Guida per l'utente dell'agente per Linux

Arcserve® Unified Data Protection

Versione 10.0

arcserve®

La presente documentazione, che include il sistema di guida in linea integrato e materiale distribuibile elettronicamente (d'ora in avanti indicata come "Documentazione"), viene fornita all'utente finale a scopo puramente informativo e può essere modificata o ritirata da Arcserve in qualsiasi momento. Questa Documentazione contiene informazioni proprietarie di Arcserve e non può essere copiata, trasmessa, riprodotta, divulgata, modificata o duplicata per intero o in parte, senza la preventiva autorizzazione scritta di Arcserve.

Se l'utente dispone di una licenza per l'utilizzo dei software a cui fa riferimento la Documentazione, avrà diritto ad effettuare copie della suddetta Documentazione in un numero ragionevole per uso personale e dei propri impiegati, a condizione che su ogni copia riprodotta siano apposti tutti gli avvisi e le note sul copyright di Arcserve.

Il diritto a stampare copie della presente Documentazione è limitato al periodo di validità della licenza per il prodotto. Qualora e per qualunque motivo la licenza dovesse cessare o giungere a scadenza, l'utente avrà la responsabilità di certificare a Arcserve per iscritto che tutte le copie anche parziali del prodotto sono state restituite a Arcserve o distrutte.

NEI LIMITI CONSENTITI DALLA LEGGE VIGENTE, ARCSERVE FORNISCE LA DOCUMENTAZIONE "COSÌ COM'È" SENZA GARANZIE DI ALCUN TIPO, INCLUSE, IN VIA ESEMPLIFICATIVA, LE GARANZIE IMPLICITE DI COMMERCIABILITÀ, IDONEITÀ A UN DETERMINATO SCOPO O DI NON VIOLAZIONE DEI DIRITTI ALTRUI. IN NESSUN CASO ARCSERVE SARÀ RITENUTA RESPONSABILE DA PARTE DELL'UTENTE FINALE O DA TERZE PARTI PER PERDITE O DANNI, DIRETTI O INDIRETTI, DERIVANTI DALL'UTILIZZO DELLA DOCUMENTAZIONE, INCLUSI, IN VIA ESEMPLIFICATIVA E NON ESAUSTIVA, PERDITE DI PROFITTI, INTERRUZIONI DELL'ATTIVITÀ, PERDITA DI AVVIAMENTO O DI DATI, ANCHE NEL CASO IN CUI ARCSERVE VENGA ESPRESSAMENTE INFORMATA IN ANTICIPO DI TALI PERDITE O DANNI.

L'utilizzo di qualsiasi altro prodotto software citato nella Documentazione è soggetto ai termini di cui al contratto di licenza applicabile, il quale non viene in alcun modo modificato dalle previsioni del presente avviso.

Il produttore di questa Documentazione è Arcserve.

Fornita con "Diritti limitati". L'uso, la duplicazione o la divulgazione da parte del governo degli Stati Uniti è soggetto alle restrizioni elencate nella normativa FAR, sezioni 12.212, 52.227-14 e 52.227-19(c)(1) - (2) e nella normativa DFARS, sezione 252.227-7014(b)(3), se applicabile, o successive.

© 2024 Arcserve, incluse affiliate e controllate. Tutti i diritti riservati. Tutti i marchi o i diritti di copyright di terze parti sono di proprietà dei rispettivi titolari.

Tabella dei contenuti

Chapter 1: Nozioni fondamentali sull'Agente Arcserve UDP (Linux) 11

Introduzione 12

Chapter 2: Installazione/disinstallazione dell'Agente Arcserve UDP (Linux) 14

Installazione di Agente Arcserve UDP (Linux) 15

Considerazioni sull'installazione 16

Installazione dell'Agente Arcserve UDP (Linux) 17

Installazione dell'Agente Arcserve UDP (Linux) in AWS Cloud 21

Verifica dell'installazione 24

Disinstallazione di Agente Arcserve UDP (Linux) 25

Considerazioni sulla disinstallazione 26

Disinstallazione dell'Agente Arcserve UDP (Linux) 27

Verifica della disinstallazione 28

Aggiornamento dell'Agente Arcserve UDP (Linux) 29

Considerazioni sull'aggiornamento 30

Aggiornamento dell'Agente Arcserve UDP (Linux) 31

Verifica dell'aggiornamento 33

Migrazione del server di backup Linux a 32 bit a un server a 64 bit 34

Chapter 3: Interfaccia utente 36

Accesso all'interfaccia utente dell'Agente Arcserve UDP (Linux) 37

Accesso al server di backup 39

Presentazione della barra dei menu 40

Presentazione del riquadro Stato 44

Presentazione del riquadro Server di backup 48

Presentazione della guida in linea 49

Registrazione ad Arcserve UDP 51

Chapter 4: Utilizzo dell'Agente Arcserve UDP (Linux) 53

Gestione delle licenze 55

Accesso a Gestione licenze 56

Informazioni sulla finestra di dialogo di Gestione licenze 57

Gestione delle licenze 59

Gestione dei processi 60

Revisione dei prerequisiti per la gestione dei processi 61

Modifica dei processi 62

Annullamento dei processi ... 63
Eliminazione dei processi ... 64
Backup di nodi Linux ... 65
Verifica delle considerazioni e dei prerequisiti di backup ... 67
Backup di più di 200 nodi ... 72
Aggiunta di nodi Linux per il backup ... 77
(Facoltativo) Registrazione della chiave pubblica di Arcserve UDP per l'avvio protetto ... 79
(Facoltativo) Registrazione della chiave pubblica Arcserve UDP per il kernel Oracle Linux UEK6 abilitato per l'avvio protetto ... 81
(Facoltativo) Preparazione del volume iSCSI come archiviazione di backup ... 85
Configurazione delle impostazioni di backup ed esecuzione del processo di backup ... 87
Verifica dell'esecuzione del backup ... 110
Modifica e nuova esecuzione di un processo di backup ... 111
Verifica dei prerequisiti per la modifica di un processo di backup ... 112
Aggiungere dei nodi a un processo esistente? ... 113
Aggiunta di nodi a un processo esistente ... 114
Riesecuzione di un processo di backup esistente ... 115
Verifica dell'esecuzione del backup ... 117
Esecuzione di un ripristino a livello di file per i nodi Linux ... 118
Verifica dei prerequisiti ... 119
Definizione del punto di ripristino per il backup senza agente basato sull'host ... 120
Definizione del punto di ripristino per il backup basato sull'agente ... 124
Definizione dei dettagli relativi al computer di destinazione ... 130
Definizione delle impostazioni avanzate ... 133
Creazione ed esecuzione del processo di ripristino ... 137
Verifica del ripristino dei file ... 138
Creazione di un Live CD di avvio ... 139
Verifica dei prerequisiti per Live CD ... 141
Installazione del pacchetto dell'utilità di ripristino ... 142
Creazione e verifica del Live CD di avvio ... 143
Utilizzo del sistema Live CD come server di backup Linux ... 144
Creazione di un Live CD di avvio per includere i driver personalizzati per AlmaLinux 9.x ... 145
Verifica dei prerequisiti ... 146
Creazione di un Live CD personalizzato ... 147
Verifica di un Live CD personalizzato ... 148
Esecuzione di un ripristino bare metal per computer Linux ... 150

Creazione di un modello di configurazione tramite la riga di comando 152
Verifica dei prerequisiti di ripristino bare metal 157
Acquisizione dell'indirizzo IP del computer di destinazione con Live CD 158
(Facoltativo) Ripristino dei dati nel volume iSCSI del computer di destinazione 160
(Facoltativo) Ripristino dei dati dal volume iSCSI nel computer di destinazione 162
Verifica del server di backup 164
Definizione dei punti di ripristino 166
Definizione dei dettagli relativi al computer di destinazione 168
Definizione delle impostazioni avanzate 170
Creazione ed esecuzione del processo di ripristino 176
Verifica del ripristino del nodo di destinazione 185
Esecuzione di un ripristino bare metal per computer Linux in AWS Cloud 186
Verifica dei prerequisiti di ripristino bare metal 187
Avvio di un'istanza tramite Live CD dell'agente Arcserve UDP 188
Revisione dell'istanza del server di backup 190
Definizione dei punti di ripristino 192
Definizione dei dettagli relativi all'istanza di destinazione 194
Definizione delle impostazioni avanzate 196
Creazione ed esecuzione del processo di ripristino 202
Verifica del ripristino dell'istanza di destinazione 210
Esecuzione di un ripristino bare metal per i computer Linux in Azure Cloud 211
Verifica dei prerequisiti di ripristino bare metal 212
Creazione di un nuovo computer su Microsoft Azure come ripristino bare metal di destinazione 213
Verifica del computer virtuale del server di backup 214
Definizione dei punti di ripristino 215
Definizione dei dettagli del computer virtuale di destinazione 216
Definizione delle impostazioni avanzate 218
Creazione ed esecuzione del processo di ripristino 219
Verifica del ripristino del computer virtuale di destinazione 220
Esecuzione di un ripristino bare metal di migrazione per computer Linux 221
Verifica dei prerequisiti per il ripristino bare metal di migrazione 222
Esecuzione di un ripristino bare metal su un computer temporaneo 223
Esecuzione del ripristino bare metal di migrazione 225
Verifica del ripristino del nodo di destinazione 227
Esecuzione di un ripristino bare metal di migrazione per computer Linux da Amazon EC2 sul computer locale 228

Verifica dei prerequisiti per il ripristino bare metal di migrazione 229
Esecuzione di un ripristino bare metal di migrazione da Amazon EC2 sul computer locale 230
Verifica del ripristino del nodo di destinazione 233
Ripristino automatico di un computer virtuale 234
Verifica delle considerazioni e dei prerequisiti 235
Creazione di un modello di configurazione 238
(Facoltativo) Creazione di un file di configurazione globale 244
Modifica del file e del modello di configurazione 246
Invio di un processo mediante l'utilità d2drestorevm 247
Verifica del ripristino del computer virtuale 248
Integrazione e automazione dell'Arcserve UDP per Linux con l'ambiente IT esistente 249
Verifica dei prerequisiti di automazione 251
Presentazione delle utilità di generazione script 252
Gestione dei pre/post script per l'automazione 262
Creazione dello script di avviso di archiviazione di backup 269
Rilevamento dei nodi mediante uno script 270
Creazione degli script per l'esecuzione del backup del database Oracle 272
Creazione degli script per l'esecuzione del backup del database MySQL 274
Utilizzo degli script per il backup e il ripristino del database PostgreSQL 278
Personalizzazione della pianificazione del processo 282
Esecuzione di un processo in batch di ripristino bare metal 284
Replica e gestione delle sessioni di backup 286
Verifica dell'utilizzabilità dei punti di ripristino 289
Gestione delle impostazioni del server di backup 295
Verifica dei prerequisiti per la gestione del server di backup 296
Configurazione delle impostazioni di conservazione della cronologia dei processi e dei registri delle attività 297
Configurazione delle impostazioni di conservazione del registro di debug 298
Configurazione della durata del timeout dell'interfaccia utente 299
Modifica del numero di porta SSH del server di backup 300
Gestione dei set di ripristino 301
Disattivazione dei servizi BOOTPD e TFTPD 302
Miglioramento delle prestazioni di query per la cronologia dei processi e il registro attività 303
Disabilitazione della verifica dei moduli CIFS e NFS 304
Disabilitazione della convalida CIFS e NFS sul server Linux di backup 305
Configurazione della cartella temporanea predefinita 306

Configurazione del percorso della snapshot per il nodo di backup 307
Configurazione delle informazioni di connessione del server Hyper-V per il computer virtuale istantaneo 308
Gestione del server di backup Linux dalla riga di comando 310
Verifica dei prerequisiti del server di backup 312
Avvio, interruzione o rilascio del server di backup 313
Modifica del numero di porta del servizio Web del server di backup 315
Configurazione dell'autenticazione con chiave privata e chiave pubblica 316
Modifica del protocollo del server di backup 318
Blocco della visualizzazione dell'errore di certificato SSL all'apertura dell'Agente Arcserve UDP (Linux) 320
Configurazione delle impostazioni di sistema in caso di modifica del nome host o dell'indirizzo IP 322
Aggiunta di un utente alla Console del server di backup Linux mediante la riga di comando 328
Verifica dei prerequisiti 329
Aggiunta di un utente alla Console del server di backup Linux mediante la riga di comando 330
Gestione degli utenti non root 332
Verifica dei prerequisiti 333
Concessione delle autorizzazioni di accesso agli utenti non root 334
Visualizzazione dell'utente predefinito nella finestra di dialogo Accedi 335
Abilitazione degli utenti non root per l'aggiunta di nodi 336
Modalità di configurazione dell'account utente sudo per i nodi Linux 338
Verifica dei prerequisiti 339
Modifica delle impostazioni sudo predefinite in SUSE 340
Configurazione del comando sudo in Debian 341
Configurazione del comando sudo in Ubuntu 342
Configurazione di sudo per l'autorizzazione senza password durante l'utilizzo dell'autenticazione con chiave pubblica SSH 343
Configurazione di Sudo per consentire soltanto il processo dell'agente di backup 344
Ripristino dei volumi su un nodo di destinazione 345
Verifica delle considerazioni e dei prerequisiti 346
Verifica dell'installazione dell'utilità d2drestorevol 347
Verifica dei dettagli volume nella sessione 348
Inoltro del processo di ripristino del volume 351
Annullamento del processo di ripristino del volume 355
Verifica del volume ripristinato 356
Download di file e cartelle senza ripristino per i nodi Linux 357

Ripristino di un database Oracle mediante l'Agente Arcserve UDP (Linux) 358
Esecuzione di un ripristino bare metal (BRM) di un server Oracle 359
Esecuzione di un ripristino istantaneo di un database Oracle 363
Esecuzione del ripristino granulare di un database Oracle 367
Esecuzione della verifica Assured Recovery dalla riga di comando 374
Verifica delle considerazioni e dei prerequisiti 375
Creazione di un modello di configurazione 376
Modifica del file e del modello di configurazione 381
Inoltro di un processo mediante l'utilità d2dar 382
Montaggio dei punti di ripristino 383
Verifica dei prerequisiti 384
Definizione del punto di ripristino per il montaggio del punto di ripristino 385
Definizione delle impostazioni per il montaggio del punto di ripristino 388
Creazione ed esecuzione del processo di montaggio del punto di ripristino 391
Montaggio della condivisione NFS o WebDAV su server Linux 392
Attivazione del supporto per i kernel Linux più recenti di RHEL, OEL (kernel RHEL), Debian, SUSE e Ubuntu 395
Verifica dei prerequisiti 396
Distribuzione manuale del pacchetto di driver RHEL, OEL (kernel RHEL), Debian, SUSE e Ubuntu aggiornati 397
(Facoltativo) Utilizzo del server di gestione temporanea per l'aggiornamento dei driver 398
(Facoltativo) Configurazione del proxy HTTP 399
Disattivazione del bit SUID durante l'esecuzione del processo di ripristino del file 400
Verifica dei prerequisiti 401
Configurazione delle impostazioni nel server di backup Linux 402
Configurazione di sudo per autorizzare il file binario d2dtar nel nodo di destinazione 403
Esecuzione del processo di ripristino dei file utilizzando le credenziali dell'utente sudo del nodo di destinazione 404
Chapter 5: Risoluzione dei problemi 405
Mancata installazione dell'Agente Arcserve UDP (Linux) sui server supportati 407
Errore di timeout dell'operazione visualizzato dall'Agente Arcserve UDP (Linux) 409
Il backup dell'agente Arcserve UDP per Linux potrebbe non riuscire quando si passa dal backup senza agente al backup basato sull'agente 410
Errore dei processi pianificati in caso di modifica dell'ora di sistema su un valore precedente all'ora corrente 411
Mancato montaggio dell'Agente Arcserve UDP (Linux) sulle periferiche Linux Software RAID 412
Errore di download e distribuzione dei driver Ubuntu aggiornati su SLES 11 e RHEL 6 da parte di Agente Arcserve UDP (Linux) 413

Se avviato mediante Live CD, il computer paravirtuale (PVM) visualizza una schermata nera nella finestra del client Virtual Network Computing (VNC). 414

Errore di raccolta delle informazioni di ripristino bare metal durante il processo di backup o errore di creazione del layout del disco durante il processo di ripristino bare metal 416

Errore del processo di backup su RHEL7.0 come server di backup Linux e RPS su Windows Server 2019 417

Controllo della sequenza di avvio del disco dopo un ripristino bare metal su Oracle VM Server 418

Ripristino della versione precedente del server di backup 420

Backup delle istanze Debian 9.X EC2 in AWS Cloud 421

Errore di avvio del nodo di destinazione dopo l'esecuzione del processo di ripristino bare metal di migrazione per i nodi Debian 10.8 e 10.10 422

Il computer virtuale produce un errore di avvio per il processo IVM/AR al server ESXi 423

Il Computer virtuale non si avvia quando si utilizza la scheda di rete e1000e sul nodo ESXi 424

IVM su Hyper-V non viene avviato correttamente per i nodi di origine Debian 10.x 424

IVM su Hyper-V non viene avviato correttamente per il nodo di origine RHEL 8.0 424

I processi basati sull'agente Linux non riescono occasionalmente 426

I processi d2drestorevm e d2dverify non vengono completati correttamente su Oracle VM Server 427

Errore di avvio del computer virtuale ESXi dopo il ripristino bare metal da un computer fisico 428

Impossibile montare CIFS sul server o sul nodo di destinazione 429

Errore di ripristino a livello di file in un computer virtuale Linux basato su host causato da un file system non supportato 431

Impossibile ripristinare il volume di sistema di SUSE15 con file system XFS 431

Impossibile accedere all'URL di montaggio del punto di ripristino condiviso da WebDAV 432

Errore di distribuzione dei driver Ubuntu mediante il comando d2dupgradetool in Ubuntu20.04 LBS 432

Contatto del Supporto tecnico di Arcserve

Il team di Supporto tecnico di Arcserve offre un insieme di risorse per la risoluzione dei problemi tecnici e fornisce l'accesso a importanti informazioni sul prodotto.

Contatto con il supporto tecnico

Con Supporto tecnico di Arcserve:

- È possibile consultare direttamente la stessa libreria di informazioni che viene condivisa internamente dagli esperti del Supporto tecnico di Arcserve. Questo sito fornisce l'accesso ai documenti della Knowledge Base (KB). Da qui, è possibile cercare e trovare facilmente gli articoli della Knowledge Base relativi al prodotto e contenenti le soluzioni testate sul campo a molti problemi principali e comuni.
- È possibile utilizzare il collegamento Chat in tempo reale per avviare una conversazione in tempo reale con il team del Supporto tecnico di Arcserve. Con la Chat in tempo reale, è possibile ottenere risposte immediate alle proprie domande e preoccupazioni, mantenendo al contempo l'accesso al prodotto.
- È possibile partecipare alla Arcserve Global User Community per porre domande e rispondere, condividere suggerimenti e consigli, discutere su procedure consigliate e partecipare a discussioni con i propri colleghi.
- È possibile aprire un ticket di supporto. Quando si apre un ticket di supporto in linea, si verrà contattati da uno degli esperti nell'area del prodotto per il quale si richiede il supporto.
- È possibile accedere ad altre risorse utili relative al prodotto Arcserve.

Chapter 1: Nozioni fondamentali sull’Agente Arcserve UDP (Linux)

La presente sezione descrive i seguenti argomenti:

Introduzione 12

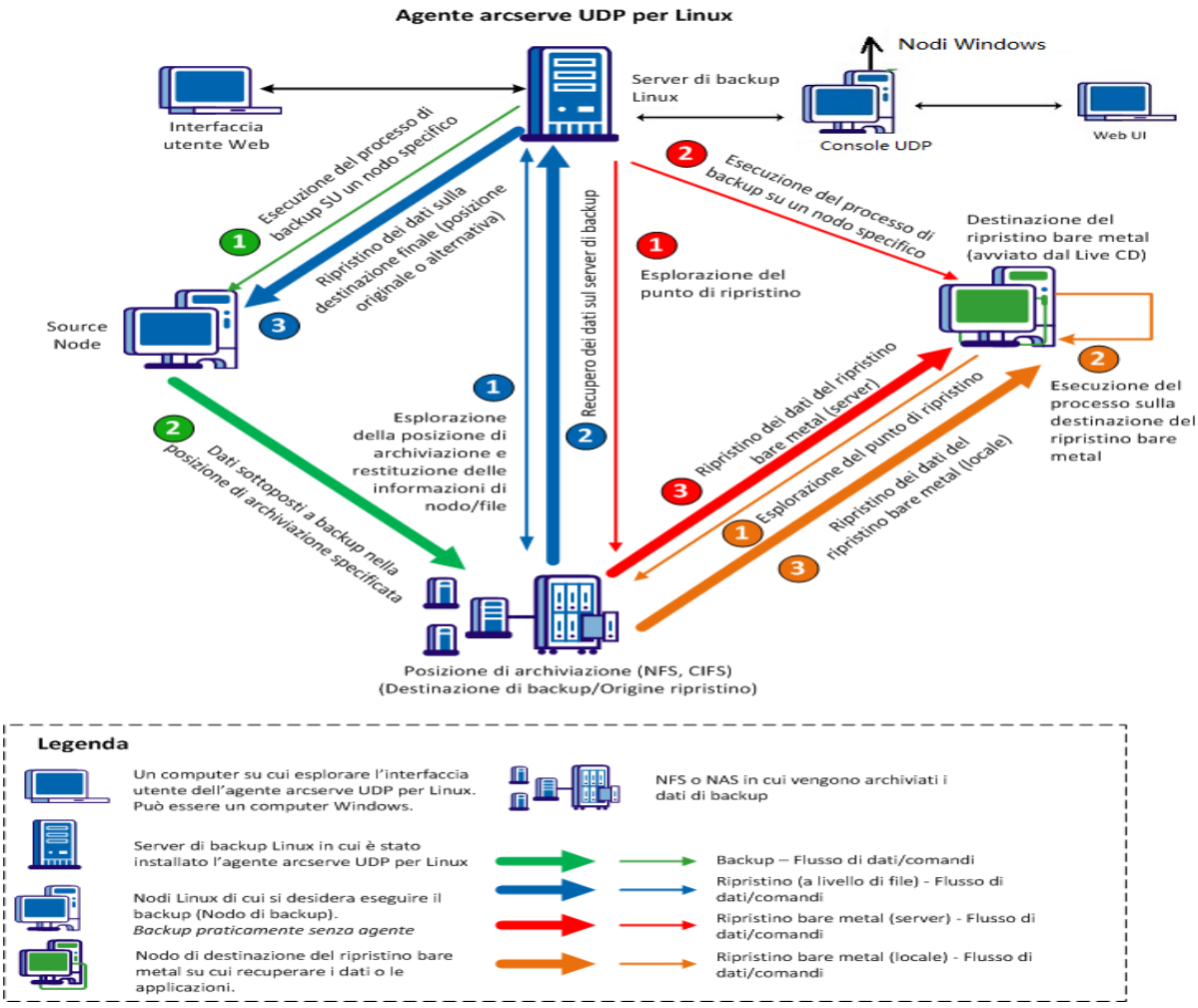
Introduzione

Arcserve UDP per Linux (Agente Arcserve UDP (Linux) è un prodotto di backup basato su disco progettato per sistemi operativi Linux. Fornisce un modo veloce, semplice, e affidabile di proteggere e recuperare informazioni aziendali critiche. Agente Arcserve UDP (Linux) tiene traccia delle modifiche in un nodo al livello di blocco, quindi esegue il backup solamente dei blocchi modificati in un processo incrementale. Di conseguenza, l'Agente Arcserve UDP (Linux) consente di eseguire backup frequenti riducendo in tal modo la dimensione di ciascun backup incrementale (e della finestra di backup) e offrendo un backup più aggiornato. Agente Arcserve UDP (Linux) consente inoltre di eseguire il ripristino di file o cartelle, nonché di eseguire ripristini bare metal a partire da un singolo backup. È possibile archiviare le informazioni di backup su una condivisione NFS (Network File System), su una condivisione CIFS (Common Internet File System) oppure sul nodo di origine del backup.

Il ripristino bare metal consiste nel ripristino di un sistema del computer avviato a partire da un sistema *bare metal*. Bare metal è un computer senza sistema operativo, driver e applicazioni software. Il ripristino comprende l'installazione del sistema operativo, le applicazioni software, i driver e il ripristino dai dati e delle impostazioni. È possibile eseguire il ripristino bare metal poiché durante il backup dei dati, l'Agente Arcserve UDP (Linux) acquisisce inoltre le informazioni relative al sistema operativo, alle applicazioni installate, ai driver e così via. Al completamento del ripristino bare metal, il nodo di destinazione avrà lo stesso sistema operativo e gli stessi dati del nodo di produzione.

Agente Arcserve UDP (Linux) si serve di un approccio praticamente senza agente per abilitare la protezione rapida e flessibile di tutti i client Linux. La funzionalità consente di eliminare totalmente l'installazione manuale degli agenti su ciascun nodo client automatizzando completamente il rilevamento, la configurazione e la protezione di tutti i client Linux. È possibile installare l'Agente Arcserve UDP (Linux) per proteggere l'intero ambiente di produzione Linux. Il server utilizzato per l'installazione dell'Agente Arcserve UDP (Linux) è noto come server di backup. Dopo aver installato l'Agente Arcserve UDP (Linux), è possibile stabilire la connessione al server di backup su una rete e aprire l'interfaccia utente mediante un browser Web.

Il diagramma seguente mostra il flusso di lavoro globale dell'Agente Arcserve UDP (Linux):


Agente arcserve UDP per Linux
Nodi Windows
Server di backup Linux
Interfaccia utente Web
Console UDP
Web UI
Esecuzione del processo di backup SU un nodo specifico
Ripristino dei dati sulla destinazione finale (posizione originale o alternativa)
Esecuzione del processo di backup su un nodo specifico
Destinazione del ripristino bare metal (avviato dal Live CD)
Esplorazione del punto di ripristino
Source Node
Esplorazione della posizione di archiviazione e restituzione delle informazioni di nodo/file
Recupero dei dati sul server di backup
Ripristino dei dati del ripristino bare metal (server)
Esplorazione del punto di ripristino
Ripristino dei dati del ripristino bare metal (locale)
Esecuzione del processo sulla destinazione del ripristino bare metal
Dati sottoposti a backup nella posizione di archiviazione specificata
Posizione di archiviazione (NFS, CIFS)
(Destinazione di backup/Origine ripristino)
Legenda
Un computer su cui esplorare l'interfaccia utente dell'agente arcserve UDP per Linux. Può essere un computer Windows.
NFS o NAS in cui vengono archiviati i dati di backup
Server di backup Linux in cui è stato installato l'agente arcserve UDP per Linux
Backup – Flusso di dati/comandi
Ripristino (a livello di file) - Flusso di dati/comandi
Nodi Linux di cui si desidera eseguire il backup (Nodo di backup).
Backup praticamente senza agente
Ripristino bare metal (server) - Flusso di dati/comandi
Nodo di destinazione del ripristino bare metal su cui recuperare i dati o le applicazioni.
Ripristino bare metal (locale) - Flusso di dati/comandi

Chapter 2: Installazione/disinstallazione dell'Agente Arcserve UDP (Linux)

La presente sezione descrive i seguenti argomenti:

Installazione di Agente Arcserve UDP (Linux) 15

Disinstallazione di Agente Arcserve UDP (Linux) 25

Aggiornamento dell'Agente Arcserve UDP (Linux) 29

Migrazione del server di backup Linux a 32 bit a un server a 64 bit 34

Installazione di Agente Arcserve UDP (Linux)

Installare l'Agente Arcserve UDP (Linux) su un server Linux per proteggere e gestire tutti i nodi di origine di backup da una singola interfaccia utente. Non è necessario installare questo software sui nodi di origine di backup.

Eseguire queste attività per installare l'Agente Arcserve UDP (Linux):

- Considerazioni sull'installazione
- Installazione dell'Agente Arcserve UDP (Linux)
- Installazione dell'agente Arcserve UDP (Linux) in AWS Cloud
- Verifica dell'installazione

Considerazioni sull'installazione

Prima di procedere con l'installazione, tenere presenti i seguenti punti:

- Quando si esegue un ripristino bare metal basato su PXE (Preboot Execution Environment), il server Arcserve UDP per Linux e i nodi di origine di produzione devono essere contenuti nella stessa subnet. Se non sono contenuti nella stessa subnet, verificare la presenza di un gateway per l'invio di pacchetti di trasmissioni tra le subnet.
- Se la destinazione di backup è un server NFS, verificare che il server NFS supporti il *blocco* . Verificare inoltre che l'utente root disponga dell'accesso in scrittura ai nodi Linux.
- Per utilizzare un server NFS come destinazione di backup, installare il pacchetto client NFS sui nodi Linux.
- Perl e sshd (Daemon SSH) vengono installati sul server Linux e sui nodi Linux di cui si desidera eseguire il backup.
- Esaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.
- L'installazione automatica o invisibile all'utente non è supportata.

Installazione dell'Agente Arcserve UDP (Linux)

Installare l'Agente Arcserve UDP (Linux) su un server Linux per gestire le operazioni di ripristino e di backup. Dopo che si è installato l'Agente Arcserve UDP (Linux), è possibile aprire l'interfaccia utente da qualsiasi computer mediante un browser Web e il server è denominato server di backup.

All'inizio dell'installazione, lo script di installazione verifica che alcune delle applicazioni obbligatorie siano installate sul server Linux e che le applicazioni siano in esecuzione.

Per il funzionamento del file di installazione sono necessarie le applicazioni obbligatorie seguenti:

- sshd (Daemon SSH)
- Perl

Il file di installazione esegue inoltre una verifica delle applicazioni facoltative seguenti all'inizio dell'installazione:

- rpc.statd: quest'applicazione viene utilizzata dal server NFS per implementare il blocco dei file.
- mkisofs - L'Agente Arcserve UDP (Linux) utilizza questa applicazione per creare un Live CD.
- mount.nfs - L'Agente Arcserve UDP (Linux) utilizza questa applicazione per montare il server NFS.
- mount.cifs - L'Agente Arcserve UDP (Linux) utilizza questa applicazione per montare il server CIFS.
- ether-wake - L'Agente Arcserve UDP (Linux) utilizza questa applicazione per inviare la richiesta di riattivazione LAN.

