente il test di connessione.

9. Fare clic su **Salva**.

   I controlli di connettività sono ora disponibili per essere eseguiti sui database Server SQL protetti.
10. Nella finestra Processi notturni, fare clic su **OK**.

    I controlli di connettività sono ora pianificati per essere eseguiti con i processi notturni.

Configurazione dei controlli notturni di connettività e troncature dei log di SQL

Per configurare i controlli notturni di connettività e troncature dei log di SQL:

1. Nell'area di navigazione sinistra della Core, selezionare la macchina per cui si desidera effettuare controlli notturni di connettività e troncatura dei log, quindi fare clic su **Impostazioni del server SQL**.
2. Passare alla Core Console.
3. Fare clic su **Configurazione** → **Impostazioni**.
4. Nella sezione **Processi notturni**, fare clic su **Modifica**.
5. Selezionare o deselezionare le seguenti impostazioni del server SQL in base alle esigenze dell'azienda:
   - **Processo di controllo di connettività**
   - **Processo di troncatura dei log (solo modello di ripristino semplice)**
6. Fare clic su **OK**.

   Le impostazioni di connettività e di troncamento dei log sono effettive per il Server SQL protetto.

Visualizzazione della diagnostica di sistema

In AppAssure, sono disponibili le informazioni di diagnostica per la visualizzazione dei dati di registro delle macchine per qualsiasi macchina protetta. Inoltre, è possibile visualizzare e caricare le informazioni di diagnostica per il Core.

Visualizzazione dei registri della macchina

Se si verificano eventuali errori o problemi alla macchina, potrebbe risultare utile visualizzare i registri per la risoluzione dei problemi.

Per visualizzare i registri della macchina:

1. Nella Core Console, fare clic su **Strumenti** → **Diagnostica** → **Visualizza registro**.

   Viene visualizzata la pagina **Scarica registro Core**.
2. Selezionare **Fare clic qui per iniziare il download**.

   Viene visualizzato un messaggio di avviso per aprire o salvare il file.
3. Scegliere il metodo preferito per la gestione del file di registro.

Caricamento dei registri della macchina

1. Passare alla Core Console, fare clic su **Strumenti** → **Diagnostica** → **Carica registro**.

   Viene visualizzata la pagina **Carica registro**.
2. Selezionare **Fare clic qui per iniziare il caricamento**.

   La scheda **Eventi** consente di visualizzare l'avanzamento del caricamento delle informazioni dei registri del core e di tutte le macchine protette.

Esportazione dei dati Windows usando l'esportazione Hyper-V

In AppAssure, è possibile scegliere di esportare i dati tramite l'esportazione su Hyper-V eseguendo un'esportazione unica o continua. Completare i passaggi delle procedure riportate di seguito per esportare tramite l'esportazione su Hyper-V per il tipo di esportazione appropriato.

Annullamento delle operazioni in una macchina

È possibile annullare le operazioni di una macchina in fase di esecuzione. È possibile annullare un'istantanea corrente o annullare tutte le operazioni correnti, incluse esportazioni e repliche.

Per annullare le operazioni su una macchina:

1. Nella Core Console, selezionare la macchina per cui si desidera annullare le operazioni.
2. In **Eventi** espandere i dettagli degli eventi per l'evento o l'operazione che si desidera annullare.
3. Fare clic su **Annulla**.

Visualizzazione dello stato della macchina e altri dettagli

Per visualizzare lo stato della macchina e altri dettagli:

1. Nella Core Console, passare alla macchina protetta che si desidera visualizzare.

Vengono visualizzate le informazioni della macchina sulla pagina **Riepilogo**. I dettagli visualizzati sono:

- Nome host
- Ultima istantanea acquisita
- Prossima istantanea pianificata
- Stato di crittografia
- Numero di versione
- Stato del controllo della possibilità di montaggio
- Stato del controllo del Checksum
- Ultima troncatura dei log eseguita

Vengono anche visualizzate le informazioni dettagliate sui volumi contenuti in questa macchina e includono:

- Nome
- Tipo di file system
- Utilizzo dello spazio
- Pianificazione corrente
- Prossima istantanea
- Dimensione totale
- Spazio utilizzato
- Spazio disponibile

Se il Server SQL è installato sulla macchina, vengono visualizzate anche le informazioni dettagliate sul server e includono:

- Stato in linea
- Nome

- Percorso di installazione
- Versione

Se il Server Exchange è installato sulla macchina, vengono visualizzate anche le informazioni dettagliate sul server e sugli archivi di posta elettronica e includono:

- Versione
- Percorso di installazione
- Percorso dei dati
- Percorso del nome dei database Exchange
- Percorso dei file di registro
- Prefisso dei registri
- Percorso di sistema
- Tipo di MailStore

Gestione di più macchine

Questo argomento descrive le attività che gli amministratori eseguono per la distribuzione del software AppAssure Agent simultaneamente su più macchine Windows.

Per distribuire e proteggere più agenti, eseguire le seguenti operazioni:

1. Distribuire AppAssure in più macchine.
   Consultare Distribuzione in più macchine.
2. Monitorare l'attività di distribuzione massiva.
   Consultare Monitoraggio della distribuzione su più macchine.
3. Proteggere più macchine.
   Consultare Protezione di più macchine .

   N.B.: Questo passaggio può essere ignorato se è stata selezionata l'opzione Proteggi la macchina dopo l'installazione durante la fase di distribuzione.
4. Monitorare l'attività di protezione massiva.
   Consultare Monitoraggio della protezione di più macchine.

Distribuzione in più macchine

È possibile semplificare la distribuzione del software AppAssure Agent su più macchine Windows tramite la funzione Distribuzione di massa di AppAssure. È possibile effettuare una Distribuzione di massa per:

- Macchine su un host virtuale vCenter/ESXi VMware
- Macchine su un dominio Active Directory
- Macchine su qualsiasi altro host

La funzione Distribuzione di massa rileva automaticamente le macchine su un host e consente di selezionare quelli su cui si desidera eseguire la distribuzione. In alternativa, è possibile inserire manualmente l'host e le informazioni sulla macchina.

N.B.: Le macchine su cui si sta eseguendo la distribuzione devono disporre di un accesso a Internet per scaricare e installare i bit poiché AppAssure utilizza la versione Web del programma di installazione dell'agente AppAssure per distribuire i componenti dell'installazione. Se l'accesso a Internet non è disponibile, è possibile trasmettere il programma di installazione dell'agente AppAssure dalla macchina core. È possibile scaricare gli aggiornamenti core e agente dal portale delle licenze.

Monitoraggio della distribuzione su più macchine

È possibile visualizzare lo stato di avanzamento della distribuzione del software AppAssure Agent sulle macchine.

Per monitorare la distribuzione su più macchine:

1. Dalla Core Console, fare clic su **Eventi** → **Avvisi**.
2. Passare alla scheda **Home** di AppAssure Core, quindi fare clic sulla scheda **Eventi**.

   Gli eventi di avviso vengono visualizzati nell'elenco che mostra l'ora in cui l'evento è stato avviato e un messaggio. Per ogni distribuzione del software Agent completata, si potrà visualizzare un avviso che indica che la macchina protetta è stata aggiunta.
3. In alternativa, fare clic su qualsiasi collegamento di una macchina protetta.

   Viene visualizzata la scheda Riepilogo della macchina selezionata, che mostra le informazioni relative come:
   - Nome host della macchina protetta
   - Ultima istantanea, se disponibile
   - Orario pianificato dell'istantanea successiva, in base alla pianificazione di protezione selezionata
   - Tempo residuo
   - Chiave di crittografia, se presente, utilizzata per questo agente protetto
   - Versione del software Agent

Protezione di più macchine

Dopo aver distribuito in massa il software AppAssure Agent alle macchine Windows, è necessario proteggere le macchine per proteggere i dati. Se si seleziona **Proteggi macchina dopo l'installazione** quando si è distribuito l'agente, è possibile ignorare questa procedura.

N.B.: Le macchine dell'agente devono essere configurate con un criterio di protezione che renda possibile l'installazione remota.

Per proteggere più macchine:

1. Dalla Core Console, fare clic su **Proteggi** → **Protezione di massa**.

   Viene visualizzata la finestra **Protezione guidata di più macchine**.
2. Selezionare l'opzione di installazione appropriata:
   - Se non è necessario definire un repository o stabilire la crittografia, selezionare **Tipica**.
   - Se non si desidera visualizzare la pagina Introduzione per la Protezione guidata della macchina in futuro, selezionare **Ignora la pagina Introduzione alla prossima apertura della procedura guidata**.
3. Fare clic su **Avanti**.

   Viene visualizzata la pagina **Connessione**.
4. Aggiungere le macchine che si desidera proteggere facendo clic su una delle seguenti opzioni.

- Fare clic su **Active Directory** per specificare le macchine in un dominio Active Directory. Immettere le credenziali come descritto nella tabella sottostante e fare clic su **Avanti**.
- Fare clic su **vCenter/ESXi** per specificare le macchine virtuali in un host virtuale vCenter/ESXi. Immettere le credenziali come descritto nella tabella sottostante e fare clic su **Avanti**.

Casella di testo	Descrizione
Host	Il nome host o l'indirizzo IP del dominio Active Directory o dell'host virtuale VMware vCenter Server/ESX(i).
Nome utente	Immettere il nome utente usato per connettersi alla macchina, per esempio amministratore.
Password	Immettere la password di sicurezza utilizzata per connettersi a questa macchina.

- Per aggiungere le macchine manualmente, selezionare **Aggiungi le macchine manualmente**. Fare clic su **Avanti**.

5. Nella pagina **Macchine**, per specificare le macchine manualmente, digitare i seguenti dettagli di connessione per ciascuna macchina in una riga separata, quindi fare clic su **Avanti**.`hostname::username::password::port`
6. Nella pagina **Macchine**, per specificare le macchine identificate da un dominio Active Directory o un host virtuale VMware vCenter/ESX(i), selezionare le macchine da proteggere dall'elenco, quindi fare clic su **Avanti**.

   Il sistema verifica ogni macchina aggiunta automaticamente e viene visualizzata la pagina **Protezione**.
7. Nella pagina **Protezione**, selezionare la pianificazione di protezione appropriata:
   - Per usare la pianificazione di protezione predefinita, nell'opzione **Impostazioni di pianificazione** selezionare **Protezione predefinita (istantanee ogni ora di tutti i volumi)**.
   - Se si desidera definire una pianificazione di protezione differente, nell'opzione **Impostazioni di pianificazione** selezionare **Protezione personalizzata** e fare clic su **Avanti**.
8. Procedere con la configurazione come indicato di seguito:
   - Se è stata selezionata la configurazione Tipica dalla **Protezione guidata di più macchine** ed è stata specificata la protezione predefinita, fare clic su **Fine** per confermare le scelte, chiudere la procedura guidata e proteggere le macchine specificate.
   - Se è stata selezionata la configurazione Tipica dalla **Protezione guidata di più macchine** ed è stata specificata la protezione personalizzata, fare clic su **Avanti** e impostare una pianificazione personalizzata.
   - Se è stata selezionata la configurazione Avanzata per la Protezione guidata della macchina, fare clic su **Avanti** e passare al punto 9 per visualizzare le opzioni di repository e crittografia.
9. Nella pagina **Repository** selezionare **Usa un repository esistente**.
10. Fare clic su **Avanti**.

    Viene visualizzata la pagina **Crittografia**.
11. Per abilitare la crittografia, nella pagina **Crittografia** selezionare **Abilita crittografia**.

    I campi di Chiave di crittografia vengono visualizzati nella pagina **Crittografia**.

    N.B.: Se si abilita la crittografia, essa verrà applicata ai dati di tutti i volumi protetti per le macchine specificate per la protezione. È possibile modificare le impostazioni in un secondo momento dalla scheda **Configurazione** nella Core Console. Per maggiori informazioni sulla crittografia, consultare Gestione della sicurezza.
12. Immettere le informazioni come indicato nella tabella seguente per aggiungere una chiave di crittografia al Core.

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

13. Fare clic su **Fine** per salvare e applicare le impostazioni.

Monitoraggio della protezione di più macchine

È possibile monitorare lo stato di avanzamento poiché AppAssure applica le regole e le pianificazioni di protezione per le macchine.

Per monitorare la protezione di più macchine passare alla Core Console, scheda **Home**, quindi fare clic su **Eventi**.

La scheda Eventi visualizza le attività, gli avvisi e gli eventi. Quando i volumi vengono trasferiti, vengono visualizzati lo stato, l'ora di inizio e di fine nel riquadro Attività. È inoltre possibile filtrare le attività per stato (attivo, in attesa, completati e non riusciti).

Man mano che ogni macchina protetta viene aggiunta, viene registrato un avviso che indica se l'operazione è stata eseguita correttamente o se se vi sono errori collegati.

5

Recupero dei dati

Gestione del ripristino

La AppAssure Core può ripristinare istantaneamente i dati o ripristinare macchine su macchine fisiche o virtuali dai punti di ripristino. I punti di ripristino contengono le istantanee dei volumi dell'agente acquisite a livello di blocchi. Queste istantanee sono compatibili con l'applicazione, il che significa che tutte le transazioni aperte e i registri delle transazioni ricorrenti sono completati e le cache vengono scaricate sul disco prima di creare l'istantanea. Utilizzando le istantanee compatibili con l'applicazione in congiunzione con Verified Recovery, consente al Core di eseguire diversi tipi di ripristino, tra cui:

- Ripristino di file e cartelle
- Ripristino dei volumi di dati, utilizzando Live Recovery
- Ripristino dei volumi di dati per Microsoft Exchange Server e Microsoft SQL Server, utilizzando Live Recovery
- Ripristino bare-metal, utilizzando Universal Recovery
- Ripristino bare-metal su altro hardware, utilizzando Universal Recovery
- Esportazione specifica e continua su macchine virtuali

Gestione delle istantanee e dei punti di ripristino

Un punto di ripristino è una raccolta di istantanee dei singoli volumi di dischi e archiviati nel repository. Le istantanee acquisiscono e archiviano lo stato di un volume di disco in un determinato momento, mentre le applicazioni che generano i dati sono ancora in uso. In AppAssure, è possibile forzare un'istantanea, sospendere temporaneamente le istantanee, e visualizzare elenchi di punti di ripristino correnti nel repository, nonché eliminare le istantanee se necessario. I punti di ripristino vengono usati per ripristinare le macchine protette o per montarle in un file system locale.

Le istantanee che AppAssure acquisisce, vengono scattate a livello di blocco e sono compatibili con l'applicazione. Ciò significa che tutte le transazioni aperte e i log di transazioni frequenti sono stati completati e le cache scaricate sul disco prima di creare l'istantanea.

AppAssure utilizza un driver del filtro di volume a basso livello che si collega ai volumi montati e quindi tiene traccia di tutte le modifiche a livello di blocco per la successiva istantanea. Viene utilizzato Microsoft Volume Shadow Services (VSS) per facilitare istantanee compatibili con arresti anomali dell'applicazione.

Visualizzazione dei punti di ripristino

Per visualizzare i punti di ripristino:

1. Nell'area di navigazione a sinistra della Core Console, selezionare la macchina della quale si desidera visualizzare i punti di ripristino, quindi fare clic sulla scheda **Punti di ripristino**.

È possibile visualizzare le informazioni relative ai punti di ripristino della macchina come descritto nella seguente tabella:

Info	Descrizione
Stato	Indica lo stato corrente del punto di ripristino.
Crittografato	Indica se il punto di ripristino è crittografato.
Contenuto	Elenca i volumi contenuti nel punto di ripristino.
Tipo	Definisce un punto di ripristino come base o differenziale.
Data di creazione	Visualizza la data in cui il punto di ripristino è stato creato.
Dimensioni	Visualizza la quantità di spazio che il punto di ripristino consuma nel repository.

Visualizzazione di un punto di ripristino specifico

Per visualizzare un punto di ripristino specifico:

1. Nell'area di navigazione a sinistra della Core Console, selezionare la macchina di cui si desidera visualizzare i punti di ripristino, quindi selezionare i **Punti di ripristino**.
2. Fare clic su **>** accanto ad un punto di ripristino nell'elenco per espandere la visualizzazione.
   È possibile visualizzare informazioni più dettagliate sul contenuto del punto di ripristino per la macchina selezionata, nonché accedere ad una serie di operazioni che possono essere eseguite nel punto di ripristino, descritti nella seguente tabella:

Informazioni	Descrizione
Azioni	Il menu **Azioni** include le seguenti operazioni che è possibile eseguire nel punto di ripristino selezionato: **Monta** - Selezionare questa opzione per montare il punto di ripristino selezionato. Per maggiori informazioni sul montaggio di un punto di ripristino selezionato, consultare Montaggio di un punto di ripristino per una macchina Windows. **Esporta** - Dall'opzione Esporta è possibile esportare il punto di ripristino selezionato per ESXi, workstation VMware o Hyper-V. **Ripristina** - Selezionare questa opzione per eseguire un ripristino dal punto di ripristino selezionato in un volume specificato dall'utente.
Contenuto	L'area Contenuto include una riga per ciascun volume nel punto di ripristino espanso ed elenca le seguenti informazioni per ogni volume: **Stato** indica lo stato corrente del punto di ripristino. **Titolo** elenca il volume specifico nel punto di ripristino. **Dimensione** visualizza la quantità di spazio che il punto di ripristino consuma nel repository.