Note:

- Assicurarsi che il server Linux disponga di almeno 2 GB di memoria. Per ulteriori informazioni sui requisiti di sistema per un server Linux, consultare le Note di rilascio di Arcserve UDP 10.0.
- Utilizzare Sudo per installare il server Linux su Microsoft Azure.
- Per i sistemi Debian/Ubuntu, la directory root non è consentita per l'accesso a ssh per impostazione predefinita. Per concedere l'autorizzazione a un utente non root per l'accesso all'interfaccia utente del server di backup di

Linux, consultare la sezione Concessione delle autorizzazioni di accesso agli utenti non root.

Effettuare le operazioni seguenti:

1. Accedere al server Linux come utente root.
2. Salvare il pacchetto di installazione dell'Agente Arcserve UDP (Linux) (file *.bin) nella cartella root.

   Importante: Se il download dei file del pacchetto di installazione viene eseguito in una cartella locale, il percorso completo di questa cartella locale non deve contenere alcun carattere speciale, salvo spazi vuoti, e può includere solamente i caratteri seguenti: a-z, A-Z, 0-9, - e _.
3. Fornire le autorizzazioni di esecuzione per il pacchetto di installazione.
4. Eseguire il comando seguente per iniziare l'installazione:

   ./<linux_installation_file_name>.bin

   Il pacchetto di installazione verifica la piattaforma supportata e mostra un messaggio di conferma.

   Se viene rilevata una piattaforma non supportata, immettere Y e premere Invio per confermare l'installazione della piattaforma non supportata.

   Note:

   - Se viene rilevato un sistema operativo non in lingua inglese, verrà richiesto di selezionare la lingua prima di continuare con il processo di installazione.
   - Per il supporto della lingua coreana con l'aggiornamento di un build, eseguire le seguenti operazioni:
     a. Modificare il seguente file di configurazione sul server dell'agente Arcserve UDP (Linux): */opt/Arcserve/d2dserver/nls/nls.cfg*
     b. Impostare D2D_LANG= ko_KR.
     c. Riavviare d2dserver utilizzando il seguente comando: *#/opt/Arcserve/d2dserver/bin/d2dserver restart*.
5. Immettere Y e premere Invio per confermare l'installazione.

   Il pacchetto di installazione mostra le informazioni relative al contratto di licenza.
6. Immettere Y e premere Invio per accettare il Contratto di licenza.

   Il processo di installazione dell'Agente Arcserve UDP (Linux) viene avviato.

Quando l'installazione del pacchetto dell'utilità di ripristino viene completata, vengono visualizzate le informazioni relative alla creazione del Live CD.

Live CD viene generato nel percorso seguente:

```
/opt/Arcserve/d2dserver/packages
```

Nota: è necessario Live CD per acquisire l'indirizzo IP del nodo di destinazione quando si esegue un ripristino bare metal (BMR).

L'Agente Arcserve UDP (Linux) viene installato e viene visualizzato l'URL per l'accesso al server di backup.

Nota: verificare che le seguenti porte in ingresso siano abilitate sul firewall del server di backup:

- Porta TCP 22 (Server SSH)
- Porta di trasmissione 67 (Server di Avvio)
- 8014 (Agente servizio Web)
- Porta 69 (Server TFTP) protocollo UDP (User Datagram Protocol)
- 8016 (servizio di ripristino bare metal immediato)
- 8021 (servizio di backup)

Verificare che la seguente porta in ingresso sia abilitata sul firewall per i nodi client di cui si desidera eseguire il backup:

- Porta TCP 22 (Server SSH)

Verificare che la porta in uscita obbligatoria per NFS, CIFS o entrambe le destinazioni di backup sia abilitata sul firewall per il server di backup Linux e i nodi di ripristino bare metal di destinazione.

Nota: per ulteriori informazioni sulle porte, consultare la sezione Porte di comunicazione utilizzate da Arcserve UDP.

7. (Facoltativo) Per installare il server di backup di Linux su un computer virtuale Amazon EC2 o Azure, eseguire le seguenti operazioni di creazione di un utente D2D:

   Nota: all'avvio del server, un messaggio di conferma richiede di creare un utente D2D per l'accesso all'interfaccia utente Web dell'agente Arcserve UDP (Linux).

   a. Immettere un nome utente.

   b. Impostare la password e confermarla immettendola nuovamente.

   c. Selezionare se si desidera impostare l'account utente come account predefinito per l'interfaccia utente Web dell'agente Arcserve UDP (Linux).

Impostazione predefinita: Y (sì)

d. Specificare il numero di errori di accesso consecutivi ricevuti dall'utente prima del blocco dell'account.

   Valore predefinito: 3

L'Agente Arcserve UDP (Linux) viene installato correttamente.

Installazione dell'Agente Arcserve UDP (Linux) in AWS Cloud

Rispetto al tradizionale installazione in un computer Linux, è possibile avviare un'istanza dell'agente Arcserve UDP (Linux) direttamente tramite Amazon Machine Image (AMI) in AWS Cloud. Dopo aver avviato l'istanza dell'agente Arcserve UDP (Linux), è possibile aprire l'interfaccia utente da qualsiasi computer mediante un browser Web e il server viene denominato server di backup.

Effettuare le operazioni seguenti:

1. Accedere alla console di gestione EC2 con il proprio account e selezionare Avvia istanza.

   Viene visualizzata la procedura guidata dell'istanza, contenente sette schede.

2. Dalla prima scheda **Scegli AMI**, selezionare l'AMI dell'agente Arcserve UDP (Linux) in **AMI della community** per la **Fase 1: Scelta di un'immagine del computer Amazon (AMI)** e fare clic su **Avanti: Scegli un tipo di istanza**.

   È possibile effettuare la ricerca dell'AMI dell'agente Arcserve UDP (Linux) tramite *Arcserve_Unified_Data_Protection_Agent_Linux* nelle AMI delle community.

   Nota: selezionare un AMI dell'agente Arcserve UDP (Linux) con la versione più recente per l'avvio dell'istanza.

   Viene visualizzata la seconda scheda **Scegli tipo di istanza**.

3. Selezionare un tipo di istanza in base ai propri requisiti per il completamento della **Fase 2: Scelta di un tipo di istanza** e fare clic su **Successivo: Configurazione dei dettagli dell'istanza**.

   Nota: verificare che il tipo di istanza sia almeno t2.medium e abbia almeno 4 GB di memoria. Per ulteriori informazioni sui requisiti di sistema per un server Linux, consultare le Note di rilascio di Arcserve UDP 10.0 - Miglioramenti dell'agente Linux.

   Viene visualizzata la terza scheda **Configurazione istanza**.

4. Selezionare i dettagli per i campi come Rete, Subnet, Assegnazione automatica o non automatica dell'indirizzo IP pubblico etc. per completare la **Fase 3: Configurazione dei dettagli dell'istanza**, quindi fare clic su **Avanti: Aggiunta di archiviazione**.

   Viene visualizzata la quarta scheda **Aggiungi archiviazione**.

5. Allocare spazio di archiviazione per l'istanza per il completamento della **Fase 4: Aggiunta di archiviazione** e fare clic su **Avanti: Aggiunta di tag**.

Nota: è possibile regolare le dimensioni del disco in base ai propri requisiti aziendali. Verificare che il disco dell'istanza Linux disponga di almeno 40 GB.

Viene visualizzata la quinta scheda **Aggiungi tag**.

5. Immettere tag per il completamento dell'istanza di destinazione AMI **Fase 5: Aggiunta di tag** e fare clic su **Avanti: Configurazione del gruppo di protezione**.

   Viene visualizzata la sesta scheda **Configurazione dei gruppi di protezione**.

6. Eseguire i passaggi seguenti per assegnare i gruppi di protezione per l'istanza AMI di destinazione per completare la **Fase 6: Configurazione del gruppo di protezione**, quindi fare clic su **Revisione e avvio**:

   Effettuare le operazioni seguenti:

   a. Creare un nuovo gruppo di protezione per SSH e l'agente Arcserve UDP (Linux).

   b. Verificare che la porta 22 sia abilitata per il **tipo** *SSH*, quindi configurare l'**origine** su *Qualsiasi.*

   c. Verificare che la porta 8014 utilizzata da tomcat sia abilitata per il *tipo* **Regola personalizzata TCP** e configurare l'**origine** su *In qualsiasi punto*.

   d. Verificare che la porta 8016 utilizzata da d2ddss e la porta 8021 utilizzata da cresvc siano abilitate per il **tipo** di regola TCP personalizzata e configurare l'**origine** della regola su Personalizzata.

      Nota: è possibile specificare l'origine personalizzata con formato CIDR in modo da consentire a d2ddss e a cresvc di servire le istanze Linux contenute nella stessa subnet con l'agente Arcserve UDP (Linux) ma non accessibili da altri computer Internet. Ad esempio, se la subnet CIDR è 102.31.16.0/20, è possibile specificare l'origine su 102.31.16.0/20.

   Viene visualizzata la settima scheda **Revisione**.

7. Verificare i dettagli selezionando o creando una coppia di chiavi per connettere l'istanza al completamento della **Fase 7: Revisione dell'avvio dell'istanza**, quindi fare clic su **Avvia istanza**.

8. Dall'istanza dell'agente Arcserve UDP (Linux) avviata, impostare una nuova password per udpuser, come indicato di seguito:

   ```
   #sudo /opt/Arcserve/d2dserver/bin/d2duser --action=passwd --username=udpuser
   ```

   Nota: il nome utente predefinito dell'interfaccia utente di gestione dell'agente Arcserve UDP (Linux) è udpuser.

9. (Facoltativo) Se si desidera passare a un'altra lingua, è possibile modificare il file di configurazione nel server dell'agente Arcserve UDP (Linux):

   /opt/Arcserve/d2dserver/nls/nls.cfg

   Impostare quindi D2D_LANG=$OTHER_LANGUAGE e riavviare d2dserver mediante il seguente comando:

   #/opt/Arcserve/d2dserver/bin/d2dserver restart

   Nota: la lingua inglese è la lingua predefinita dell'agente Arcserve UDP (Linux).

   L'agente Arcserve UDP (Linux) è ora pronto per l'utilizzo in AWS Cloud e l'URL per l'esplorazione del server di backup Linux è https://$INSTANCE_IP:8014.

   L'Agente Arcserve UDP (Linux) è stato installato correttamente in AWS Cloud.

Verifica dell'installazione

Verificare il completamento dell'installazione dopo aver installato l'Agente Arcserve UDP (Linux).

Effettuare le operazioni seguenti:

1. Aprire un browser Web da qualsiasi computer Windows.
2. Immettere l'URL del server di backup Linux visualizzato nella schermata di installazione.

   Esempio: https://hostname:8014

   Viene visualizzata la pagina di accesso all'Agente Arcserve UDP (Linux).
3. Immettere le credenziali di accesso e fare clic su Accedi.

   Viene visualizzata l'interfaccia utente dell'Agente Arcserve UDP (Linux).

   L'Agente Arcserve UDP (Linux) viene installato correttamente e verificato.

Disinstallazione di Agente Arcserve UDP (Linux)

Disinstallare Agente Arcserve UDP (Linux) dal server di backup Linux per interrompere la protezione dei nodi.

Il diagramma seguente mostra il processo di disinstallazione di Agente Arcserve UDP (Linux):

Eseguire queste attività per disinstallare Agente Arcserve UDP (Linux):

- Considerazioni sulla disinstallazione
- Disinstallazione di Agente Arcserve UDP (Linux)
- Verifica della disinstallazione

Considerazioni sulla disinstallazione

Prima di procedere con la disinstallazione, tenere presenti i seguenti punti:

- Si dispone delle credenziali di accesso per l'utente root al server di backup.
- Esaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Disinstallazione dell'Agente Arcserve UDP (Linux)

È possibile disinstallare l'Agente Arcserve UDP (Linux) dalla riga di comando del server di backup. Il processo di disinstallazione rimuove tutti i file e le directory creati durante l'installazione del software.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Accedere alla cartella *bin* di installazione di Arcserve UDP per Linux immettendo il seguente comando:

   ```
   # cd /opt/Arcserve/d2dserver/bin/
   ```

3. Eseguire il comando seguente per disinstallare l'Agente Arcserve UDP (Linux):

   ```
   # ./d2duninstall
   ```

   Al completamento della disinstallazione, viene visualizzato un messaggio.

   L'Agente Arcserve UDP (Linux) viene disinstallato dal server.

Verifica della disinstallazione

Verificare che l'Agente Arcserve UDP (Linux) sia stato rimosso dal server una volta completato il processo di disinstallazione.

Accedere alla cartella seguente e verificare che l'Agente Arcserve UDP (Linux) sia stato rimosso:

```
/opt/Arcserve/d2dserver
```

La disinstallazione dell'Agente Arcserve UDP (Linux) è stata verificata. L'Agente Arcserve UDP (Linux) viene rimosso dal server Linux.

Aggiornamento dell'Agente Arcserve UDP (Linux)

Eseguire l'aggiornamento dell'Agente Arcserve UDP (Linux) alla versione successiva per poter usufruire dei tanti miglioramenti e delle numerose modifiche delle funzionalità e delle prestazioni dell'Agente Arcserve UDP (Linux).

Nel diagramma seguente viene illustrato il processo di aggiornamento dell'Agente Arcserve UDP (Linux):

Eseguire queste attività per aggiornare l'Agente Arcserve UDP (Linux):

- Considerazioni sull'aggiornamento
- Aggiornamento dell'Agente Arcserve UDP (Linux)
- Verifica dell'aggiornamento

Considerazioni sull'aggiornamento

Prima di procedere con l'aggiornamento, tenere presenti i seguenti punti:

- Assicurarsi di pianificare l'aggiornamento quando non sono in esecuzione processi di backup.
- Esaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Aggiornamento dell'Agente Arcserve UDP (Linux)

Eseguire l'aggiornamento dell'Agente Arcserve UDP (Linux) alla versione successiva per poter usufruire dei tanti miglioramenti e delle numerose modifiche delle funzionalità e delle prestazioni dell'Agente Arcserve UDP (Linux).

Quando si installa l'aggiornamento, l'Agente Arcserve UDP (Linux) prova a individuare un'installazione esistente.

- Se l'Agente Arcserve UDP (Linux) individua un'installazione esistente, esegue automaticamente il processo di aggiornamento. Tutte le configurazioni esistenti (ad esempio file di configurazione, database) vengono salvate e aggiornate.
- Se l'Agente Arcserve UDP (Linux) non individua alcuna installazione esistente, esegue automaticamente una nuova installazione.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Salvare il pacchetto di installazione dell'Agente Arcserve UDP (Linux) (file *.bin) nella cartella root.

   Importante! Se il download dei file del pacchetto di installazione viene eseguito in una cartella locale, il percorso completo di questa cartella locale non deve contenere alcun carattere speciale, salvo spazi vuoti, e può includere solamente i caratteri seguenti: a-z, A-Z, 0-9, - e _.
3. Fornire le autorizzazioni di esecuzione per il pacchetto di installazione.
4. Eseguire il comando seguente per iniziare l'installazione:

   ```
   ./<llinux_installation_file_name>.bin
   ```

   Il pacchetto di installazione verifica la piattaforma supportata e mostra un messaggio di conferma.

   Se viene rilevata una piattaforma non supportata, immettere Y e premere Invio per confermare l'installazione della piattaforma non supportata.

   Il pacchetto di installazione individua un'installazione esistente e viene visualizzato un messaggio di conferma per l'aggiornamento.
5. (Facoltativo) Immettere Y e premere Invio per confermare le dipendenze dell'applicazione.

6. Immettere Y e premere Invio per confermare l'installazione.

   Il pacchetto di installazione mostra le informazioni relative al contratto di licenza.

7. Immettere Y e premere Invio per accettare il Contratto di licenza.

   Il processo di installazione dell'Agente Arcserve UDP (Linux) viene avviato.

   Quando l'installazione del pacchetto dell'utilità di ripristino viene completata, vengono visualizzate le informazioni relative alla creazione del Live CD.

   Live CD viene generato nel percorso seguente:

   `/opt/Arcserve/d2dserver/packages`

   Nota: è necessario Live CD per acquisire l'indirizzo IP del nodo di destinazione quando si esegue un ripristino bare metal (BMR).

L'Agente Arcserve UDP (Linux) è stato aggiornato correttamente.

Verifica dell'aggiornamento

Verificare che l'aggiornamento sia completo dopo avere eseguito l'aggiornamento dell'Agente Arcserve UDP (Linux) alla versione successiva. Il server di backup archivia un backup dei file di configurazioni esistenti. Dopo che la verifica è stata completata, eliminare il backup dei file di configurazione esistenti.

Effettuare le operazioni seguenti:

1. Aprire un browser Web da qualsiasi computer Windows.
2. Immettere l'URL del server di backup.

   Esempio: https://hostname:8014

   Viene visualizzata la pagina di accesso all'Agente Arcserve UDP (Linux).
3. Immettere le credenziali di accesso e fare clic su Accedi.

   Viene visualizzata l'interfaccia utente dell'Agente Arcserve UDP (Linux).
4. Verificare che il server di backup funzioni correttamente.
5. Accedere al server di backup come utente root.
6. Accedere alla cartella d2dserver.bak ed eliminarla.

   `/opt/Arcserve/d2dserver.bak`

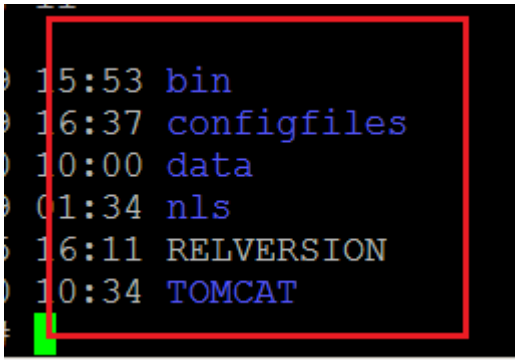
   L'Agente Arcserve UDP (Linux) è stato aggiornato e verificato correttamente.

Migrazione del server di backup Linux a 32 bit a un server a 64 bit

A partire dalla versione 6, l'Agente Arcserve UDP (Linux) non supporterà i server a 32 bit per il server di backup Linux. Per utilizzare l'Agente Arcserve UDP (Linux) versione 6, eseguire la migrazione del server Linux a 32 bit a un server Linux a 64 bit.

Effettuare le operazioni seguenti:

1. Riservare i seguenti file e cartelle nella cartella di installazione dell'Agente Arcserve UDP (Linux):



   Una cartella di installazione tipica per Agente Arcserve UDP (Linux) versione 5 era '/opt/CA/d2dserver'/.

   Nota: se la cartella TOMCAT è una cartella di grandi dimensioni, riservare solo la cartella TOMCAT/conf.

2. Copiare i file e le cartelle riservati in un'altra posizione, come ad esempio '/opt/d2dserver_32bit/'.
3. Organizzare i file e le cartelle riservati nella posizione seguente:

   ```
   tar -czf UDP_LINUX_AGENT.tar.gz /ultraconservative
   ```

4. Copiare il file compresso dal sistema operativo Linux a 32 bit nel sistema operativo Linux a 64 bit utilizzando scp o ftp.
5. Creare una cartella sul server del sistema operativo a 64 bit utilizzando il comando seguente:

   ```
   mkdir -p /opt/CA/d2dserver
   ```

6. Estrarre il file compresso sul sistema operativo Linux a 64 bit utilizzando il comando seguente:

   ```
   tar -xzf UDP_LINUX_AGENT.tar.gz
   ```

7. Copiare i file e le cartelle riservati nella posizione seguente:

   `/opt/CA/d2dserver`

   Ad esempio: cp -Rp /opt/d2dserver_32bit/* /opt/CA/d2dserver

8. Eseguire il pacchetto di installazione del server Linux a 64 bit dell'Agente Arcserve UDP (Linux) versione 6.0.
9. Il server di backup di Linux viene aggiornato automaticamente.

   Nota: se viene modificato il nome host o l'indirizzo IP, consultare la sezione Configurazione delle impostazioni di sistema in caso di modifica del nome host o dell'indirizzo IP.

Chapter 3: Interfaccia utente

La presente sezione descrive i seguenti argomenti:

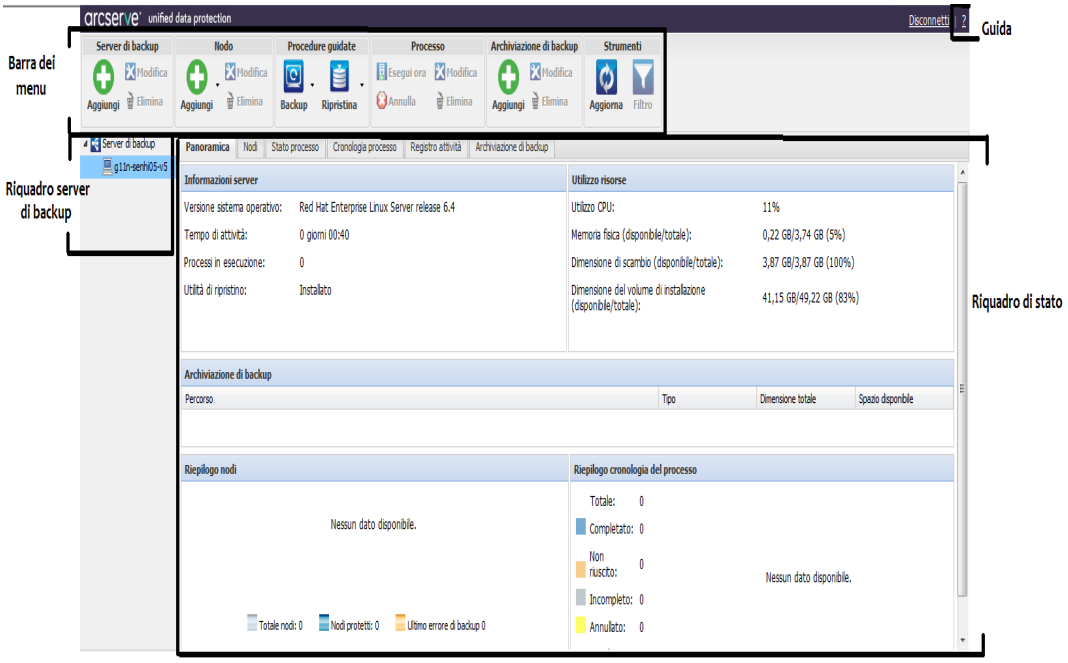
Accesso all'interfaccia utente dell'Agente Arcserve UDP (Linux) 37

Registrazione ad Arcserve UDP 51

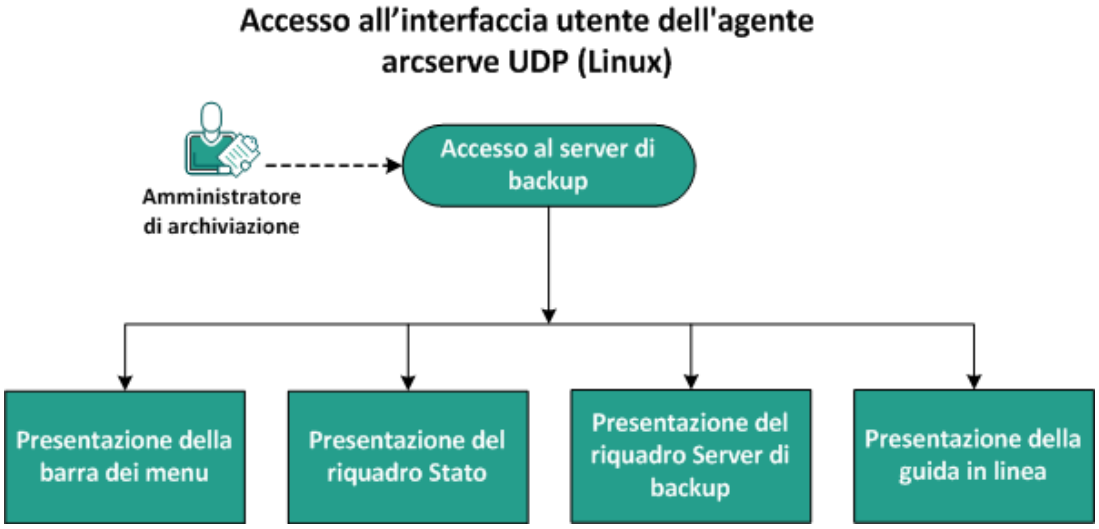
Accesso all'interfaccia utente dell'Agente Arcserve UDP (Linux)

Prima di utilizzare l'Agente Arcserve UDP (Linux), è necessario acquisire una certa dimestichezza con l'interfaccia utente. Tramite l'interfaccia è possibile gestire i nodi, i percorsi di archiviazione di backup, i processi di ripristino e backup e accedere alle sezioni della guida in linea.

L'interfaccia della pagina principale comprende quattro aree principali: la barra dei menu, il riquadro Stato, il riquadro Server di backup e la guida in linea.



Nel diagramma seguente è possibile visualizzare il processo per l'esplorazione dell'interfaccia dell'Agente Arcserve UDP (Linux):



Completare le seguenti attività per acquisire familiarità con l'interfaccia del server di backup:

- Accesso al server di backup
- Presentazione della barra dei menu
- Presentazione del riquadro Stato
- Presentazione del riquadro Server di backup
- Presentazione della guida in linea

Accesso al server di backup

In qualità di manager dell'archiviazione, è possibile accedere al server di backup mediante l'interfaccia Web. Eseguire l'accesso al server di backup con le credenziali utente root o non root. Utilizzare l'indirizzo IP ricevuto durante l'installazione dell'Agente Arcserve UDP (Linux) per accedere al server. Se è stata effettuata la registrazione del nome host del server, sarà possibile eseguire l'accesso al server utilizzando tale nome host.

Nota: per ulteriori informazioni sulla concessione delle autorizzazioni di accesso agli utenti non root, consultare la sezione Concessione delle autorizzazioni di accesso agli utenti non root.

Effettuare le operazioni seguenti:

1. Aprire un browser Web e immettere l'indirizzo IP del server di backup.

   Nota: Per impostazione predefinita, il server di backup segue il protocollo HTTPS e utilizza la porta 8014.

2. Immettere le credenziali di accesso e fare clic su Accedi.

   Viene visualizzata l'interfaccia del server di backup.

   L'accesso al server di backup è stato eseguito correttamente.

Presentazione della barra dei menu

La barra dei menu consente di eseguire le seguenti attività:

- Gestione dei server di backup
- Gestione dei nodi
- Gestione dei processi di backup
- Gestione dei processi di ripristino
- Gestione dei percorsi di archiviazione del backup
- Ricerche di filtri
- Aggiornamento pagine

La schermata seguente mostra la barra dei menu:

La barra dei menu include le opzioni seguenti:

Server di backup

Consente di aggiungere, modificare ed eliminare i server su cui è installato l'Agente Arcserve UDP (Linux). È possibile installare l'Agente Arcserve UDP (Linux) su più server e gestire tutti i server installati da un'interfaccia utente centralizzata. I nodi gestiti dal server selezionato vengono visualizzati nel riquadro Stato. Tutti i server aggiunti vengono visualizzati nel riquadro Server di backup. Non è possibile modificare o eliminare il server centrale. Il server centrale è il primo server visualizzato nel riquadro Server di backup. È possibile modificare ed eliminare gli altri server dal riquadro Server di backup. Il pulsante Modifica consente di aggiornare solo il numero di porta dei server.

Nodo

Consente di aggiungere, modificare, ed eliminare i nodi di cui si desidera eseguire il backup. I nodi rappresentano i computer di cui si desidera eseguire il backup. È possibile aggiungere più nodi per essere sottoposti al backup. È inoltre possibile rilevare i nodi presenti nella rete mediante uno script. È possibile aggiungere un massimo di 200 nodi per ciascun server.

Se viene eliminato un nodo, il server di backup cancella tutte le informazioni relative al nodo dal database, comprese le informazioni sul processo di bac-

kup. Il server di backup elimina inoltre i driver dal nodo. L'eliminazione completa dei driver potrebbe richiedere alcuni minuti.

Procedure guidate

Consente di avviare le procedure guidate di backup e ripristino che forniscono assistenza all'utente durante i processi di backup e ripristino.

- La procedura guidata di backup include un elenco a discesa contenente tre opzioni disponibili:

  Esegui backup

  Utilizzare questa opzione se non sono stati aggiunti nodi in precedenza per il backup. La selezione dell'opzione consente di avviare la procedura guidata di backup e di aggiungere i nodi durante il processo.

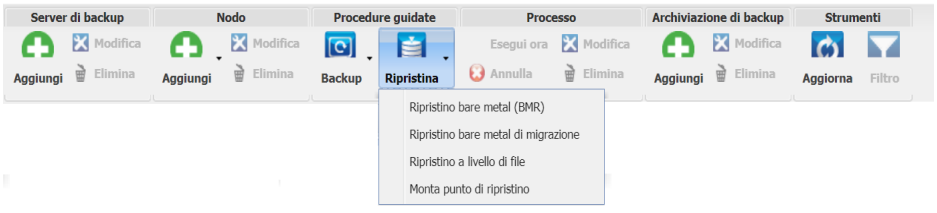
  Esegui il backup dei nodi selezionati

  Utilizzare questa opzione se i nodi sono stati aggiunti prima dell'avvio della procedura guidata di backup. Se si seleziona Esegui il backup dei nodi selezionati senza aggiungere alcun nodo o selezionare i nodi esistenti, verrà visualizzato un messaggio di errore. Per evitare questo errore, selezionare il nodo dalla scheda Nodi e selezionare Esegui il backup dei nodi selezionati.

  Aggiunta dei nodi selezionati a un processo esistente

  Utilizzare questa opzione se è presente un processo di backup esistente e si desidera applicare le stesse impostazioni di backup ai nuovi nodi. Non è necessario configurare la procedura guidata di backup.

- La procedura guidata di ripristino include un elenco a discesa contenente tre opzioni disponibili:



  Ripristino bare metal (BMR)

  Utilizzare questa opzione per eseguire un ripristino bare metal. È possibile eseguire un ripristino bare metal mediante l'indirizzo IP o l'indirizzo MAC del computer bare metal di cui si desidera eseguire il ripristino.

Ripristino bare metal di migrazione

Utilizzare questa opzione per eseguire un ripristino bare metal di migrazione.

Ripristino a livello di file

Utilizzare questa opzione per eseguire un ripristino a livello di file. È possibile selezionare file specifici da un punto di ripristino e ripristinare tali file.