3. Fare clic su **>** accanto ad un volume nel punto di ripristino selezionato per espandere la visualizzazione.

È possibile visualizzare le informazioni sul volume selezionato nel punto di ripristino espanso come descritto nella seguente tabella:

Casella di testo	Descrizione
Titolo	Indica il volume specifico nel punto di ripristino.
Capacità raw	Indica la quantità di spazio di archiviazione raw nell'intero volume.
Capacità formattata	Indica la quantità di spazio di archiviazione nel volume che è disponibile per i dati dopo la formattazione del volume.
Capacità utilizzata	Indica la quantità di spazio di archiviazione attualmente usato dal volume.

Montaggio di un punto di ripristino per una macchina Windows

In AppAssure, è possibile montare un punto di ripristino per una macchina Windows per accedere ai dati archiviati attraverso un file system locale.

Per montare un punto di ripristino per una macchina Windows:

1. Dalla Core Console, selezionare la macchina che si desidera montare su un file system locale.
   Viene visualizzata la scheda **Riepilogo** della macchina selezionata.
2. Selezionare la scheda **Punti di ripristino**.
3. Nell'elenco dei punti di ripristino, fare clic su **>** per espandere il punto di ripristino che si desidera montare.
4. Nei dettagli estesi di quel punto di ripristino, fare clic su **Monta**.
   Viene visualizzata la finestra di dialogo **Monta punti di ripristino**.
5. Nella finestra di dialogo **Monta**, modificare le caselle di testo per il montaggio di un punto di ripristino come descritto nella seguente tabella:

Casella di testo	Descrizione
Percorso montaggio: cartella locale	Specificare il percorso utilizzato per accedere al punto di ripristino montato.
Immagini di volumi	Specificare le immagini dei volumi che si desidera montare.
Tipo montaggio	Specificare la modalità di accesso ai dati per il punto di ripristino montato: • Montaggio di sola lettura. • Montaggio di sola lettura con scritture precedenti. • Montaggio scrivibile.
Crea una condivisione Windows per questo montaggio	In alternativa, selezionare la casella di controllo per specificare se il punto di ripristino montato può essere condiviso, quindi impostare i diritti di accesso relativi inclusi il nome della condivisione e i gruppi di accesso.

6. Fare clic su **Monta** per montare il punto di ripristino.

Smontaggio dei punti di ripristino selezionati

Per smontare i punti di ripristino selezionati:

1. Passare alla Core Console, fare clic su **Strumenti** → **Montaggi**.
2. Nella pagina **Montaggi locali**, accanto al punto di montaggio del punto di ripristino che si desidera smontare, fare clic su **Smonta**.
3. Nella finestra di smontaggio del punto di ripristino, fare clic su **Sì** per confermare.

Smontaggio di tutti i punti di ripristino

Per smontare tutti i punti di ripristino:

1. Passare alla Core Console, fare clic su **Strumenti** → **Montaggi**.
2. Nella pagina **Montaggi locali**, fare clic su **Smonta tutti**.
3. Nella finestra **Smontaggio di un punto di ripristino**, fare clic su **Sì** per confermare.

Montaggio di un punto di ripristino per una macchina Linux

Utilizzando l'utility **aamount** in AppAssure, è possibile montare in remoto un volume da un punto di ripristino come un volume locale, su una macchina Linux.

1. Creare una nuova directory per il montaggio del punto di ripristino (ad esempio, è possibile utilizzare il comando **mkdir**).
2. Verificare l'esistenza della directory (ad esempio, utilizzando il comando **ls**).
3. Eseguire l'utility **aamount** di AppAssure come root o come il super utente, ad esempio: **sudo aamount**
4. Al prompt di montaggio di AppAssure, inserire il seguente comando per elencare le macchine protette. **lm**
5. Quando richiesto, inserire l'indirizzo IP o il nome host del server Core.
6. Inserire le credenziali di accesso al server Core, vale a dire il nome utente e la password.

   Verrà visualizzato un elenco delle macchine protette dal server di AppAssure. Ogni macchina viene identificata mediante: numero linea dell'elemento, indirizzo host/IP e un numero ID della macchina. Ad esempio: 293cc667-44b4-48ab-91d8-44bc74252a4f
7. Inserire il seguente comando per elencare i punti di ripristino disponibili per una specifica macchina: **lr <line_number_of_machine>**
8. Inserire il seguente comando per selezionare e montare il punto di ripristino specificato sul punto/percorso di montaggio specificato. **m <volume_recovery_point_ID_number> <path>**
9. Per verificare se il montaggio è stato completato, inserire il seguente comando, che elenca i volumi remoti collegati: **l**

Rimozione dei punti di ripristino

È possibile rimuovere facilmente dal repository i punti di ripristino per una determinata macchina. Quando si eliminano i punti di ripristino in AppAssure, è possibile specificare una delle seguenti opzioni:

Casella di testo	Descrizione
Elimina tutti i punti di ripristino	Rimuove dal repository tutti i punti di ripristino per la macchina agente selezionata.

Casella di testo	Descrizione
Elimina un intervallo di punti di ripristino	Rimuove tutti i punti di ripristino in un intervallo specificato prima del corrente, fino a e includendo l'immagine base, ovvero tutti i dati presenti sulla macchina, nonché tutti i punti di ripristino dopo il corrente fino all'immagine base successiva.

N.B.: Non è possibile recuperare i punti di ripristino eliminati.

Per rimuovere i punti di ripristino:

1. Nell'area di navigazione a sinistra della Core Console, selezionare la macchina della quale si desidera visualizzare i punti di ripristino, quindi fare clic sulla scheda **Punti di ripristino**.
2. Fare clic sul menu **Azioni**.
3. Selezionare una delle seguenti opzioni:
   - Per eliminare tutti i punti di ripristino attualmente archiviati, fare clic su **Elimina tutti**.
   - Per eliminare una serie di punti di ripristino in un determinato intervallo dati, fare clic su **Elimina intervallo**. Viene visualizzata la finestra di dialogo **Elimina**. Nella finestra di dialogo **Elimina intervallo**, specificare l'intervallo dei punti di ripristino che si desidera eliminare mediante una data e un'ora di inizio e di fine, quindi fare clic su **Elimina**.

Eliminazione di una catena di punti di ripristino orfani

Un punto di ripristino orfano è un'istantanea incrementale che non è associata ad un'immagine base. Le successive istantanee continuano a svilupparsi su questo punto di ripristino. Senza l'immagine base, i punti di ripristino derivanti sono incompleti ed è improbabile che contengano i dati necessari per completare il ripristino. Questi punti di ripristino vengono considerati come parte integrante della catena dei punti di ripristino orfani. Se si verifica questa situazione, la soluzione migliore è eliminare la catena e creare una nuova immagine base. Per ulteriori informazioni su come forzare un'immagine di base, consultare Forzatura di un'istantanea.

N.B.: La possibilità di eliminare una catena di punti di ripristino orfani non è disponibile per i punti di ripristino replicati su un core di destinazione.

Per eliminare una catena di punti di ripristino orfani:

1. Nella Core Console, selezionare la macchina protetta per cui si desidera eliminare la catena di punti di ripristino orfani.
2. Fare clic sulla scheda **Punti di ripristino**.
3. In **Punti di ripristino**, espandere il punto di ripristino orfano.
   Questo punto di ripristino è denominato nella colonna **Tipo** come **Orfano incrementale**.
4. Accanto ad **Azioni**, fare clic su **Elimina**.
   Viene visualizzata la finestra **Elimina i punti di ripristino**.
5. Nella finestra **Elimina i punti di ripristino**, fare clic su **Sì**.

ATTENZIONE: L'eliminazione di questo punto di ripristino elimina l'intera catena dei punti di ripristino, compresi eventuali punti di ripristino incrementali che si verificano prima o dopo l'eliminazione, fino all'immagine base successiva. Questa operazione non può essere annullata.

Forzatura di un'istantanea

La forzatura di un'istantanea consente di forzare un trasferimento di dati per la macchina protetta corrente. Quando si forza un'istantanea, il trasferimento viene avviato immediatamente o viene aggiunto in coda. Vengono trasferiti solo i dati che sono stati modificati da un punto di ripristino precedente. Se

non vi è alcun punto di ripristino precedente, vengono trasferiti tutti i dati sui volumi protetti, indicato come un'immagine base.

Per forzare un'istantanea:

1. Nella Core Console, selezionare la macchina o cluster con il punto di ripristino per il quale si desidera forzare un'istantanea.
2. Fare clic sulla scheda **Riepilogo** nella sezione **Volumi**, quindi selezionare una delle opzioni descritte come segue:
   - **Forza istantanea** - acquisisce un'istantanea incrementale dei dati aggiornati da quando è stata acquisita l'ultima istantanea.
   - **Forza immagine base** - acquisisce un'istantanea completa di tutti i dati presenti nei volumi della macchina.
3. Quando nella finestra di dialogo **Stato di trasferimento** viene visualizzata la notifica che l'istantanea è stata inserita in coda, fare clic su **OK**.

   Viene visualizzata una barra di avanzamento accanto alla macchina nella scheda **Macchine** e visualizza l'avanzamento dell'istantanea.

Ripristino dei dati

Con AppAssure è possibile ripristinare o recuperare immediatamente i dati per le macchine fisiche (per macchine Windows o Linux) o per le macchine virtuali da punti di ripristino archiviati per le macchine Windows. Questa sezione descrive in che modo è possibile esportare uno specifico punto di ripristino per macchine Windows su una macchina virtuale o per eseguire il rollaback su una macchina a un punto di ripristino precedente.

Se si dispone di una replica impostata tra due core (di origine e di destinazione), è possibile esportare i dati solo dal core di destinazione a seguito del completamento della replica iniziale.

Informazioni sull'esportazione dei dati protetti da macchine Windows su macchine 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 poi eseguire il recupero.

Il diagramma seguente mostra una tipica distribuzione dell'esportazione di dati su una macchina virtuale.

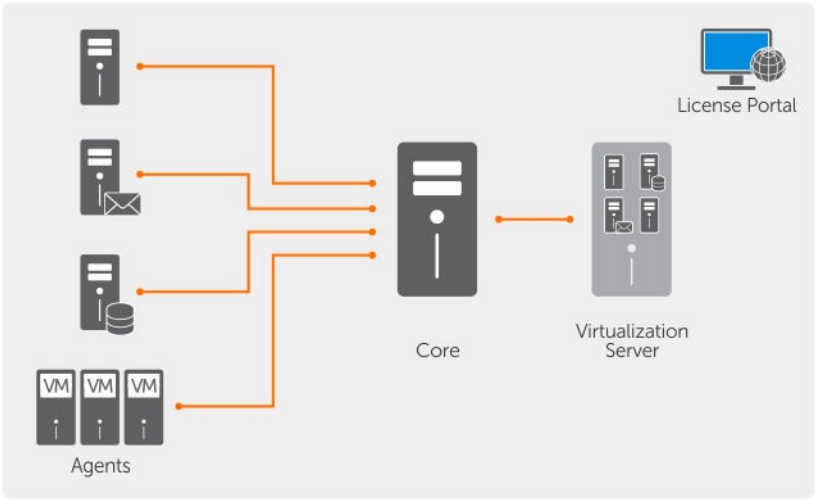


Figura 4. Esportazione di dati su una macchina virtuale

È possibile creare uno standby virtuale tramite l'esportazione continua dei dati protetti dalla propria macchina Windows su una macchina virtuale. Quando si esporta su una macchina virtuale, verranno esportati tutti i dati di backup da un punto di ripristino, nonché i parametri definiti per la pianificazione di protezione per la macchina.

È possibile eseguire l'esportazione virtuale dei punti di ripristino per macchine Windows o Linux protette su VMware, ESXi, Hyper-V e Oracle VirtualBox.

N.B.: La scheda Appliance visualizza tutte le macchine virtuali, ma supporta solo la gestione di macchine virtuali Hyper-V e ESXi. Per gestire le altre macchine virtuali utilizzare gli strumenti di gestione hypervisor.

N.B.: La macchina virtuale su cui si desidera esportare deve essere una versione concessa in licenza di ESXi, VMware Workstation o Hyper-V e non una versione di prova o gratuita.

Limitazioni del supporto per volumi base e dinamici

Dell AppAssure supporta la creazione di istantanee di tutti i volumi dinamici e base. AppAssure supporta inoltre l'esportazione dei volumi dinamici semplici che si trovano su un disco fisico singolo. I volumi dinamici semplici non sono volumi con striping, mirroring o spanning.

I dischi dinamici (tranne i dischi dinamici semplici come descritti in precedenza) non sono disponibili per la selezione nella procedura guidata di esportazione. I volumi dinamici non semplici hanno le geometrie arbitrarie del disco che non possono essere completamente interpretate. AppAssure pertanto non supporta l'esportazione dei volumi dinamici complessi o non semplici.

Gestione delle esportazioni

Nella scheda **Standby virtuale** nella Core Console, è possibile visualizzare lo stato delle esportazioni impostate, incluse le esportazioni uniche e continue per lo standby virtuale. In questa scheda, è possibile gestire le esportazioni sospendendole, arrestandole o rimuovendole, oppure visualizzando la coda delle esportazioni in uscita.

N.B.: Solo le configurazioni da 3 TB con 2 VM del Dell 1300 e da 4 TB con 2 VM del DL1300 supportano l'esportazione unica e continua nelle VM di standby virtuale.

1. Nella Core Console, andare alla scheda **Standby virtuale**.

   Nella scheda **Standby virtuale** è possibile visualizzare una tabella delle impostazioni di esportazione salvate, che include le informazioni descritte nella tabella seguente.

Menu	Descrizione
Stato	**N.B.:** Lo stato della configurazione di standby virtuale è definito dal colore dell'icona. Verde - Lo Standby virtuale è stato configurato correttamente, è attivo e non sospeso. La successiva esportazione di Standby virtuale verrà eseguita dopo l'istantanea seguente. Giallo - Lo Standby virtuale è sospeso ed è ancora salvato dal Core. Tuttavia, dopo un nuovo trasferimento, il processo di esportazione non si avvierà automaticamente e non vi saranno nuove esportazioni di Standby virtuale per questo agente.
Nome computer	Il nome del computer di origine.
Destinazione	La macchina virtuale e il percorso in cui i dati vengono esportati.
Tipo di esportazione	Il tipo di piattaforma di macchina virtuale per l'esportazione, come ESXi, VMware, Hyper-V o VirtualBox.
Ultima esportazione	La data e l'ora dell'ultima esportazione. Se un'esportazione è stata appena aggiunta ma non è stata completata, viene visualizzato un messaggio che indica che l'esportazione non è stata ancora eseguita. Se un'esportazione non è riuscita o è stata annullata, viene visualizzato un messaggio corrispondente.

2. Per gestire le impostazioni di esportazione salvate selezionare un'esportazione, quindi fare clic su una delle seguenti opzioni:
   - **In pausa**: per sospendere l'esportazione.
   - **Riprendi**: per riavviare un'esportazione sospesa.
   - **Forza**: per forzare una nuova esportazione. Questa opzione potrebbe essere utile quando lo standby virtuale viene sospeso e poi ripreso, il che significa che il processo di esportazione verrà riavviato solo dopo un nuovo trasferimento. Se non si desidera attendere il nuovo trasferimento, è possibile forzare un'esportazione.
3. Per rimuovere un'esportazione dal sistema, fare clic su **Rimuovi**. Quando si rimuove un'esportazione, questa viene rimossa definitivamente dal sistema e non sarà possibile riavviarla.
4. Per visualizzare i dettagli sulle esportazioni attive da completare attualmente in coda, fare clic su **Mostra coda esportazioni**.

   Viene visualizzata la tabella seguente:

Menu	Descrizione
Nome computer	Il nome del computer di origine.

Menu	Descrizione
Destinazione	Lo Standby virtuale è stato configurato correttamente, è attivo e non sospeso. La successiva esportazione di Standby virtuale verrà eseguita dopo l'istantanea seguente.
Tipo di esportazione	Lo Standby virtuale è sospeso ed è ancora salvato dal Core. Tuttavia, dopo un nuovo trasferimento, il processo di esportazione non si avvierà automaticamente e non vi saranno nuove esportazioni di Standby virtuale per questo agente.
Tipo di pianificazione	Il tipo di esportazione Unica o Continua.
Stato	L'avanzamento dell'esportazione, visualizzato come percentuale in una barra di avanzamento.