Monta punto di ripristino

Utilizzare questa opzione per eseguire un montaggio del punto di ripristino. Il montaggio del punto di ripristino può condividere i file in un punto di ripristino tramite NFS o WebDAV. Per accedere a questi file, montare la posizione nel server Linux.

Processo

Consente di gestire i processi creati. Un processo è un'istanza di un'operazione di backup o ripristino. Dopo avere creato un processo di backup per un nodo, non sarà necessario creare un altro processo per eseguire un backup per lo stesso nodo in un momento successivo. Tuttavia, è necessario creare un processo di ripristino ogni volta che si desidera eseguire un ripristino bare metal.

Archiviazione di backup

Consente di aggiungere e gestire i percorsi dell'archiviazione di backup. Il percorso di archiviazione del backup può essere una condivisione NFS (Network File System), CIFS (Common Internet File System), una condivisione Locale oppure un server RPS. La condivisione locale corrisponde a un percorso locale del server di backup. Il server RPS è il Recovery Point Server. Il server RPS viene installato durante l'installazione di Arcserve UDP. Dal server RPS, è possibile creare gli archivi dati in cui vengono archiviati i punti di ripristino. Quando si aggiunge un server RPS, è necessario specificare l'archivio dati.

Quando viene aggiunto un percorso di archiviazione di backup, sarà necessario specificare le credenziali per il percorso di archiviazione di backup selezionato. È possibile modificare soltanto il nome utente e la password della condivisione CIFS. Non è possibile modificare i dettagli relativi alla condivisione NFS. Selezionare la casella di controllo Esegui script quando lo spazio libero disponibile è inferiore a per eseguire lo script *backup_storage_alert.sh* quando lo spazio libero è inferiore al valore specificato. Questo valore può essere una percentuale dello spazio totale nella destinazione di

backup o una quantità minima di spazio (in MB) nella destinazione di backup. È possibile configurare lo script backup_storage_alert.sh per l'invio di un avviso quando lo spazio libero disponibile diventa minore del valore specificato.

Nota: per ulteriori informazioni sulla configurazione dello script backup_storage_alert.sh, consultare la sezione *Integrazione e automazione dell'Agente Arcserve UDP (Linux) con l'ambiente IT esistente*.

Dopo aver aggiunto il percorso dell'archiviazione di backup, è possibile visualizzare le dimensioni totali del file e lo spazio libero su disco dal riquadro Stato. Selezionare un percorso di archiviazione di backup per visualizzare i set di ripristino e i punti di ripristino nonché lo spazio utilizzato per ciascun nodo di cui si esegue il backup in quel percorso di archiviazione di backup. Le destinazioni di archiviazione aggiunte vengono inoltre visualizzate nella pagina Destinazione di backup della procedura guidata di backup e nella pagina Punti di ripristino della procedura guidata di ripristino.

Strumenti

Il menu Strumento include il pulsante Aggiorna e il pulsante Filtro.

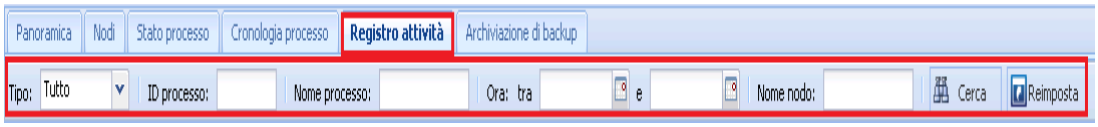
Aggiorna

Consente di aggiornare l'area selezionata del riquadro Stato, compreso il Registro attività per visualizzare gli ultimi messaggi relativi allo stato di backup o ripristino.

Filtro

Consente di filtrare le informazioni visualizzate nel riquadro Stato in base ai valori immessi. Il pulsante Filtro funziona come un interruttore e consente di visualizzare e nascondere i filtri mediante lo stesso pulsante. Quando i filtri sono visualizzati, i campi di ricerca vengono visualizzati nel riquadro Stato. Quando i filtri sono nascosti, i campi di ricerca vengono rimossi dal riquadro Stato.

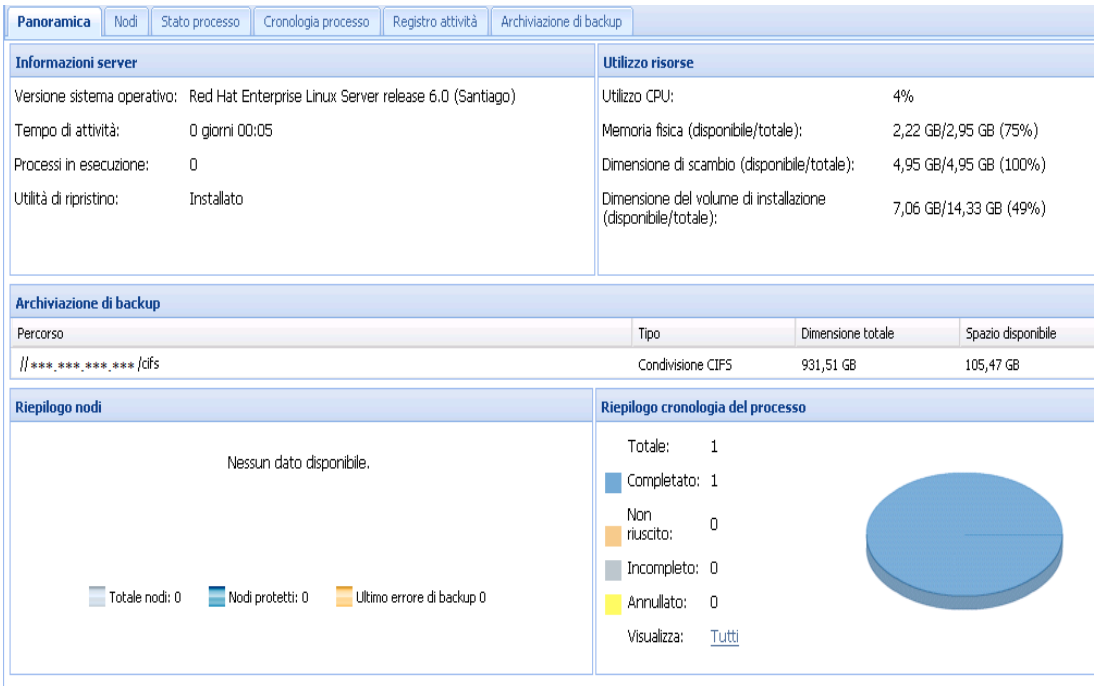
La schermata seguente mostra i filtri applicati al Registro attività:



Presentazione del riquadro Stato

Il riquadro Stato corrisponde all'area in cui vengono visualizzate tutte le informazioni dell'interfaccia utente. Il riquadro Stato include sei schede che consentono di visualizzare le informazioni in base alla scheda selezionata.

La schermata seguente mostra il riquadro Stato:



Il riquadro Stato include le schede seguenti:

Panoramica

Fornisce un riepilogo dei seguenti elementi:

Informazioni server

Mostra la versione del sistema operativo, il tempo trascorso dall'avvio del server e le informazioni relative alla licenza dell'Agente Arcserve UDP (Linux). Indica, inoltre, se l'utilità di ripristino è installata sul server.

Utilizzo risorse

Mostra l'uso della CPU, la memoria fisica totale e disponibile e le dimensioni di scambio. Mostra inoltre le dimensioni del volume di installazione.

Archiviazione di backup

Mostra tutti i percorsi delle sessioni di backup aggiunti e lo spazio disponibile per ogni percorso. Tali informazioni consentono di pianificare il percorso successivo di backup in base allo spazio di archiviazione disponibile.

Riepilogo nodi

Mostra una rappresentazione grafica dei nodi protetti e dei nodi il cui ultimo backup ha prodotto un errore. Il Riepilogo nodi include le seguenti categorie:

Totale nodi: mostra il numero di nodi inclusi nell'Agente Arcserve UDP (Linux) indipendentemente dallo stato di backup.

Nodi protetti: mostra il numero di nodi il cui backup più recente è stato eseguito correttamente e che vengono considerati protetti in caso di un ripristino di emergenza.

Ultimo errore di backup: mostra il numero di nodi il cui backup più recente ha prodotto un errore (non riuscito, annullato o incompleto). A seconda dell'errore che ha causato la mancata riuscita di un backup, alcuni nodi non sono protetti in caso di un ripristino di emergenza.

Riepilogo cronologia del processo

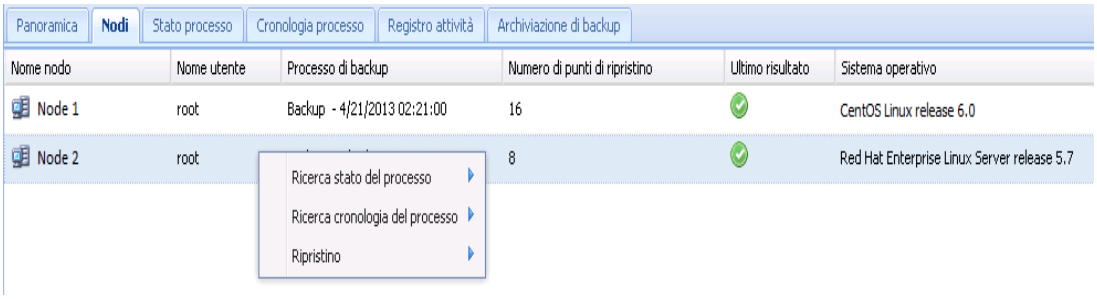
Visualizza un grafico a torta contenente la cronologia di tutti i processi. Il riepilogo non include i processi in esecuzione.

I seguenti campi richiedono una spiegazione aggiuntiva:

- Incompleto: indica il numero di processi eseguiti correttamente con modifiche minori. Ad esempio, quando si ripristinano dei file da Red Hat 6 a Red Hat 5, questi file vengono ripristinati correttamente ma alcuni attributi sono mancanti nei file ripristinati.
- Altro: mostra il numero di processi annullati.

Nodi

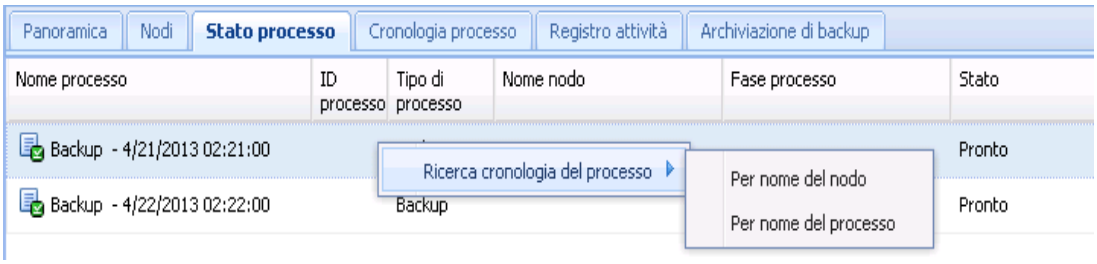
Mostra tutti i nodi aggiunti al server di backup. È possibile applicare i filtri alla scheda Nodi per eseguire la ricerca dei nodi richiesti. La scheda Nodi include anche un menu di scelta rapida. Il menu di scelta rapida consente di cercare lo stato o la cronologia dei processi del nodo selezionato. Inoltre consente il ripristino dei dati. È possibile filtrare la cronologia o lo stato dei processi mediante il nome del processo o del nodo. Se si cerca il nodo selezionato nella cronologia del processo, viene visualizzata la scheda Cronologia processo con il filtro di ricerca applicato alla scheda. Allo stesso modo, se si cerca lo stato di processo, viene visualizzata la scheda Stato processo con il filtro di ricerca applicato alla scheda. L'opzione Ripristino consente di eseguire ripristino bare metal o a livello di file. Consente di aprire la procedura guidata di ripristino guidato con la visualizzazione di tutti i punti di ripristino del nodo selezionato.



Stato processo

Mostra l'elenco dei processi di backup e ripristino creati, compreso lo stato relativo a ciascun processo. Utilizzare questa scheda per eseguire un processo di backup o di ripristino e ripetere un processo di backup. È possibile visualizzare l'avanzamento dei processi di backup o ripristino eseguiti. È possibile applicare i filtri alla scheda Stato processo per eseguire la ricerca dei nodi richiesti. La scheda Stato processo include anche un menu di scelta rapida. Il menu di scelta rapida consente di cercare la cronologia dei processi per il processo selezionato. È possibile filtrare la cronologia dei processi mediante il nome del processo o del nodo. Se si effettua una ricerca nella cronologia dei processi per il processo selezionato, la scheda Cronologia processo si apre con il filtro di ricerca applicato.

La schermata seguente mostra il menu di scelta rapida nella scheda Stato processo:



Cronologia processi

Mostra l'elenco dei processi di backup e ripristino eseguiti precedentemente. È possibile applicare i filtri alla scheda Cronologia processo per eseguire la ricerca della cronologia dei processi. Quando si seleziona un processo, lo stato di tale processo viene visualizzato nella parte inferiore della pagina.

Registro attività

Mostra un elenco dei messaggi di elaborazione e di stato per i processi di backup e ripristino. Aggiornare il Registro attività per ottenere i messaggi più recenti relativi ai processi di backup e ripristino. È possibile applicare filtri alla scheda Registro attività per eseguire la ricerca dei registri attività richiesti.

Archiviazione di backup

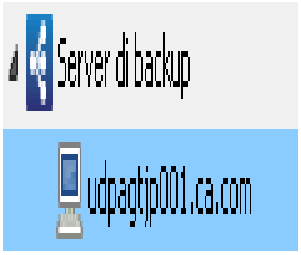
Mostra la destinazione di backup che è stata aggiunta dalla barra dei menu. È possibile visualizzare lo spazio di archiviazione disponibile e gestire la destinazione di backup. Questa opzione è utile se si desidera conoscere lo spazio libero disponibile su qualsiasi destinazione di backup per la pianificazione del proprio backup. Quando si aggiunge una destinazione di archiviazione, questa destinazione viene visualizzata nella procedura guidata di backup.

Presentazione del riquadro Server di backup

Nel riquadro Server di backup viene visualizzato l'elenco dei server di backup gestiti dal server corrente. È possibile aggiungere server dalla barra dei menu, nonché gestire tutti i server a partire da una singola interfaccia. Se sono stati aggiunti server multipli, il riquadro Stato mostrerà lo stato del server selezionato. Ogni server può gestire almeno 200 nodi client.

Il primo server visualizzato nel riquadro Server di backup è generalmente il server di backup centrale, mentre gli altri sono server membri. Se si stanno gestendo più server da un server centrale, verificare che la versione del server centrale e quella dei server membri sia la stessa.

Nella schermata seguente viene visualizzato il riquadro Server di backup:



Presentazione della guida in linea

La finestra di dialogo ? consente di accedere agli argomenti della guida in linea dell'Agente Arcserve UDP (Linux). Dall'elenco a discesa della Guida in linea è possibile eseguire le seguenti attività:

Le opzioni seguenti sono disponibili nell'elenco a discesa della Guida in linea:

Knowledge Center

Consente di accedere al bookshelf.

Supporto in linea

Consente di accedere al sito Web del Supporto tecnico di Arcserve.

Guida alle Soluzioni

Consente di accedere alla versione HTML della Guida alle soluzioni dell'agente Arcserve UDP.

Guida all'agente per Linux

Consente di accedere alla versione HTML della Guida per l'utente.

Chiedi al Supporto tecnico: Chat in tempo reale

Consente di aprire una finestra di chat in tempo reale e contattare un responsabile del Supporto tecnico di Arcserve per una chat in tempo reale.

Commenti e suggerimenti

Consente di accedere al sito Web del Supporto tecnico di Arcserve e di fornire un feedback al team di sviluppo.

Video

Consente di accedere ai video relativi e alle esercitazioni in linea dell'Agente Arcserve UDP (Linux).

Gestione licenze

Consente di accedere alla finestra di dialogo Gestione licenze per gestire tutte le licenze in uso da un'interfaccia centrale.

Product Improvement Program

Consente di fornire suggerimenti per migliorare il prodotto Arcserve.

informazioni

Consente di visualizzare le informazioni relative al prodotto (numero di versione e di build) e di accedere alle Note di rilascio dell'agente Arcserve UDP.

Registrazione ad Arcserve UDP

Dopo aver installato Arcserve UDP, è necessario registrare il prodotto dalla console. La registrazione consente ad Arcserve di raccogliere automaticamente le statistiche e dati sull'utilizzo della console.

Importante! Arcserve non raccoglie alcuna informazione personale o di importanza critica per l'azienda come il nome del nodo, l'indirizzo IP, le credenziali di accesso, il nome di dominio e i nomi delle reti.

Se la console non è stata registrata, l'utente riceverà il seguente messaggio di notifica nella scheda **Messaggi** della console.

```
La copia di Arcserve Unified Data Protection non è stata
registrata nel programma Arcserve Product Improvement Pro-
gram. Registrarla.
```

Effettuare le operazioni seguenti:

1. Dalla console, fare clic su **?**, **Arcserve Product Improvement Program**.

   Viene visualizzata la finestra di dialogo **Arcserve Product Improvement Program**.

2. Selezionare la casella di controllo **Aderisci al programma Arcserve Product Improvement Program**.
3. Specificare i seguenti dettagli:

   Nome

   Specificare il nome dell'utente.

   Azienda

   Specificare il nome della propria azienda.

   Numero di telefono

   Specificare il numero di telefono nel seguente formato:

   Codice Paese - Numero di telefono. Esempio: 000-1122334455

   Indirizzo di posta elettronica

   Specificare il proprio indirizzo di posta elettronica. Il campo è obbligatorio. L'e-mail di verifica verrà inviata all'indirizzo fornito.

   Numero di esecuzione

   Specificare il numero di esecuzione. L'utente deve avere ricevuto questo numero in un messaggio di posta elettronica durante il download di Arcserve UDP.

4. Fare clic su **Invia e-mail di verifica**.

   Il messaggio di verifica viene inviato all'indirizzo di posta elettronica specificato nella finestra di dialogo **Arcserve Product Improvement Program**.

5. Accedere all'account di posta elettronica e aprire il messaggio ricevuto.
6. Fare clic sul collegamento di verifica contenuto nell'e-mail.

   Arcserve UDP è stato registrato correttamente.

   Dopo la registrazione si attiva il pulsante Annulla adesione.

   Per annullare la registrazione, fare clic su **Annulla adesione**.

   Se si desidera aggiornare l'indirizzo di posta elettronica, è necessario ripetere la registrazione. Per farlo, seguire la stessa procedura già descritta in questo argomento.

Chapter 4: Utilizzo dell'Agente Arcserve UDP (Linux)

La presente sezione descrive i seguenti argomenti:

Gestione delle licenze 55

Gestione dei processi 60

Backup di nodi Linux 65

Modifica e nuova esecuzione di un processo di backup 111

Esecuzione di un ripristino a livello di file per i nodi Linux 118

Creazione di un Live CD di avvio 139

Creazione di un Live CD di avvio per includere i driver personalizzati per AlmaLinux 9.x 145

Esecuzione di un ripristino bare metal per computer Linux 150

Esecuzione di un ripristino bare metal per computer Linux in AWS Cloud 186

Esecuzione di un ripristino bare metal per i computer Linux in Azure Cloud 211

Esecuzione di un ripristino bare metal di migrazione per computer Linux 221

Esecuzione di un ripristino bare metal di migrazione per computer Linux da Amazon EC2 sul computer locale 228

Ripristino automatico di un computer virtuale 234

Integrazione e automazione dell'Arcserve UDP per Linux con l'ambiente IT esistente 249

Gestione delle impostazioni del server di backup 295

Gestione del server di backup Linux dalla riga di comando 310

Aggiunta di un utente alla Console del server di backup Linux mediante la riga di comando 328

Gestione degli utenti non root 332

Modalità di configurazione dell'account utente sudo per i nodi Linux 338

Ripristino dei volumi su un nodo di destinazione 345

Download di file e cartelle senza ripristino per i nodi Linux 357

Ripristino di un database Oracle mediante l'Agente Arcserve UDP (Linux) 358

Esecuzione della verifica Assured Recovery dalla riga di comando 374

Montaggio dei punti di ripristino 383

Attivazione del supporto per i kernel Linux più recenti di RHEL, OEL (kernel RHEL), Debian, SUSE e Ubuntu 395

Disattivazione del bit SUID durante l'esecuzione del processo di ripristino del file 400

Gestione delle licenze

Per garantire l'accesso autorizzato e continuo ai componenti dell'Agente Arcserve UDP (Linux), è necessario eseguire la registrazione della licenza di prodotto corrispondente. Inoltre, se si desidera eseguire la distribuzione di Arcserve UDP per Linux su posizioni remote, è necessario disporre della licenza per tali siti remoti per poter usufruire dei vantaggi offerti dall'Agente Arcserve UDP (Linux).

È possibile utilizzare l'Agente Arcserve UDP (Linux) per un periodo di prova di 30 giorni dopo il primo utilizzo. Per poter continuare a usarlo, sarà necessario applicare il codice di licenza appropriato. L'Agente Arcserve UDP (Linux) consente di gestire le licenze di tutti i server di backup da un'interfaccia centrale.

Il diagramma seguente mostra il processo di gestione delle licenze:

Completare le attività seguenti per gestire le licenze:

- Accesso a Gestione licenze
- Informazioni sulla finestra di dialogo di Gestione licenze
- Gestione delle licenze

Accesso a Gestione licenze

Per gestire tutte le licenze, è necessario accedere alla finestra di dialogo di Gestione licenze dall'interfaccia Web dell'Agente Arcserve UDP (Linux).

Effettuare le operazioni seguenti:

1. Accedere all'interfaccia Web dell'Agente Arcserve UDP (Linux).
2. Dalla pagina principale, fare clic su ?, Gestisci licenze.

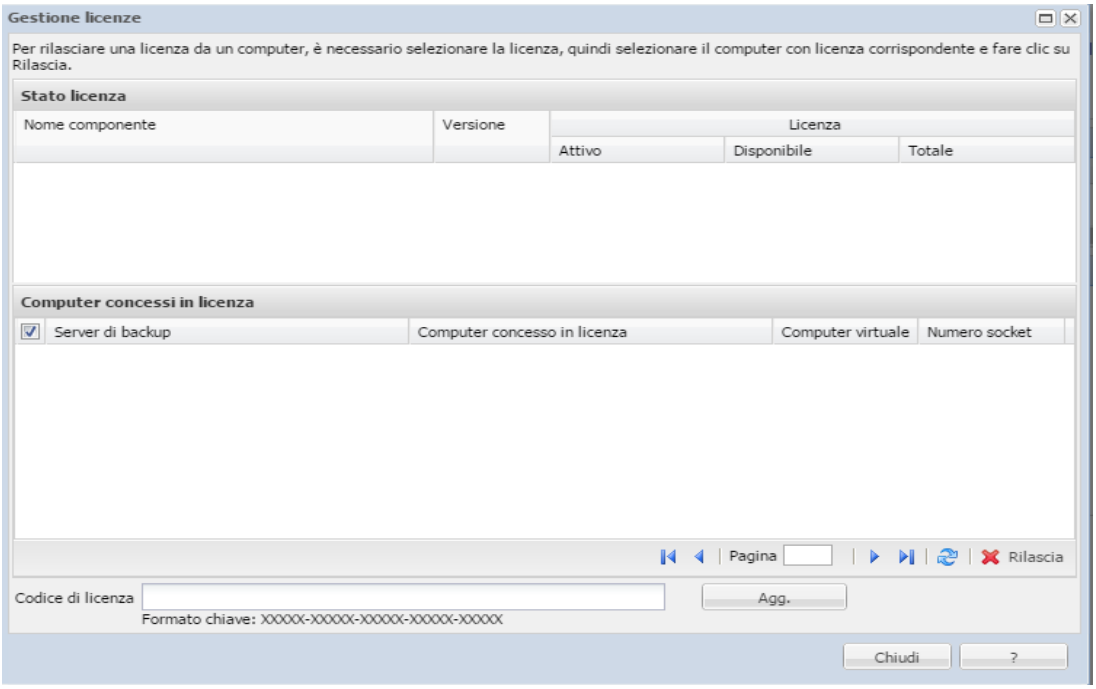
   Viene visualizzata la finestra di dialogo Gestione licenze.

   Si accede al gestore licenze.

Informazioni sulla finestra di dialogo di Gestione licenze

La finestra di dialogo Gestione licenze consente di gestire tutte le licenze dell'Agente Arcserve UDP (Linux). È possibile gestire le licenze per più server di backup Linux da un'unica interfaccia.

La schermata seguente mostra la finestra di dialogo Gestione licenze:



La finestra di dialogo Gestione licenze è suddivisa in due sezioni, Stato licenza e Computer concesso in licenza.

Stato licenza

Nome componente

Identifica il nome della licenza.

Versione

Identifica il numero di versione della licenza.

Attivo

Identifica il numero di licenze attualmente utilizzate per eseguire il backup dei nodi.

Disponibile

Identifica il numero di licenze ancora disponibili nel pool delle licenze e che è possibile utilizzare per eseguire il backup dei computer Linux.

Totale

Identifica il numero totale di licenze ottenute per eseguire il backup del computer. Il totale è la somma delle licenze con stato Attivo e Disponibile.

Computer concessi in licenza

Server di backup

Identifica il server Linux in cui è stato installato l'Agente Arcserve UDP (Linux).

Computer concessi in licenza

Identifica i computer Linux ai quali è stata applicata una licenza a scopo di protezione.

Gestione delle licenze

È possibile aggiungere e rilasciare licenze dalla finestra di dialogo di Gestione licenze. La licenza aggiunta viene visualizzata nella finestra di dialogo di Gestione licenze. Se non si desidera eseguire il backup di un computer, è possibile rilasciare la licenza dal computer in questione.

Per aggiungere una licenza, attenersi alle seguenti istruzioni:

a. L'utilizzo del Portale di licenza Arcserve consente di generare la chiave di licenza. Per ulteriori informazioni, consultare la sezione Generazione delle chiavi di licenza Arcserve per gli agenti standalone.

b. Immettere la chiave di licenza nel campo Chiave di licenza della finestra di dialogo Gestione licenze e fare clic su Aggiungi.

c. Chiudere e aprire la finestra di dialogo di Gestione licenze.

La licenza viene aggiunta e classificata nell'area Stato licenza.

Per rilasciare una licenza, attenersi alle seguenti istruzioni:

a. Selezionare la licenza dall'area Stato licenza della finestra di dialogo Gestione licenze.

b. Selezionare il server di backup in Computer concessi in licenza e fare clic su Rilascia.

c. Chiudere e aprire la finestra di dialogo di Gestione licenze.

La licenza viene rilasciata dal computer.

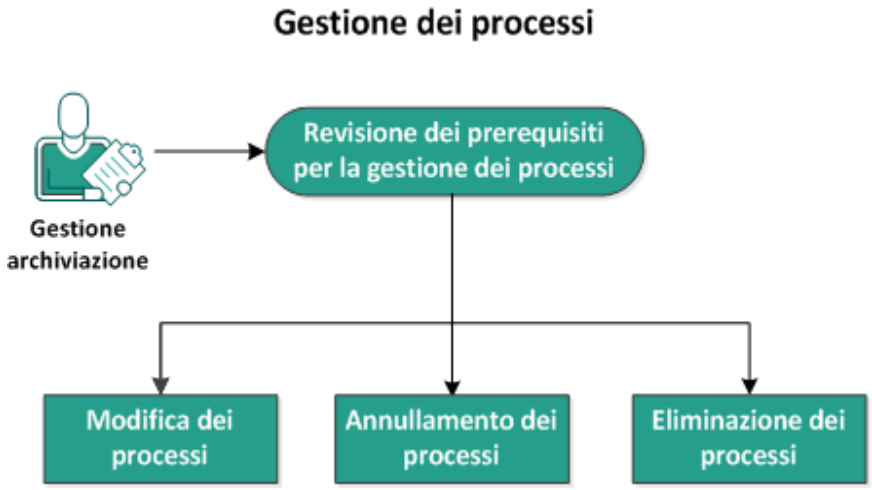
Le licenze sono gestite correttamente.

Gestione dei processi

Dopo aver creato un processo di backup o di ripristino, è possibile gestire tutti i processi dal menu Processo. La gestione di un processo prevede le attività seguenti:

- Modifica di un processo
- Annullamento un processo
- Eliminazione di un processo

Il diagramma seguente mostra il processo di gestione dei processi:



Completare le attività seguenti per gestire i processi:

- Verifica dei prerequisiti
- Modifica dei processi
- Annullamento dei processi
- Eliminazione dei processi

Revisione dei prerequisiti per la gestione dei processi

Considerare i prerequisiti seguenti prima di procedere con la gestione dei processi:

- Si dispone di un processo esistente valido da gestire
- Si possiede l'autorizzazione appropriata per la gestione dei processi.
- Esaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Modifica dei processi

È possibile aprire qualsiasi processo esistente e modificarne le impostazioni dall'interfaccia Web. Ad esempio, se si desidera modificare la destinazione di backup per un computer già protetto, non è necessario creare un nuovo processo. È possibile aprire il processo esistente che protegge il computer e modificare solo la sezione relativa alla destinazione di backup. Tutte le altre impostazioni restano invariate, tranne le impostazioni relative alla destinazione di backup.

Effettuare le operazioni seguenti:

1. Selezionare un processo dalla scheda Stato processo.
2. Fare clic su Modifica dal menu Processo.

   Viene visualizzata la procedura guidata per il processo selezionato.
3. Modificare le impostazioni nella procedura guidata.
4. Fare clic su Invia nella pagina Riepilogo della procedura guidata.

   Il processo viene inviato ed eseguito in base alle impostazioni inserite.

   Il processo è stato modificato correttamente.

Annullamento dei processi

È possibile annullare un processo in esecuzione dall'interfaccia Web dell'Agente Arcserve UDP (Linux).

Effettuare le operazioni seguenti:

1. Selezionare un processo dalla scheda Stato processo.
2. Fare clic su Annulla dal menu Processo.

   Viene visualizzata la finestra di dialogo Annulla processo.

3. Selezionare una delle opzioni seguenti dall'elenco a discesa Annulla processo per:

   Nodo selezionato

   Specifica che il processo viene annullato solo per il nodo selezionato.

   Tutti i nodi sono protetti dal processo selezionato

   Specifica che il processo viene annullato per tutti i nodi protetti dal processo selezionato.

4. Fare clic su OK.

   Il processo è stato annullato.