Esportazione delle informazioni di backup dalla propria macchina Windows ad una macchina virtuale

È possibile esportare i dati dalle macchine Windows ad una macchina virtuale (VMware, ESXi, Hyper-V e VirtualBox) tramite l'esportazione di tutte le informazioni di backup da un punto di ripristino, nonché i parametri definiti per la pianificazione di protezione per la macchina.

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

Per esportare le informazioni di backup di Windows ad una macchina virtuale:

1. Nella Core Console, fare clic sulla scheda **Macchine protette**.
2. Nell'elenco delle macchine protette, selezionare la macchina o il cluster con il punto di ripristino che si desidera esportare.
3. Nel menu a discesa **Azioni** di quella macchina, fare clic su **Esporta**, quindi selezionare il tipo di esportazione che si desidera eseguire. È possibile scegliere tra le seguenti opzioni:
   - Unica
   - Standby virtuale

   Viene visualizzata la finestra di dialogo **Procedura guidata di esportazione**.

Esportazione dei dati Windows usando l'esportazione ESXi

In AppAssure, è possibile scegliere di esportare i dati tramite l'esportazione su ESXi eseguendo un'esportazione unica o continua.

Esecuzione di un'esportazione ESXi unica

Per eseguire l'esportazione ESXi 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 delle informazioni della macchina virtuale per eseguire l'esportazione ESXi

Per definire le informazioni della macchina virtuale per eseguire l'esportazione ESXi:

1. Sulla pagina **Destinazione** nell'**Esportazione guidata**, nel menu a discesa **Ripristina su macchina virtuale**, selezionare **ESX(i)**.
2. Immettere i parametri per l'accesso alla macchina virtuale descritto come segue:

Casella di testo	Descrizione
Nome host	Immettere un nome per la macchina host.
Porta	Immettere la porta per la macchina host. La porta predefinita è 443.
Nome utente	Immettere le credenziali di accesso per la macchina host.
Password	Immettere le credenziali di accesso per la macchina host.

3. Nella pagina **Opzioni macchina virtuale**, immettere le informazioni descritte nella tabella riportata di seguito.

Casella di testo	Descrizione
Pool di risorse	Selezionare un pool di risorse dall'elenco a discesa.
Archivio dati	Selezionare un archivio di dati dall'elenco a discesa.
Nome macchina virtuale	Immettere un nome per la macchina virtuale.
Memoria	Specificare l'utilizzo della memoria.
Provisioning del disco	Selezionare il tipo di provisioning del disco Thin o Thick.
Mapping del disco	Specificare il tipo di mapping del disco come Automatico o Manuale.
Versione	Selezionare la versione della macchina virtuale.

4. Fare clic su **Avanti**.
5. Sulla pagina **Volumi**, selezionare i volumi che si desidera esportare, quindi fare clic su **Avanti**.
6. Nella pagina **Riepilogo**, fare clic su **Fine** per completare la procedura guidata e avviare l'esportazione.

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

Esecuzione di un'esportazione di ESXi (standby virtuale) continua

Per eseguire un'esportazione di ESXi (standby virtuale) continua:

1. Nella Core Console, eseguire una delle seguenti operazioni:
   - Nella scheda Standby virtuale, fare clic su **Aggiungi** per avviare l'**Esportazione guidata**. Nella pagina **Macchine protette** di **Esportazione guidata** selezionare la macchina protetta da esportare e fare clic su **Avanti**.
   - Passare alla macchina che si desidera esportare e fare clic su **Azioni** → **Esporta** → **Standby virtuale**.
2. Nella pagina **Destinazione** di **Esportazione guidata**, nel menu a discesa **Ripristina in una macchina virtuale** selezionare **ESXi**.
3. Immettere le informazioni per accedere alla macchina virtuale come indicato nella tabella seguente e fare clic su **Avanti**.

Casella di testo	Descrizione
Nome host	Immettere un nome per la macchina host.
Porta	Immettere la porta per la macchina host. L'impostazione predefinita è 443.
Nome utente	Immettere le credenziali di accesso per la macchina host.
Password	Immettere le credenziali di accesso per la macchina host.

4. Nella pagina **Opzioni della macchina virtuale**, immettere le informazioni descritte nella tabella seguente.

Casella di testo	Descrizione
Pool di risorse	Selezionare un pool di risorse dall'elenco a discesa.
Archivio dati	Selezionare un archivio dati dall'elenco a discesa.
Nome macchina virtuale	Immettere un nome per la macchina virtuale.
Memoria	Fare clic su Usa una quantità specifica di RAM per specificare quanta RAM utilizzare, per esempio 4096 MB. La quantità minima consentita è 512 MB e la massima è determinata da capacità e limitazioni delle macchine host (scelta consigliata).
Provisioning del disco	Selezionare il tipo di provisioning del disco Thin o Thick.
Mapping del disco	Specificare il tipo di mapping del disco Automatico o Manuale.
Versione	Selezionare la versione della macchina virtuale.

5. Fare clic su **Avanti**.
6. Nella pagina **Volumi** selezionare i volumi da esportare, quindi fare clic su **Avanti**.
7. Nella pagina **Riepilogo**, fare clic su **Fine** per completare la procedura guidata e iniziare l'esportazione.

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

Esportazione dei dati Windows usando l'esportazione di workstation VMware

In AppAssure, è possibile scegliere di esportare i dati tramite l'esportazione su workstation VMware eseguendo un'esportazione unica o continua. Completare i passaggi delle procedure riportate di seguito per esportare tramite l'esportazione su VMware Workstation per il tipo di esportazione appropriato.

Esecuzione di un'esportazione VMware Workstation unica

Per eseguire l'esportazione VMware Workstation unica:

1. Nella Core Console, spostarsi sul computer che si desidera esportare.
2. In **Riepilogo** fare clic su **Azioni** → **Esporta** → **Una volta**.

   L'**Esportazione guidata** viene visualizzata sulla pagina **Macchine protette**.
3. Selezionare una macchina 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 VMware Workstation

Per definire le impostazioni per l'esecuzione di un'esportazione VMware Workstation:

1. Sulla pagina **Destinazione** nella **Esportazione guidata**, nel menu a discesa **Eseguire il ripristino su macchina virtuale**, selezionare **VMware Workstation**, quindi fare clic su **Avanti**.
2. Nella pagina **Opzioni macchina virtuale**, inserire i parametri per l'accesso alla macchina virtuale come descritto nella tabella riportata di seguito.

Casella di testo	Descrizione
Posizione	Specificare il percorso della cartella o condivisione di rete locale sul quale creare la macchina virtuale. **N.B.:** Se è stato specificato un percorso di condivisione di rete, è necessario inserire le credenziali di accesso valide per un account che è registrato sul computer di destinazione. L'account deve disporre delle autorizzazioni di lettura e scrittura per la condivisione di rete.
Nome utente	Immettere le credenziali di accesso per la macchina virtuale. • Se è stato specificato un percorso di condivisione di rete, è necessario inserire un nome utente valido per un account che è registrato sul computer di destinazione. • Se è stato inserito un percorso locale, non è necessario un nome utente.
Password	Immettere le credenziali di accesso per la macchina virtuale. • Se è stato specificato un percorso di condivisione di rete, è necessario inserire una password valida per un account che è registrato sul computer di destinazione. • Se è stato inserito un percorso locale, non è necessaria una password.
Nome macchina virtuale	Immettere un nome per la macchina virtuale in corso di creazione; ad esempio, VM-0A1B2C3D4. **N.B.:** Il nome predefinito è il nome della macchina di origine.
Versione	Specificare la versione di VMware Workstation per la macchina virtuale. È possibile scegliere tra le seguenti opzioni. • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0
Memoria	Specificare l'utilizzo della memoria per la macchina virtuale, facendo clic su uno dei seguenti elementi: • Usa la stessa quantità di RAM della macchina di origine - Per specificare che la configurazione della RAM è uguale a quella della macchina di origine. • Utilizza una specifica quantità di RAM - Per specificare la quantità di RAM da utilizzare; ad esempio, 4096 megabyte (MB). La quantità minima

Casella di testo	Descrizione
	consentita è 512 MB e il massimo è determinato dalle funzionalità e limitazioni della macchina host (consigliato).

3. Fare clic su **Avanti**.
4. Nella pagina **Riepilogo**, fare clic su **Fine** per completare la procedura guidata e avviare l'esportazione.

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

Esecuzione di un'esportazione di workstation VMware (standby virtuale) continua

Per eseguire un'esportazione di workstation VMware (standby virtuale) continua:

1. Nella Core Console, eseguire una delle seguenti operazioni:
   - Nella scheda Standby virtuale, fare clic su **Aggiungi** per avviare l'**Esportazione guidata**. Nella pagina **Macchine protette** di **Esportazione guidata** selezionare la macchina protetta da esportare e fare clic su **Avanti**.
   - Passare alla macchina che si desidera esportare e, nella scheda **Riepilogo** nel menu a discesa **Azioni** di tale macchina, fare clic su **Esporta → Standby virtuale**.
2. Nella pagina **Destinazione** di **Esportazione guidata**, fare clic su **Ripristina in una macchina virtuale → Workstation VMware**.
3. Fare clic su **Avanti**.
4. Nella pagina **Opzioni della macchina virtuale**, immettere i parametri per accedere alla macchina virtuale come indicato nella tabella seguente.

Casella di testo	Descrizione
Percorso di destinazione	Specificare il percorso della cartella locale o condivisione di rete in cui creare la macchina virtuale. N.B.: Se è stato specificato un percorso di condivisione di rete, inserire le credenziali di accesso valide per un account che viene registrato nella macchina di destinazione. L'account deve disporre delle autorizzazioni di lettura e scrittura per la condivisione di rete.
Nome utente	Immettere le credenziali di accesso per la macchina virtuale. • Se è stato specificato un percorso di condivisione di rete, è necessario inserire un nome utente valido per un account che viene registrato nella macchina di destinazione. • Se è stato inserito un percorso locale, il nome utente non è necessario.
Password	Immettere le credenziali di accesso per la macchina virtuale. • Se è stato specificato un percorso di condivisione di rete, è necessario inserire una password valida per un account che viene registrato nella macchina di destinazione. • Se è stato inserito un percorso locale, la password non è necessaria.
Macchina virtuale	Immettere un nome per la macchina virtuale da creare, per esempio VM-0A1B2C3D4.

Casella di testo	Descrizione
	N.B.: Il nome predefinito è il nome della macchina di origine.
Versione	Specificare la versione di workstation VMware per la macchina virtuale. È possibile scegliere tra: • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0
Memoria	Specificare la memoria per la macchina virtuale selezionando uno dei seguenti: • Usa la stessa quantità di RAM della macchina di origine - Per specificare che la configurazione RAM è la stessa della macchina di origine. • Usa una quantità specifica di RAM - Per specificare quanta RAM utilizzare, per esempio 4096 Megabyte (MB). La quantità minima consentita è 512 MB e la massima è determinata da capacità e limitazioni della macchina host.

5. Selezionare **Esegui esportazione ad-hoc iniziale** per effettuare l'esportazione virtuale immediatamente e non dopo l'istantanea successiva pianificata.
6. Fare clic su **Avanti**.
7. Nella pagina **Volumi** selezionare i volumi da esportare, per esempio C:\ e D:\, quindi fare clic su **Avanti**.
8. Nella pagina **Riepilogo**, fare clic su **Fine** per completare la procedura guidata e iniziare l'esportazione.

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

Esportazione dei dati Windows usando l'esportazione Hyper-V

In AppAssure, è possibile scegliere di esportare i dati tramite l'esportazione su Hyper-V eseguendo un'esportazione unica o continua. Completare i passaggi delle procedure riportate di seguito per esportare tramite l'esportazione su Hyper-V per il tipo di esportazione appropriato.

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.
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**

Esportazione dei dati Windows usando l'esportazione di Oracle VirtualBox

In AppAssure, è possibile scegliere di esportare i dati tramite VirtualBox Export eseguendo un'esportazione unica o continua, oppure tramite l'esportazione continua (per standby virtuale).

Completare i passaggi nelle procedure seguenti per il tipo di esportazione appropriata.

N.B.: Per eseguire questo tipo di esportazione, è necessario che Oracle VirtualBox sia installato nella macchina Core. VirtualBox versione 4.2.18 o superiori sono supportate per gli host Windows.

Esecuzione di un'esportazione Oracle VirtualBox unica

Per eseguire un'esportazione Oracle VirtualBox unica:

1. Nella Core Console, passare alla macchina Linux che si desidera esportare.
2. Nella scheda **Riepilogo**, fare clic su **Azioni → Esporta → Una volta**.

   L'**Esportazione guidata** viene visualizzata sulla pagina **Macchine protette**.
3. Selezionare una macchina 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**.
5. Sulla pagina **Destinazione** in **Esportazione guidata**, nel menu a discesa **Ripristina su macchina virtuale**, selezionare **VirtualBox**, fare clic su **Avanti**.
6. Sulla pagina **Opzioni macchina virtuale**, selezionare **Macchina Linux remota**.
7. Immettere i parametri per l'accesso alla macchina virtuale come segue:

Casella di testo	Descrizione
Nome host VirtualBox	Immettere l'indirizzo IP o il nome host del server VirtualBox. Questo campo indica l'indirizzo IP o il nome host del server remoto VirtualBox.
Porta	Immettere un numero di porta per la macchina. Tale numero rappresenta la porta attraverso la quale il core comunica con questa macchina.
Nome macchina virtuale	Specificare un percorso di destinazione per creare la macchina virtuale.
Nome utente	Nome utente dell'account sulla macchina di destinazione, ad esempio, root.
Password	Immettere le credenziali di accesso per la macchina host.

Casella di testo	Descrizione
Memoria	Specificare la memoria per la macchina virtuale.

8. Sulla pagina **Volumi**, selezionare i volumi di dati da esportare, quindi fare clic su **Avanti**.
9. Nella pagina **Riepilogo**, fare clic su **Fine** per completare la procedura guidata e avviare l'esportazione.

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

Esecuzione di un'esportazione continua Oracle VirtualBox (standby virtuale)

Per eseguire un'esportazione continua VirtualBox (standby virtuale):

1. Nella Core Console, effettuare una delle operazioni riportate di seguito:
   - Nella scheda **Standby virtuale**, fare clic su **Aggiungi** per avviare la **procedura guidata di esportazione**. Nella pagina **Macchine protette** della **procedura guidata di esportazione**, selezionare la macchina protetta che si desidera esportare, e quindi fare clic su **Avanti**.
   - Passare alla macchina che si desidera esportare e, nella scheda **Riepilogo** nel menu a discesa **Azioni** per quella macchina, fare clic su **Esporta → Standby virtuale**.
2. Nella pagina **Destinazione** nella **procedura guidata di esportazione**, nel menu a discesa **Ripristino su macchina virtuale**, selezionare **VirtualBox**, quindi fare clic su **Avanti**.
3. Nella pagina **Opzioni della macchina virtuale**, selezionare **Usa una macchina Windows**.
4. Immettere i parametri per l'accesso alla macchina virtuale come descritto nella seguente tabella.

Casella di testo	Descrizione
Nome macchina virtuale	Immettere un nome per la macchina virtuale in corso di creazione. **N.B.:** Il nome predefinito è il nome della macchina di origine.
Percorso di destinazione	Specificare un percorso locale o remoto di destinazione per creare la macchina virtuale. **N.B.:** Il percorso di destinazione non deve essere una directory root. Se si specifica un percorso di condivisione di rete, sarà necessario immettere credenziali di accesso valide (nome utente e password) per un account che è registrato nella macchina di destinazione. L'account deve disporre delle autorizzazioni di lettura e scrittura per la condivisione di rete.
Memoria	Specificare la memoria per la macchina virtuale. • Fare clic su **Usa la stessa quantità di RAM della macchina di origine** per specificare che la configurazione della RAM è uguale a quella della macchina di origine. • Fare clic su **Usa una specifica quantità di RAM** per specificare la quantità RAM da utilizzare; ad esempio, 4096 megabyte (MB). La quantità minima consentita è 512 MB e il massimo è determinato dalle funzionalità e limitazioni della macchina host.

5. Per specificare un account utente per la macchina virtuale, selezionare **Specificare l'account utente per la macchina virtuale esportata**, quindi inserire le seguenti informazioni. Questo si riferisce a un account utente specifico per cui la macchina virtuale verrà registrata nel caso ci siano più account utente sulla macchina virtuale. Quando questo account utente ha eseguito l'accesso, solo questo utente vedrà questa macchina virtuale in VirtualBox Manager. Se un account non è specificato, allora

la macchina virtuale verrà registrata per tutti gli utenti esistenti sulla macchina Windows con VirtualBox.

- Nome utente - immettere il nome utente per il quale la macchina virtuale è registrata.
- Password - immettere la password per questo account utente.

6. Selezionare **Esegui esportazione ad-hoc iniziale** per eseguire l'esportazione virtuale immediatamente invece che dopo l'istantanea successiva pianificata.
7. Fare clic su **Avanti**.
8. Nella pagina **Volumi**, selezionare i volumi da esportare, ad esempio, C:\ e D:\, quindi fare clic su **Avanti**.
9. Nella pagina **Riepilogo**, fare clic su **Fine** per completare la procedura guidata e per avviare l'esportazione.

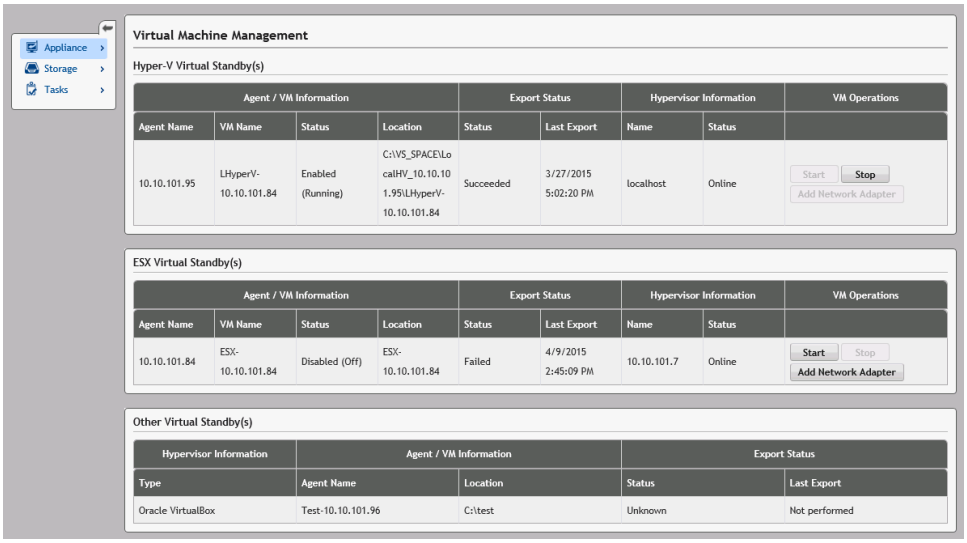
N.B.: È possibile monitorare lo stato e l'avanzamento dell'esportazione, controllando la scheda **Standby virtuale** o **Eventi**.

Gestione delle macchine virtuali

N.B.: La gestione della macchina virtuale dalla scheda Appliance può essere configurata solo nei sistemi che supportano la creazione della macchina virtuale.

La scheda **Gestione macchine virtuali** visualizza lo stato delle macchine protette. È possibile avviare, arrestare e aggiungere schede di rete (applicabile solo per macchine virtuali Hyper-V e ESXi). Per passare alla scheda Gestione macchine virtuali, fare clic su **Appliance → Gestione macchine virtuali**.

N.B.: Possono essere necessari fino a 30 secondi prima che vengano visualizzati i pulsanti Avvia, Arresta e Aggiungi scheda di rete ogni volta che la scheda **Appliance → Gestione macchine virtuali** viene selezionata.



Gestione macchine virtuali per standby virtuali Hyper-V ed ESXi

Campo	Descrizione
Informazioni agente/macchina virtuale	**Nome agente**: indica il nome della macchina protetta di cui si è creato lo standby virtuale.

Campo	Descrizione
	Nome macchina virtuale: indica il nome della macchina virtuale. **N.B.:** Si consiglia di utilizzare un nome che deriva dal nome dell'agente o uno che corrisponde al nome dell'agente. È inoltre possibile creare un nome derivato dal tipo di hypervisor, l'indirizzo IP o il nome DNS. **Stato**: indica lo stato della macchina virtuale. Valori possibili sono: • In esecuzione • Interrotto • In avvio • Sospeso • In interruzione • Sconosciuto (stato temporaneo) **N.B.:** I valori di stato precedenti dipendono dal tipo di hypervisor. Non tutti gli hypervisor visualizzano tutti i valori di stato. **Posizione**: indica la posizione della macchina virtuale. Ad esempio, D:\export. La posizione della macchina virtuale deve disporre di spazio sufficiente per contenere le unità virtuali e dei metadati della macchina virtuale necessarie per la macchina virtuale.
Stato di esportazione	**Stato** 1. Indica il seguente stato di un processo di esportazione: • Completo • Non riuscito • In corso • Non eseguito 2. Se un'esportazione è attualmente in corso, viene visualizzata la percentuale di esportazione. **Ultima esportazione**: indica l'ora dell'ultima esportazione.
Informazioni sull'hypervisor	**Nome**: indica il nome dell'hypervisor su cui viene creata la macchina virtuale. **Stato**: indica lo stato di connessione agli hypervisor Hyper-V ed ESXi. • In linea • Non in linea • Sconosciuto (stato temporaneo) **N.B.:** Lo stato viene visualizzato solo per hypervisor Hyper-V ed ESXi.
Operazioni macchina virtuale	Consente di avviare o arrestare la macchina virtuale, e aggiungere una scheda di rete.

Gestione macchine virtuali per altri standby virtuali

Campo	Descrizione
Informazioni sull'hypervisor	**Tipo**: indica il tipo di hypervisor.
Informazioni agente/macchina virtuale	**Nome agente**: indica il nome della macchina protetta di cui si è creato lo standby virtuale. **Posizione**: indica la posizione della macchina virtuale. Ad esempio, D:\export. La posizione della macchina virtuale deve disporre di spazio sufficiente per contenere le unità virtuali e dei metadati della macchina virtuale necessarie per la macchina virtuale.
Stato di esportazione	**Stato** 1. Indica il seguente stato di un processo di esportazione: • Completo • Non riuscito • In corso • Non eseguito 2. Se un'esportazione è attualmente in corso, viene visualizzata la percentuale di esportazione con una barra di stato. **Ultima esportazione**: indica l'ora dell'ultima esportazione.

Creazione di una scheda di rete virtuale

Le macchine virtuali devono disporre di una o più schede di rete virtuali (VNAs) per la connessione a Internet. Una macchina virtuale deve avere una scheda di rete virtuale (VNA) per ciascuna scheda di rete reale (RNA) sulla macchina protetta. La VNA e la RNA corrispondente devono disporre di una configurazione simile. È possibile aggiungere più VNA alla macchina virtuale al momento della creazione dello Standby virtuale, altrimenti è possibile farlo in un secondo momento.

Quando si crea uno standby virtuale, è presente una scheda consigliata per ogni scheda nella macchina protetta, se si configura una macchina virtuale. È possibile aggiungere o rimuovere tutte o parte delle schede consigliate. Il numero massimo di VNA per ogni macchina virtuale dipende dal tipo di hypervisor. Per Hyper-V è possibile aggiungere fino a 8 schede per ogni macchina virtuale.

Per creare una scheda di rete virtuale:

1. Passare alla pagina **Gestione VM**.
2. Fare clic sul pulsante **Aggiungi scheda di rete** associato alla macchina virtuale per aggiungere una VNA.

   N.B.: Non aggiungere schede ad una macchina virtuale per uno Standby virtuale in caso di backup o esportazioni in esecuzione di macchine protette. Le VNA aggiuntive possono causare anomalie per future esportazioni.

   N.B.: Si consiglia di aggiungere le VNA prima di avviare la macchina virtuale in sostituzione della macchina protetta. Accertarsi di interrompere o sospendere le esportazioni in sospeso della macchina virtuale tramite la scheda Standby virtuale.

   Viene visualizzata la finestra **Switch e schede di rete virtuali**.
3. Fare clic su **Crea** per creare una scheda di rete virtuale.

Viene visualizzata la finestra **Crea scheda di rete virtuale**.

4. Scegliere uno switch virtuale esistente dal menu a discesa.

   N.B.: Nella selezione degli switch virtuali per ESXi, il menu a discesa elenca solo gli switch che contengono "VM" o "Virtual Machine" nel nome. Solo selezionando uno switch di tipo **Virtual Machine Port Group**, è possibile verificare il tipo di switch tramite la GUI dell'hypervisor ESXi.

5. Fare clic su **Crea**.

   N.B.: Per rimuovere una scheda di rete virtuale, utilizzare l'interfaccia di gestione hypervisor.

Avvio di una operazione su una macchina virtuale

Per avviare un'operazione su una macchina virtuale:

1. Passare alla finestra **Gestione macchine virtuali**.
2. Fare clic sul pulsante **Start** associato alla macchina virtuale da avviare.

   N.B.: L'interfaccia utente grafica (GUI) potrebbe avere un lag nel mostrare lo stato corretto della macchina. Il pulsante Start può rimanere disattivato fino a 30 secondi dopo l'utilizzo dei pulsanti. Il pulsante Start è abilitato solo se la macchina virtuale può essere avviata.

   N.B.: Non fare clic sul pulsante Start se è in esecuzione un'attività di esportazione sulla macchina virtuale o è probabile che inizi a breve. Verificare la pianificazione dell'attività di esportazione successiva controllando la scheda **Macchine protette** e la scheda **Standby Virtuale**. Se è stata pianificata un'attività di esportazione nel prossimo futuro, annullare o ignorare l'attività di esportazione o attendere che l'attività di esportazione sia completata prima di avviare la macchina virtuale. L'esportazione dei dati non riesce se eseguita quando la macchina virtuale è in esecuzione, anche se è possibile avviare una macchina virtuale quando un'attività di esportazione è in esecuzione.

   N.B.: Si consiglia di non avviare la macchina virtuale gestita come standby virtuale. Le macchine virtuali in standby virtuale sono destinate ad essere attive o avviate in sostituzione di una macchina protetta guasta. Se la macchina protetta è ancora attiva, è innanzitutto necessario arrestare o sospendere le esportazioni in sospeso per la macchina virtuale tramite la scheda Standby Virtuale prima di avviare la macchina virtuale.

Interruzione di un'operazione della macchina virtuale

Per interrompere un'operazione di una macchina virtuale:

1. Passare alla finestra **Gestione macchine virtuali**.
2. Fare clic sul pulsante **Interrompi** associato alla macchina virtuale da interrompere.

   N.B.: Il pulsante Interrompi è abilitato solo se la macchina virtuale è attualmente in esecuzione ed è disponibile entro 30 secondi (circa) dopo l'avvio della macchina virtuale.

   N.B.: Il pulsante Start è abilitato entro 30 secondi (circa) dopo l'arresto della macchina virtuale.

   N.B.: Una volta che la macchina virtuale protetta viene ripristinata, rimuovere la macchina virtuale dall'hypervisor e dal suo standby virtuale corrispondente. Ricreare lo standby virtuale per la macchina protetta ripristinata. In questo modo viene garantito che la macchina virtuale in standby virtuale rifletta fedelmente la macchina protetta.

Ripristino dei volumi da un punto di ripristino

È possibile ripristinare i volumi su una macchina protetta dai punti di ripristino memorizzati nell'AppAssure Core. Per ripristinare i volumi da un punto di ripristino:

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

   Viene visualizzato il **Ripristino guidato della macchina**.
2. Dalla pagina **Macchine protette**, selezionare la macchina protetta per la quale si desidera ripristinare i dati, quindi fare clic su **Avanti**.

   N.B.: È necessario che il software agente sia installato sulla macchina protetta e che tale macchina 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 l'istantanea che si desidera ripristinare sulla macchina 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**. Passare al punto 7.
   - 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**. Passare al punto 7.
   - Se si desidera ripristinare da un punto di ripristino selezionato sullo stesso computer o un altro computer utilizzando un CD di avvio e se i volumi che si desidera ripristinare non includono il volume di sistema, selezionare **Ripristina in qualsiasi macchina di destinazione usando un CD di avvio**.
   - Per continuare e creare il CD di avvio con le informazioni dal punto di ripristino selezionato, fare clic su **Avanti** e passare al punto 10.
   - Se si è già creato il CD di avvio e il computer di destinazione è stato avviato utilizzando il CD di avvio, passare al punto 17.
   - 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 un BMR. Per ulteriori informazioni sull'esecuzione di un BMR per Windows, consultare Avvio del ripristino bare metal per macchine Windows.
   - Per ulteriori informazioni sull'esecuzione di un BMR per Linux, fare riferimento alle linee guida per l'esecuzione di un ripristino bare metal per macchine Linux Avvio del ripristino bare metal per una macchina Linux.
6. Per la connessione alla Universal Recovery Console (URC) sul computer di destinazione, eseguire le operazioni riportate di seguito:

a. Selezionare **Dispongo già di un CD di avvio in esecuzione sul computer di destinazione**.
b. Nella casella di testo indirizzo IP, inserire l'indirizzo IP del computer di destinazione con il CD di avvio.
c. Nella casella di testo Chiave di autenticazione, inserire la chiave di autenticazione dalla URC sul computer di destinazione, quindi fare clic su **Avanti**.

Viene visualizzata la pagina **Mapping del disco**. Passare al punto 20.

7. 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**.
8. 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, 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.
9. Passare al punto 20.
10. Sulla pagina del CD di avvio, effettuare le operazioni riportate di seguito:
    a. Nel campo di testo **Percorso di output**, digitare il percorso in cui l'immagine ISO del CD di avvio deve essere archiviata.
    b. In **Ambiente** selezionare l'architettura più adatta per l'hardware che si desidera ripristinare:
       - Per eseguire il ripristino su qualsiasi macchina Windows con un'architettura a 64 bit, selezionare **Windows 8 a 64 bit**.
       - Per eseguire il ripristino su qualsiasi macchina con un'architettura a 32 bit (x86), selezionare **Windows 7 a 32 bit**.
11. Facoltativamente, per impostare i parametri di rete per l'agente ripristinato, o per utilizzare UltraVNC, selezionare **Mostra opzioni avanzate** ed effettuare una delle operazioni riportate di seguito:
    - Per stabilire una connessione di rete per la macchina ripristinata, selezionare **Utilizza il seguente indirizzo IP** come descritto nella tabella riportata di seguito.

Opzione	Descrizione
Indirizzo IP	Specificare un indirizzo IP o nome host della macchina ripristinata.
Subnet mask	Specificare la subnet mask per la macchina ripristinata.
Gateway predefinito	Specificare il gateway predefinito per la macchina ripristinata.
Server DNS	Specificare il server del nome del dominio per la macchina ripristinata.

    - Per definire le informazioni di UltraVNC, selezionare **Aggiungi UltraVNC** come descritto nella tabella riportata di seguito. Utilizzare questa opzione se è necessario l'accesso remoto alla console di ripristino. Non è possibile accedere utilizzando Microsoft Terminal Services durante l'utilizzo del CD di avvio.

Opzione	Descrizione
Password	Specificare una password per questa connessione UltraVNC.

Opzione	Descrizione
Porta	Specificare una porta per questa connessione UltraVNC. La porta predefinita è 5900.

12. Fare clic su **Avanti**.
13. Per inserire un driver, effettuare le operazioni riportate di seguito:
    a. Selezionare **Aggiungi un archivio di driver**.
    b. Passare a un file ZIP contenente l'archivio, selezionare il file ZIP, e fare clic su **Apri**. L'archivio si carica e compare nella pagina di inserimento del driver .
    c. Fare quindi clic su **Avanti**.
14. Sulla pagina **Immagine ISO**, è possibile vedere lo stato mentre viene creata l'immagine ISO del CD di avvio. Quando il CD di avvio viene completato correttamente, fare clic su **Avanti**.

    Viene visualizzata la pagina **Connessione**.
15. Avviare la macchina agente per cui si desidera ripristinare i dati dal CD di avvio.
    - Avviare la macchina agente da un'immagine ISO, se possibile.
    - Altrimenti, copiare l'immagine ISO su supporti fisici (un CD o DVD), caricare il disco nella macchina agente, configurare la macchina per caricare dal CD avvio e riavviare dal CD di avvio.

    N.B.: Potrebbe essere necessario modificare le impostazioni del BIOS della macchina agente per verificare che il volume che si carica per primo è il CD di avvio.

    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 dall'AppAssure 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.
16. Nella Core Console sulla pagina **Connessione**, inserire le informazioni di autenticazione dall'istanza della URC della macchina che si desidera ripristinare come indicato di seguito:
    a. Nella casella di testo Indirizzo IP, inserire l'indirizzo IP del computer in cui si esegue il ripristino da un punto di ripristino.
    b. Nella casella di testo Chiave di autenticazione, inserire le informazioni dalla URC.
    c. Fare clic su **Avanti**.

    Viene visualizzata la pagina **Mapping del disco**.
17. Per eseguire il mapping dei volumi manualmente, passare al punto 18. Per eseguire il mapping automatico dei volumi, effettuare le seguenti operazioni:
    a. Selezionare **Mapping automatico dei volumi**.
    b. Nell'area **Mapping automatico dei volumi**, selezionare i volumi che si desidera ripristinare. Se non si desidera ripristinare un volume elencato, deselezionare l'opzione.