Eliminazione dei processi

È possibile eliminare un processo quando non si desidera più proteggere o ripristinare un computer. È possibile inoltre eliminare un processo che protegge un gruppo di nodi. Quando si elimina un processo, i punti di ripristino sottoposti a backup in precedenza restano ancora disponibili nella destinazione di backup specificata. È possibile utilizzare quei punti di ripristino per ripristinare i dati.

Per un processo in esecuzione, l'opzione Elimina non è attiva. È necessario annullare il processo in esecuzione per poi eliminarlo.

Effettuare le operazioni seguenti:

1. Selezionare un processo dalla scheda Stato processo.
2. Fare clic su Elimina dal menu Processo.

   Viene visualizzata la finestra di dialogo Elimina processo.
3. Selezionare una delle opzioni seguenti dall'elenco a discesa Elimina processo per:

   Nodo selezionato

   Specifica che il processo viene eliminato solo per il nodo selezionato.

   Tutti i nodi sono protetti dal processo selezionato

   Specifica che il processo viene eliminato per tutti i nodi protetti dal processo selezionato.
4. Fare clic su OK.

   Il processo è stato eliminato.

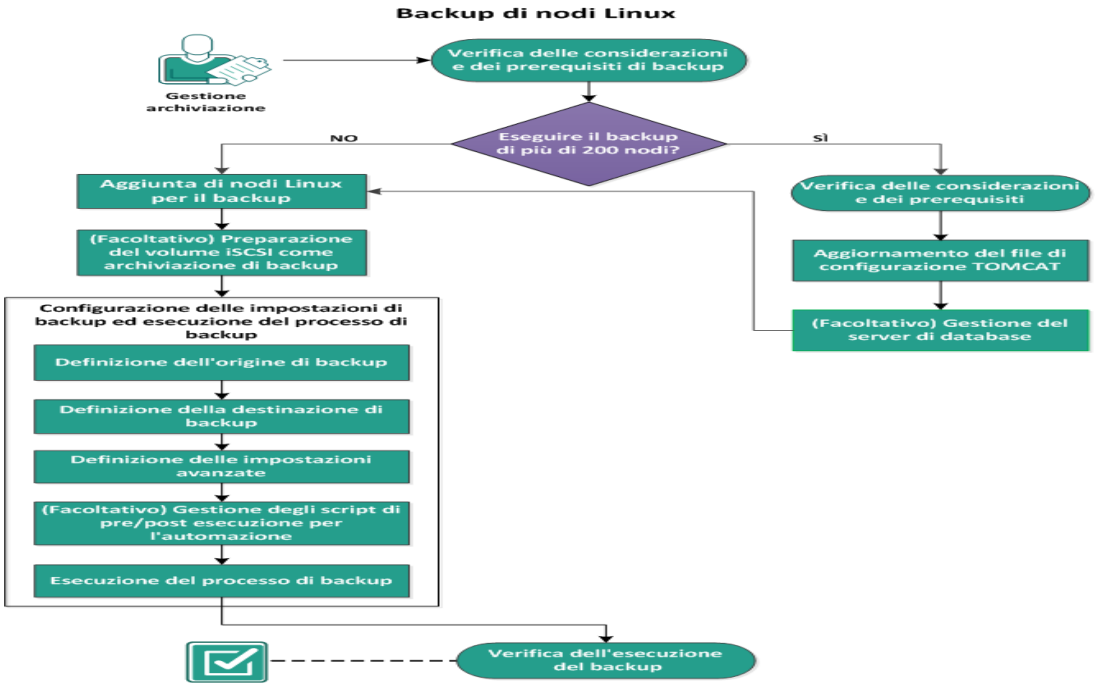
Backup di nodi Linux

L'Agente Arcserve UDP (Linux) consente di eseguire il backup dei nodi Linux e dei dati in essi archiviati. Inoltre è possibile eseguire il backup dello stesso server di backup come qualsiasi altro nodo Linux. Il server di backup è in grado di eseguire il backup di un massimo di 200 nodi.

Quando l'Agente Arcserve UDP (Linux) esegue un backup di dati, acquisisce anche informazioni relative al sistema operativo, alle applicazioni installate e ai driver ecc. a partire dal nodo di produzione. Di conseguenza, quando viene eseguito il ripristino dei dati sottoposti a backup, è possibile eseguire un ripristino bare metal oppure eseguire il ripristino dei dati richiesti.

Nota: se il nodo di origine di backup viene riavviato, il backup successivo viene convertito in un backup di verifica (per backup di non deduplicazione) o in un backup completo (per backup di deduplicazione).

Il seguente diagramma mostra la procedura di backup dei nodi Linux:



Eseguire le seguenti attività per l'esecuzione di un backup di un nodo Linux:

- Verifica delle considerazioni e dei prerequisiti di backup
- Backup di più di 200 nodi
  - Verifica delle considerazioni e dei prerequisiti
  - Aggiornamento del file di configurazione TOMCAT
  - Gestione del server di database

- Aggiunta di nodi Linux per il backup
- (Facoltativo) Registrazione della chiave pubblica di Arcserve per l'avvio protetto
- (Facoltativo) Preparazione del volume iSCSI come archiviazione di backup
- Configurazione delle impostazioni di backup ed esecuzione del processo di backup
  - Definizione dell'origine di backup
  - Definizione della destinazione di backup
  - Definizione delle impostazioni avanzate
  - (Facoltativo) Gestione di pre/post script per l'automazione
  - Esecuzione del processo di backup
- Verifica dell'esecuzione del backup

Verifica delle considerazioni e dei prerequisiti di backup

Verificare i requisiti seguenti prima di eseguire un backup:

- Si dispone dei requisiti di hardware e software per il nodo di backup.

  Nota: per ulteriori informazioni sull'hardware supportato e sui requisiti software, consultare le *Arcserve UDP Note di rilascio*.

- Si dispone di una destinazione di backup valida per l'archiviazione dei dati sottoposti a backup.
- Si dispone dei nomi utente e delle password dei nodi di cui si desidera eseguire il backup.
- La cartella */temp* del nodo di backup dispone di uno spazio minimo di 300 MB. La cartella*/temp* viene utilizzata per elaborare l'accumulo di blocchi incrementali.
- Perl e sshd (Daemon SSH) vengono installati sui nodi di cui si desidera eseguire il backup.
- Il nodo di backup può accedere alla destinazione di backup e si dispone dell'autorizzazione di scrittura.
- Esaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Per ripetere un processo di backup, verificare di aver eseguito il backup del nodo e di disporre di un processo di backup valido.

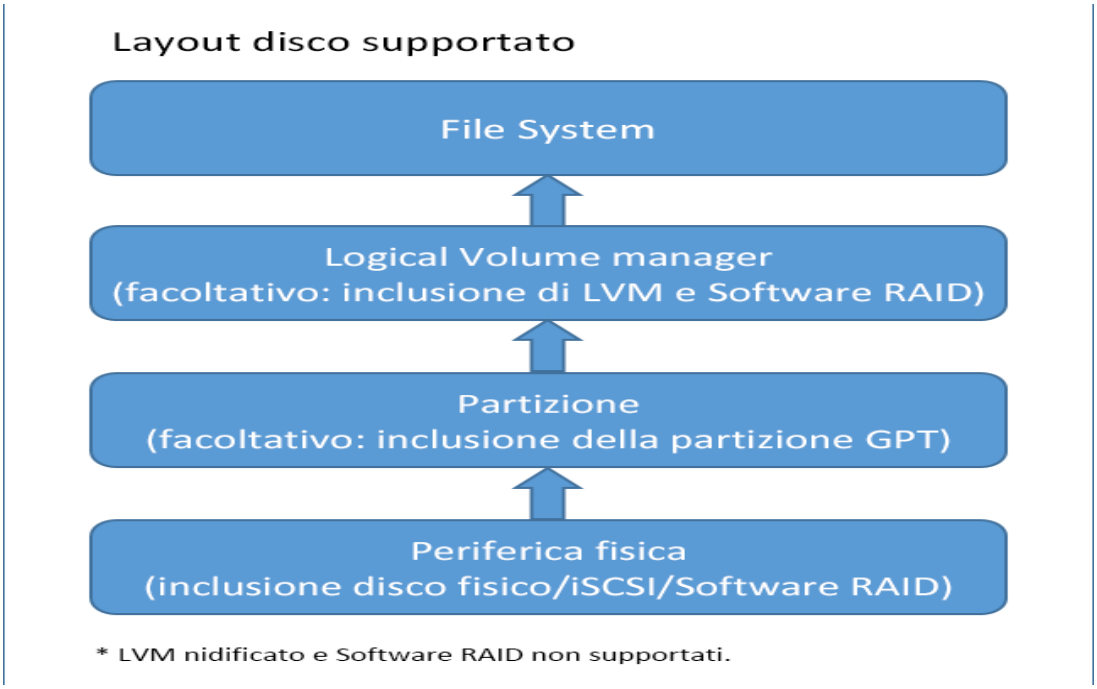
Verificare le seguenti considerazioni di backup:

- Per ottimizzare la gestione dei punti di ripristino, considerare le seguenti raccomandazioni durante la pianificazione della frequenza dei backup:
  - Per sistemi protetti con backup incrementali eseguiti ogni 15 minuti, pianificare un backup completo ogni settimana per aggiornare l'immagine di base.

Nota: se il valore di spazio utilizzato per archiviare le immagini di backup costituisce un problema, si consiglia di pianificare l'esecuzione dei backup completi con una frequenza inferiore per ridurre lo spazio di archiviazione.

Layout di disco supportati dall'Agente Arcserve UDP (Linux)

L'immagine seguente mostra il layout del disco supportato dall'origine di backup dell'agente Arcserve UDP (Linux):



Dischi supportati dall' Agente Arcserve UDP (Linux)

Per i dischi di backup e l'origine di backup dell'Agente Arcserve UDP (Linux) sono supportati diversi tipi di dischi. La seguente matrice elenca i tipi di dischi supportati per ciascuna funzionalità.

Supporto ripristino bare metal e backup		
Tipo di (volume) disco	**Come origine di backup**	**Come destinazione di backup**
Volume montato (Partizione tradizionale del disco e LVM ***2**)	Sì	Sì
Volume RAW (Non formattato)	No	No
Volume crittografato	No	No
Scambio	No	Non applicabile
Disco GPT:		
■ Disco dati GPT (Tabella di partizione GUID)	Sì	Sì
■ Disco di avvio GPT (Tabella di partizione GUI)	Sì	Non applicabile
Disco RAID *1:		
■ Software RAID (RAID-0 (stripe))	Sì	Sì
■ Software RAID (RAID-1 (con mirroring))	Sì	Sì
■ Software RAID-5	Sì	Sì
■ Hardware RAID (con RAID incorporato)	Sì	Sì
File system:		
■ EXT2	Sì	Sì
■ EXT3	Sì	Sì
■ EXT4	Sì	Sì
■ Reiserfs versione 3	Sì	Sì
■ XFS *3	Sì	Sì
■ Btrfs *4	Sì	Sì
Volume condiviso:		
■ Volume condiviso di Windows (Condivisione CIFS)	Non applicabile	Sì
■ Volume condiviso di Linux (condivisione samba)	No	Sì
■ Condivisione NFS di Linux	No	Sì
Tipo periferica:		

■ Disco rimovibile (ad esempio Memory Stick, RDX)	Sì	Sì
*1	Il RAID falso, denominato anche RAID incorporato, fornito dal BIOS nella scheda madre non è supportato dall'Agente Arcserve UDP (Linux).	
*2	L'LVM incorporato non è supportato.	
*3	Il ripristino a livello di file per una versione superiore di XFS non è supportato su un server di backup Linux che utilizza una versione precedente di XFS. Ad esempio, l'esecuzione del ripristino a livello di file per XFS su RHEL7.X non è supportata su RHEL6.x come server di backup. Tuttavia, è possibile utilizzare Live CD come server di backup temporaneo per eseguire il ripristino a livello di file. **Nota**: RedHat Enterprise Linux 8, CentOS 8 e Oracle Linux 8 presentano limitazioni che non sono in grado di supportare il ripristino bare metal, il computer virtuale istantaneo e Assured Recovery per il filesystem di Arcserve UDP 7.0, build U1.	
*4	Il ripristino a livello di file per i file system basati su btrfs (server SLES) non è supportato su CentOS 8.0 e su RHEL 8.0 LBS (server di backup Linux). Il ripristino a livello di file sul computer di origine non è supportato. Ad	

	esempio, installare il server di backup Linux sul computer A, eseguire il backup del computer A, quindi eseguire il ripristino dal punto di ripristino A sul computer A. Il filtro di file/cartelle non è supportato. Il processo di bilanciamento/pulitura del file system verrà annullato all'inizio del backup. BTRFS RAID supporta: RAID-0 e RAID-1. Interfaccia utente del filtro di volume: viene visualizzato soltanto il volume principale. Non è una limitazione, ma si tratta del comportamento previsto.

Backup di più di 200 nodi

Per impostazione predefinita, i server di backup possono gestire un numero massimo di 200 nodi. Se si desidera eseguire il backup di un numero di nodi superiore a 200, è possibile impostare server di backup membri. e utilizzare un server di backup centrale per gestire tutti i server membri.

Nel caso in cui sia necessario gestire più di 200 nodi e si disponga di un server di backup dedicato, è possibile abilitare le impostazioni corrispondenti per la gestione di più di 200 nodi.

Verifica delle considerazioni e dei prerequisiti

Verificare i seguenti prerequisiti prima di procedere al backup di un numero di nodi di Linux superiore a 200:

- Il server di backup supporta unicamente Linux a 64 bit.
- Il server di backup deve essere un server dedicato. L'Agente Arcserve UDP (Linux) modifica le impostazioni di sistema per soddisfare il requisito di alta di scalabilità del server.
- Il server deve soddisfare i requisiti minimi hardware riportati di seguito. Se si dispone di un numero di nodi elevato, le specifiche hardware devono essere superiori ai requisiti minimi.
  - Memoria di 8 GB
  - 10 GB di spazio libero su disco per la cartella /opt

Verificare le seguenti considerazioni:

- Se l'Agente Arcserve UDP (Linux) viene abilitato per il backup di più di 200 nodi, il server utilizza un nuovo database (postgresql) per soddisfare il requisito di alta scalabilità. Tutti i nodi e le informazioni di processo esistenti nel database precedente (sqlite) vengono migrate al nuovo database, salvo la cronologia di processo e il registro attività. Una volta eseguita la migrazione non è possibile tornare al database precedente (sqlite).
- In seguito alla migrazione, viene utilizzato un formato diverso per l'output del comando d2djobhistory.
- Come procedura ottimale, si consiglia di impostare ciascun processo di backup per il backup di un numero di nodi inferiore a 1000.

Aggiornamento del file di configurazione TOMCAT

Durante l'aggiornamento all'Agente Arcserve UDP (Linux) dalla versione precedente, ad esempio r16.5 SP1, è necessario aggiornare il file di configurazione di TOMCAT per supportare il requisito di alta scalabilità del server di backup. Questo aggiornamento consente di sottoporre a backup più di 200 nodi con un solo server di backup.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Accedere alla cartella bin:

   ```
   /opt/Arcserve/d2dserver/bin
   ```

3. Verificare nessun processo sia in esecuzione e interrompere il server di backup utilizzando il comando seguente:

   ```
   ./d2dserver stop
   ```

   Nel caso in cui siano presenti processi in esecuzione, attendere il completamento di tali processi prima di interrompere il server di backup.

   ```
   /opt/Arcserve/d2dserver/TOMCAT/conf/
   ```

4. Aggiornare i parametri seguenti.

   Se si utilizza il protocollo HTTPS, aggiornare i parametri seguenti:

   ```
   <Connector port="8014" connectionTimeout="180000" protocol="HTTP/1.1" SSLEnabled="true" maxThreads="300" acceptCount="200" scheme="https" secure="true" clientAuth="false" sslProtocol="TLSv1, TLSv1.1, TLSv1.2" keystoreFile="${catalina.home}/conf/server.keystore keystorePass="LinuxD2D"/>
   ```

   Se si utilizza il protocollo HTTP, aggiornare i parametri seguenti:

   ```
   <Connector connectionTimeout="180000" port="8014" maxThreads="300" acceptCount="200" protocol="HTTP/1.1"/>
   ```

   Il file di configurazione di TOMCAT è stato aggiornato correttamente.

5. Interrompere il server di backup.

   ```
   ./d2dserver stop
   ```

6. Eseguire il comando seguente per avviare il server di backup:

   ```
   ./pgmgr init
   ```

Questo comando verifica che tutte le modifiche necessarie siano state completate e avvia il server di backup.

```
[root@<Machine Name> bin]# ./d2dserver stop
arcserve UDP Agent(Linux) è stato arrestato.
[root@<Machine Name> bin]# ./pgmgr init
Il processo di installazione è stato avviato per il database Postgresql. Il regi
stro di debug è disponibile alla seguente posizione: /opt/CA/d2dserver/logs/pgin
it.log.
La base de données Postgresql a été installée.
Les données ont été migrées vers la nouvelle base de données.
arcserve UDP Agent(Linux) a été démarré.
```

Il server di backup e il server di database sono stati avviati correttamente.

Gestione del server di database

Il comando *d2dserver start* esegue l'avvio del server di database e del server di backup. Se non è presente alcun processo in corso di esecuzione, il comando *d2dserver stop* interrompe entrambi i server.

Se si desidera avviare e interrompere il server di database manualmente, eseguire i comandi seguenti:

pgmgr start

Avvia il server di database.

pgmgr stop

Interrompe il server di database.

pgmgr status

Visualizza lo stato del server di database. Indica se il server di database è in esecuzione o se è stato interrotto.

Nota: se il database contiene un numero molto elevato di dati, la Console dell'Agente Arcserve UDP (Linux) richiederà tempi più lunghi per eseguire il caricamento dei dati relativi alla cronologia di processo e del registro attività. Per migliorare il processo di query del database, consultare la sezione Miglioramento delle prestazioni di query per la cronologia dei processi e il registro attività.

Aggiunta di nodi Linux per il backup

Aggiungere i nodi Linux di cui si desidera eseguire il backup in una posizione di archiviazione di backup. Tali nodi Linux rappresentano i computer di cui si desidera eseguire il backup. È possibile aggiungere i nodi manualmente oppure eseguire uno script per il rilevamento e l'aggiunta dei nodi.

Effettuare le operazioni seguenti:

1. Immettere l'URL del server di backup in un browser Web per aprire l'interfaccia utente.

   Nota: l'URL per l'accesso e la gestione del server viene fornito all'utente durante l'installazione dell'agente Arcserve UDP (Linux).

2. Per rilevare i nodi che utilizzano uno script, eseguire le seguenti operazioni:
   a. Fare clic su Aggiungi dal menu Nodo e selezionare Rilevamento.

      Verrà visualizzata la finestra di dialogo Rilevamento nodi.

   b. Selezionare uno script dall'elenco a discesa Script.

      Nota: per ulteriori informazioni sulla creazione dello script di rilevamento nodi, consultare la sezione Rilevamento dei nodi mediante uno script del capitolo Integrazione e automazione dell'agente Arcserve UDP (Linux) con l'ambiente IT esistente.

   c. Specificare la Pianificazione e fare clic su OK.

      La finestra di dialogo Rilevamento nodi viene chiusa e ha inizio il processo di rilevamento. La scheda Registro attività viene aggiornata con un messaggio nuovo.

3. Eseguire le attività seguenti se si desidera aggiungere ciascun nodo manualmente:
   a. Fare clic su Aggiungi dal menu Nodo e selezionare Nome Host/Indirizzo IP.

      Verrà visualizzata la finestra di dialogo di aggiunta dei nodi.

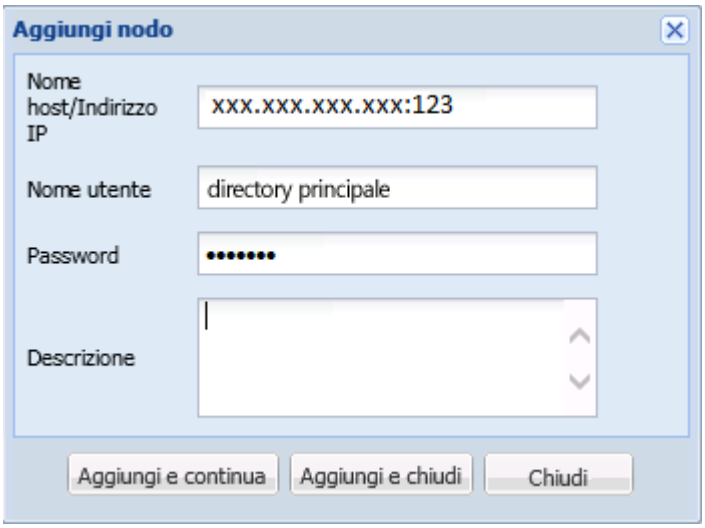
   b. Immettere il nome host o l'indirizzo IP del nodo Linux, il nome utente che dispone di autorizzazioni root e la password.

      Nota: Se la porta SSH predefinita del nodo viene modificata, è possibile aggiungere il nodo nel seguente modo:

      ```
      <IP Name>:Port Number
      ```

Esempio: xxx.xxx.xxx.xxx:123

Dove xxx.xxx.xxx.xxx è l'indirizzo IP e 123 è il numero della porta.



c. (Facoltativo) Specificare una descrizione per il nodo al fine di facilitarne l'individuazione.

d. Selezionare una delle seguenti opzioni.

Aggiungi e continua

Consente di aggiungere più nodi contemporaneamente. Dopo aver aggiunto i nodi, fare clic su Aggiungi e chiudi o su Chiudi per chiudere la finestra di dialogo Aggiungi nodo.

Aggiungi e chiudi

Consente di aggiungere un nodo e di chiudere la finestra di dialogo Aggiungi nodo.

Chiudi

Chiude la finestra di dialogo senza aggiungere nessun nodo.

4. Fare clic sulla scheda Nodi e verificare che siano elencati i nuovi nodi.

I nodi Linux vengono aggiunti per il backup.

(Facoltativo) Registrazione della chiave pubblica di Arcserve UDP per l'avvio protetto

Durante l'esecuzione in modalità di avvio protetto, il nodo di origine di backup richiede l'installazione manuale della chiave pubblica di Arcserve per il driver di backup attendibile. Soltanto con la registrazione della chiave, la gestione del nodo e la funzionalità di backup funzioneranno correttamente. Il presente argomento descrive la modalità di registrazione della chiave pubblica di Arcserve per il nodo abilitato per l'avvio protetto.

Prerequisiti:

- Verificare di disporre dell'accesso alla chiave pubblica Arcserve.
- Verificare che il sistema disponga del pacchetto corrispondente del file MokManager.efi o mmx64.efi, contenuto nella seguente cartella:

  RedHat: /boot/efi/EFI/redhat

  CentOS: /boot/efi/EFI/centos

  Ubuntu: /boot/efi/EFI/ubuntu

  SLES: /boot/efi/EFI/SLES12

Effettuare le operazioni seguenti:

1. Accedere all'ambiente della shell del nodo di origine di backup.
2. Individuare la chiave pubblica Arcserve nel percorso seguente:

   `/tmp/arcserve_public_key_for_secureboot.der`
3. Dal documento della distribuzione Linux in esecuzione per l'aggiunta della chiave pubblica all'elenco UEFI MOK, eseguire le seguenti operazioni illustrate nel seguente esempio:
   a. Importare la certificazione in MOK:

      mokutil [--root-pw] --import

      `/tmp/arcserve_public_key_for_secureboot.der`

      L'opzione --root-pw consente l'utilizzo diretto dell'utente root. La password root è necessaria per effettuare la registrazione della chiave in seguito al riavvio del sistema.

      Nota: in SLES15 SP2, utilizzare la seguente chiave pubblica durante l'importazione della certificazione in MOK per le versioni kernel da *linux-5.3.18-24.52* a *linux-5.14.21-150400.24.18*:

```
/tmp/arcserve_public_key_for_secureboot_v1.der
```

b. Specificare una password per la certificazione se l'opzione --root-pw non è disponibile.

   La password è necessaria per effettuare la registrazione della chiave in seguito al riavvio del sistema.

c. Verificare l'elenco dei certificati pronti per la registrazione da mokutil:

   mokutil --list-new>

   L'elenco deve disporre della chiave pubblica di Arcserve.

d. Riavviare il sistema.

   Il sistema avvia lo strumento di gestione della chiave shim di UEFI.

   Nota: se lo strumento di gestione della chiave UEFI non viene avviato, il sistema potrebbe non disporre del file MokManager.efi.

e. Immettere la password specificata durante l'importazione della chiave pubblica di Arcserve per la registrazione della certificazione all'elenco MOK.

f. Verificare che la nuova chiave importata venga visualizzata come registrata in seguito all'avvio del sistema:

   mokutil --list-enrolled

   L'elenco deve disporre della chiave pubblica di Arcserve.

4. Aggiungere o eseguire nuovamente il backup del nodo per verificare che la chiave pubblica di Arcserve sia stata registrata correttamente.

   Il nodo abilitato per l'avvio protetto è pronto per essere protetto dall'agente Arcserve UDP (Linux).

(Facoltativo) Registrazione della chiave pubblica Arcserve UDP per il kernel Oracle Linux UEK6 abilitato per l'avvio protetto

Questa sezione fornisce informazioni sulla registrazione della chiave pubblica Arcserve per il kernel UEK6 di Oracle Linux abilitato per l'avvio protetto.

Prerequisiti:

- Verificare di disporre delle credenziali root.
- Verificare di disporre dell'accesso alla chiave pubblica Arcserve.
- Verificare di disporre dell'accesso al file di chiave della piattaforma Arcserve (PKCS12).
- Verificare che il sistema disponga del pacchetto corrispondente del file **mmx64.efi** contenuto nella seguente cartella:

  /boot/efi/EFI/redhat
- Installare i seguenti pacchetti in base alle proprie esigenze:
  - Oracle Linux 7.x
    - *sudo yum install kernel-uek-devel*
    - *sudo yum update*
    - *sudo yum-config-manager –enable ol7_optional_latest*
    - *sudo yum install keyutils mokutil pesign*
  - Oracle Linux 8.x
    - *sudo dnf install kernel-uek-devel*
    - *sudo dnf update*
    - *sudo dnf install keyutils mokutil pesign*

Effettuare le operazioni seguenti:

1. Accedere all'ambiente della shell del nodo di origine di backup.
2. Individuare la chiave pubblica di Arcserve nel percorso seguente:

   `/tmp/arcserve_public_key_for_secureboot.der`
3. Individuare il file della chiave della piattaforma Arcserve (PKCS12) nel seguente percorso:

   `/tmp/arcserve_p12key_for_secureboot.p12`

4. Dalla documentazione di Oracle Linux relativa all'inserimento del certificato del modulo nel kernel e alla firma dell'immagine per il kernel UEK6, procedere come segue:

   a. Per passare alla directory in cui si trovano i file di chiave pubblica e di piattaforma di Arcserve, eseguire il comando seguente:

      ```
      # cd /tmp
      ```

   b. Per inserire il certificato del modulo nell'immagine kernel utilizzando l'utilità *insert-sys-cert*, eseguire il seguente comando:

      ```
      # /usr/src/kernels/$(uname -r)/scripts/insert-sys-cert
      -s /boot/System.map-$(uname -r) -z /boot/vmlinuz-$(u-
      name -r) -c arcserve_public_key_for_secureboot.der
      ```

   c. Per configurare il database NSS, progettato per archiviare il set completo di chiavi, eseguire il seguente comando:

      ```
      # certutil -d . -N

      Enter a password which will be used to encrypt your keys.
      The password should be at least 8 characters long,
      and should contain at least one non-alphabetic character.

      Enter new password:
      Re-enter password:
      ```

      Viene richiesto di immettere una password per il database NSS. Immettere una password per il database, richiesta durante la firma del kernel.

   d. Aggiungere la versione PKCS#12 della chiave di firma del kernel al nuovo database. Viene innanzitutto richiesta la password del database NSS creata nel passaggio precedente, quindi viene richiesta la password utilizzata durante l'esportazione del file di chiave PKCS#12 (dove 'cad2d' è la password utilizzata per la chiave PKCS#12).

      # pk12util -d . -i arcserve_p12key_for_secureboot.p12

      ```
      Enter Password or Pin for "NSS Certificate DB":
      Enter password for PKCS12 file:
      pk12util: PKCS12 IMPORT SUCCESSFUL
      ```

   e. Firmare l'immagine del kernel utilizzando l'utilità pesign.

      ```
      # pesign -u 0 -i /boot/vmlinuz-$(uname -r) --remove-signature -o vmlinuz.unsigned
      # pesign -n . -c cert -i vmlinuz.unsigned -o vmlinuz.signed -s
      Enter Password or Pin for "NSS Certificate DB":

      # cp -bf vmlinuz.signed /boot/vmlinuz-$(uname -r)
      ```

5. Per aggiornare il database MOK, procedere come segue:

a. Per importare la certificazione in MOK, eseguire il seguente comando:

   mokutil [--root-pw] --import

   /tmp/arcserve_public_key_for_secureboot.der

   L'opzione --root-pw consente l'utilizzo diretto dell'utente root. La password root è necessaria per effettuare la registrazione della chiave in seguito al riavvio del sistema.

b. Specificare una password per la certificazione se l'opzione --root-pw non è disponibile.

   La password è necessaria per effettuare la registrazione della chiave in seguito al riavvio del sistema.

c. Verificare l'elenco dei certificati pronti per la registrazione da mokutil utilizzando il seguente comando:

   mokutil --list-new>

   L'elenco deve includere la chiave pubblica di Arcserve.

d. Riavviare il sistema.

   Il sistema avvia lo strumento di gestione della chiave shim di UEFI.

   Nota: se lo strumento di gestione della chiave UEFI non viene avviato, il sistema potrebbe non disporre del file *mmx64.efi*.

e. Immettere la password specificata durante l'importazione della chiave pubblica di Arcserve per la registrazione della certificazione nell'elenco MOK.