       N.B.: Almeno un volume deve essere selezionato per eseguire il ripristino.
    c. Selezionare il disco di destinazione per il ripristino.
    d. Fare clic su **Avanti**, quindi passare al punto 19.
18. Se si desidera eseguire il mapping dei volumi manualmente, effettuare le operazioni riportate di seguito.
    a. Selezionare **Mapping manuale dei volumi**.
    b. Nell'area **Mapping manuale dei volumi**, dall'elenco a discesa **Volumi di destinazione** per ciascun volume, selezionare il volume che si desidera ripristinare. Se non si desidera ripristinare un volume elencato, deselezionare l'opzione.

       N.B.: Almeno un volume deve essere selezionato per eseguire il ripristino.
    c. Fare clic su **Fine**.

ATTENZIONE: Se si seleziona Fine, tutte le partizioni esistenti e i dati nell'unità di destinazione verranno rimossi definitivamente, e sostituiti con il contenuto del punto di ripristino selezionato, incluso il sistema operativo e tutti i dati.

Il **Ripristino guidato della macchina** si chiude e i dati vengono ripristinati dai volumi selezionati del punto di ripristino sul computer di destinazione. Proseguire con il punto 22.

19. Nella pagina **Anteprima mapping disco**, rivedere i parametri delle azioni di ripristino selezionate. Per eseguire il ripristino, fare clic su **Fine**.

    ATTENZIONE: Se si seleziona Fine, tutte le partizioni esistenti e i dati nell'unità di destinazione verranno rimossi definitivamente, e sostituiti con il contenuto del punto di ripristino selezionato, incluso il sistema operativo e tutti i dati.

    Il **Ripristino guidato della macchina** si chiude e i dati vengono ripristinati dai volumi selezionati del punto di ripristino sul computer di destinazione. Proseguire con il punto 22.

20. 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**.
21. Fare clic su **OK** per confermare il messaggio di stato che il processo di ripristino è stato avviato.
22. Per monitorare l'avanzamento del processo di ripristino, sulla Core Console fare clic su **Eventi**.

Ripristino dei volumi per una macchina Linux usando la riga di comando

In AppAssure, è possibile ripristinare volumi su macchine Linux protette usando l'utility `aamount` della riga di comando. Per ripristinare i volumi per una macchina Linux utilizzando la riga di comando:

ATTENZIONE: Non tentare di ripristinare il volume di sistema o root (/).

1. Eseguire l'utility `aamount` di AppAssure come root, ad esempio:

   ```
   sudo aamount
   ```

2. Al prompt di montaggio di AppAssure, inserire il seguente comando per elencare le macchine protette:

   ```
   lm
   ```

3. Quando richiesto, inserire l'indirizzo IP o il nome host del server AppAssure Core.
4. Immettere le credenziali di accesso, ovvero il nome utente e la password, per questo server.

   Viene visualizzato un elenco delle macchine protette da questo server AppAssure. Vi sono elencate le macchine agente rilevate mediante numero linea dell'elemento, indirizzo host/IP e un numero ID della macchina (ad esempio: `293cc667-44b4-48ab-91d8-44bc74252a4f`).

5. Immettere il seguente comando per visualizzare l'elenco dei punti di ripristino attualmente montati sulla macchina specificata:

   ```
   lr <machine_line_item_number>
   ```

   N.B.: Inoltre, è possibile inserire il numero ID della macchina in questo comando al posto del numero linea dell'elemento.

   Viene visualizzato un elenco che mostra i punti di ripristino base e incrementali per tale macchina. Questo elenco include un numero linea dell'elemento, date/timestamp, la posizione del volume, le dimensioni del punto di ripristino, e un numero ID per il volume che include un numero di sequenza alla fine (ad esempio: `"293cc667-44b4-48ab-91d8-44bc74252a4f:2"`), che identifica il punto di ripristino.

6. Per selezionare il punto di ripristino per il rollback, immettere il seguente comando:

`r [volume_recovery_point_ID_number] [path]`

Questo comando effettua il rollback dell'immagine del volume specificato mediante l'ID dal core al percorso specificato. Il percorso per il rollback è il percorso per il descrittore del file del dispositivo e non è la directory in cui è montato.

N.B.: Per identificare il punto di ripristino, è inoltre possibile specificare un numero di linea nel comando al posto del numero ID del punto di ripristino. In questo caso, utilizzare il numero di linea dell'agente/macchina (dall'output di `lm`), seguito dal numero di linea e lettera del volume del punto di ripristino, seguiti dal percorso, ad esempio, `r [machine_line_item_number] [recovery_point_line_number] [volume_letter] [path]`. In questo comando, [percorso] è il descrittore del file per l'effettivo volume.

Ad esempio, se l'output di `lm` elenca tre macchine agente, e si immette il comando `lr` per la numero 2, e si desidera eseguire il rollback del volume b a 23 punti di ripristino sul volume che è stato montato sulla directory `/mnt/data`, il comando è: `r2 23 b /mnt/data`.

7. Quando viene richiesto di procedere, immettere `y` per Sì.

   dopo che il rollback viene avviato, viene visualizzata una serie di messaggi che informano l'utente dello stato.

8. Al termine di un rollback, l'utility `aamount` monta automaticamente e ricollega il modulo del kernel sul volume per cui è stato eseguito il rollback se la destinazione è stata precedentemente protetta e montata. In caso contrario, montare il volume per cui è stato eseguito il rollback sul disco locale, quindi verificare che i file siano stati ripristinati.

   Ad esempio, è possibile utilizzare il comando `sudo mount` e quindi il comando `ls`.

Avvio del ripristino bare metal per macchine Windows

AppAssure offre la possibilità di eseguire un Bare Metal Restore (BMR) per le macchine Windows sia per hardware simili che per hardware diversi. Questo processo prevede la creazione di un'immagine del CD di avvio, masterizzazione dell'immagine su disco, avviando il server di destinazione dal disco, connessione a un'istanza della console di ripristino, mapping dei volumi, avvio del ripristino e il monitoraggio del processo. A seguito del completamento del ripristino bare metal, è possibile continuare con l'operazione di caricamento del sistema operativo e delle applicazioni software sul server ripristinato, seguito dalle impostazioni e configurazione univoche.

Le altre circostanze in cui è possibile scegliere di eseguire il ripristino bare metal sono l'aggiornamento hardware o la sostituzione del server.

La funzione BMR è supportata anche dalle macchine Linux protette tramite la utility della riga di comando `aamount`. Per ulteriori informazioni, consultare Avvio del ripristino bare metal per una macchina Linux.

Roadmap per l'esecuzione di un ripristino bare metal per un computer Windows

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.

Creazione di un'immagine ISO su CD di avvio

Per eseguire un ripristino BMR per una macchina Windows, è necessario creare un CD di avvio/immagine ISO nella Core Console, che contiene l'interfaccia dell'AppAssure Universal Recovery Console. L'AppAssure Universal Recovery Console è un ambiente utilizzato per il ripristino l'unità di sistema o dell'intero server direttamente dall'AppAssure Core.

L'immagine ISO che si sta creando è fatta su misura per la macchina che viene ripristinata; pertanto, deve contenere la rete corretta e i driver di archiviazione di massa. Se si prevede l'esecuzione del ripristino su hardware diverso dalla macchina su cui si sta creando il CD di avvio, è necessario includere il controller dell'archiviazione e altri driver nel CD di avvio, consultare Inserimento dei driver in un CD di avvio.

N.B.: L'International Organization for Standardization (ISO) è un ente internazionale di rappresentanti provenienti da diverse organizzazioni nazionali con lo scopo di determinare e definire gli standard del file system. L'ISO 9660 è uno standard di file system utilizzato per i supporti del disco ottico per lo scambio dati. Supporta diversi sistemi operativi, tra cui Windows. Un'immagine ISO è un file di archivio o immagine disco, che contiene i dati di ogni porzione del disco, nonché il file system del disco.

Per creare un'immagine ISO su CD di avvio:

1. Dalla Core Console su cui si trova il server che si desidera ripristinare, selezionare **Core**, quindi fare clic sulla scheda **Strumenti**.
2. Fare clic su **CD di avvio**.
3. Selezionare **Azioni**, quindi fare clic su **Crea ISO di avvio**.

   Viene visualizzata la finestra di dialogo **Crea CD di avvio**. Per completare la finestra di dialogo, utilizzare le procedure descritte di seguito.

Denominazione del file del cd di avvio e impostazione del percorso

Per denominare il file del CD di avvio e impostare il percorso:

Nella finestra di dialogo **Crea CD di avvio**, inserire il percorso ISO nel quale archiviare l'immagine di avvio sul server Core.

Se la condivisione nella quale si desidera archiviare l'immagine non dispone di sufficiente spazio su disco, è possibile impostare il percorso in base alle necessità; ad esempio, D:\nomefile.iso.

N.B.: L'estensione del file deve essere .iso. Per specificare il percorso, utilizzare solo caratteri alfanumerici, il trattino e il punto (solo per separare i nomi host e i domini). Le lettere dalla a alla z rilevano la distinzione tra maiuscole e minuscole. Non utilizzare spazi. Non sono consentiti altri simboli o caratteri di punteggiatura.

Creazione di connessioni

Per creare connessioni:

1. In **Opzioni di connessione** effettuare una delle operazioni riportate di seguito:
   - Per ottenere l'indirizzo IP dinamicamente tramite il Dynamic Host Configuration Protocol (DHCP), selezionare **Ottieni indirizzo IP automaticamente**.

- Facoltativamente, per specificare un indirizzo IP statico per la console di ripristino, selezionare **Utilizza il seguente indirizzo IP** e inserire l'indirizzo IP, subnet mask, gateway predefinito e server DNS nei campi appropriati. È necessario specificare tutti questi campi.

2. Se necessario, in **Opzioni UltraVNC**, selezionare **Aggiungi UltraVNC**, quindi inserire le opzioni UltraVNC. Le impostazioni UltraVNC consentono di gestire la console di ripristino in remoto mentre è in uso.

   N.B.: Questo passaggio è facoltativo. Per l'accesso in remoto alla console di ripristino, è necessario configurare e utilizzare UltraVNC. Non è possibile accedere utilizzando Microsoft Terminal Services durante l'utilizzo del CD di avvio.

Inserimento dei driver in un CD di avvio

L'inserimento del driver è utilizzato per facilitare l'operabilità tra la console di ripristino, la scheda di rete e lo spazio di archiviazione sul server di destinazione.

Se si prevede il ripristino su un hardware diverso, è necessario inserire il controller dell'archiviazione, RAID, AHCI, chipset e altri driver nel CD di avvio. Questi driver permettono al sistema operativo di rilevare e azionare con successo tutti i dispositivi.

N.B.: Tenere presente che il CD di avvio conterrà automaticamente i driver a 32-bit di Windows 7 PE.

Per inserire i driver in un CD di avvio:

1. Scaricare i driver dal sito web del produttore per il server ed estrarli dal pacchetto.
2. Comprimere la cartella che contiene i driver utilizzando un'utility di compressione file, come WinZip.
3. Nella finestra di dialogo **Crea CD di avvio**, nel riquadro **Driver**, fare clic su **Aggiungi driver**.
4. Per individuare il file compresso del driver, esplorare il sistema di archiviazione. Selezionare il file, quindi fare clic su **Apri**.

   I driver inseriti saranno evidenziati nel riquadro **Driver**.

Creazione del CD di avvio

Per creare un CD di avvio, dopo aver denominato il CD di avvio, specificato il percorso, creato un collegamento e, facoltativamente inserito i driver, dalla schermata **Creare un CD di avvio**, fare clic su **Crea CD di avvio**. Viene quindi creata l'immagine ISO.

Visualizzazione dell'avanzamento della creazione di un'immagine ISO

Per visualizzare l'avanzamento della creazione di un'immagine ISO, selezionare la scheda **Eventi** e, in **Attività**, è possibile monitorare l'avanzamento della creazione dell'immagine ISO.

N.B.: È anche possibile visualizzare l'avanzamento della creazione dell'immagine ISO nella finestra di dialogo **Monitora attività in corso**.

Quando la creazione dell'immagine ISO è completa, è disponibile sulla pagina **CD di avvio**, accessibile dal menu **Strumenti**.

Accesso all'immagine ISO

Per accedere all'immagine ISO, passare al percorso di output specificato. In alternativa, è possibile fare clic sul collegamento per scaricare l'immagine in una posizione da cui è possibile caricarla sul nuovo sistema. Ad esempio, un'unità di rete.

Caricamento di un CD di avvio

Dopo aver creato l'immagine del CD di avvio, avviare il server di destinazione con il CD di avvio appena creato.

N.B.: Se si è creato il CD avvio utilizzando DHCP, prendere nota dell'indirizzo IP e della password.

Per caricare un CD di avvio:

1. Passare al nuovo server, caricare il CD di avvio, quindi avviare la macchina.
2. Specificare **Avvia da CD-ROM**, che carica i seguenti:
   - Windows 7 PE
   - Software AppAssure Agent

   La AppAssure Universal Recovery Console si avvia e visualizza l'indirizzo IP e la password di autenticazione per la macchina.
3. Prendere nota dell'indirizzo IP visualizzato nel riquadro Impostazioni schede di rete e la password di autenticazione visualizzata nel riquadro Autenticazione. Queste informazioni saranno utilizzate in seguito durante il processo di ripristino dei dati per accedere nuovamente alla console.
4. Se si desidera modificare l'indirizzo IP, selezionarlo e fare clic su **Modifica**.

   N.B.: Se è stato specificato un indirizzo IP nella finestra di dialogo Crea CD di avvio, la Universal Recovery Console lo utilizza e lo visualizza nella schermata **Impostazioni scheda di rete**.

Inserimento dei driver nel server di destinazione

Se si effettua un ripristino su un hardware diverso, è necessario avere inserito lo storage controller, RAID, AHCI, chipset e altri driver se non si trovano già nel CD di avvio. Questi driver permettono al sistema operativo di far funzionare con successo tutti i dispositivi sul server di destinazione.

Se non si è certi di quali siano i driver che il server di destinazione richiede, fare clic sulla scheda **Informazioni di sistema** nella Universal Recovery Console. Questa scheda mostra tutti i tipi di dispositivi e hardware di sistema del server di destinazione su cui si desidera eseguire il ripristino.

N.B.: Tenere presente che il server di destinazione contiene automaticamente i driver di Windows 7 PE a 32 bit.

Per inserire i driver nel server di destinazione:

1. Scaricare i driver dal sito web del produttore per il server ed estrarli dal pacchetto.
2. Comprimere la cartella contenente i driver utilizzando un'utilità di compressione dei file (ad esempio Winzip) e copiarlo nel server di destinazione.
3. Nella Universal Recovery Console, fare clic su **Inserimento driver**.
4. Per individuare il file del driver compresso, esplorare il sistema di archiviazione e selezionare il file.
5. Se si è fatto clic su **Inserimento driver** al punto 3, fare clic su **Aggiungi driver**. Se si è fatto clic su **Carica driver** al punto 3, fare clic su **Apri**.

   I driver selezionati sono inseriti e verranno caricati nel sistema operativo dopo il riavvio del server di destinazione.

Avvio di un ripristino dal Core

Per avviare un ripristino dal Core:

1. Se le schede NIC su qualsiasi sistema in fase di ripristino sono raggruppate (collegate), rimuovere tutti i cavi di rete tranne uno.

   N.B.: AppAssure Restore non riconosce le schede NIC raggruppate. Il processo non è in grado di decidere quale scheda NIC utilizzare nel caso in cui si trovasse di fronte a più di una connessione attiva.
2. Tornare al server Core e aprire la Core Console.

3. Nella scheda **Macchine**, selezionare la macchina da cui si desidera ripristinare i dati.
4. Fare clic sul menu **Azioni** della macchina, fare clic su **Punti di ripristino** per visualizzare un elenco di tutti i punti di ripristino per quella macchina.
5. Espandere il punto di ripristino da cui si desidera eseguire il ripristino, quindi fare clic su **Rollback**.
6. Nella finestra di dialogo **Rollback**, sotto Scegli **destinazione**, selezionare **Istanza console di ripristino**.
7. Nelle caselle di testo **Host** e **Password**, inserire l'indirizzo IP e la password di autenticazione del nuovo server sul quale si desidera ripristinare i dati.

   N.B.: I valori Host e Password sono le credenziali annotate nella precedente attività. Per ulteriori informazioni, consultare Caricamento CD di avvio.
8. Fare clic su **Carica volumi** per caricare i volumi di destinazione nella nuova macchina.

Mapping dei volumi

È possibile scegliere di mappare automaticamente o manualmente i volumi ai dischi nel server di destinazione. Per l'allineamento automatico del disco, il disco viene pulito e ripartizionato, e vengono eliminati tutti i dati. L'allineamento viene eseguito nell'ordine in cui sono elencati i volumi e questi vengono allocati ai dischi in modo appropriato in base a dimensioni, ecc. Più volumi possono utilizzare un disco. Se si mappano manualmente le unità, non è possibile utilizzare lo stesso disco due volte.

Per eseguire il mapping manuale, è necessario disporre già della nuova macchina formattata correttamente prima di ripristinarla.

Per mappare i volumi:

1. Per mappare automaticamente i volumi, eseguire le operazioni seguenti:
   a. Nella pagina **Mapping dei dischi** del **Ripristino guidato della macchina**, selezionare la scheda **Mappa automaticamente i volumi**.
   b. Nell'area **Mapping dei dischi**, in **Volume di origine** verificare che il volume di origine sia selezionato e che i volumi idonei siano elencati nel seguito e selezionati.
   c. Se il disco di destinazione mappato automaticamente è il volume di destinazione corretto, selezionare **Disco di destinazione**.
   d. Fare clic su **Ripristina** e passare al punto 3.
2. Per mappare manualmente i volumi, eseguire le operazioni seguenti:
   a. Nella pagina **Mapping dei dischi** del **Ripristino guidato della macchina**, selezionare la scheda **Mappa manualmente i volumi**.
   b. Nell'area **Mapping dei volumi**, in **Volume di origine** verificare che il volume di origine sia selezionato e che i volumi idonei siano elencati nel seguito e selezionati.
   c. In **Destinazione**, dal menu a discesa selezionare la destinazione appropriata che rappresenta il volume di destinazione per eseguire il ripristino bare metal del punto di ripristino selezionato, quindi fare clic su **Rollback**.
3. Nella finestra di dialogo di conferma **RollbackURC** controllare il mapping dell'origine del punto di ripristino e il volume di destinazione per il rollback. Per eseguire il rollback, fare clic su **Ripristina**.

   ATTENZIONE: Se si seleziona Inizia rollback, tutte le partizioni e i dati esistenti nell'unità di destinazione verranno rimossi definitivamente e sostituiti con il contenuto del punto di ripristino selezionato, inclusi sistema operativo e tutti i dati.

Visualizzazione dell'avanzamento del ripristino

Per visualizzare l'avanzamento del ripristino:

1. Dopo aver avviato il processo di rollback, viene visualizzata la finestra di dialogo **Attività in corso** che mostra il rollback in esecuzione.

N.B.: Questo aspetto della finestra di dialogo **Attività in corso** non indica il completamento andato a buon fine dell'attività.

2. In alternativa, per monitorare lo stato di avanzamento dell'attività di rollback, dalla finestra di dialogo Attività in corso, fare clic su **Apri finestra di monitoraggio**. È possibile visualizzare lo stato del ripristino, nonché l'ora di inizio e di fine dalla finestra **Monitora l'attività aperta**.

   N.B.: Per tornare ai punti di ripristino della macchina di origine dalla finestra di dialogo **Attività in corso**, fare clic su **Chiudi**.

Avvio del server di destinazione ripristinato

Per avviare il server di destinazione ripristinato:

1. Tornare al server di destinazione e nell'interfaccia **AppAssure Universal Recovery Console**, fare clic su **Riavvia** per riavviare la macchina.
2. Specificare l'avvio normale di Windows.
3. Accedere alla macchina.

   Viene ripristinato lo stato del sistema precedente al ripristino bare metal.

Risoluzione dei problemi di avvio

Si ricorda che, se si è effettuato un ripristino su un hardware diverso, è necessario avere inserito il controller dell'archiviazione, RAID, AHCI, chipset e altri driver se non si trovano già nel CD di avvio. Questi driver permettono al sistema operativo di far funzionare correttamente tutte le periferiche sul server di destinazione.

Per risolvere i problemi di avvio:

1. Se si verificano problemi durante l'avvio del server di destinazione ripristinato, aprire la Universal Recovery Console ricaricando il CD di avvio.
2. Nella Universal Recovery Console, fare clic su **Inserimento driver**.
3. Nella finestra di dialogo Inserimento driver, fare clic su **Correggi problemi di avvio**.

   I parametri di avvio nel record di avvio del server di destinazione vengono automaticamente ripristinati.
4. Nella Universal Recovery Console, fare clic su **Riavvia**.

Avvio del ripristino bare metal per una macchina Linux

Il DL1300 può eseguire un Bare Metal Restore (BMR) per una macchina Linux includendo il rollback del volume di sistema. Usando l'utility della riga di comando AppAssure `aamount`, eseguire il rollback sull'immagine di base del volume di avvio. Prima di poter eseguire un BMR per una macchina Linux, è innanzitutto necessario effettuare le operazioni riportate di seguito:

- Ottenere un file del CD del BMR Live dal supporto AppAssure, che include una versione di Linux avviabile.

  N.B.: È anche possibile scaricare il file del CD Linux Live dal portale delle licenze all'indirizzo **https://licenseportal.com**.
- 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.
- Identificare il percorso per il rollback, che è il percorso per il descrittore del file del dispositivo. Per identificare il percorso del descrittore del file del dispositivo, utilizzare il comando `fdisk` da una finestra terminale.

N.B.: Prima di iniziare ad utilizzare i comandi AppAssure, è possibile installare l'utilità schermo. L'utilità schermo consente di scorrere la schermata per visualizzare maggiori quantità di dati, ad esempio un elenco di punti di ripristino.

Per eseguire un ripristino bare-metal per una macchina Linux:

1. Utilizzando il file del CD Live ricevuto da AppAssure, avviare la macchina Linux e aprire una finestra terminale.
2. Se necessario, creare una nuova partizione del disco, per esempio, eseguendo il comando `fdisk` comando come root, e rendere questa partizione avviabile utilizzando il comando `a`.
3. Eseguire l'utility `aamount` di AppAssure come root, ad esempio:

   ```
   sudo aamount
   ```
4. Al prompt di montaggio di AppAssure, inserire il seguente comando per elencare le macchine protette:

   ```
   lm
   ```
5. Quando richiesto, inserire l'indirizzo IP o il nome host del server AppAssure Core.
6. Immettere le credenziali di accesso, ovvero il nome utente e la password, per questo server.

   Viene visualizzato un elenco delle macchine protette da questo server AppAssure Core. Vi sono elencate le macchine rilevate mediante numero linea dell'elemento, indirizzo host/IP e un numero ID della macchina (ad esempio: `293cc667-44b4-48ab-91d8-44bc74252a4f`).
7. Per elencare i punti di ripristino attualmente montati per la macchina che si desidera ripristinare, inserire il seguente comando:

   ```
   lr <machine_line_item_number>
   ```

   N.B.: Inoltre, è possibile inserire il numero ID della macchina in questo comando al posto del numero linea dell'elemento.

   Viene visualizzato un elenco che mostra i punti di ripristino base e incrementali per tale macchina. Questo elenco include un numero linea dell'elemento, date/timestamp, la posizione del volume, le dimensioni del punto di ripristino, e un numero ID per il volume che include un numero di sequenza alla fine (ad esempio: "`293cc667-44b4-48ab-91d8-44bc74252a4f:2`"), che identifica il punto di ripristino.
8. Per selezionare il punto di ripristino dell'immagine di base per il rollback, immettere il seguente comando:

   ```
   r <volume_base_image_recovery_point_ID_number> <path>
   ```

   ATTENZIONE: L'utente deve accertarsi che il volume di sistema non sia montato.

   Questo comando effettua il rollback dell'immagine del volume specificato mediante l'ID dal core al percorso specificato. Il percorso per il rollback è il percorso per il descrittore del file del dispositivo e non è la directory in cui è montato.

   N.B.: È inoltre possibile specificare un numero di linea nel comando al posto del numero ID del punto di ripristino per identificare il punto di ripristino. Utilizzare il numero di linea dell'agente/macchina (dall'output di lm), seguito dal numero di linea e lettera del volume del punto di ripristino, seguiti dal percorso, ad esempio, **r <machine_line_item_number> <base_image_recovery_point_line_number> <volume_letter> <path>**. In questo comando, `<path>` è il descrittore del file per l'effettivo volume.
9. Quando viene richiesto di procedere, immettere `y` per Sì.

   Dopo che il rollback viene avviato, viene visualizzata una serie di messaggi che informano l'utente dello stato.

10. Al termine di un rollback, se necessario, aggiornare il record di avvio principale con il boot loader ripristinato.

    N.B.: La riparazione o impostazione del boot loader è necessaria solo se questo disco è nuovo. Se si tratta di un semplice rollback sullo stesso disco, l'impostazione del boot loader non è necessaria.

    ATTENZIONE: Non smontare un volume protetto di Linux manualmente. Nel caso in cui sia necessario smontare manualmente un volume protetto di Linux, è necessario eseguire il seguente comando prima di smontare il volume: bsctl -d <percorso per il volume>

    In questo comando, `<path to volume>` non si riferisce al punto di montaggio del volume ma al descrittore del file del volume; deve essere in un formato analogo a quello di questo esempio: **/dev/sda1**.

Installazione dell'utilità schermo

Prima di iniziare ad utilizzare i comandi AppAssure, è possibile installare l'utilità schermo. L'utilità schermo consente di scorrere la schermata per visualizzare maggiori quantità di dati, ad esempio un elenco di punti di ripristino.

Per installare l'utilità schermo:

1. Utilizzando il file Live CD, avviare la macchina Linux.

   Si apre una finestra terminale.
2. Inserire il seguente comando: `sudo apt-get install screen`.
3. Per avviare l'utilità schermo, digitare `screen` nel prompt dei comandi.

Creazione di partizioni avviabili su una macchina Linux

Per creare partizioni avviabili su una macchina Linux utilizzando la riga di comando:

1. Collegare tutti i dispositivi che utilizzano l'utility **bsctl** con il seguente comando come root: `sudo bsctl --attach-to-device /dev/<restored volume>`

   N.B.: Ripetere l'operazione per ogni volume ripristinato.
2. Montare ciascun volume ripristinato utilizzando i seguenti comandi:

   ```
   mount /dev/<restored volume> /mnt

   mount /dev/<restored volume> /mnt
   ```

   N.B.: Alcune configurazioni del sistema potrebbero includere la directory di avvio come parte del volume principale.
3. Montare i metadati delle istantanee per ciascun volume ripristinato utilizzando i seguenti comandi:

   ```
   sudo bsctl --reset-bitmap-store /dev/<restored volume>

   sudo bsctl --map-bitmap-store /dev/<restored volume>
   ```
4. Verificare che l'UUID (Universally Unique Identifier) contenga i nuovi volumi utilizzando il comando `blkid` o il comando `ll /dev/disk/by-uuid`.
5. Verificare che `/etc/fstab` contenga gli UUID corretti per i volumi principali e di avvio.
6. Installare Grand Unified Bootloader (GRUB) utilizzando i seguenti comandi:

   ```
   mount --bind /dev/ /mnt/dev
   ```

```
mount --bind /proc/ /mnt/proc

chroot/mnt/bin/bash

grub-install/dev/sda
```

7. Verificare che il file **/boot/grub/grub.conf** contenga il corretto UUID per il volume principale o l'aggiornamento in base alle necessità, utilizzando un editor di testo.
8. Rimuovere il disco CD Live dall'unità CD-ROM e riavviare la macchina Linux.

6

Replica dei punti di ripristino

Replica

La replica è il processo di copia dei punti di ripristino e del loro trasferimento in una posizione secondaria ai fini del disaster recovery. Il processo richiede la presenza di un rapporto origine-destinazione associato tra due core. La replica è gestita su una base di singola macchina protetta; questo significa che le istantanee del backup di una macchina protetta vengono replicate al core di replica di destinazione. Quando viene impostata la replica, il core di origine trasmette in modo asincrono e in modo continuativo i dati incrementali delle istantanee al core di destinazione. È possibile configurare la replica in uscita per il data center della propria azienda o di un sito remoto per il disaster recovery (cioè un core di destinazione "autogestito") o per un provider di servizi gestiti (MSP), offrendo servizi di backup e disaster recovery off-site. Quando si effettua la replica su un MSP, è possibile utilizzare i workflow integrati che consentono di richiedere connessioni e ricevere notifiche automatiche dei feedback.

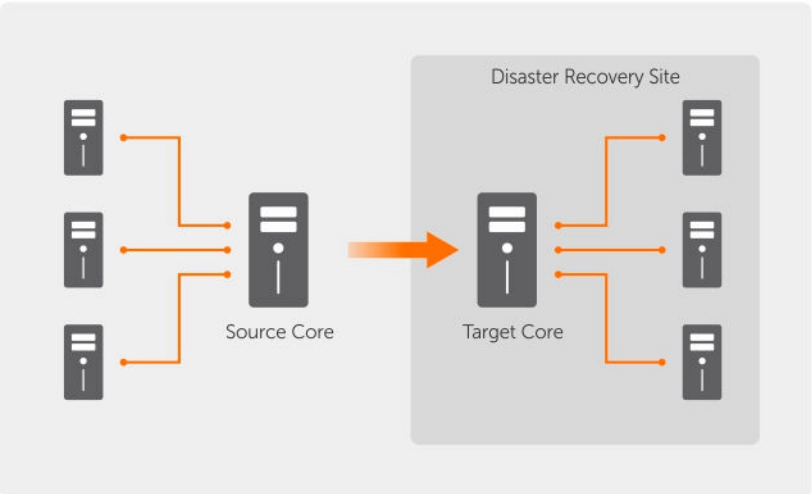


Figura 5. Architettura base della replica

La replica inizia con il seeding. Il trasferimento iniziale di immagini deduplicate di base e di copie istantanee incrementali degli agenti protetti, 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.

Roadmap per l'esecuzione di una replica

Per replicare i dati utilizzando AppAssure, è necessario configurare il core di origine e di destinazione per la replica. Una volta configurata la replica, quindi, è possibile replicare i dati della macchina protetta, monitorare e gestire la replica ed eseguire il ripristino.

L'esecuzione della replica in AppAssure prevede l'esecuzione delle seguenti operazioni:

- Configurazione della replica autogestita. Per ulteriori informazioni sull'esecuzione della replica su un core di destinazione autogestito, consultare Replica su un core autogestito.
- Configurazione della replica di terzi. Per ulteriori informazioni sull'esecuzione della replica su un core di destinazione di terzi, consultare Replica su un core gestito da terzi.
- Replicare una nuova macchina protetta collegata al core di origine. Per ulteriori informazioni sull'esecuzione della replica di macchine protette, consultare Replica di una nuova macchina protetta.
- Replicare una macchina protetta esistente. Per ulteriori informazioni su come configurare un agente per la replica, consultare Replica dei dati agente su una macchina.
- Impostare la priorità di replica per un agente. Per ulteriori informazioni sulla definizione delle priorità della replica di agenti, consultare Impostazione delle priorità di replica per un agente.
- Monitorare le repliche in base alle necessità. Per ulteriori informazioni sul monitoraggio delle repliche, consultare Monitoraggio della replica.
- Gestire le impostazioni di replica in base alle necessità. Per ulteriori informazioni sulla gestione delle impostazioni delle repliche, consultare Gestione delle impostazioni di replica.
- Ripristino dei dati replicati in caso di emergenza o perdita dei dati. Per ulteriori informazioni sul ripristino dei dati replicati, consultare Ripristino dei dati replicati.

Replica su un core autogestito

Un core autogestito è un core a cui si ha accesso, spesso perché è gestito dall'azienda in posizioni fuori sede. La replica può essere completata interamente sul core di origine, a meno che non si scelga il seeding dei dati. Il seeding richiede che vega consumata l'unità seed sul core di destinazione dopo aver configurato la replica sul core di origine.

N.B.: Questa configurazione è valida per la replica in posizioni fuori sede e per la replica reciproca. Il core deve essere installato su tutte le macchine di origine e di destinazione. Se si sta configurando il sistema per la replica multi-punto per punto, è necessario eseguire questa attività su tutti i core di origine e sul core di destinazione.

Configurazione del core di origine per replicare in un core di destinazione autogestito

Per configurare il core di origine per replicare in un core di destinazione autogestito:

1. Nel Core, fare clic sulla scheda **Replica**.
2. Fare clic su **Aggiungi core di destinazione**.
   Viene visualizzata la procedura guidata **Replica**.
3. Selezionare **Ho un Core di origine personale**, quindi immettere le informazioni come descritto nella tabella seguente.

Casella di testo	Descrizione
Nome host	Immettere il nome host o l'indirizzo IP della macchina del Core che si desidera replicare.

Casella di testo	Descrizione
Porta	Immettere il numero di porta in cui AppAssure Core comunica con la macchina. Il numero di porta predefinita è 8006.
Nome utente	Immettere il nome utente per accedere alla macchina, per esempio **Amministratore**.
Password	Immettere la password per accedere alla macchina.