6. Per UEK R6, solo le chiavi elencate in *builtin_trusted_keys* del kernel sono considerate attendibili per la firma del modulo. Per questo motivo, le chiavi di firma del modulo vengono aggiunte all'immagine kernel come parte del processo di firma dei moduli. Eseguire il comando seguente per convalidare l'attendibilità della chiave:

   # keyctl show %:.builtin_trusted_keys

   Keyring: *335047181 ---lswrv 0 0 keyring: .builtin_trusted_keys*

   1042239099 ---lswrv 0 0 _ asymmetric: Oracle CA Server: *58bd7ea9c4f-ba3a4a62720d5d06f1e96053ddf4d*

   24285436 ---lswrv 0 0 _ asymmetric: Arcserve kernel module signing key: *fb4c19-dca60d31bb203499bf6cb384af6615699d*

   362335717 ---lswrv 0 0 _ asymmetric: Oracle America, Inc.: Ksplice Kernel Module Signing Key: *09010ebef5545fa7c54b626ef518e077b5b1ee4c*

   448587676 ---lswrv 0 0 _ asymmetric: Oracle Linux Kernel Module Signing Key: *2bb352412969a3653f0eb6021763408ebb9bb5ab*

Note:

- L'elenco deve includere la chiave pubblica di Arcserve.
- Se sono installati più kernel di versione UEK, la firma di un solo kernel non consente l'accesso ad altri kernel. Ad esempio, se sono stati installati i kernel UEK5 e UEK6, se è stata importata una chiave e si è firmato il kernel UEK6 utilizzando i passaggi precedenti, l'avvio non viene eseguito mediante il kernel UEK5.

Il kernel UEK6 di Oracle Linux abilitato per l'avvio protetto è pronto per la protezione.

(Facoltativo) Preparazione del volume iSCSI come archiviazione di backup

È possibile archiviare i punti di ripristino in un volume iSCSI (Internet Small Computer System Interface). iSCSI viene utilizzato per la gestione del trasferimento e l'archiviazione di dati tramite una rete mediante lo standard IP.

Verificare che nel server di backup sia installata l'ultima versione del software iniziatore di iSCSI. Nei sistemi RHEL, il software iniziatore viene organizzato come iscsi-initiator-utils. Nei sistemi SLES, il software iniziatore viene organizzato come open-iscsi.

Effettuare le operazioni seguenti:

1. Accedere all'ambiente della shell del nodo di origine di backup.
2. Eseguire uno dei seguenti comandi per avviare il daemon iniziatore di iSCSI.
   - Per i sistemi RHEL:

     ```
     /etc/init.d/iscsid start
     ```

     Il servizio sui sistemi RHEL è denominato iscsid
   - Per i sistemi SLES:

     ```
     /etc/init.d/open-iscsi start
     ```

     Il servizio sui sistemi SLES è denominato open-iscsi.
3. Eseguire uno script di rilevamento per rilevare l'host di destinazione di iSCSI.

   ```
   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>
   ```

   Il valore predefinito della porta dell'host di destinazione di iSCSI è 3260.
4. Prendere nota del nome completo iSCSI (IQN) dell'host di destinazione di iSCSI rilevato dallo script di rilevamento prima di accedere manualmente alla destinazione individuata.
5. Elencare la periferica di blocco disponibile del nodo di origine di backup.

   ```
   #fdisk -l
   ```
6. Accedere alla destinazione rilevata.

   ```
   iscsiadm -m node -T <iSCSI Target IQN name> -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>  -l
   ```

   È possibile visualizzare una periferica di blocco nella directory /dev del nodo di origine di backup.

7. Eseguire il comando seguente per ottenere il nuovo nome della periferica:

   ```
   #fdisk –l
   ```

   È possibile visualizzare una periferica aggiuntiva chiamata /dev/sd<x> nel nodo di origine di backup.

   Ad esempio, supporre che il nome della periferica sia /dev/sdc. Tale nome della periferica viene utilizzato per creare una partizione e un file system nelle seguenti fasi.

8. Formattare e montare il volume iSCSI.
9. Creare una partizione e un file system sul nodo di origine di backup mediante i comandi seguenti.

   ```
   # fdisk /dev/sdc
   ```

   Se è stata creata soltanto una partizione, utilizzare il comando seguente per creare un file system per la partizione singola:

   ```
   # mkfs.ext3 /dev/sdc1
   ```

10. Montare la nuova partizione utilizzando i seguenti comandi:

    ```
    # mkdir /iscsi
    # mount /dev/sdc1 /iscsi
    ```

    La nuova partizione viene montata e il volume iSCSI è pronto a essere utilizzato come archiviazione di backup in un processo di backup.

11. (Facoltativo) Aggiungere il record seguente alla cartella /etc/fstab in modo che il volume iSCSI si connetta automaticamente al server di backup dopo il riavvio del server.

    ```
    /dev/sdc1 /iscsi ext3 _netdev 0 0
    ```

    Il volume iSCSI è pronto a essere utilizzato come archiviazione di backup.

Configurazione delle impostazioni di backup ed esecuzione del processo di backup

Configurare le impostazioni di backup mediante la procedura guidata di backup. È possibile eseguire il backup dei dati su una posizione Network File System (NFS), su una rete NAS, su sistemi Common Internet File System (CIFS) oppure su una posizione locale di origine. Una posizione locale di origine è una posizione del nodo di origine di backup in cui vengono archiviati i nodi sottoposti a backup. Il processo di backup viene avviato da un processo di backup. La procedura guidata di backup crea il processo di backup ed esegue tale processo. L'esecuzione di un backup implica la creazione di un punto di ripristino. Un punto di ripristino è una copia temporizzata del nodo di backup.

Definizione dell'origine di backup

Specificare i nodi di origine del backup nella procedura guidata di backup, in modo che sia possibile eseguire il backup di tali nodi sulla posizione desiderata. La pagina Origine di backup della procedura guidata di backup mostra il nodo di cui si desidera eseguire il backup. Utilizzare il pulsante Aggiungi presente nella pagina per aggiungere più nodi per il backup.

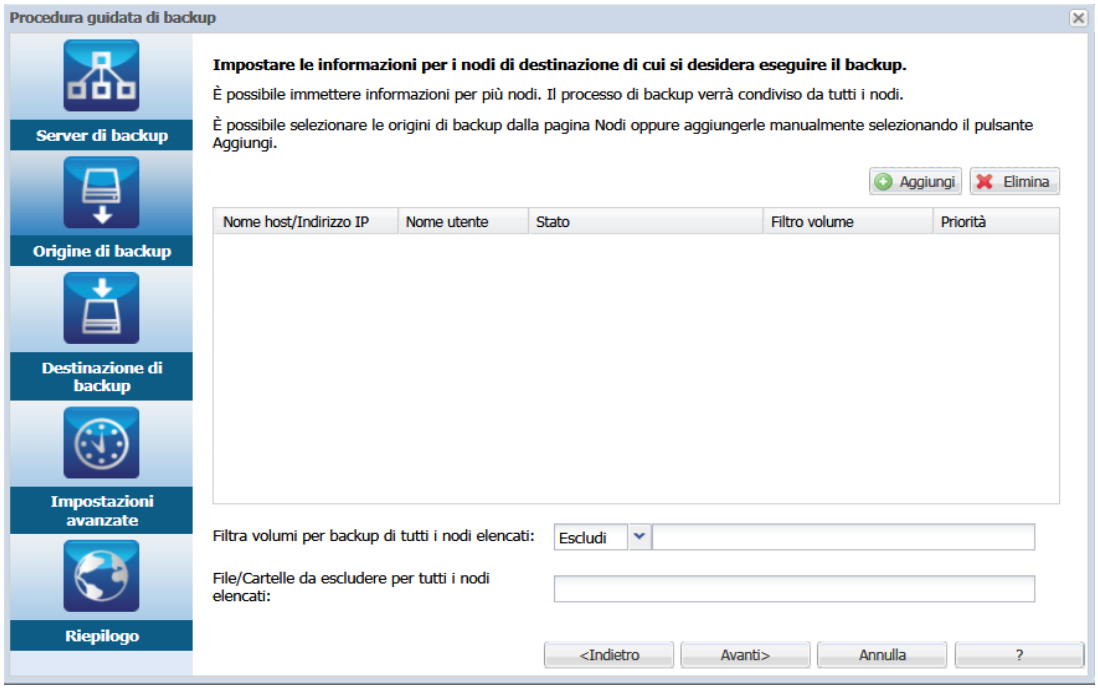
Nota: se viene aperta la procedura di backup mediante il pulsante Esegui il backup dei nodi selezionati, tutti i nodi selezionati verranno elencati nella pagina della procedura guidata. Se la procedura guidata di backup viene aperta mediante il pulsante Esegui backup, i nodi non verranno elencati nella pagina della procedura guidata. È necessario aggiungere i nodi mediante il pulsante Aggiungi della pagina della procedura guidata.

Effettuare le operazioni seguenti:

1. Selezionare i nodi di cui si desidera eseguire il backup dalla scheda Nodi.
2. Fare clic su Backup, quindi selezionare l'opzione Esegui il backup dei nodi selezionati dal menu Procedura guidata.

   Viene visualizzata la pagina Server di backup della procedura guidata di backup. Nella pagina Server di backup viene visualizzato il nome del server.
3. Fare clic su Avanti.

   Viene visualizzata la pagina Origine di backup. I nodi precedentemente selezionati vengono mostrati su questa pagina.



4. (Facoltativo) Fare clic su Aggiungi della pagina Origine di backup per aggiungere più nodi e fornire dettagli nella finestra di dialogo Aggiungi nodo.
5. (facoltativo) Specificare i volumi in **Volumes to be filtered for all listed nodes (Volumi da filtrare per tutti i nodi elencati)**.

   Selezionare Include (Includi) o Exclude (Escludi) dall'elenco a discesa. L'opzione Include (Includi) consente di specificare che solo i volumi specificati saranno inclusi nel backup. Non verrà eseguito il backup di tutti i volumi non specificati. Exclude (Escludi) consente di specificare che i volumi verranno esclusi dal backup.
6. (Facoltativo) Immettere i file/cartelle in **File/Cartelle da escludere per tutti i nodi elencati**.

   Specificare i file/cartelle utilizzando un nome di percorso assoluto e separandoli con i due punti (:). I caratteri jolly, quali * e ?, sono supportati e devono essere utilizzati dopo l'ultima barra del nome di percorso assoluto. Se il nome dei file/cartelle dopo l'ultima barra è racchiuso tra parentesi, tali file/cartelle verranno esclusi in modo ricorsivo, in caso contrario i file/cartelle verranno esclusi direttamente.

   Ad esempio:

   `/home/user/a/foo*:/home/user/b/(foo*)`

   La prima parte (home/user/a/foo*) esclude unicamente i file/cartelle corrispondenti a foo* in "/home/user/a", ma esegue il backup delle directory secon-

darie. La seconda parte (/home/user/b/(foo*) esclude tutti i file/cartelle corrispondenti a foo* in "/home/user/b", incluse tutte le cartelle secondarie.

Note:

- Se si esclude un numero elevato di file/cartelle da un volume, si consiglia di escludere il volume corrispondente.
- Se si esclude un numero elevato di file/cartelle, la fase e lo stato del processo potrebbero essere visualizzati rispettivamente come Backup del volume e Attivo durante un lungo periodo di tempo dopo l'avvio del processo di backup.
- Se il valore di **File/Cartelle da escludere per tutti i nodi elencati** viene modificato, il processo di backup verrà convertito in backup completo.

Se alcuni file di sistema vengono esclusi dal backup, il sistema operativo Linux potrebbe non venire avviato e il ripristino bare metal non funziona correttamente. Tali file di sistema includono, ma non si limitano a:

- File e cartelle nelle directory /bin, /sbin, /usr, /etc, /lib, /lib64, /boot, /var
- Cartelle /proc, /sys, /dev, /tmp

Se si escludono i file di sistema, si consiglia di verificare la funzione di ripristino bare metal e di confermare se il sistema operativo Linux viene avviato correttamente.

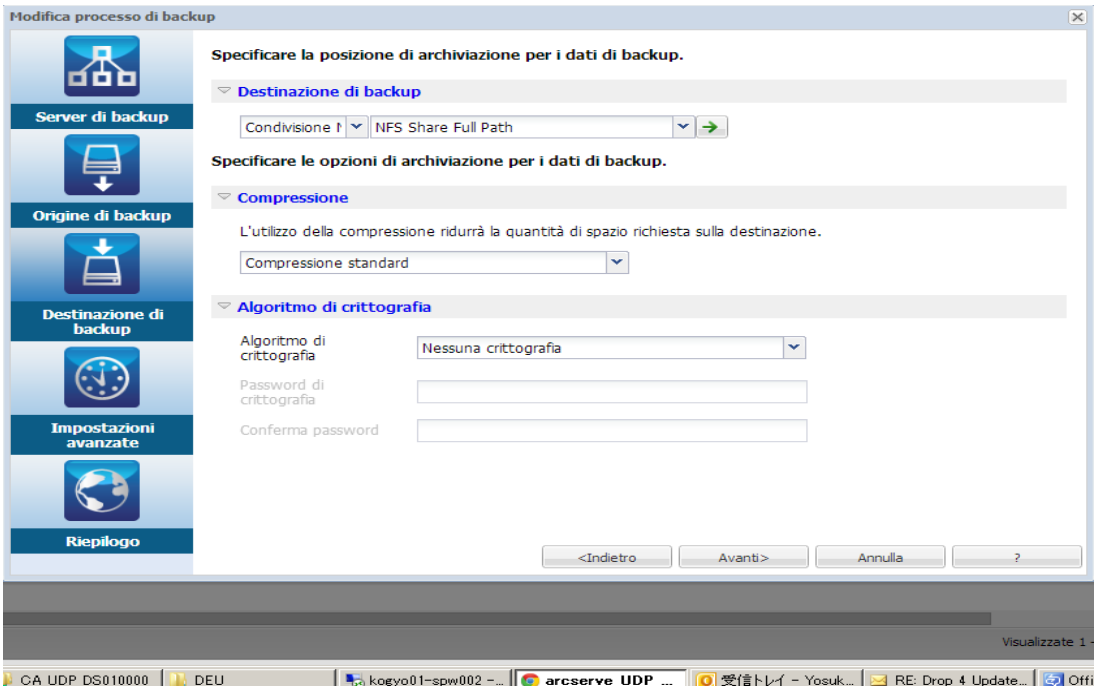
7. Fare clic su Avanti.

   Viene visualizzata la pagina Destinazione di backup.

   L'origine di backup viene specificata.

Definizione della destinazione di backup

Specificare una posizione per l'archiviazione dei dati sottoposti a backup (punti di ripristino) nella pagina Destinazione di backup della procedura guidata di backup. La destinazione di backup può essere una condivisione NFS, una condivisione CIFS o un'origine locale. L'origine locale corrisponde al nodo di origine di backup. Se la destinazione di backup è Origine locale, i dati di backup vengono scritti direttamente sul disco locale.



Se un disco fisico include due volumi logici, sarà possibile specificare un volume come origine di backup e l'altro volume come destinazione di backup.

Nota: Se si seleziona Origine locale come destinazione di backup, il server di backup non sarà in grado di gestire i punti di ripristino. Per gestire i set di ripristino, consultare Gestione dei set di ripristino in Gestione delle impostazioni del server di backup.

Effettuare le operazioni seguenti:

1. Selezionare una destinazione dall'elenco a discesa Destinazione di backup, quindi immettere il percorso completo della posizione di archiviazione.

   - Se è stata selezionata la condivisione NFS, specificare i dettagli relativi alla destinazione di backup nel seguente formato:

     `IP_address_of_the_NFS_Share:/full_path_of_the_storage_location`

Nota: alcune versioni di Data Domain NAS non supportano il meccanismo di blocco di file di NFS. Di conseguenza, non è possibile utilizzare la condivisione NFS come destinazione di backup. Per ulteriori informazioni su questo problema, consultare la sezione Problemi di compatibilità con l'Agente Arcserve UDP (Linux) delle Note di rilascio.

- Se è stata selezionata la condivisione CIFS, specificare i dettagli relativi alla destinazione di backup nel seguente formato:

  `//hostname/share_folder`

  Nota: il nome di cartella condivisa non può contenere spazi.

- Se è stata selezionata l'opzione Origine locale, è necessario modificare alcune impostazioni in modo che il server di backup sia in grado di gestire i punti di ripristino. Ad esempio, considerare server-A come il nome host del server di backup e node-B come il nome host del nodo di origine. Attenersi, quindi, alle istruzioni riportate di seguito per modificare le impostazioni di node-B:
  - Verificare che il server NFS sia in esecuzione. È possibile eseguire il comando seguente per verificare lo stato del server NFS:

    service nfs status

  - Se il server NFS non è in esecuzione, è possibile eseguire il seguente comando per avviare il server NFS:

    service nfs start

  - Se la cartella di destinazione di backup su node-B è */backup/test*, aggiungere la seguente riga a */etc/exports*:

    /backup/test server-A(rw,no_root_squash)

    Eseguire il seguente comando:

    exportfs -a

  - Nell'interfaccia utente del server di backup, aggiungere *node-b:/backup/test* come percorso di archiviazione del backup. Il percorso di archiviazione di Origine locale viene visualizzato nell'elenco a discesa Destinazione di backup.

- Se è stata selezionata l'opzione Amazon S3, specificare i dettagli relativi alla destinazione di backup nel seguente formato:

  //S3_Region_ID/S3_bucket_name

  Note:

- //./ può essere utilizzato come collegamento per l'account globale cloud di Amazon. Esempio: //./Global_bucket_name
- //China/ può essere utilizzato come collegamento per l'account China cloud di Amazon. Esempio: //China/China_bucket_name
- Se si desidera esportare il bucket Amazon S3 come condivisione CIFS, è possibile fare clic sulla casella di controllo Abilita accesso client CIFS. Il numero predefinito della porta è 8017.

  Questa funzione comprende il seguente file di configurazione:

  /opt/Arcserve/d2dserver/configfiles/ofs.cfg

  Non modificarne il contenuto originale. È tuttavia possibile aggiungere il contenuto seguente:

  - PROXY_HOST = (se si desidera utilizzare il proxy, immettere qui il nome del proxy)
  - PROXY_USERNAME = (nome utente del proxy)
  - PROXY_PASSWORD_ENC = (password del proxy, che deve essere crittografata)
  - PROXY_PORT = (porta del proxy)
  - WRITE_THROUGHPUT = (se si desidera limitare la velocità effettiva di scrittura, unità: KB/s)
  - HTTPS = yes/no (valore predefinito: yes)
  - S3_STORAGE_CLASS = STANDARD/STANDARD_IA/REDUCED_REDUNDANCY (valore predefinito: STANDARD)
  - DEBUG_LEVEL = (livello di log di debug: 0,1,2,3, 3 in grado di stampare un numero maggiore di log)

2. Fare clic sul pulsante di freccia per convalidare le informazioni relative alla destinazione di backup.

   Se la destinazione di backup non è valida, verrà visualizzato un messaggio di errore.

3. Selezionare un livello di compressione dall'elenco a discesa Compressione per specificare un tipo di compressione utilizzato per il backup.

   Le opzioni disponibili per la Compressione sono:

   Compressione standard

Questa opzione fornisce un buon bilanciamento tra l'utilizzo della CPU e l'utilizzo dello spazio su disco. Per impostazione predefinita viene utilizzata la compressione standard.

Compressione massima

L'opzione implica un utilizzo massimo di CPU (velocità minima) ma utilizza anche una quantità minore di spazio su disco per l'immagine di backup.

4. Selezionare un algoritmo dall'elenco a discesa Algoritmo di crittografia, quindi specificare la password di crittografia, se necessario.
   a. Selezionare il tipo di algoritmo di crittografia da utilizzare per i backup.

      La crittografia dei dati consiste nella conversione dei dati in un formato incomprensibile senza un meccanismo di decifrazione. La protezione dei dati dell'Agente Arcserve UDP (Linux) utilizza algoritmi di crittografia AES (Advanced Encryption Standard) per ottenere la massima protezione e riservatezza dei dati specificati.

      Le opzioni di formato disponibili sono Nessuna crittografia, AES-128, AES-192 e AES-256. Per disattivare l'opzione di crittografia, selezionare Nessuna crittografia.

      - Il backup completo e i backup incrementali correlati devono utilizzare lo stesso algoritmo di crittografia.
      - Se l'algoritmo di crittografia per un backup incrementale è stato modificato, sarà necessario eseguire un backup completo.

        Ad esempio, se si modifica il formato dell'algoritmo e viene eseguito un backup incrementale, il tipo di backup verrà convertito automaticamente in un backup completo.

   b. Nel caso in cui venga selezionato un algoritmo di crittografia, è necessario specificare e confermare una password di crittografia.
      - La password di crittografia può contenere un massimo di 23 caratteri.
      - Il backup completo e i relativi backup incrementali devono utilizzare la stessa password di crittografia.
5. Fare clic su Avanti.

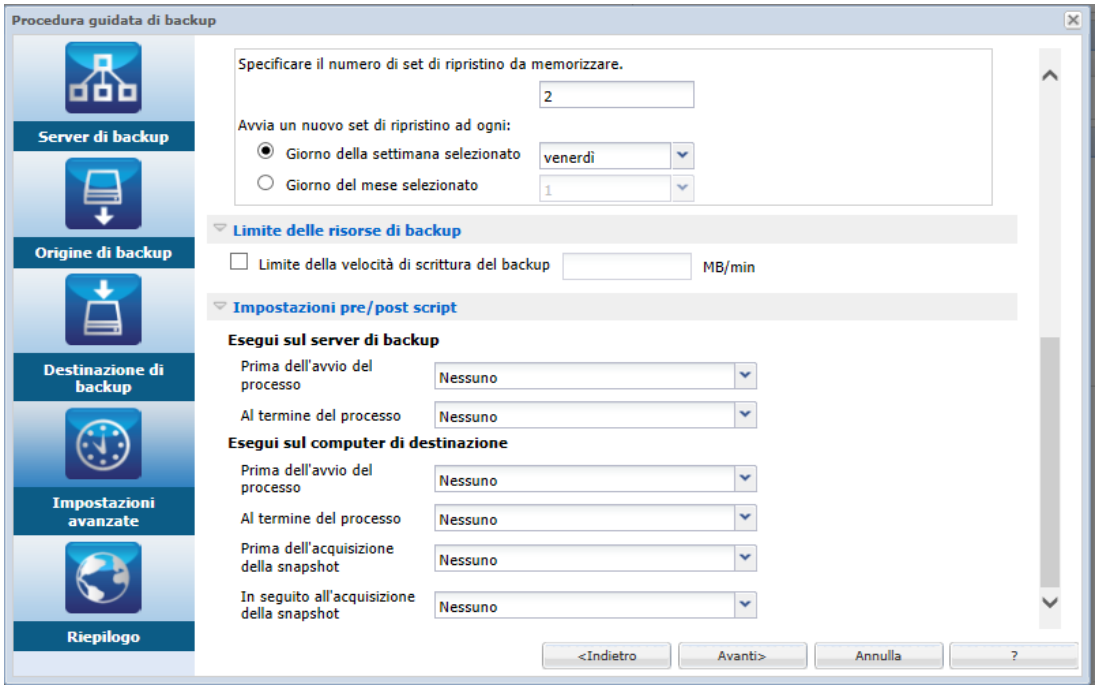
   Viene visualizzata la pagina Impostazioni avanzate.

   La destinazione di backup viene specificata.

Definizione delle impostazioni avanzate

Specificare la pianificazione di backup, le impostazioni del set di ripristino, le impostazioni di pre e post backup dalla pagina Impostazioni avanzate.

Il diagramma seguente illustra la pagina Impostazioni avanzate della procedura guidata di backup. In questo diagramma, l'opzione Nessuno è stata selezionata per il Tipo di pianificazione.



Le seguenti impostazioni sono disponibili nella pagina Impostazioni avanzate:

- Le impostazioni di pianificazione garantiscono che il processo di backup venga eseguito periodicamente a intervalli specificati.

  Importante: Impostare lo stesso fuso orario tra il server UDP e il server di backup di Linux. Dopo aver modificato il fuso orario in entrambi i server, è necessario riavviare il servizio di gestione UDP o il server di backup di Linux affinché le modifiche abbiano effetto.

- L'opzione Impostazioni del set di ripristino garantisce una manutenzione periodica dei set di ripristino. Se il numero di set di ripristino supera il numero specificato, il set di ripristino meno recente viene eliminato per mantenere il numero specificato.
- L'impostazione Limite di velocità del backup consente di abilitare e specificare la velocità massima (MB/min) di scrittura dei backup.
- L'opzione Impostazioni pre/post script definisce gli script che è possibile eseguire sul server di backup e sul nodo di destinazione. È possibile configurare

gli script per eseguire azioni specifiche prima dell'inizio di un processo, durante l'esecuzione del processo o dopo il suo completamento.

Per ottimizzare la gestione dei punti di ripristino, considerare le seguenti raccomandazioni durante la pianificazione della frequenza dei backup:

- Per sistemi protetti con backup incrementali eseguiti ogni 15 minuti, pianificare un backup completo ogni settimana per aggiornare l'immagine di base.
- Per sistemi protetti con backup incrementali eseguiti ogni ora, pianificare un backup completo ogni mese per aggiornare l'immagine di base.

Nota: se il valore di spazio utilizzato per archiviare le immagini di backup costituisce un problema, si consiglia di pianificare l'esecuzione dei backup completi con una frequenza inferiore per ridurre lo spazio di archiviazione.

Effettuare le operazioni seguenti:

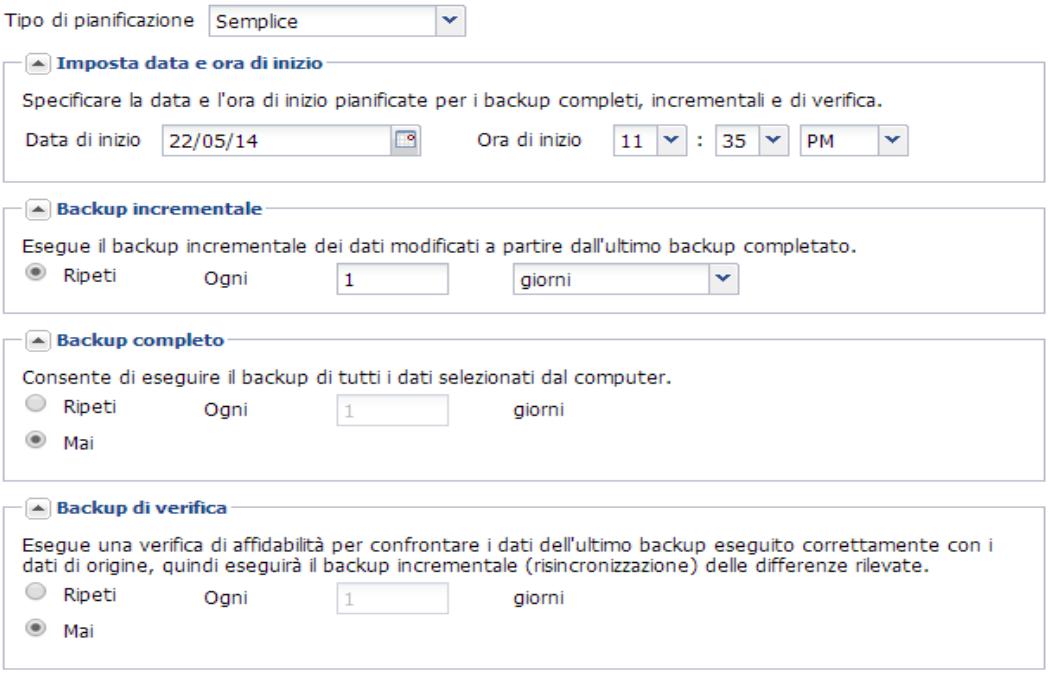
1. Impostare la data e l'ora di inizio selezionando una delle opzioni seguenti dall'elenco a discesa Tipo di pianificazione:

   Semplice

   Il tipo di pianificazione **semplice** non è disponibile quando si crea una nuova pianificazione. Tuttavia, se si modifica un processo di backup precedente con pianificazione semplice, è possibile configurare la pianificazione semplice.

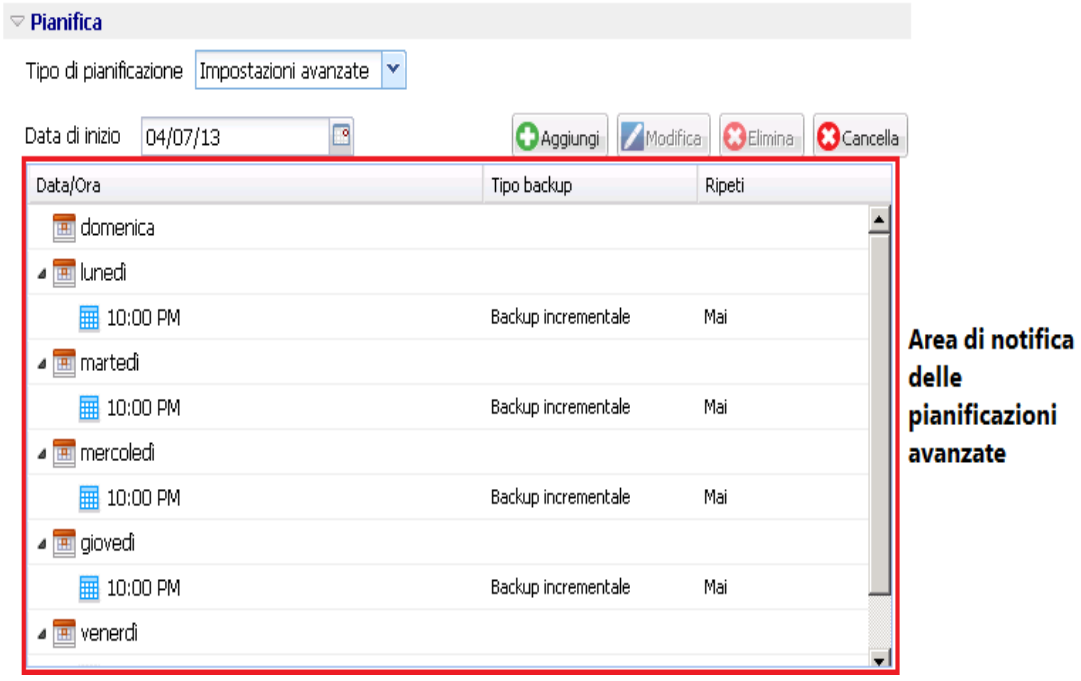
   Selezionare l'opzione Semplice per pianificare il backup incrementale, il backup completo e il backup di verifica per la data di inizio e l'ora di inizio specificate. Per ciascun tipo di backup, è possibile specificare anche per quanto tempo ripetere il backup o di non ripeterlo mai. La data e l'ora di inizio sono fisse per tutti i tipi di backup. Pertanto, non è possibile specificare una data e un'ora di inizio differenti per i diversi tipi di backup.