Se il Core che si desidera aggiungere è stato associato a questo core in precedenza, effettuare uno dei seguenti:

a. Selezionare **Usa un core di destinazione esistente**.
b. Selezionare il core di destinazione dall'elenco a discesa.
c. Fare clic su **Avanti**.
d. Passare al punto 7.

4. Fare clic su **Avanti**.
5. Nella pagina **Dettagli** immettere un nome per questa configurazione di replica, per esempio SourceCore1. Se si sta reinizializzando o ripristinando una configurazione di replica precedente, selezionare **Il mio Core è stato migrato e desidero ripristinare la replica**
6. Fare clic su **Avanti**.
7. Nella pagina **Agenti** selezionare gli agenti da replicare, quindi usare gli elenchi a discesa nella colonna **Repository** per selezionare un repository per ogni agente.
8. Se si pianifica di eseguire il processo di seeding per il trasferimento dei dati di base, eseguire le operazioni seguenti:

   N.B.: Poiché nel dispositivo di archiviazione portatile devono essere copiate grandi quantità di dati, si consiglia l'utilizzo di una connessione eSATA, USB 3.0 o ad alta velocità di altro tipo.

   a. Nella pagina **Agenti** selezionare **Usa un'unità seed per eseguire il trasferimento iniziale**. Se attualmente si dispone di una o più macchine che eseguono la replica in un core di destinazione, è possibile includere tali macchine protette nell'unità seed selezionando **Già replicate**.
   b. Fare clic su **Avanti**.
   c. Nella pagina **Posizione dell'unità seed** usare l'elenco a discesa **Tipo di posizione** per selezionare uno dei seguenti:
      - Locale: nella casella di testo **Posizione** immettere il percorso in cui salvare l'unità seed, per esempio D:\work\archive.
      - Rete: nella casella di testo **Posizione** immettere il percorso in cui salvare l'unità seed, poi immettere le credenziali della condivisione di rete nelle caselle di testo **Nome utente** e **Password**.
      - Cloud: nella casella di testo **Account** selezionare l'account. Per selezionare un account cloud, è necessario averlo aggiunto prima nella Core Console. Per maggiori informazioni, consultare Aggiunta di un account cloud. Selezionare il **Contenitore** associato all'account. Selezionare il **Nome cartella** in cui salvare i dati archiviati.
   d. Fare clic su **Avanti**.

9. Nella casella di dialogo **Opzione dell'unità seed**, immettere le informazioni descritte come segue:

Casella di testo	Descrizione
Dimensione massima	Gli archivi di dati di grandi dimensioni possono essere suddivisi in più segmenti. Selezionare la dimensione massima del segmento che si desidera riservare per creare l'unità seed effettuando una delle seguenti operazioni:

Casella di testo	Descrizione
	• Selezionare **Intera destinazione** per riservare tutto lo spazio disponibile nel percorso fornito nella pagina Posizione dell'unità seed per uso futuro (per esempio se la posizione è D:\work\archive, tutto lo spazio disponibile nell'unità D: è riservato se necessario per copiare l'unità seed, ma non viene riservato immediatamente dopo l'avvio del processo di copia). • Selezionare la casella di testo vuota, immettere una quantità, quindi selezionare un'unità di misura dall'elenco a discesa per personalizzare lo spazio massimo da riservare.
ID cliente (opzionale)	Facoltativamente, immettere l'ID del cliente che è stato assegnato all'utente dal provider di servizi.
Azione riciclo	Nel caso in cui il percorso contenga già un'unità seed, selezionare una delle seguenti opzioni: • **Non riutilizzare** - Non sovrascrive o cancella gli eventuali dati esistenti dalla posizione. Se la posizione non è vuota, la scrittura dell'unità seed non viene eseguita. • **Sostituisci questo core** - Sovrascrive gli eventuali dati preesistenti relativi a questo core, ma lascia intatti i dati degli altri core. • **Cancella completamente** - Cancella tutti i dati dalla directory prima di scrivere la nuova unità seed.
Commento	Immettere un commento o la descrizione dell'archivio.
Aggiungi tutti gli agenti all'unità seed	Selezionare gli agenti che si desidera replicare utilizzando l'unità seed.
Creare catene RP (correggere gli orfani)	Selezionare questa opzione per replicare l'intera catena di punti di ripristino nell'unità seed. Questa opzione è selezionata per impostazione predefinita. Il seeding tipico in AppAssure replica solo il punto di ripristino più recente nell'unità seed, il che riduce la quantità di tempo e lo spazio richiesto per creare l'unità seed. La scelta della creazione di catene di punti di ripristino (RP) nell'unità seed richiede spazio sufficiente in essa per archiviare i punti di ripristino più recenti dall'agente o dagli agenti specificati, e può richiedere tempo aggiuntivo per completare l'attività.
Usa formato compatibile	Selezionare questa opzione per creare l'unità seed in un formato che sia compatibile con versioni nuove e precedenti di AppAssure Core.

10. Nella pagina **Agenti** selezionare gli agenti da replicare nel core di destinazione usando l'unità seed.
11. Fare clic su **Fine**.
12. Se è stata creata un'unità seed, inviarla al core di destinazione.

    L'associazione del core di origine al core di destinazione è stata completata. La replica inizia ma produce punti di ripristino orfani nel core di destinazione finché l'unità seed viene consumata e fornisce le immagini di base necessarie.

Consumo dell'unità seed in un core di destinazione

Questa procedura è necessaria solo se è stata creata un'unità seed durante la Configurazione della replica per un core autogestito.

Per consumare l'unità seed in un core di destinazione:

1. Se l'unità seed è stata salvata in un dispositivo di archiviazione portatile, come un'unità USB, connettere l'unità al core di destinazione.
2. Dalla Core Console del core di destinazione, selezionare la scheda **Replica**.
3. In **Replica in entrata**, selezionare il core di origine corretto usando il menu a discesa, quindi fare clic su **Consumo**.

   Viene visualizzata la finestra Consumo.
4. Per **Tipo di posizione**, selezionare una delle seguenti opzioni dall'elenco a discesa:
   - Locale
   - Rete
   - Cloud
5. Immettere le informazioni seguenti, se necessario:

Casella di testo	Descrizione
Posizione	Immettere un percorso in cui deve trovarsi l'unità seed, come un'unità USB o una condivisione di rete (per esempio D:\).
Nome utente	Immettere il nome utente per l'unità o cartella condivisa. Il nome utente è richiesto solo per un percorso di rete.
Password	Immettere la password per l'unità o cartella condivisa. La password è richiesta solo per un percorso di rete.
Account	Selezionare un account dall'elenco a discesa. Per selezionare un account cloud, è necessario averlo aggiunto prima nella Core Console.
Contenitore	Selezionare un contenitore associato all'account dal menu a discesa.
Nome cartella	Immettere il nome della cartella in cui vengono salvati i dati archiviati; ad esempio, -Archive-[DATA CREAZIONE]- [ORA CREAZIONE]

6. Fare clic su **Controlla file.**

   Dopo che il Core controlla il file, esso popola automaticamente l'**Intervallo date** con le date dei punti di ripristino meno recente e più recente contenuti nell'unità seed, ed importa anche gli eventuali commenti inseriti in Configurazione della replica per un core autogestito.
7. Sotto **Nomi agenti** nella finestra **Consumo**, selezionare le macchine di cui si desiderano i dati di consumo, quindi fare clic su **Consumo**.

   N.B.: Per monitorare l'avanzamento del consumo dei dati selezionare la scheda **Eventi**.

Abbandonare un'unità seed in sospeso

Se si crea un'unità seed con l'intento di consumarla sul core di destinazione ma si scegliere di non inviarla alla posizione remota, rimane un collegamento per l'unità seed in sospeso nella scheda **Replica** del core di origine. Si può scegliere di abbandonare l'unità seed in sospeso a favore di dati seed diversi o più attuali.

N.B.: Questa procedura rimuove il collegamento all'unità seed in sospeso dalla Core Console sul core di origine. Non rimuove l'unità dalla posizione di archiviazione su cui è stata salvata.

Per abbandonare un'unità seed in sospeso:

1. Dalla Core Console del core di origine, selezionare la scheda **Replica**.
2. Fare clic su **Unità seed in sospeso (n.)**.

Viene visualizzata la sezione **Unità seed in sospeso** , che include il nome del core di destinazione remoto, i dati e l'ora in cui l'unità seed è stata creata e il range di dati dei punti di ripristino incluso nell'unità seed.

3. Fare clic sul menu a discesa dell'unità che si desidera abbandonare, quindi selezionare **Abbandona**.

   Viene visualizzata la finestra **Unità seed in sospeso**.

4. Fare clic su **Sì** per confermare l'azione.

   L'unità seed viene rimossa. Se non vi sono più unità seed nel core di origine, la volta successiva che si aprirà la scheda **Replica**, il collegamento **Unità seed in sospeso (n.)** e la sezione **Unità seed in sospeso** non verranno visualizzati.

Replica su un core gestito da terzi

Un core di terze parti è un core di destinazione gestito e mantenuto da un MSP. La replica su un core gestito da terzi non richiede l'accesso dell'utente al core di destinazione. Dopo che un cliente configura la replica su uno o più core di origine, l'MSP completa la configurazione sul core di destinazione.

N.B.: Questa configurazione è valida per la replica ospitata e in cloud. È necessario che AppAssure Core sia installato su tutte le macchine del core di origine.

Replica di un nuovo agente

Quando si aggiunge un AppAssure Agent per la protezione in un core di destinazione, AppAssure consente di replicare il nuovo agente in un core di destinazione esistente.

Per replicare un nuovo agente:

1. Passare alla Core Console, quindi fare clic sulla scheda **Macchine**.
2. Nel menu a discesa **Azioni** fare clic su **Proteggi macchina**.
3. Nella finestra di dialogo **Proteggi macchina**, immettere le informazioni descritte nella tabella seguente.

Casella di testo	Descrizione
Host	Immettere il nome host o l'indirizzo IP della macchina che si desidera proteggere.
Porta	Immettere il numero di porta che AppAssure Core usa per comunicare con l'agente nella macchina.
Nome utente	Immettere il nome utente usato per connettersi alla macchina, per esempio amministratore.
Password	Immettere la password utilizzata per connettersi a questa macchina.

4. Fare clic su **Connetti** per connettersi a questa macchina.
5. Fare clic su **Mostra opzioni avanzate** e modificare le seguenti impostazioni a seconda delle necessità.

Casella di testo	Descrizione
Nome visualizzato	Immettere un nome per la macchina da visualizzare nella Core Console.
Repository	Selezionare il repository nell'AppAssure Core in cui vengono archiviati i dati da questa macchina.

Casella di testo	Descrizione
Chiave di crittografia	Specificare se la crittografia deve essere applicata ai dati per ogni volume presente in questa macchina memorizzata nell'archivio. N.B.: Le impostazioni per la crittografia per un repository sono definite nella scheda **Configurazione** nella Core Console.
Core remoto	Specificare il core di destinazione in cui si desidera replicare l'agente.
Repository remoto	Il nome del repository desiderato nel core di destinazione in cui archiviare i dati replicati da questa macchina.
In pausa	Selezionare questa casella di controllo se si desidera sospendere la replica; ad esempio, per sospenderla finché AppAssure acquisisce un'immagine di base del nuovo agente.
Pianificazione	Selezionare una delle seguenti opzioni: • Proteggi tutti i volumi con pianificazione predefinita • Proteggi volumi specifici con pianificazione personalizzata N.B.: La pianificazione predefinita è ogni 15 minuti.
Sospendi inizialmente protezione	Selezionare questa casella di controllo se si desidera sospendere la protezione, ad esempio per evitare che AppAssure acquisisca l'immagine di base fino a dopo le ore di utilizzo massimo.

6. Fare clic su **Proteggi**.

Replica dei dati dell'agente in una macchina

La replica è il rapporto tra il core di origine e il core di destinazione nello stesso sito o tra due siti con collegamento lento su una base per agente. Quando viene configurata la replica tra due core, il core di origine trasmette in modo asincrono i dati incrementali delle istantanee degli agenti selezionati al core di origine o di destinazione. La replica in uscita può essere configurata al Managed Service Provider che fornisce un servizio di backup e disaster recovery off-site o ad un core autogestito. Per replicare i dati dell'agente in una macchina:

1. Dalla Core Console, fare clic sulla scheda **Macchine**.
2. Selezionare la macchina che si desidera replicare.
3. Nel menu a discesa **Azioni**, fare clic su **Replica**, quindi completare una delle opzioni riportate di seguito:
   - Se si sta configurando la replica, fare clic su **Abilita**.
   - Se si dispone già di un'impostazione di replica esistente, fare clic su **Copia**.

   Viene visualizzata la finestra di dialogo **Abilita repliche**.
4. Nella casella di testo **Host**, inserire un nome host.
5. In **Agenti**, selezionare la macchina che possiede l'agente e i dati che si desidera replicare.
6. Se necessario, selezionare la casella di controllo **Usa un'unità seed per eseguire il trasferimento iniziale**.
7. Fare clic su **Aggiungi**.
8. Per sospendere o riprendere la replica, fare clic su **Replica** nel menu a discesa **Azioni**, quindi fare clic su **Interrompi** o **Riprendi** a seconda delle necessità.

Impostazione della priorità di replica per un agente

Per impostare la priorità di replica per un agente:

1. Dalla Core Console, selezionare la macchina protetta per cui si desidera impostare la priorità di replica, quindi fare clic sulla scheda **Configurazione**.
2. Fare clic su **Selezionare le impostazioni di trasferimento**, quindi utilizzare l'elenco a discesa **Priorità** per selezionare una delle opzioni riportate di seguito:
   - **Predefinita**
   - **Massima**
   - **Minima**
   - **1**
   - **2**
   - **3**
   - **4**

   N.B.: La priorità predefinita è 5. Se ad un agente è assegnata la priorità 1 e ad un altro agente è assegnata la priorità Massima, l'agente con priorità Massima replica prima dell'agente con priorità 1.
3. Fare clic su **OK**.

Monitoraggio della replica

Quando viene impostata la replica, è possibile monitorare lo stato delle attività di replica per i core di origine e destinazione. È possibile aggiornare le informazioni sullo stato, visualizzare i dettagli sulle repliche, ecc.

Per monitorare la replica:

1. Nella Core Console, fare clic sulla scheda **Replica**.
2. In questa scheda, è possibile visualizzare le informazioni e monitorare lo stato delle attività di replica descritte nel modo seguente:

Tabella 5. Monitoraggio della replica

Sezione	Descrizione	Azioni disponibili
Richieste di replica in sospeso	Elenca l'ID del cliente, l'indirizzo di posta elettronica e il nome host quando una richiesta di replica viene inviata a un provider di servizi di terze parti. Vengono elencate qui finché l'MSP accetta la richiesta.	Nel menu a discesa, fare clic su **Ignora** per ignorare o rifiutare la richiesta.
Unità seed rilevanti	Elenca le unità seed che sono state scritte, ma non ancora consumate dal core di destinazione. Include il nome del core remoto, la data in cui è stato creato e l'intervallo di date.	Nel menu a discesa, fare clic su **Abbandona** per abbandonare o annullare il processo seed.

Sezione	Descrizione	Azioni disponibili
Replica in uscita	Elenca tutti i core di destinazione in cui il core di origine esegue la replica. Include il nome del core remoto, lo stato di esistenza, il numero di macchine protette da replicare e l'avanzamento di una trasmissione di replica.	In un core di origine, nel menu a discesa, è possibile selezionare le seguenti opzioni: • **Dettagli** — Elenca ID, URI, nome visualizzato, stato, ID cliente, indirizzo di posta elettronica e commenti per il core replicato. • **Modifica impostazioni** — Elenca il nome visualizzato e consente di modificare host e porta del core di destinazione. • **Aggiungi agenti** — Consente di selezionare un host da un elenco a discesa, selezionare le macchine protette per la replica e creare un'unità seed per il trasferimento iniziale delle nuove macchine protette.
Replica in entrata	Elenca tutte le macchine di origine da cui la destinazione riceve i dati replicati. Include nome, stato, macchine e avanzamento del core remoto.	In un core di destinazione, nel menu a discesa, è possibile selezionare le seguenti opzioni: • **Dettagli** — Elenca ID, nome host, ID del cliente, indirizzo di posta elettronica e commenti per il core replicato. • **Consumo** — Consuma i dati iniziali dall'unità seed e li salva nel repository locale.

3. Fare clic sul pulsante **Aggiorna** per aggiornare le sezioni di questa scheda con le informazioni più recenti.

Gestione delle impostazioni di replica

È possibile regolare determinate impostazioni della modalità di esecuzione della replica sul core di origine e di destinazione.