   Nota: per ulteriori informazioni sui tipi di backup, consultare la sezione *Informazioni sui tipi di backup*.



Personalizzato

Selezionare l'opzione Personalizzato per specificare pianificazioni di backup multiple ogni giorno della settimana. È possibile specificare una data e un'ora di inizio differenti per i diversi tipi di backup. È possibile aggiungere, modificare, eliminare e cancellare la pianificazione personalizzata. Quando si fa clic su Cancella, tutte le pianificazioni di backup personalizzate vengono eliminate dall'area di notifica delle pianificazioni avanzate.

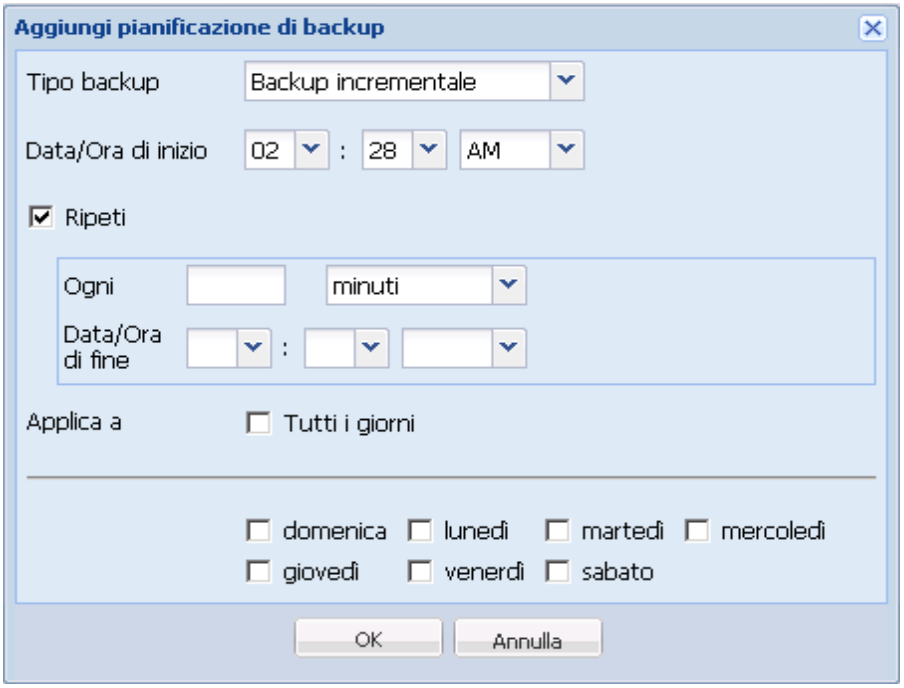


Area di notifica delle pianificazioni avanzate

Per aggiungere una pianificazione di backup, attenersi alle seguenti istruzioni:

a. Fare clic su Aggiungi.

Viene visualizzata la finestra di dialogo Aggiungi pianificazione di backup.



b. Specificare le opzioni per la pianificazione del backup e fare clic su OK.

La pianificazione di backup specificata viene visualizzata nell'area di notifica delle pianificazioni avanzate.

Nessuna

Selezionare l'opzione Nessuno per creare il processo di backup e archiviarlo nella scheda Stato processo. Questa opzione permette di non eseguire il processo perché non ci sono pianificazioni specificate. Quando si invia il processo, lo stato del processo si modifica in Pronto. Se si desidera eseguire il processo, sarà necessario selezionare il processo e fare clic su Esegui ora dal menu Processo. Per poter eseguire il processo sarà necessario eseguire il processo manualmente. È inoltre possibile scrivere uno script per l'esecuzione del processo in base alla pianificazione personalizzata.

2. Specificare le impostazioni del set di ripristino.

Nota: per ulteriori informazioni sui set di ripristino, consultare la sezione *Informazioni sui set di ripristino*.

Specificare il numero di set di ripristino da memorizzare

Specifica il numero di set di ripristino conservati.

Avvia un nuovo set di ripristino ad ogni:

Giorno della settimana selezionato

Specifica il giorno della settimana selezionato per avviare un nuovo set di ripristino.

Giorno del mese selezionato

Specifica il giorno del mese selezionato per avviare un nuovo set di ripristino. Specificare un valore da 1 a 30 oppure l'ultimo giorno del mese.

Nota: Il server di backup verifica ogni 15 minuti il numero di set di ripristino nell'archiviazione di backup configurata ed elimina eventuali set di ripristino aggiuntivi dal percorso di archiviazione del backup.

3. Specificare il limite di velocità del backup.

   È possibile specificare la velocità massima di scrittura (MB/min) del backup. e di limitare la velocità di backup per ridurre l'utilizzo della CPU o della rete. Tuttavia, la limitazione della velocità di backup potrebbe influire sul tempo di completamento del processo di backup. Con una velocità di backup inferiore, il tempo di completamento del backup aumenta. Nel caso di un processo di backup, la scheda Stato processo visualizzerà la velocità media di lettura e scrittura del processo in corso e il limite di velocità impostato.

   Nota: per impostazione predefinita, l'opzione Limite delle risorse di backup non è attivata e la velocità di backup non viene controllata.

4. Specificare le impostazioni di pre e post backup nel campo Impostazioni pre/post script.

   Questi script eseguono comandi di script per le azioni da eseguire prima dell'inizio del processo e/o al completamento del processo.

   Nota: i campi Impostazioni pre/post script vengono popolati solamente se un file di script è già stato creato e collocato nel percorso seguente:

   `/opt/Arcserve/d2dserver/usr/prepost`

   Nota: per ulteriori informazioni sulla creazione di pre/post script, consultare la sezione *Gestione di pre/post script per l'automazione*.

5. Fare clic su Avanti.

   Viene visualizzata la pagina Riepilogo.

Viene specificata la pianificazione personalizzata.

Nota: in caso di pianificazione simultanea di più tipi di backup, l'ordine di esecuzione verrà stabilito in base alle seguenti priorità:

- Priorità 1 - Backup completo
- Priorità 2 - Backup di verifica
- Priorità 3 - Backup incrementale

Ad esempio, se è prevista l'esecuzione simultanea di questi tre tipi di backup, l'Agente Arcserve UDP (Linux) esegue il backup completo. Se non è stato pianificato un backup completo, ma è prevista l'esecuzione simultanea di un backup incrementale e di un backup di verifica, l'Agente Arcserve UDP (Linux) esegue il backup di verifica. Il backup incrementale pianificato verrà eseguito solo nel caso in cui non esista alcun conflitto con un altro tipo di backup.

La presente sezione descrive i seguenti argomenti:

- Informazioni sui tipi di backup
- Informazioni sui set di ripristino

Informazioni sui tipi di backup

Dalla pagina Impostazioni avanzate della procedura guidata di backup, è possibile specificare i seguenti tipi di backup:

Backup incrementale

Esegue il backup dei blocchi modificati rispetto all'ultimo backup. I backup incrementali hanno il vantaggio di essere particolarmente rapidi e di generare immagini di backup di dimensioni molto ridotte. L'Arcserve UDP per Linux utilizza un driver per monitorare i blocchi modificati sul nodo di origine a partire dall'ultimo backup completato correttamente.

Le opzioni disponibili sono Ripeti e Mai. Se si seleziona l'opzione Ripeti, è necessario specificare il l'intervallo di tempo (in minuti, ore o giorni) tra i tentativi di backup.

Valore minimo: 15 minuti

Valore predefinito: 1 giorno

Backup completo

Esegue il backup dell'intero nodo di origine. In base alla dimensione del volume del nodo di backup, il backup completo produce un'immagine di backup di grandi dimensioni, pertanto richiede più tempo per il completamento. Le opzioni disponibili sono Ripeti e Mai.

Se si seleziona l'opzione Ripeti, è necessario specificare il l'intervallo di tempo (in minuti, ore o giorni) tra i tentativi di backup.

Valore minimo: 1 giorno

Valore predefinito: Mai (nessuna ripetizione pianificata)

Backup di verifica

Controlla che i dati protetti siano validi e completi eseguendo una verifica di affidabilità dell'immagine di backup archiviata sull'origine di backup originale. Se necessario esegue la risincronizzazione dell'immagine. Un backup di verifica controlla il backup più recente di ogni blocco e lo confronta con il contenuto e le informazioni di origine. Questo confronto consente di verificare che il blocco di backup più recente rappresenti le informazioni corrispondenti all'origine. Se l'immagine di backup di un blocco non corrisponde all'origine (probabilmente a causa di modifiche apportate al sistema dall'ultimo backup), l'Arcserve UDP per Linux aggiorna (risincronizza) il backup del blocco non corrispondente. Sebbene si tratti di una procedura poco frequente, il backup di verifica può essere

utilizzato per ottenere le stesse garanzie di un backup completo, senza occupare lo spazio richiesto da questo tipo di backup.

Vantaggi: questo tipo di backup genera un'immagine di backup con dimensioni ridotte rispetto al backup completo, in quanto esegue solamente il backup dei blocchi modificati, ovvero dei blocchi che non corrispondono al backup più recente.

Svantaggi: il backup di verifica richiede tempi di esecuzione più lunghi, in quanto esegue il confronto di tutti i blocchi originali con i blocchi del backup più recente.

Le opzioni disponibili sono Ripeti e Mai. Se si seleziona l'opzione Ripeti, è necessario specificare il l'intervallo di tempo (in minuti, ore o giorni) tra i tentativi di backup.

Valore minimo: 1 giorno

Valore predefinito: Mai (nessuna ripetizione pianificata)

Il tipo di backup eseguito dipende dalle seguenti situazioni:

- Se si esegue il processo di backup per la prima volta per i nodi selezionati, il primo backup corrisponderà sempre a un Backup completo.
- Se il processo di backup viene eseguito nuovamente per lo stesso set di nodi e la destinazione di backup è la stessa, il tipo di backup corrisponderà a Backup incrementale.
- Se il processo di backup viene eseguito per lo stesso set di nodi ma la destinazione di backup è differente, il tipo di backup corrisponderà a Backup completo. Ciò si verifica perché è stata modificata la destinazione di backup e la nuova destinazione corrisponde al primo backup. Pertanto, il primo backup corrisponderà sempre a un Backup completo.
- Se il nodo viene eliminato e poi raggiunto ma non viene modificata la destinazione di backup, il backup corrisponderà a un Backup di verifica. Ciò si verifica perché tale nodo è già stato sottoposto a backup in processi di backup precedenti. Se il nodo viene eliminato e poi raggiunto, il processo di backup verifica tutti i blocchi associati a tale nodo con l'ultima immagine di backup. Dopo che il processo di backup ha rilevato che si tratta dello stesso nodo, verrà eseguito solamente il backup dei blocchi modificati. Se il processo di backup non è in grado di individuare un'immagine di backup per il nodo nella destinazione di backup, il tipo di backup corrisponderà a Backup completo.

Informazioni sui set di ripristino

Un set di ripristino è un'impostazione di archiviazione in cui un gruppo di punti di ripristino viene sottoposto a backup per un periodo di tempo specificato e memorizzato come un singolo set. Un set di ripristino contiene una serie di backup, a partire da un backup completo seguito da backup incrementali, di verifica o completi. È possibile specificare il numero di set di ripristino da memorizzare.

Le Impostazioni del set di ripristino garantiscono un mantenimento periodico dei set di ripristino. Quando il limite specificato viene superato, il set di ripristino meno recente viene eliminato. I valori seguenti definiscono i set di ripristino predefiniti, minimi e massimi nell'Agente Arcserve UDP (Linux):

Impostazione predefinita : 2

Valore minimo: 1

Numero massimo di set di ripristino: 100

Numero massimo di punti di ripristino (incluso un backup completo): 1344

Nota: Per eliminare un set di ripristino e disporre di uno spazio di archiviazione maggiore per il backup, ridurre il numero di set memorizzati in modo che il server di backup elimini automaticamente il set di ripristino meno recente. Non tentare di eliminare il set di ripristino manualmente.

Set 1 di esempio:

- Completo
- Incrementale
- Incrementale
- Verifica
- Incrementale

Set 2 di esempio:

- Completo
- Incrementale
- Completo
- Incrementale

È necessario un backup completo per avviare un nuovo set di ripristino. Il backup di avvio del set verrà convertito automaticamente in un backup completo, incluso nel caso in cui l'esecuzione del backup completo non sia stata configurata né pianificata. Dopo aver modificato l'impostazione del set di ripristino (ad esempio, il

punto di avvio del set di ripristino è stato modificato dal primo backup di lunedì al primo backup di giovedì), il punto di avvio dei set di ripristino esistenti non verrà modificato.

Nota: i set di ripristino incompleti non vengono inclusi nel calcolo del set di ripristino esistente. Un set di ripristino viene considerato completo solo in seguito alla creazione del backup di avvio del set di ripristino successivo.

Esempio 1 - Memorizzazione di 1 set di ripristino:

- Specificare 1 come numero dei set di ripristino da memorizzare.

  Il server di backup memorizza sempre due set in modo da avere un set completo prima dell'avvio del set di ripristino successivo.

Esempio 2 - Memorizzazione di 2 set di ripristino:

- Specificare 2 come numero dei set di ripristino da memorizzare.

  Il server di backup elimina il primo set di ripristino quando il quarto set di ripristino sta per iniziare. In questo modo, quando il primo backup viene eliminato e il quarto è in fase di avvio, restano disponibili sul disco ancora due set di ripristino (il set di ripristino 2 e 3).

  Nota: anche se si sceglie di memorizzare un solo set di ripristino, è necessario disporre di spazio sufficiente per almeno due backup completi.

Esempio 3 - Memorizzazione di 3 set di ripristino:

- La data/ora di inizio del backup è 06:00 del 20 agosto 2012.
- Ogni 12 ore viene eseguito un backup incrementale.
- Un nuovo set di ripristino viene avviato con l'ultimo backup del venerdì.
- Si desidera memorizzare 3 set di ripristino.

In base alla configurazione delineata, ogni giorno viene eseguito un backup incrementale alle 06:00 e alle 18:00. Il primo set di ripristino viene creato una volta eseguito il primo backup (deve essere un backup completo). Il primo backup completo viene quindi contrassegnato come backup di avvio del set di ripristino. Durante l'esecuzione del backup pianificato alle 18:00 di venerdì, questo viene convertito in un backup completo e contrassegnato come backup di avvio del set di ripristino.

(Facoltativo) Gestione di pre/post script per l'automazione

Gli script di pre/post esecuzione consentono di eseguire regole di business in fasi specifiche di un processo in esecuzione. È possibile specificare quando eseguire gli script nelle **Impostazioni pre/post script** della **Procedura guidata di backup** e della **Procedura guidata di ripristino** nella console. È possibile eseguire gli script sul server di backup in base alle impostazioni dell'utente.

La gestione del pre/post script è un processo costituito da due passaggi: la creazione del pre/post script e la sua collocazione nella cartella prepost.

Creazione di pre/post script

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Creare un file di script mediante le variabili di ambiente nel linguaggio di scripting preferito.

Variabili di ambiente del pre/post script

Per creare lo script, utilizzare le variabili di ambiente seguenti:

D2D_JOBNAME

Indica il nome del processo.

D2D_JOBID

Identifica l'ID del processo. L'ID di processo è un numero attribuito al processo durante la sua esecuzione. Se si esegue lo stesso processo nuovamente, verrà fornito un nuovo numero di processo.

D2D_TARGETNODE

Identifica il nodo di cui viene eseguito il backup o il ripristino.

D2D_JOBTYPE

Identifica il tipo di processo in esecuzione. I valori seguenti identificano la variabile D2D_JOBTYPE:

backup.full

Identifica il processo come backup completo.

backup.incremental

Identifica il processo come backup incrementale.

backup.verify

Identifica il processo come backup di verifica.

restore.bmr

Identifica il processo come ripristino bare metal (BMR). Si tratta di un processo di ripristino.

restore.file

Identifica il processo come ripristino a livello di file. Si tratta di un processo di ripristino.

D2D_SESSIONLOCATION

Identifica la posizione in cui vengono archiviati i punti di ripristino.

D2D_PREPOST_OUTPUT

Identifica un file temp. Il contenuto della prima linea del file temp viene visualizzato nel registro attività.

D2D_JOBSTAGE

Indica la fase del processo. I valori seguenti identificano la variabile D2D_JOBSTAGE:

pre-job-server

Identifica lo script eseguito sul server di backup prima dell'avvio del processo.

post-job-target

Identifica lo script eseguito sul computer di destinazione prima del completamento del processo.

pre-job-target

Identifica lo script eseguito sul computer di destinazione prima dell'avvio del processo.

pre-snapshot

Identifica lo script eseguito sul computer di destinazione prima dell'acquisizione della snapshot.

post-snapshot

Identifica lo script eseguito sul computer di destinazione dopo l'acquisizione della snapshot.

D2D_TARGETVOLUME

Identifica il volume di cui viene eseguito il backup durante un processo di backup. Questa variabile è adatta per gli script di snapshot di pre/post automazione per un processo di backup.

D2D_JOBRESULT

Identifica il risultato di uno script del processo di post-esecuzione. I valori seguenti identificano la variabile di D2D_JOBRESULT:

success

Identifica il risultato come corretto.

fail

Identifica il risultato come non corretto.

D2DSVR_HOME

Identifica la cartella in cui è installato il server di backup. È possibile applicare la variabile agli script in esecuzione sul server di backup.

D2D_RECOVERYPOINT

Identifica il punto di ripristino creato dal processo di backup. Questo valore è applicabile soltanto allo script post-backup.

D2D_RPSSCHEDULETYPE

Identifica il tipo di pianificazione durante il backup in un archivio dati su server RPS. I valori seguenti identificano la variabile di D2D_RPSSCHEDULETYPE:

giornaliero

Identifica la pianificazione come backup giornaliero.

settimanale

Identifica la pianificazione come backup settimanale.

mensile

Identifica la pianificazione come backup mensile.

Lo script viene creato.

Nota: per tutti gli script, un valore restituito pari a zero indica un'operazione riuscita, mentre un valore restituito diverso da zero indica la presenza di un errore.

Collocare lo script nella cartella prepost ed eseguire la verifica

Tutti gli script di pre/post per un server di backup sono gestiti centralmente dalla cartella prepost nella posizione seguente:

```
/opt/Arcserve/d2dserver/usr/prepost
```

Effettuare le operazioni seguenti:

1. Collocare il file nella posizione seguente del server di backup:

   `/opt/Arcserve/d2dserver/usr/prepost`

2. Fornire le autorizzazioni di esecuzione per il file di script.
3. Accedere all'interfaccia Web dell'Agente Arcserve UDP (Linux).
4. Aprire la procedura guidata di **backup** o **ripristino** ed accedere alla scheda **Impostazioni avanzate**.
5. Selezionare il file di script nell'elenco del menu a discesa **Impostazioni di pre/post script**, quindi inviare il processo.
6. Fare clic sul **Registro attività** e verificare che lo script venga eseguito per il processo di backup specificato.

   Lo script viene eseguito.

   I pre/post script vengono creati correttamente e inseriti nella cartella prevista.

Esecuzione del processo di backup

Eseguire il processo di backup per poter creare un punto di ripristino. È possibile utilizzare questo punto di ripristino per ripristinare i dati.

Dalla pagina Riepilogo, è possibile visualizzare il riepilogo dei dettagli di backup e specificare un nome per il processo in modo da poterlo distinguere da altri processi.

Effettuare le operazioni seguenti:

1. Rivedere il riepilogo ed immettere un nome per il processo.

   Il campo Nome processo è associato a un nome predefinito. È possibile specificare un nuovo nome per il processo ma non è possibile lasciare il campo vuoto.

2. (Facoltativo) Fare clic Indietro per modificare le impostazioni delle pagine di procedura guidata.
3. Fare clic su Invia.

   Verrà avviato il processo di backup. Dalla scheda Stato processo, il processo viene aggiunto e viene visualizzato lo stato del backup.

   Il processo di backup viene creato ed eseguito.

Verifica dell'esecuzione del backup

Al completamento del processo di backup, verificare che il punto di ripristino venga creato nella destinazione specificata.

Effettuare le operazioni seguenti:

1. Accedere alla destinazione specificata in cui sono stati archiviati i dati di backup.
2. Verificare che la destinazione contenga i dati di backup.

   Ad esempio, se il nome del processo di backup corrisponde a *Demo* e la destinazione di backup è xxx.xxx.xxx.xxx:/Data, accedere alla destinazione di backup e verificare che sia stato generato un nuovo punto di ripristino.

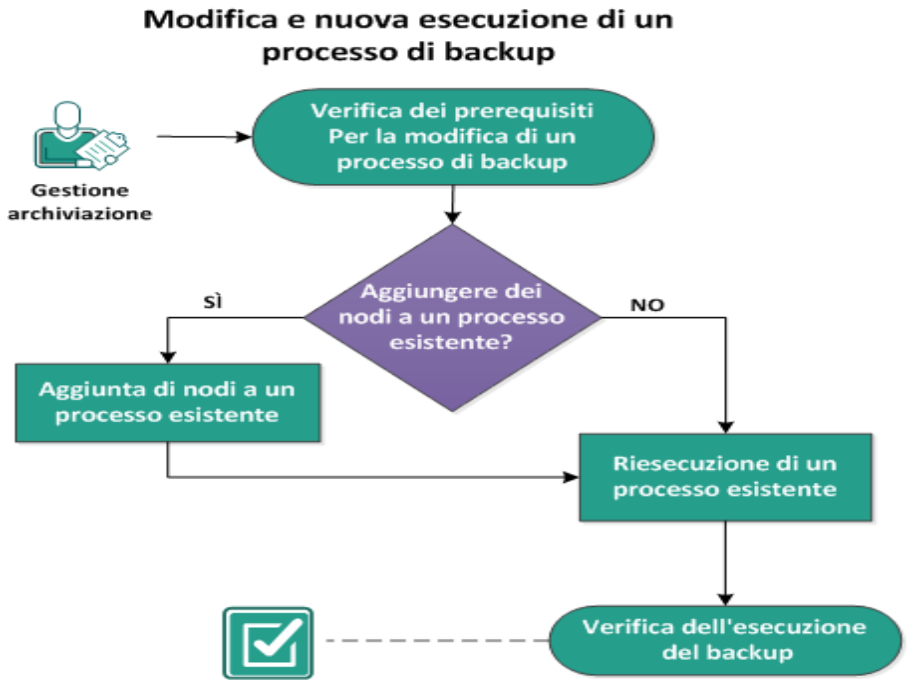
   I dati di backup vengono verificati correttamente.

   Il backup dei nodi Linux viene eseguito correttamente.

Modifica e nuova esecuzione di un processo di backup

Se è stato già creato un processo per un nodo, è possibile modificarlo ed eseguirlo nuovamente più volte. Non è necessario creare un altro processo per proteggere lo stesso nodo. Se non si desidera apportare alcuna modifica al processo, è anche possibile eseguire il processo senza modificarlo. La modifica di un processo comprende l'aggiunta di un nodo a un processo esistente, la configurazione delle impostazioni del processo oppure entrambe.

Il diagramma seguente mostra il processo per la modifica e la nuova esecuzione di un processo di backup:



Eseguire queste attività per modificare ed eseguire nuovamente un processo di backup:

- Verifica dei prerequisiti per la modifica di un processo di backup
- Aggiungere dei nodi a un processo esistente?
- Aggiunta di nodi a un processo esistente
- Riesecuzione di un processo esistente
- Verifica dell'esecuzione del backup

Verifica dei prerequisiti per la modifica di un processo di backup

Verificare i seguenti requisiti prima di modificare ed eseguire nuovamente un processo di backup:

- Esiste un processo di backup valido.
- I nodi sono stati aggiunti a Arcserve UDP.
- Esaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Aggiungere dei nodi a un processo esistente?

Se si dispone già di un processo di backup e si desidera proteggere i nuovi nodi con le stesse impostazioni di backup, è possibile aggiungere nodi a un processo esistente. Dopo avere aggiunto i nodi, è anche possibile modificare le impostazioni di backup ed eseguire il processo.

Aggiunta di nodi a un processo esistente

È possibile aggiungere nuovi nodi a un processo di backup, quindi eseguire il processo. Tutte le impostazioni del processo selezionato vengono applicate al nuovo nodo e non sarà necessario configurare ulteriori impostazioni di backup. Utilizzare questa opzione se si desidera mantenere le stesse impostazioni di backup per tutti i nodi.

Effettuare le operazioni seguenti:

1. Selezionare tutti i nuovi nodi nuovi dalla scheda Nodi del riquadro Stato.
2. Dal menu Procedura guidata, fare clic su Backup e selezionare Aggiungi nodi selezionati a un processo esistente.

   Viene visualizzata la finestra di dialogo Aggiungi nodi selezionati a un processo esistente.
3. Selezionare un processo dall'elenco a discesa Nome processo, quindi fare clic su OK.

   Il nodo viene aggiunto al processo di backup selezionato e la colonna Protetto della scheda Nodi viene modificato in Sì.

   I nodi vengono aggiunti a un processo esistente.

Riesecuzione di un processo di backup esistente

Ripetere il processo di backup per acquisire un altro backup dei nodi specificati. Viene creato un punto di ripristino in seguito a ogni backup. Se è già stato eseguito il backup di un nodo, non sarà necessario creare un altro processo di backup per eseguire nuovamente il backup di tale nodo. Tutti i processi precedenti vengono elencati nella scheda Stato processo nel riquadro Stato.

Quando si ripete un processo di backup, specificare il tipo di processo che si desidera ripetere.

Nota: se vengono aggiornate informazioni nella pagina Destinazione di backup della procedura guidata di backup prima della ripetizione di un processo, il tipo di processo verrà modificato nuovamente in *Backup completo*.

Effettuare le operazioni seguenti:

1. Immettere l'URL dell'Agente Arcserve UDP (Linux) in un browser Web per aprire l'interfaccia utente.

   Nota: durante l'installazione dell'Agente Arcserve UDP (Linux), l'URL per l'accesso e la gestione del server viene fornito all'utente.

2. Fare clic sulla scheda **Stato processo** e selezionare il processo che si desidera eseguire.
3. Verificare che lo stato del processo selezionato corrisponda a Fine o Pronto.

   Fine significa che il processo non è pianificato, mentre Pronto significa che il processo è pianificato.

4. Eseguire una delle seguenti operazioni:
   - Per eseguire il processo senza alcuna modifica, procedere come segue:

   a. Fare clic su **Esegui ora** dal menu Processo.

      Verrà visualizzata la finestra di dialogo Esegui processo di backup.

   b. Selezionare Tipo di backup.
   c. Selezionare un'opzione dall'elenco a discesa Esegui processo per:

      Nodo selezionato

      Specifica che il processo di backup viene eseguito solo per il nodo selezionato.

      Tutti i nodi sono protetti dal processo selezionato

Specifica che il processo di backup viene eseguito per tutti i nodi protetti dal processo selezionato.

d. Fare clic su **OK**.

La finestra di dialogo Esegui processo di backup verrà chiusa. Lo stato del processo viene modificato in Attivo nella scheda Stato processo e lo stesso processo viene eseguito nuovamente.

- Per modificare il processo prima di eseguire il processo, attenersi alla procedura riportata di seguito:

a. Selezionare un processo e fare clic su **Modifica**.

Verrà visualizzata la finestra di dialogo Esegui processo di backup.

b. Aggiornare il campo obbligatorio nella procedura guidata di backup.

c. Fare clic su **Invia**.

Il processo viene eseguito nuovamente a seconda della pianificazione del processo.

Il processo di backup viene eseguito nuovamente.

Verifica dell'esecuzione del backup

Al completamento del processo di backup, verificare che il punto di ripristino venga creato nella destinazione specificata.

Effettuare le operazioni seguenti:

1. Accedere alla destinazione specificata in cui sono stati archiviati i dati di backup.
2. Verificare che la destinazione contenga i dati di backup.

   Ad esempio, se il nome del processo di backup corrisponde a *Demo* e la destinazione di backup è xxx.xxx.xxx.xxx:/Data, accedere alla destinazione di backup e verificare che sia stato generato un nuovo punto di ripristino.

   I dati di backup vengono verificati correttamente.

   Il processo di backup viene modificato e rieseguito correttamente.

Esecuzione di un ripristino a livello di file per i nodi Linux

Un recupero a livello di file esegue il ripristino di singoli file e cartelle a partire da un punto di ripristino. È possibile ripristinare un minimo di un file dal punto di ripristino. Questa opzione è utile se si desidera ripristinare i file selezionati e non l'intero punto di ripristino.

Eseguire queste attività per un recupero a livello di file:

- Verifica dei prerequisiti di ripristino
- Definizione del punto di ripristino per il backup senza agente basato sull'host
- Definizione del punto di ripristino per il backup basato sull'agente
- Definizione dei dettagli relativi al computer di destinazione
- Definizione delle impostazioni avanzate
  - (Facoltativo) Gestione di pre/post script per l'automazione
- Creazione ed esecuzione del processo di ripristino
- Verifica del ripristino dei file

Verifica dei prerequisiti

Prima di eseguire un recupero a livello di file, è necessario tenere presenti le seguenti considerazioni:

- Si dispone di un punto di ripristino valido e della password di crittografia.
- Si dispone di un nodo di destinazione valido per il recupero dei dati.
- Se la destinazione di un processo di backup corrisponde all'origine locale, per eseguire un processo di ripristino a livello di file dalla destinazione, è necessario esportare la destinazione dell'origine locale tramite NFS o CIFS e specificare il punto di ripristino come disponibile nella condivisione NFS o CIFS.
- Si è verificato che il server di backup di Linux supporta il file system che si desidera ripristinare.

  Ad esempio, RedHat 7.x non supporta il file system *reiserfs*. Se il sistema operativo del server di backup è RedHat 7.x e si desidera ripristinare il file system reiserfs, è necessario installare il driver del file system per supportare reiserfs. Inoltre, è possibile utilizzare il Live CD dell'Agente Arcserve UDP (Linux) per il ripristino a livello di file, in quanto il Live CD supporta tutti i tipi di file system.
- Sul server di backup Linux sono stati installati i seguenti pacchetti:
  - mdadm
  - kpartx
  - lvm2
- Esaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Definizione del punto di ripristino per il backup senza agente basato sull'host

L'esecuzione di un backup implica la creazione di un punto di ripristino. Specificare le informazioni relative al punto di ripristino della **Procedura guidata di ripristino**, in modo da poter eseguire il ripristino dei dati desiderati. È possibile ripristinare file specifici o tutti i file in base alle proprie esigenze.

Effettuare le operazioni seguenti:

1. Accedere alla procedura guidata di ripristino in uno dei modi seguenti:

   - Da Arcserve UDP:

   a. Fare clic sulla scheda **Risorse**.

   b. Selezionare **Tutti i nodi** nel riquadro sinistro.

      Tutti i nodi aggiunti vengono visualizzati nel riquadro centrale.

   c. Nel riquadro centrale, selezionare il nodo e fare clic su **Azioni**.

   d. Fare clic su **Ripristina file** dal menu a discesa **Azioni**.

      Viene visualizzata l'interfaccia Web dell'Agente Arcserve UDP (Linux). La finestra di dialogo di selezione del tipo di ripristino viene visualizzata nell'interfaccia utente dell'agente.

   e. Selezionare il tipo di ripristino e fare clic su **OK**.

      Nota: si accede automaticamente al nodo agente e la **Procedura guidata di ripristino** viene visualizzata dal nodo agente.

   - Da Agente Arcserve UDP (Linux):

   a. Aprire l'interfaccia Web dell'Agente Arcserve UDP (Linux).

      Nota: durante l'installazione dell'Agente Arcserve UDP (Linux), l'URL per l'accesso e la gestione del server viene fornito all'utente. Accedere all'Agente Arcserve UDP (Linux).

   b. Fare clic su **Ripristino** dal menu **Procedura guidata** e selezionare **Ripristino a livello di file**.

      Viene visualizzata la schermata **Procedura guidata di ripristino - Ripristino file**.

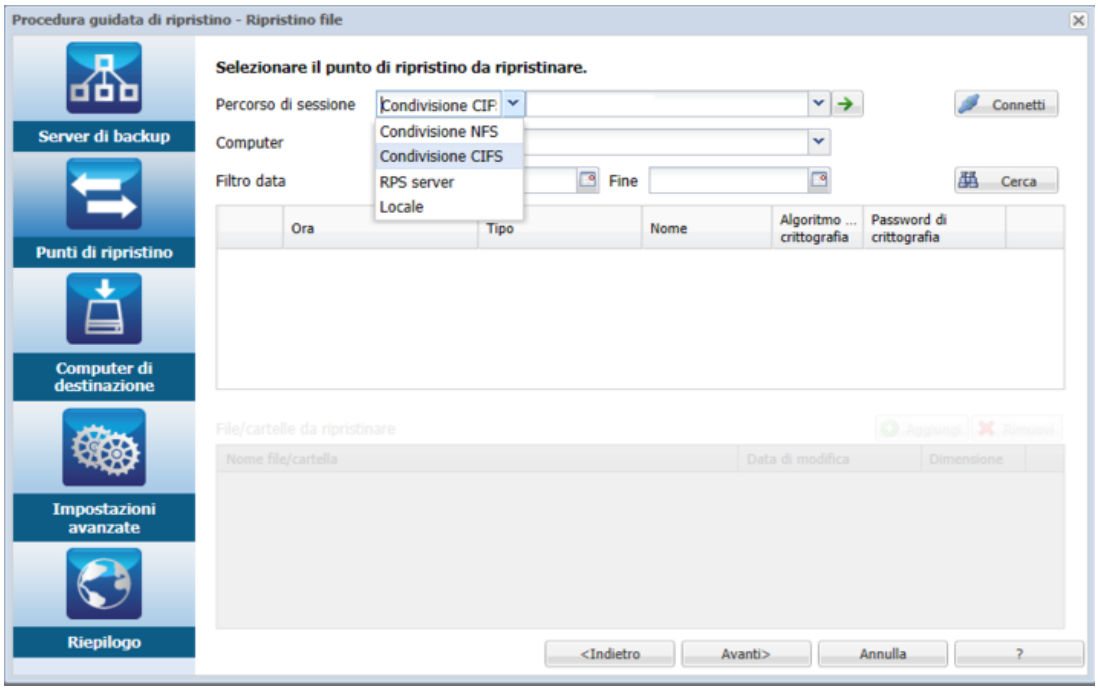
È possibile visualizzare il server di backup selezionato nella pagina **Server di backup** della **Procedura guidata di ripristino**.

Non è possibile selezionare alcuna opzione dall'elenco a discesa **Server di backup**.

2. Fare clic su **Avanti**.

Viene visualizzata la pagina **Punti di ripristino** della **Procedura guidata di ripristino**.

Importante: Se la procedura guidata è stata aperta dalla console, vengono visualizzati automaticamente i dettagli della posizione della sessione e del computer. È possibile andare al passaggio 5.



3. Selezionare una **condivisione CIFS** o un **server RPS** dall'elenco a discesa **Percorso di sessione**.

Nota: Non è possibile selezionare una condivisione NFS o locale per il ripristino delle sessioni di backup senza agente basate su host.

4. Eseguire una delle operazioni riportate di seguito in base al percorso di sessione:

Per la condivisione CIFS

a. Specificare il percorso completo della condivisione CIFS e fare clic su **Connetti**.

b. Specificare il nome utente e la password per connettersi alla condivisione CIFS, quindi fare clic su **OK**.

Per il server RPS

a. Selezionare il server RPS e fare clic su Aggiungi.

   Viene visualizzata la finestra di dialogo **Informazioni sul server del punto di ripristino**.

a. Fornire i dettagli RPS e fare clic sul pulsante Carica.

b. Selezionare l'archivio dati dall'elenco a discesa e fare clic su **Sì**.

   La finestra di dialogo **Informazioni sul server del punto di ripristino** viene chiusa e viene visualizzata la procedura guidata.

c. Fare clic su **Connetti.**

   Tutti i computer vengono elencati nell'elenco a discesa Computer.

d. Selezionare il computer dall'elenco a discesa.

   Tutti i punti di ripristino del computer selezionato vengono visualizzati sotto l'opzione **Filtro data**.

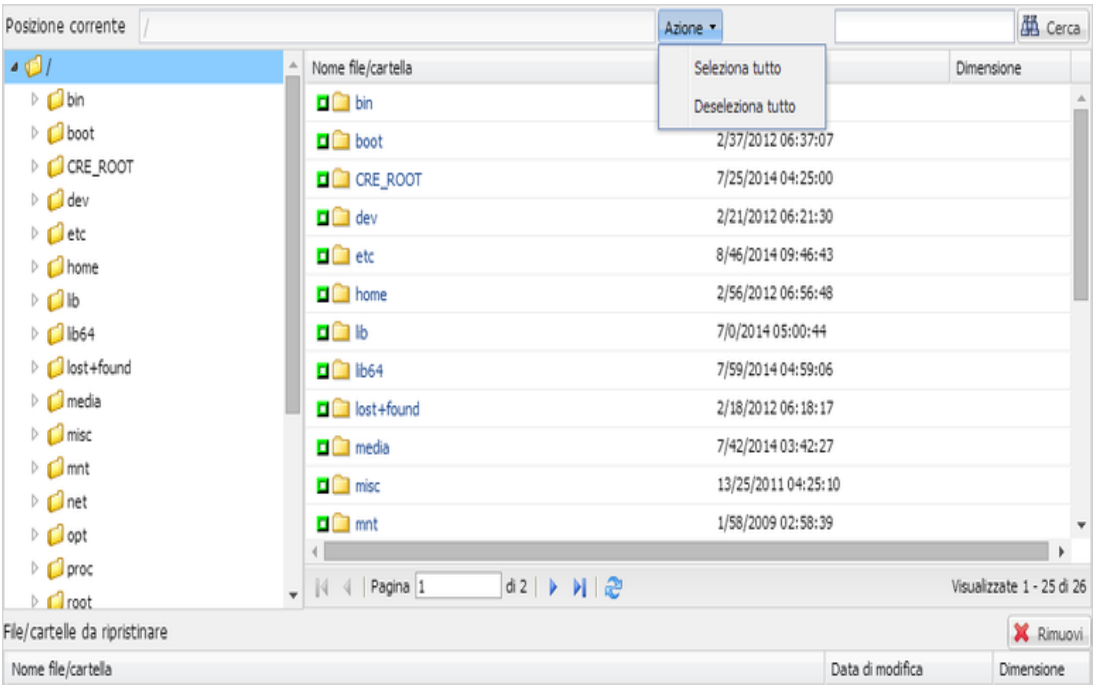
5. Applicare il filtro data per visualizzare i punti di ripristino generati tra le date specificate e fare clic su **Cerca**.

   Valore predefinito: ultime due settimane.

   Vengono visualizzati tutti i punti di ripristino disponibili tra le date specificate.

6. Selezionare il punto di ripristino di cui si desidera eseguire il ripristino e fare clic su **Aggiungi**. Se il punto di ripristino è crittografato, specificare la password di crittografia per il ripristino dei dati.

   Viene visualizzata la finestra di dialogo **Sfoglia-<nome nodo>**.



Importante: Se viene visualizzato il messaggio di avviso "I file o le cartelle vengono visualizzati nel file di periferica. Fare clic per ulteriori informazioni." nella Console, fare riferimento alla seguente Nota per la risoluzione.

Nota: Per alcuni layout di disco complessi, viene visualizzato il file system in base al file di periferica. La modifica del comportamento di visualizzazione del file system non influisce sulla funzione di ripristino a livello di file del computer virtuale Linux basato su host. È possibile cercare il file system nel file di periferica. Inoltre, è possibile utilizzare la funzione di ricerca per eseguire la ricerca di un determinato file o una determinata directory.

7. Selezionare i file e le cartelle di cui si desidera eseguire il ripristino e fare clic su **OK**.

   Nota: se si esegue la ricerca di un file o una cartella mediante il campo **Cerca**, accertarsi di selezionare la cartella più elevata nella gerarchia. La ricerca viene condotta in tutte le cartelle figlie della cartella selezionata.

   La finestra di dialogo **Sfoglia <nome nodo>** viene chiusa e si verrà reindirizzati alla pagina **Punti di ripristino**. I file e le cartelle selezionati sono contenuti nell'elenco **File/Cartelle da ripristinare**.

8. Fare clic su **Avanti**.

   Verrà visualizzata la pagina **Computer di destinazione**.

   Il punto di ripristino viene specificato.

Definizione del punto di ripristino per il backup basato sull'agente

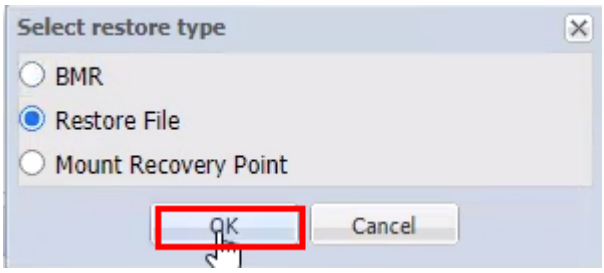
L'esecuzione di un backup implica la creazione di un punto di ripristino. Specificare le informazioni relative al punto di ripristino della Procedura guidata di ripristino, in modo da poter eseguire il ripristino dei dati desiderati. È possibile ripristinare file specifici o tutti i file in base alle proprie esigenze.

Effettuare le operazioni seguenti:

1. Accedere alla procedura guidata di ripristino in uno dei modi seguenti:
   - **Dall'Arcserve UDP:**
     a. Accedere a Arcserve UDP.
     b. Accedere a **Risorse** > **Nodo** > **Tutti i nodi**.

        Tutti i nodi aggiunti vengono visualizzati nel riquadro centrale.
     c. Fare clic con il pulsante destro del mouse sul nodo, quindi selezionare **Ripristina**.

        Vengono visualizzate l'interfaccia Web dell'agente Arcserve UDP (Linux) e la finestra di dialogo Seleziona tipo di ripristino.
     d. Nella finestra di dialogo Seleziona tipo di ripristino, fare clic sull'opzione **Ripristina file**, quindi su **OK**.

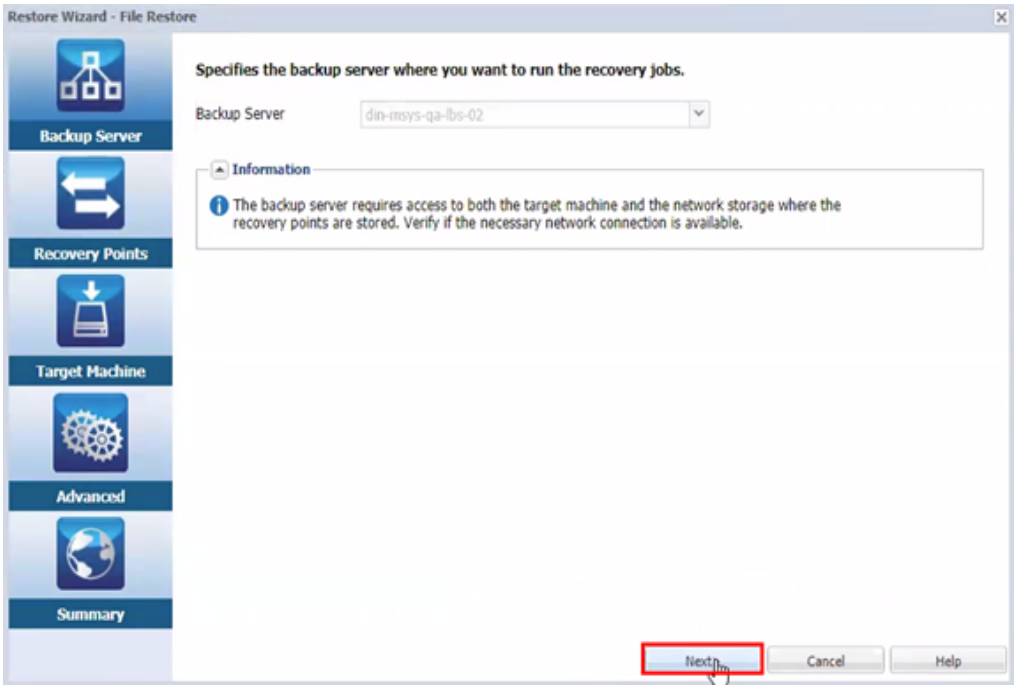
        Nota: si accede automaticamente al nodo dell'agente e la Procedura guidata di ripristino viene visualizzata dal nodo dell'agente.
   - **Da Agente Arcserve UDP (Linux):**
     a. Aprire l'interfaccia Web dell'Agente Arcserve UDP (Linux).

        Nota: durante l'installazione dell'Agente Arcserve UDP (Linux), l'URL per l'accesso e la gestione del server viene fornito all'utente. Accedere a Agente Arcserve UDP (Linux).

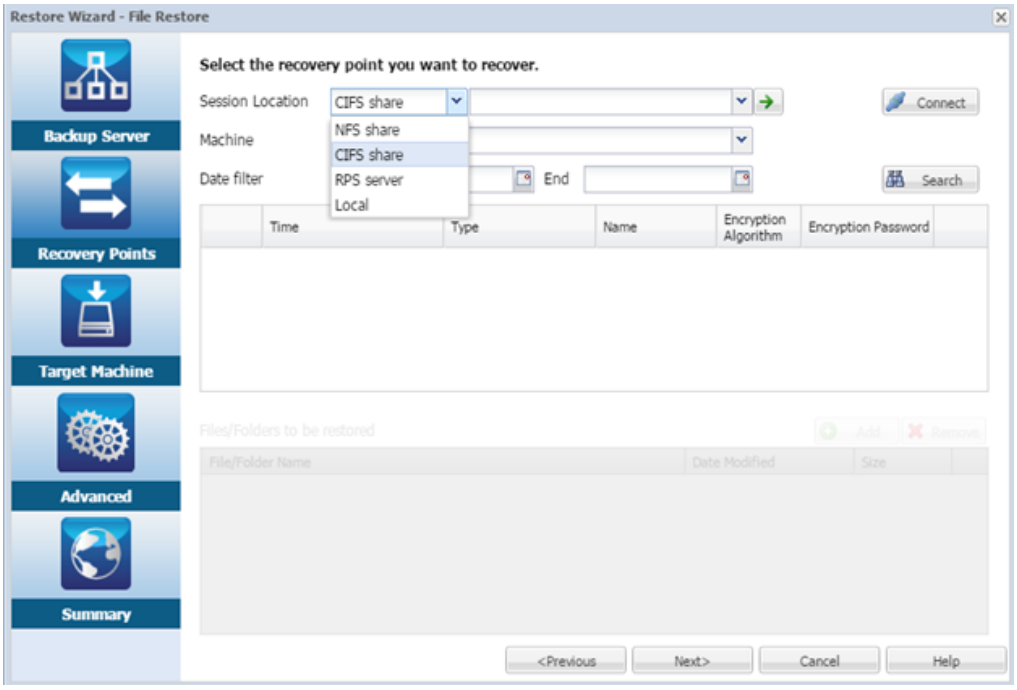
b. Dal menu Procedura guidata, fare clic su **Ripristina**, quindi selezionare **Ripristina file**.

   Viene visualizzata la finestra di dialogo Procedura guidata di ripristino - Ripristino file.

2. Nella pagina Server di backup della procedura guidata di ripristino, è possibile visualizzare il server di backup. Non è possibile selezionare alcuna opzione dall'elenco a discesa Server di backup. Fare clic su **Avanti**.



3. Nella pagina Punti di ripristino della procedura guidata di ripristino, eseguire le seguenti operazioni:



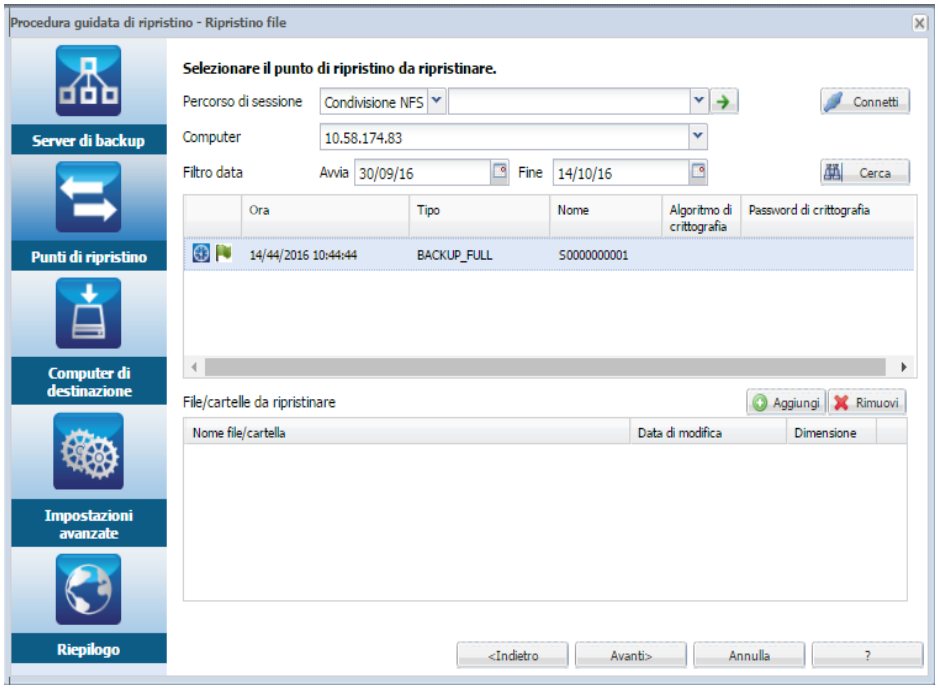
Importante: Se la procedura guidata è stata aperta dalla console, vengono visualizzati automaticamente i dettagli della posizione della sessione e del computer. È possibile andare al passaggio 4.

a. Selezionare **Condivisione CIFS/Condivisione NFS/Server RPS/Locale** dall'elenco a discesa Percorso di sessione.

b. Se si seleziona **Condivisione CIFS/Condivisione NFS/Locale**, specificare il percorso completo della Condivisione CIFS/Condivisione NFS/Locale, quindi fare clic su **Connetti**.

   Tutti i computer vengono elencati nell'elenco a discesa Computer.

   Nota: se si seleziona l'opzione di **condivisione CIFS**, specificare il nome utente e la password.



c. Se si seleziona il **server RPS**, procedere come segue:

   1. Selezionare il server RPS dall'elenco a discesa, quindi fare clic su **Aggiungi**.

      Viene visualizzata la finestra di dialogo Informazioni sul server del punto di ripristino.

   2. Fornire i dettagli RPS e fare clic su **Sì**.

   3. Selezionare l'archivio dati dall'elenco a discesa.

      La finestra di dialogo Informazioni sul server del punto di ripristino viene chiusa e viene visualizzata la procedura guidata.

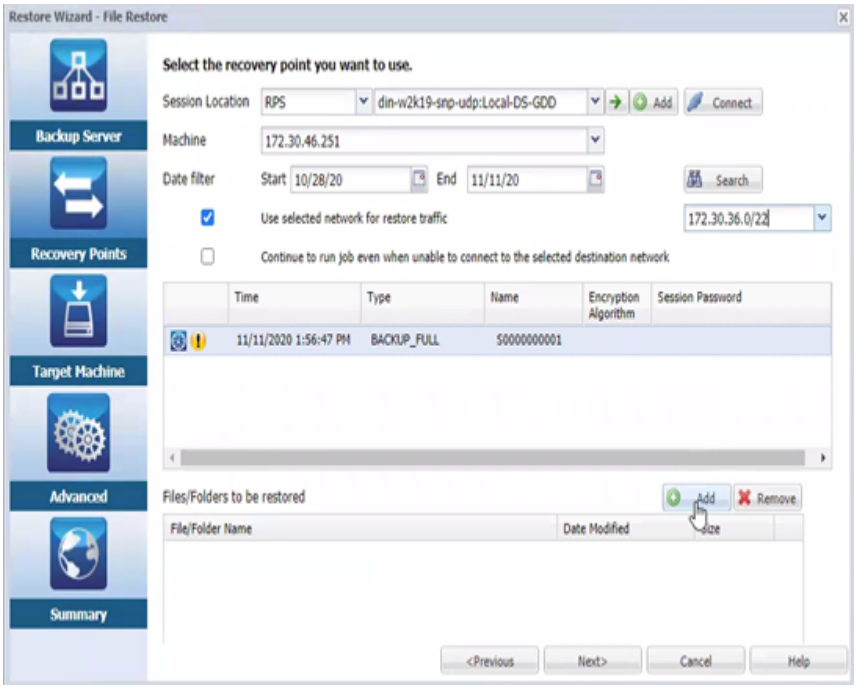
   4. Fare clic su **Connetti.**

      Tutti i nodi di cui è stato eseguito il backup per il percorso specificato saranno contenuti nell'elenco a discesa Computer.

   5. Dall'elenco a discesa Computer, selezionare il nodo che si desidera ripristinare.

      Verrà creato un elenco contenente tutti i punti di ripristino per il

nodo selezionato.



4. Applicare il filtro data per visualizzare i punti di ripristino generati tra le date specificate e fare clic su **Cerca**.

   Valore predefinito: ultime due settimane.

   Vengono visualizzati tutti i punti di ripristino disponibili tra le date specificate.

5. Per abilitare la comunicazione tra l'agente Linux e il Recovery Point Server, selezionare la casella di controllo **Usa rete selezionata per il traffico di ripristino**, quindi selezionare la rete dall'elenco a discesa.

   Nota: se la rete di backup selezionata non è accessibile, per continuare il processo di backup con la rete disponibile o con la rete predefinita, fare clic sulla casella di controllo **Procedere con l'esecuzione del processo anche nel caso in cui sia impossibile stabilire la connessione alla rete di backup selezionata**.

6. Selezionare il punto di ripristino desiderato. Se il punto di ripristino è crittografato, specificare la password di crittografia per il ripristino dei dati.

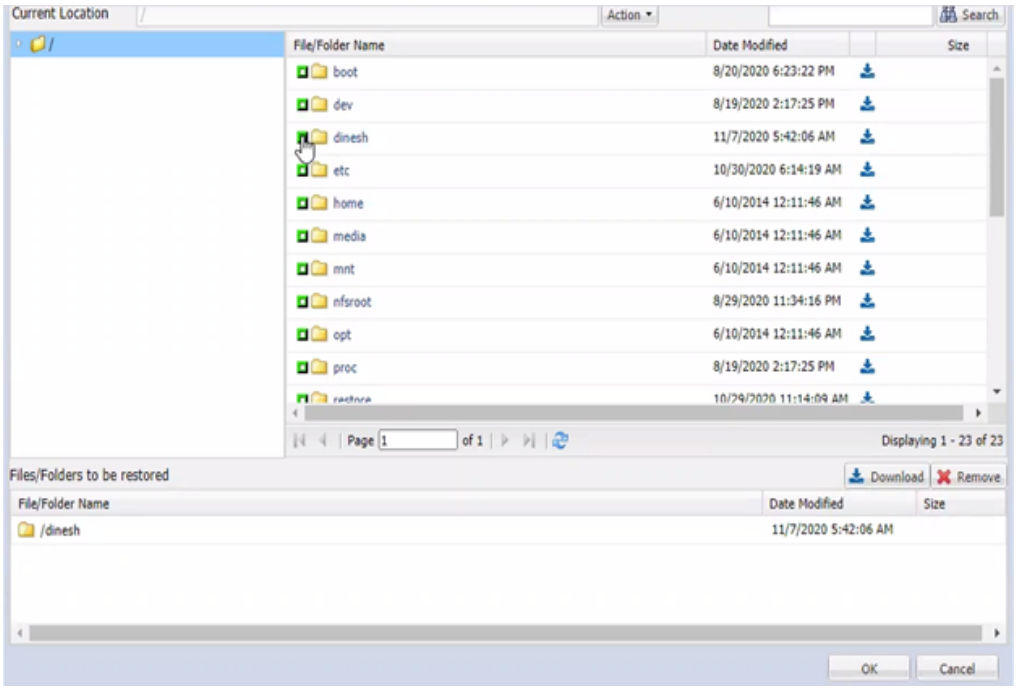
7. Per i file o le cartelle da ripristinare, fare clic su **Aggiungi**.

   Viene visualizzata la finestra di dialogo Sfoglia-<nome nodo>.

   Importante: Se viene visualizzato il messaggio di avviso "I file o le cartelle vengono visualizzati nel file di periferica. Fare clic per ottenere ulteriori informazioni." nella Console, fare riferimento alla seguente Nota per la risoluzione.

Nota: Per alcuni layout di disco complessi, viene visualizzato il file system in base al file di periferica. La modifica del comportamento di visualizzazione del file system non influisce sulla funzione di ripristino a livello di file del computer virtuale Linux basato su host. È possibile cercare il file system nel file di periferica. Inoltre, è possibile utilizzare la funzione di ricerca per eseguire la ricerca di un determinato file o una determinata directory.

8. Nella finestra di dialogo Sfoglia-<nome nodo>, selezionare il file o la cartella che si desidera ripristinare, quindi fare clic su **OK**.



Nota: se si esegue la ricerca di un file o una cartella mediante il campo **Cerca**, accertarsi di selezionare la cartella più elevata nella gerarchia. La ricerca viene condotta in tutte le cartelle figlie della cartella selezionata.

La finestra di dialogo Sfoglia <nome nodo> viene chiusa e si verrà reindirizzati alla pagina Punti di ripristino. I file e le cartelle selezionati sono contenuti nell'elenco File/Cartelle da ripristinare.

9. Fare clic su **Avanti**.

   Verrà visualizzata la pagina Computer di destinazione.

Il punto di ripristino viene specificato.

Definizione dei dettagli relativi al computer di destinazione

Specificare i dettagli relativi al nodo di destinazione in modo che i dati vengano ripristinati su tale computer. È possibile eseguire il ripristino delle cartelle o dei file selezionati sul nodo di origine o su un nuovo nodo.

Per eseguire il ripristino sul nodo di backup dei dati, attenersi alla procedura riportata di seguito:

1. Nella pagina Computer di destinazione, selezionare **Ripristina in posizione originale**.

2. Immettere il nome utente e la password del nodo.
3. Per risolvere i file in conflitto, selezionare una delle seguenti opzioni:

   Sovrascrivi i file esistenti

   Indica che se il file è presente sul computer di destinazione, il file di backup del punto di ripristino sostituirà il file esistente.

   Rinomina file

   Specifica che se il file esiste nel computer di destinazione, viene creato un nuovo file con lo stesso nome file e con *.d2dduplicate<x>* come estensione file. <x> specifica il numero di volte in cui il file viene ripristinato. Tutti i dati vengono ripristinati nel nuovo file.

Ignora file esistenti

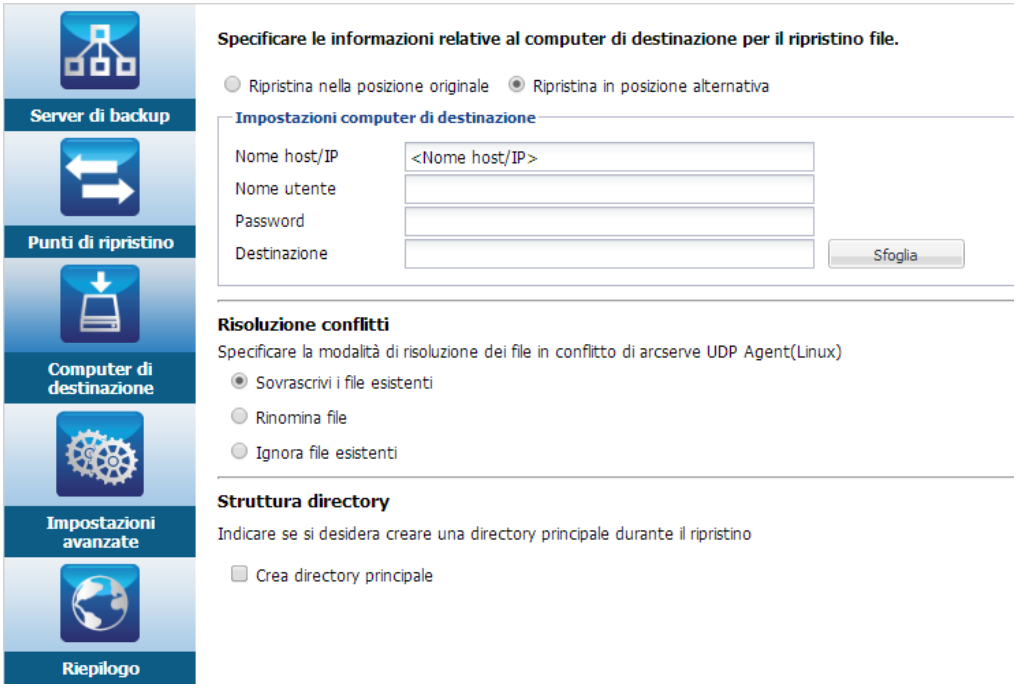
Specifica che se lo stesso file è già presente nel computer di destinazione, il ripristino di tali file non verrà eseguito a partire dal punto di ripristino.