Per gestire le impostazioni di replica:

1. Nella Core Console, fare clic sulla scheda **Replica**.
2. Nel menu a discesa **Azioni**, fare clic su **Impostazioni**.
3. Nella finestra **Impostazioni di replica**, modificare le impostazioni di replica descritte come segue:

Opzione	Descrizione
Durata della cache	Specificare l'intervallo di tempo che deve intercorrere tra ciascuna richiesta di stato del core di destinazione eseguita dal core di origine.
Timeout della sessione	Specificare l'intervallo di tempo in cui il core di origine tenta di trasferire un'immagine del volume al core di destinazione.

Opzione	Descrizione
dell'immagine del volume	
Massimo di processi di replica simultanei	Specificare il numero di macchine protette cui è consentito replicare sul core di destinazione contemporaneamente.
Massimo di flussi paralleli	Specificare il numero di connessioni di rete consentite che un'unica macchina protetta può utilizzare per replicare i dati della macchina contemporaneamente.

4. Fare clic su **Salva**.

Rimozione di una replica

È possibile interrompere la replica e rimuovere le macchine protette dalla replica in diversi modi. Le opzioni sono:

- Rimozione di un agente dalla replica sul core di origine
- Rimozione di un agente sul core di destinazione
- Rimozione di un core di destinazione dalla replica
- Rimozione di un core di origine dalla replica

N.B.: Rimozione degli esiti di un core di origine durante la rimozione di tutte le macchine replicate che sono protette da tale core.

Rimozione di una macchina protetta dalla replica sul core di origine

Per rimuovere una macchina protetta dalla replica sul core di origine:

1. Dal core di origine, aprire la Core Console, quindi fare clic sulla scheda **Replica**.
2. Espandere la sezione **Replica in uscita**.
3. Nel menu a discesa della macchina protetta che si desidera rimuovere dalla replica, fare clic su **Elimina**.
4. Nella finestra di dialogo **Replica in uscita**, fare clic su **Sì** per confermare l'eliminazione.

Rimozione di una macchina protetta nel Core di destinazione

Per rimuovere una macchina protetta dal Core di destinazione:

1. Nel core di destinazione, aprire la Core Console, quindi fare clic sulla scheda **Replica**.
2. Espandere la sezione **Replica in entrata**.
3. Nel menu a discesa della macchina protetta che si desidera rimuovere dalla replica, fare clic su **Elimina**, quindi selezionare una delle opzioni riportate di seguito.

Opzione	Descrizione
Solo relazione	Rimuove la macchina protetta dalla replica ma conserva i punti di ripristino replicati.

Opzione	Descrizione
Con punto di ripristino	Rimuove la macchina protetta dalla replica ed elimina tutti i punti di ripristino replicati ricevuti dalla macchina.

Rimozione di un core di destinazione dalla replica

Per rimuovere un core di destinazione dalla replica:

1. Sul core di origine, aprire la Core Console e fare clic sulla scheda**Replica**.
2. In **Replica in uscita**, fare clic sul menu a discesa accanto al core remoto che si desidera eliminare e fare clic su **Elimina**.
3. Nella finestra di dialogo **Replica in uscita**, fare clic su **Sì** per confermare l'eliminazione.

Rimozione di un core di origine dalla replica

N.B.: Rimozione degli esiti del core di origine durante la rimozione di tutti gli agenti replicati protetti da tale core.

Per rimuovere un core di origine dalla replica:

1. Nel core di destinazione, aprire la Core Console, quindi fare clic sulla scheda **Replica**.
2. In **Replica in entrata**, nel menu a discesa, fare clic su **Elimina**, quindi selezionare una delle opzioni riportate di seguito.

Opzione	Descrizione
Solo relazione	Rimuove il core di origine dalla replica ma conserva i punti di ripristino replicati.
Con punti di ripristino	Rimuove il core di origine dalla replica ed elimina tutti punti di ripristino replicati ricevuti dalla macchina.

3. Nella finestra di dialogo**Replica in entrata**, fare clic su **Sì** per confermare l'eliminazione.

Ripristino dei dati replicati

La funzione di replica giornaliera viene mantenuta sul core di origine, mentre solo core di destinazione è in grado di completare le funzioni necessarie per il disaster recovery.

Per il disaster recovery, il core di destinazione può utilizzare i punti di ripristino replicati per ripristinare gli agenti protetti e il core.

È possibile eseguire le seguenti opzioni di ripristino dal core di destinazione:

- Montare i punti di ripristino.
- Eseguire il rollback sui punti di ripristino.
- Eseguire un'esportazione su una macchina virtuale (VM).
- Eseguire un ripristino bare metal (BMR).
- Eseguire il failback (nel caso in cui sia impostato un ambiente di replica failover/failback).

Informazioni su failover e failback

AppAssure supporta il failover e il failback in ambienti replicati, in caso di un grave guasto che comporta il malfunzionamento del core di origine e degli agenti. Il failover si riferisce al passare ad una destinazione

superflua o in standby (AppAssure Core) in caso di guasto del sistema o interruzione anomala del core di origine e degli agenti associati. L'obiettivo principale del failover è avviare un nuovo agente identico a quello non riuscito. L'obiettivo secondario è far passare il core di destinazione ad una nuova modalità così che il core di destinazione protegga l'agente di failover nello stesso modo in cui il core di origine protegge l'agente iniziale prima che vada in anomalia. Il core di destinazione può ripristinare le istanze dagli agenti replicati e iniziare immediatamente la protezione sulle macchine con failover.

Failback è il processo di ripristino di un'agente e di un core al loro stato originale (prima dell'errore). L'obiettivo principale del failback è ripristinare l'agente (nella maggior parte dei casi, si tratta di una nuova macchina che sostituisce un agente non riuscito) ad uno stato identico allo stato più recente dell'agente temporaneo nuovo. Quando è ripristinato, è protetto da un core di origine ripristinato. Anche la replica viene ripristinata e il core di destinazione agisce di nuovo come destinazione di replica.

Esecuzione del failover

Quando si verifica una situazione di emergenza dove il core di origine e gli agenti associati sono guasti, è possibile abilitare il failover in AppAssure per passare la protezione allo stesso core failover (di destinazione). Il core di destinazione diventa l'unico core che protegge i dati nell'ambiente, in seguito si procede all'avvio di un nuovo agente per sostituire temporaneamente l'agente guasto.

Per eseguire il failover sul core di destinazione:

1. Passare alla Core Console sul core di destinazione, quindi fare clic sulla scheda **Replica**.
2. In **Replica in entrata**, selezionare il core di origine, quindi espandere i dettagli sotto i singoli agenti.
3. Nel menu **Azioni** per quel core, fare clic su **Failover**.

   Viene visualizzata la finestra di dialogo **Failover** che elenca la procedura necessaria per il completamento di un failover.
4. Fare clic su **Continua**.
5. Nell'area di navigazione a sinistra, sotto **Macchine protette**, selezionare la macchina che ha il software AppAssure Agent associato ai punti di ripristino.
6. Esportare le informazioni di backup del punto di ripristino su tale agente ad una macchina virtuale.
7. Avviare la macchina virtuale che contiene ora le informazioni di backup esportate.

   È necessario attendere che il software del driver del dispositivo sia installato.
8. Riavviare la macchina virtuale e attendere che il servizio dell'agente si avvii.
9. Tornare alla Core Console del core di destinazione e verificare che il nuovo agente venga visualizzato sotto **Macchine protette** e sulla scheda **Replica** in **Replica in entrata**.
10. Forzare più istantanee e verificarne il corretto completamento.

    Per ulteriori informazioni, consultare Forzatura di un'istantanea.
11. Ora è possibile procedere con l'esecuzione del failback.

    Per ulteriori informazioni, consultare Esecuzione del failback.

Esecuzione del failback

Dopo aver riparato o sostituito il core e gli agenti di origine originali guasti, è necessario trasferire i dati dalle macchine guaste per ripristinare le macchine di origine.

Per eseguire il failback:

1. Passare alla Core Console sul core di destinazione, quindi fare clic sulla scheda **Replica**.
2. In **Replica in entrata**, selezionare l'agente failover ed espandere i dettagli.
3. Dal menu **Azioni** fare clic su **Failback**.

La finestra di dialogo **Failback** si apre e descrive la procedura necessaria da seguire prima di fare clic sul pulsante **Continua** per completare il failback.

4. Fare clic su **Annulla**.
5. Se sulla macchina guasta è in esecuzione Microsoft SQL Server o Microsoft Exchange Server, interrompere questi servizi.
6. Forzare una istantanea della macchina. Per ulteriori informazioni, consultare Forzatura di un'istantanea.
7. Spegnere la macchina guasta.
8. Creare un archivio dell'agente guasto e trasferirlo sul disco o su una rete condivisa.

   Per ulteriori informazioni sulla creazione di archivi, consultare Creazione di un archivio.
9. Dopo la creazione dell'archivio, passare alla Core Console sul core di origine appena riparato, quindi fare clic sulla scheda **Strumenti**.
10. Importare l'archivio appena creato nel punto 8.

    Per ulteriori informazioni, consultare Importazione di un archivio.
11. Tornare alla Core Console sul core di destinazione, quindi fare clic sulla scheda **Replica**.
12. In **Replica in entrata**, selezionare l'agente failover ed espandere i dettagli.
13. Nella finestra di dialogo **Failback** fare clic su **Continua**.
14. Spegnere la macchina che contiene l'agente esportato che è stato creato durante il failover.
15. Eseguire un ripristino bare-metal (BMR) per il core e l'agente di origine.

    N.B.: All'avvio del ripristino, è necessario utilizzare i punti di ripristino che sono stati importati dal core di destinazione all'agente sulla macchina virtuale.
16. Attendere il riavvio del ripristino bare-metal e il riavvio del servizio dell'agente, quindi visualizzare e registrare i dettagli sulla connessione di rete della macchina.
17. Passare alla Core Console sul core di origine e, nella scheda **Macchine**, modificare le impostazioni di protezione per aggiungere i nuovi dettagli della connessione di rete.

    Per ulteriori informazioni Impostazioni di configurazione della macchina.
18. Passare alla Core Console sul core di destinazione, quindi eliminare l'agente dalla scheda **Replica**.
19. Nella Core Console del core di origine, impostare nuovamente la replica tra il core di origine e il core di destinazione, facendo clic sulla scheda **Replica**, quindi aggiungere il core di destinazione per la replica.

7

Creazione di rapporti

Informazioni sui rapporti

L'appliance DL consente di generare e visualizzare informazioni di conformità, errori e di riepilogo delle macchine con più core e con agenti.

È possibile scegliere di visualizzare i rapporti online, stamparli, o esportarli e salvarli in uno dei numerosi formati supportati. I formati fra cui è possibile scegliere sono i seguenti:

- PDF
- XLS
- XLSX
- RTF
- MHT
- HTML
- TXT
- CSV
- Immagine

Informazioni sulla barra degli strumenti dei rapporti

La barra degli strumenti disponibile per tutti i rapporti consente di stampare e salvare in due modi diversi. La tabella seguente descrive le opzioni di salvataggio e di stampa.

Icona	Descrizione
	Stampa il rapporto
	Stampa la pagina corrente
	Esporta un rapporto e salva su disco
	Esporta un rapporto e mostra in una nuova finestra Utilizzare questa opzione per copiare, incollare ed inviare tramite e-mail l'URL ad altri utenti per visualizzare il rapporto con un browser Web.

Informazioni sui rapporti di conformità

I rapporti di conformità sono disponibili per il Core e l'agente AppAssure. Forniscono all'utente un modo per visualizzare lo stato dei processi eseguiti da un core o un agente selezionato. I processi non riusciti vengono visualizzati in rosso. Le informazioni nel Core Compliance Report che non sono associate a un agente sono assenti.

I dettagli sui processi vengono presentati in formato colonna ed includono le seguenti categorie:

- Core
- Agente protetto
- Tipo
- Riepilogo
- Stato
- Errore
- Ora di inizio
- Ora di fine
- Ora
- Operazione totale

Informazioni sui rapporti di errore

I rapporti sugli errori sono sottoinsiemi dei Rapporti di conformità e sono disponibili per i Core e gli Agenti AppAssure. I Rapporti sugli errori comprendono solo i processi non riusciti elencati nei Rapporti di conformità che vengono compilati in un unico rapporto che può essere stampato ed esportato.

I dettagli sugli errori vengono presentati in formato colonna con le seguenti categorie:

- Core
- Agente
- Tipo
- Riepilogo
- Errore
- Ora di inizio
- Ora di fine
- Tempo trascorso
- Operazione totale

.

Informazioni sul rapporto di riepilogo del Core

Il **Rapporto di riepilogo del Core** fornisce informazioni relative ai repository nel Core selezionato e agli agenti protetti dal core. Le informazioni sono visualizzate sotto forma di due riepiloghi all'interno di un rapporto.

Riepilogo dei repository

La sezione **Repository** del **Rapporto di riepilogo del Core** contiene i dati dei repository collocati nel core selezionato. I dettagli relativi ai repository vengono presentati in formato colonna con le seguenti categorie:

- Nome
- Percorso dei dati
- Percorso dei metadati

- Spazio allocato
- Spazio utilizzato
- Spazio disponibile
- Rapporto compressione/deduplicazione

Riepilogo degli agenti

La sezione **Agenti** di **Rapporto di riepilogo del core** contiene i dati relativi a tutti gli agenti protetti dal core selezionato.

I dettagli sugli agenti vengono presentati in formato colonna con le seguenti categorie:

- Nome
- Volumi protetti
- Spazio totale protetto
- Spazio attuale protetto
- Velocità di variazione giornaliera (**Media**, **Mediana**)
- Statistiche dei processi (**Completato**, **Non riuscito**, **Annullato**)

Generazione di un rapporto per un core o per un agente

Per generare un rapporto per un core o agente:

1. Passare alla Core Console e selezionare il core o l'agente per il quale si desidera eseguire il rapporto.
2. Fare clic sulla scheda **Strumenti**.
3. Dalla scheda **Strumenti**, espandere **Rapporti** nell'area di navigazione a sinistra.
4. Nell'area di navigazione a sinistra, selezionare il rapporto che si desidera eseguire. I rapporti disponibili dipendono dalla scelta effettuata al punto 1 e sono descritti di seguito.

Macchina	Rapporti disponibili
Core	Rapporto di conformità
	Rapporto di riepilogo
	Rapporto errori
Agente	Rapporto di conformità
	Rapporto errori

5. Nel calendario a discesa **Ora di inizio**, selezionare una data di inizio, quindi inserire un'ora di inizio del rapporto.

   N.B.: Nessun dato è disponibile prima dell'ora di distribuzione del core o dell'agente.
6. Nel calendario a discesa **Ora di fine**, selezionare una data di fine, quindi inserire un'ora di fine del rapporto.
7. Per un **Rapporto di riepilogo del Core**, selezionare la casella di controllo **Tutte le ore** se si desidera che l'**ora di inizio** e l'**ora di fine** coprano l'intera durata del Core.
8. Per un **Rapporto di conformità del Core** o un **Rapporto errori del Core**, utilizzare l'elenco a discesa **Core di destinazione** per selezionare il core per il quale si desidera visualizzare i dati.
9. Fare clic su **Genera rapporto**.

Al termine della creazione del rapporto è possibile utilizzare la barra degli strumenti per stampare o esportare il rapporto.

Informazioni sui rapporti del core della Central Management Console

L'appliance DL consente di generare e visualizzare le informazioni di conformità, errori e di riepilogo per più core. I dettagli sui core vengono visualizzati in formato colonna con le stesse categorie descritte in questa sezione.

Generazione di un rapporto dalla Central Management Console

Per generare un rapporto dalla Central Management Console:

1. Dalla schermata di introduzione della **Central Management Console**, fare clic sul menu a discesa nell'angolo superiore destro.
2. Dal menu a discesa, fare clic su **Rapporti**, quindi selezionare una delle opzioni riportate di seguito:
   - **Rapporto di conformità**
   - **Rapporto di riepilogo**
   - **Rapporto sulle anomalie**
3. Dall'area di navigazione a sinistra, selezionare il o i Core per cui si desidera eseguire il rapporto.
4. Nel calendario a discesa **Ora di inizio**, selezionare una data di inizio, quindi inserire un'ora di inizio del rapporto.

   N.B.: Nessun dato è disponibile prima della distribuzione dei Core.
5. Nel calendario a discesa **Ora di fine**, selezionare una data di fine, quindi inserire un'ora di fine del rapporto.
6. Fare clic su **Genera rapporto**.

   Al termine della creazione del rapporto è possibile utilizzare la barra degli strumenti per stampare o esportare il rapporto.

8

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

Dell fornisce diverse opzioni di supporto e assistenza telefonica e in linea. Se non si è in possesso di una connessione Internet attiva, è possibile ricercare 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 all'acquisto di prodotti, supporto tecnico o servizio 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.