4. (Facoltativo) Selezionare **Crea directory principale**.
5. Fare clic su **Avanti**.

   Viene visualizzata la pagina Impostazioni avanzate.

Per eseguire il ripristino di un nuovo nodo, attenersi alla procedura riportata di seguito:

1. Nella pagina Computer di destinazione, selezionare **Ripristina in posizione alternativa**.



2. Immettere il nome host o l'indirizzo IP del nodo di destinazione.
3. Immettere il nome utente e la password del nodo.
4. Immettere il percorso di ripristino dei dati oppure fare clic su **Sfoglia** per selezionare la cartella di ripristino dei dati, quindi fare clic su **OK**.
5. Per risolvere i file in conflitto, selezionare una delle seguenti opzioni:

   Sovrascrivi i file esistenti

   Indica che se il file è presente sul computer di destinazione, il file di backup del punto di ripristino sostituirà il file esistente.

   Rinomina file

Specifica che se il file esiste nel computer di destinazione, viene creato un nuovo file con lo stesso nome file e con *.d2dduplicate<x>* come estensione file. <x> specifica il numero di volte in cui il file viene ripristinato. Tutti i dati vengono ripristinati nel nuovo file.

Ignora file esistenti

Specifica che se lo stesso file è già presente nel computer di destinazione, il ripristino di tali file non verrà eseguito a partire dal punto di ripristino.

6. (Facoltativo) Selezionare **Crea directory principale**.
7. Fare clic su **Avanti**.

   Viene visualizzata la pagina Impostazioni avanzate.

Vengono specificati i dettagli relativi al computer di destinazione.

Definizione delle impostazioni avanzate

Specificare le impostazioni avanzate per eseguire un recupero pianificato dei dati. Il recupero pianificato garantisce che i dati vengano recuperati all'ora specificata anche in caso di assenza dell'utente.

Effettuare le operazioni seguenti:

1. Impostare la data e l'ora di inizio selezionando una delle seguenti opzioni:

   Esegui ora

   Avvia il processo di ripristino a livello di file dopo l'invio del processo.

   Imposta data e ora di inizio

   Avvia il processo di ripristino a livello di file nella data e ora specificata dopo l'invio del processo.

2. (Facoltativo) Selezionare **Stima dimensioni del file**.
3. (Facoltativo) Selezionare uno script dall'opzione **Impostazioni pre/post script**.

   Questi script eseguono comandi di script per le azioni da eseguire prima dell'inizio del processo e/o al completamento del processo.

   Nota: i campi **Impostazioni pre/post script** vengono popolati solamente se un file di script è già stato creato e collocato nel percorso seguente:

   `/opt/Arcserve/d2dserver/usr/prepost`

   Nota: per ulteriori informazioni sulla creazione di pre/post script, consultare la sezione *Gestione di pre/post script per l'automazione*.

4. Fare clic su **Avanti**.

   Viene visualizzata la pagina Riepilogo**.**

   Vengono specificate le impostazioni avanzate.

   La presente sezione descrive i seguenti argomenti:

   - (Facoltativo) Gestione di pre/post script per l'automazione

(Facoltativo) Gestione di pre/post script per l'automazione

Gli script di pre/post esecuzione consentono di eseguire regole di business in fasi specifiche di un processo in esecuzione. È possibile specificare quando eseguire gli script nelle **Impostazioni pre/post script** della **Procedura guidata di backup** e della **Procedura guidata di ripristino** dell'interfaccia utente. È possibile eseguire gli script sul server di backup in base alle impostazioni dell'utente.

La gestione del pre/post script è un processo costituito da due passaggi: la creazione del pre/post script e la sua collocazione nella cartella prepost.

Creazione di pre/post script

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Creare un file di script mediante le variabili di ambiente nel linguaggio di scripting preferito.

Variabili di ambiente del pre/post script

Per creare lo script, utilizzare le variabili di ambiente seguenti:

D2D_JOBNAME

Indica il nome del processo.

D2D_JOBID

Identifica l'ID del processo. L'ID di processo è un numero attribuito al processo durante la sua esecuzione. Se si esegue lo stesso processo nuovamente, verrà fornito un nuovo numero di processo.

D2D_TARGETNODE

Identifica il nodo di cui viene eseguito il backup o il ripristino.

D2D_JOBTYPE

Identifica il tipo di processo in esecuzione. I valori seguenti identificano la variabile D2D_JOBTYPE:

backup.full

Identifica il processo come backup completo.

backup.incremental

Identifica il processo come backup incrementale.

backup.verify

Identifica il processo come backup di verifica.

restore.bmr

Identifica il processo come ripristino bare metal (BMR). Si tratta di un processo di ripristino.

restore.file

Identifica il processo come ripristino a livello di file. Si tratta di un processo di ripristino.

D2D_SESSIONLOCATION

Identifica la posizione in cui vengono archiviati i punti di ripristino.

D2D_PREPOST_OUTPUT

Identifica un file temp. Il contenuto della prima linea del file temp viene visualizzato nel registro attività.

D2D_JOBSTAGE

Indica la fase del processo. I valori seguenti identificano la variabile D2D_JOBSTAGE:

pre-job-server

Identifica lo script eseguito sul server di backup prima dell'avvio del processo.

post-job-server

Identifica lo script eseguito sul server di backup dopo il completamento del processo.

pre-job-target

Identifica lo script eseguito sul computer di destinazione prima dell'avvio del processo.

post-job-target

Identifica lo script eseguito sul computer di destinazione dopo il completamento del processo.

pre-snapshot

Identifica lo script eseguito sul computer di destinazione prima dell'acquisizione della snapshot.

post-snapshot

Identifica lo script eseguito sul computer di destinazione dopo l'acquisizione della snapshot.

D2D_TARGETVOLUME

Identifica il volume di cui viene eseguito il backup durante un processo di backup. Questa variabile è adatta per gli script di snapshot di pre/post automazione per un processo di backup.

D2D_JOBRESULT

Identifica il risultato di uno script del processo di post-esecuzione. I valori seguenti identificano la variabile di D2D_JOBRESULT:

success

Identifica il risultato come corretto.

fail

Identifica il risultato come non corretto.

D2DSVR_HOME

Identifica la cartella in cui è installato il server di backup. È possibile applicare la variabile agli script in esecuzione sul server di backup.

Lo script viene creato.

Nota: per tutti gli script, un valore restituito pari a zero indica un'operazione riuscita, mentre un valore restituito diverso da zero indica la presenza di un errore.

Collocare lo script nella cartella prepost ed eseguire la verifica

Tutti gli script di pre/post per un server di backup sono gestiti centralmente dalla cartella prepost nella posizione seguente:

/opt/Arcserve/d2dserver/usr/prepost

Effettuare le operazioni seguenti:

1. Collocare il file nella posizione seguente del server di backup:

   `/opt/Arcserve/d2dserver/usr/prepost`

2. Fornire le autorizzazioni di esecuzione per il file di script.
3. Accedere all'interfaccia Web dell'Agente Arcserve UDP (Linux).
4. Aprire la procedura guidata di **backup** o **ripristino** ed accedere alla scheda **Impostazioni avanzate**.
5. Selezionare il file di script nell'elenco del menu a discesa **Impostazioni di pre/post script**, quindi inviare il processo.
6. Fare clic sul **Registro attività** e verificare che lo script venga eseguito per il processo di backup specificato.

   Lo script viene eseguito.

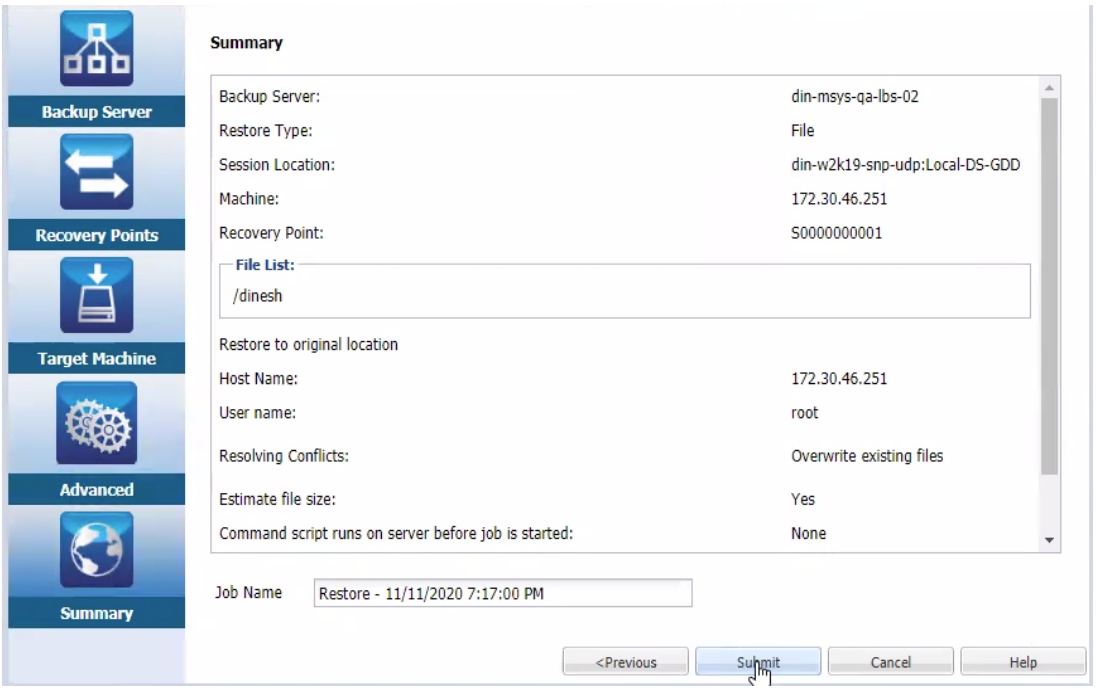
   I pre/post script vengono creati correttamente e inseriti nella cartella prevista.

Creazione ed esecuzione del processo di ripristino

Creare e eseguire il processo di ripristino in modo da poter avviare il recupero a livello di file. Verificare le informazioni relative al punto di ripristino prima di eseguire il ripristino dei file. Se necessario, è possibile tornare indietro e modificare le impostazioni di ripristino nella procedura guidata.

Effettuare le operazioni seguenti:

1. Nella pagina Riepilogo della procedura guidata di ripristino, verificare i dettagli del ripristino.



2. Eseguire una delle seguenti operazioni:
   - Se le informazioni di riepilogo non sono corrette, fare clic su **Indietro** e accedere alla finestra di dialogo corrispondente per modificare le impostazioni non corrette.
   - Se le informazioni di riepilogo sono corrette, immettere un nome per il processo, quindi fare clic su **Invia** per avviare il processo di ripristino.

Nota: il campo Nome processo è associato a un nome predefinito. È possibile specificare un nuovo nome per il processo ma non è possibile lasciare il campo vuoto.

La procedura guidata di ripristino viene chiusa. È possibile visualizzare lo stato del processo dalla scheda Stato processo.

Il processo di ripristino viene creato ed eseguito correttamente.

Verifica del ripristino dei file

Al completamento del processo di ripristino, verificare che tutti i nodi siano stati ripristinati sul nodo di destinazione. Selezionare **Cronologia processo** e le schede **Registro attività** nel riquadro **Stato** per monitorare l'avanzamento del processo di ripristino.

Effettuare le operazioni seguenti:

1. Accedere al computer di destinazione su cui sono stati ripristinati i dati.
2. Verificare che i dati obbligatori del punto di ripristino vengano ripristinati.

   La verifica dei file viene eseguita correttamente.

   Il recupero a livello di file viene eseguito correttamente.

Creazione di un Live CD di avvio

Il responsabile dell'archiviazione può creare un sistema Live CD di avvio. Una volta creato, il sistema Live CD di avvio contiene un'immagine completa di sola lettura del sistema operativo del computer, e può essere utilizzata per fornire funzioni temporanee del sistema operativo. Live CD include tutte le impostazioni di sistema e i file del sistema operativo e può essere utilizzato per l'esecuzione delle funzioni seguenti:

- È possibile utilizzare l'Agente Arcserve UDP (Linux) senza in realtà installare il prodotto. In questo modo si può provare e valutare il prodotto senza installarlo o apportare modifiche al disco rigido in uso del computer.
- È possibile installare l'Agente Arcserve UDP (Linux) su più server utilizzando un solo pacchetto di installazione. Senza Live CD è necessario installare due file separati (un file .iso e il pacchetto dell'utilità di ripristino) per installare l'Agente Arcserve UDP (Linux). Il pacchetto dell'utilità di ripristino è incluso nello stesso pacchetto di installazione di Live CD.
- È possibile eseguire un ripristino bare metal (BMR). È possibile utilizzare il Live CD per acquisire l'indirizzo IP del computer di destinazione (richiesto durante il ripristino bare metal).

La cartella bin contiene gli script che è possibile eseguire dalla riga di comando per creare un Live CD di avvio. La cartella bin si trova nel seguente percorso:

```
# /opt/Arcserve/d2dserver/bin
```

Il diagramma seguente mostra il processo di creazione del Live CD di avvio:

Il seguente elenco descrive le attività necessarie per la creazione di un Live CD di avvio:

- Verifica dei prerequisiti per Live CD
- Installazione del pacchetto dell'utilità di ripristino
- Creazione e verifica del Live CD di avvio
- Utilizzo del sistema Live CD come server di backup Linux

Verifica dei prerequisiti per Live CD

Prima di installare un Live CD, tenere presenti i seguenti prerequisiti:

- Si dispone delle credenziali di accesso per l'utente root per il server di backup.
- Sono state lette le note di rilascio relative al funzionamento del sistema Live CD.
- Si dispone delle conoscenze necessarie per la generazione di script Linux.
- Lo strumento *mkisofs* è stato installato nel server di backup. Il server di backup utilizza lo strumento mkisofs per creare il file Live CD.iso.
- Si dispone di almeno 1024 MB di memoria libera sul computer per l'avvio e l'esecuzione di CD Live.
- Esaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Installazione del pacchetto dell'utilità di ripristino

Per poter eseguire una qualsiasi operazione di ripristino, è necessario installare il pacchetto dell'utilità di ripristino. Se tale pacchetto non viene installato, non sarà possibile eseguire un ripristino a livello di file o un ripristino bare metal. È possibile installare il pacchetto dell'utilità di ripristino durante l'installazione dell'Agente Arcserve UDP (Linux). È inoltre possibile scaricare e installare il pacchetto dell'utilità di ripristino in un qualsiasi momento dopo l'installazione dell'Agente Arcserve UDP (Linux).

Dopo aver installato il pacchetto dell'utilità di ripristino, sarà possibile creare un Live CD.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Accedere alla cartella bin mediante il seguente comando:

   ```
   # cd /opt/Arcserve/d2dserver/bin
   ```

3. Eseguire il comando seguente per installare il pacchetto dell'utilità di ripristino:

   ```
   #./configutility
   ```

   Viene visualizzato un messaggio che richiede di fornire il percorso del pacchetto dell'utilità di ripristino.

4. Fornire il percorso completo di download del pacchetto dell'utilità di ripristino.

   Viene avviata la procedura di installazione.

   Il pacchetto dell'utilità di ripristino viene installato.

Creazione e verifica del Live CD di avvio

Il sistema Live CD crea l'ambiente del server di backup senza dover installare il software. Il sistema Live CD facilita il ripristino bare metal grazie all'uso di un indirizzo IP in una rete privata.

Live CD è un sistema operativo di computer di avvio completo che viene eseguito nella memoria del computer piuttosto che con il caricamento dal disco rigido. Il sistema Live CD consente di utilizzare e valutare un sistema operativo senza eseguirne l'installazione né apportare modifiche al sistema operativo esistente sul computer.

Effettuare le operazioni seguenti:

1. Accedere alla cartella bin mediante il seguente comando:

   ```
   # cd /opt/Arcserve/d2dserver/bin
   ```

2. Eseguire il comando seguente per creare un Live CD:

   ```
   # ./makelivecd
   ```

3. Accedere al percorso seguente e verificare che il file LiveCD.iso sia stato creato:

   ```
   /opt/Arcserve/d2dserver/packages
   ```

   Il Live CD di avvio è stato creato e verificato correttamente. Se si desidera utilizzare Live CD su una rete virtuale, è possibile montare direttamente il file LiveCD.iso sul computer virtuale. Se si desidera utilizzare Live CD su un computer fisico, è necessario masterizzare l'immagine LiveCD.iso su un supporto multimediale (CD o DVD) e, quindi, utilizzare il file masterizzato per avviare il computer.

Utilizzo del sistema Live CD come server di backup Linux

È possibile utilizzare il sistema Live CD come server di backup Linux.

Effettuare le operazioni seguenti:

1. Creare un Live CD dal server di backup Linux in uso.

   Per creare il Live CD dalla pagina principale:

   - Fare clic su Ripristino, Ripristino bare metal (BMR).
   - Accedere a Procedura guidata di ripristino - Ripristino Bare Metal, fare clic sul collegamento **Fare clic qui per scaricare Live CD**, quindi salvarlo.

2. Avviare un computer virtuale o fisico con il Live CD.

   Nota: si consiglia una memoria da 4 GB per questo computer.

   All'avvio del computer con il sistema Live CD, è possibile visualizzare il messaggio seguente:

   Utilizzare il seguente URL per accedere e gestire questo agente Arcserve Unified Data Protection per Linux: https://xxx.xxx.xxx.xxx:8014.

   xxx.xxx.xxx.xxx si riferisce all'URL corrente utilizzato dal computer.

3. Immettere l'URL *https://xxx.xxx.xxx.xxx:8014* nel browser.

   Viene visualizzata la pagina principale del server di backup Linux.

4. Utilizzare le funzioni del server di backup Linux per eseguire un processo.

   Ad esempio, fare clic su Ripristino, Ripristino a livello di file, quindi trovare il percorso della sessione di backup ed eseguire il processo di ripristino a livello di file.

Creazione di un Live CD di avvio per includere i driver personalizzati per AlmaLinux 9.x

La funzionalità Live CD personalizzata consente di creare un Live CD di avvio per AlmaLinux 9.0 per includere i driver personalizzati.

Quando utilizzare il Live CD personalizzato:

Utilizzare il Live CD personalizzato quando il Live CD predefinito non riesce a identificare le periferiche di archiviazione e di rete a causa della mancata disponibilità di un driver di periferica.

Nota: i punti di ripristino che si desidera ripristinare non includono i driver delle periferiche del sistema di archiviazione del computer di ripristino bare metal di destinazione. Di conseguenza, l'agente Arcserve Unified Data Protection per Linux bloccherà tempestivamente qualsiasi tentativo di eseguire un processo di ripristino bare metal.

La cartella bin contiene gli script che è possibile eseguire dalla riga di comando per creare un Live CD di avvio. La cartella bin si trova nel seguente percorso:

 # /opt/Arcserve/d2dserver/bin

Verifica dei prerequisiti

Verificare il completamento delle seguenti azioni preliminari:

1. UDP Linux versione 10.0 (o versioni successive) deve essere installato in LBS.
2. I driver del dispositivo (file *.ko o *.rpm) devono essere preparati e archiviati in una cartella all'interno di LBS.

   Ad esempio, archiviare i driver del dispositivo nella cartella /tmp/drivers.

   Nota: è necessario fornire il driver del dispositivo corrispondente alla versione del kernel del Live CD predefinito di UDPLinux. Attualmente, le versioni del sistema operativo e del kernel per il Live CD di UDP Linux sono le seguenti:

   - Versione sistema operativo: AlmaLinux 9.0
   - Versione kernel: 5.14.0-70.13.1.el9_0.x86_64
3. Per creare un Live CD personalizzato all'interno di LBS, è necessario allocare spazio sufficiente.

   Ad esempio, se il percorso desiderato per l'output del Live CD personalizzato è /tmp/iso, lo spazio della posizione /tmp/iso deve essere maggiore o uguale alla dimensione predefinita del Live CD più i driver e gli rpm totali dell'utente oltre a 500 MB.

Creazione di un Live CD personalizzato

La funzionalità Live CD personalizzata consente di avviare un computer di destinazione del ripristino bare metal e di eseguire un processo di ripristino bare metal. Per creare un Live CD personalizzato, vengono utilizzati i seguenti file:

driverinlivecd

Script utilizzato per rimasterizzare il Live CD predefinito.

UDP_Agent_Linux-LiveCD.iso

Live CD predefinito disponibile per l'agente UDPLinux.

Effettuare le operazioni seguenti:

1. Accedere alla posizione seguente:

   /opt/Arcserve/d2dserver/bin

2. Eseguire il seguente comando:

   driverinlivecd <full_path_to_default_LiveCD> <path_where_device_driver(s)_are_stored> <path_where_customized_LiveCD_should_be_stored>

   Esempio: ./driverinlivecd /opt/Arcserve/d2dserver/packages/UDP_Agent_Linux-LiveCD.iso /tmp/drivers /tmp/iso

   Lo script crea il Live CD personalizzato in base ai driver del dispositivo forniti, quindi archivia il file dell'immagine ISO nella posizione desiderata.

   Esempio: */tmp/iso/ UDP_Agent_Linux-LiveCD.iso*

Verifica di un Live CD personalizzato

In questa sezione vengono fornite informazioni su come verificare il Live CD personalizzato.

Effettuare le operazioni seguenti:

1. Avviare un nodo di destinazione con il Live CD personalizzato risultante (UDP_Agent_Linux-LiveCD.iso) creato nella posizione desiderata:

   /tmp/iso/

2. Aprire la shell o la riga di comando.
3. Per verificare se gli rpm sono inclusi nel Live CD personalizzato, eseguire il seguente comando:

   ls /user_rpms/

4. Per verificare se i file *.ko sono inclusi nel Live CD personalizzato, eseguire il comando seguente:

   ls /lib/modules/5.14.0-70.13.1.el9_0.x86_64/kernel/drivers/users/

5. Verificare le informazioni dei driver del dispositivo.

   Esempio: modinfo “driver_name”

   Se l'output non è vuoto o NULL, l'output dovrà mostrare le informazioni relative al driver del dispositivo caricato.

   Il Live CD personalizzato è stato verificato correttamente. A questo punto, è possibile eseguire il processo di ripristino bare metal per il nodo di origine desiderato.

Note:

- In caso di pacchetti rpm, verificare che i pacchetti siano installabili semplicemente utilizzando le utilità rpm. Non dovranno essere presenti altre dipendenze o pacchetti in sospeso.

  Ad esempio, per eseguire la verifica, provare a installare il pacchetto rpm sul computer virtuale AlmaLinux 9.0 (kernel: 5.14.0-70.13.1.el9_0.x86_64) prima di utilizzare questa funzionalità.

- Se i pacchetti rpm contengono driver del dispositivo (file *.ko), a volte i driver potrebbero non essere caricati correttamente nel nodo di destinazione dopo l'esecuzione dello script *driverinlivecd* e la creazione del Live CD personalizzato. In questi casi, estrarre i pacchetti rpm per ottenere i file ko richiesti, i quali devono essere caricati nel nodo di destinazione. Durante

l'esecuzione dello script *driverinlivecd*, conservare i file ko direttamente nel percorso in cui sono archiviati i driver del dispositivo invece di conservare il pacchetto rpm.

Esecuzione di un ripristino bare metal per computer Linux

Un ripristino bare metal esegue il ripristino del sistema operativo e delle applicazioni software ed esegue il ripristino di tutti i dati sottoposti a backup. Il ripristino bare metal consiste nel ripristino di un sistema del computer avviato a partire da un sistema *bare metal*. Bare metal è un computer senza sistema operativo, driver e applicazioni software. Al completamento del ripristino, il computer di destinazione viene riavviato automaticamente sullo stesso ambiente operativo del nodo di origine del backup e tutti i dati vengono ripristinati.

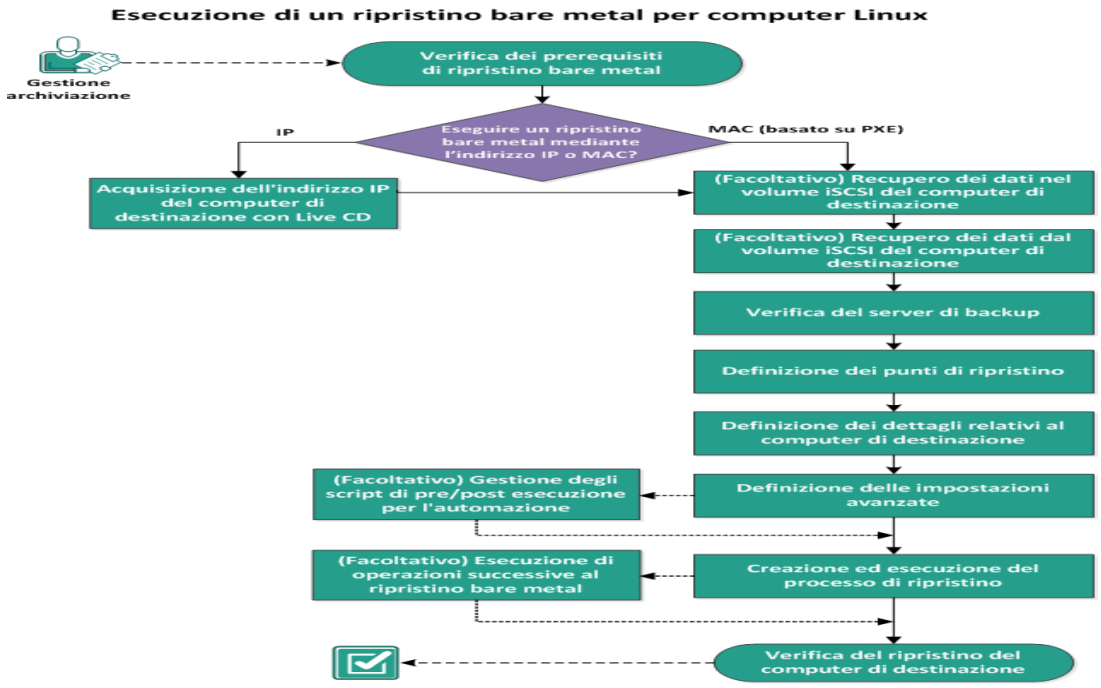
È possibile eseguire un ripristino bare metal completo poiché quando si esegue un backup di dati, esso acquisisce anche informazioni relative al sistema operativo, alle applicazioni installate, ai driver e così via.

È possibile eseguire un ripristino bare metal utilizzando una delle seguenti opzioni:

- Tramite l'opzione della riga di comando. Per ulteriori informazioni, consultare la sezione Creazione di un modello di configurazione tramite la riga di comando.
- Tramite l'indirizzo IP o l'indirizzo MAC (Media Access Control) del computer di destinazione. Se il computer di destinazione viene avviato mediante il sistema Live CD dell'Agente Arcserve UDP (Linux), è possibile ottenere l'indirizzo IP del computer di destinazione.

  Nota: è possibile avviare il computer. È configurata una sola scheda NIC.

Il diagramma seguente mostra il processo per eseguire un ripristino bare metal mediante l'indirizzo IP o MAC:



Completare le attività seguenti per eseguire un ripristino bare metal:

- Verifica dei prerequisiti di ripristino bare metal
- Acquisizione dell'indirizzo IP del computer di destinazione con Live CD
- (Facoltativo) Ripristino dei dati nel volume iSCSI del computer di destinazione
- (Facoltativo) Ripristino dei dati dal volume iSCSI nel computer di destinazione
- Verifica del server di backup
- Definizione dei punti di ripristino
- Definizione dei dettagli relativi al computer di destinazione
- Definizione delle impostazioni avanzate
- (Facoltativo) Gestione di pre/post script per l'automazione
- Creazione ed esecuzione del processo di ripristino
- (Facoltativo) Esecuzione di operazioni successive al ripristino bare metal
- Verifica del ripristino del computer di destinazione

Creazione di un modello di configurazione tramite la riga di comando

Creare un file di configurazione in modo che il comando d2bmr possa ripristinare i computer virtuali sulla base dei parametri specificati nel file. Il file d2dbmr raccoglie tutte le specifiche dal file ed esegue il ripristino in base a tali specifiche. Il comando d2dbmr viene utilizzato per eseguire il ripristino bare metal dalla riga di comando.

Sintassi

d2dbmr --createtemplate=[save path]

L'utilità d2dutil --encrypt crittografa la password e fornisce una password crittografata. È necessario utilizzare questa utilità per crittografare tutte le password. Se si utilizza il parametro --pwdfile=pwdfilepath, occorre crittografare la password. È possibile utilizzare l'utilità con uno dei metodi seguenti:

Metodo 1

```
echo 'string' | ./d2dutil --encrypt
```

string corrisponde alla password specificata.

Metodo 2

Immettere il comando d2dutil –encrypt, quindi specificare la password. Premere Invio: il risultato verrà visualizzato sulla schermata. In questo metodo, la password immessa non viene visualizzata nella schermata.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Creare il modello di configurazione utilizzando il seguente comando:

   ```
   d2dbmr --createtemplate=[save path]
   ```

   [save path] indica la posizione in cui viene creato il modello di configurazione.
3. Aprire il modello di configurazione e aggiornare i seguenti parametri:

   job_name

   Specifica il nome del processo di ripristino.

   storage_location_type

   Specifica il tipo di posizione di archiviazione della sessione. La posizione di archiviazione può essere CIFS, NFS o RPS.

   storage_location

Specifica la posizione del server di archiviazione della sessione. La posizione di archiviazione può essere CIFS o NFS.

storage_username

Specifica il nome utente quando si utilizza CIFS come posizione di archiviazione.

storage_password

Specifica la password quando si utilizza CIFS come posizione di archiviazione. La password viene crittografata mediante l'utilità di crittografia d2dutil.

rps_server

Specifica il nome del Recovery Point Server quando il valore di **storage_location_type** è RPS.

rps_server_username

Specifica il nome utente del Recovery Point Server quando il valore di **storage_location_type** è RPS.

rps_server_password

Specifica la password del Recovery Point Server quando il valore di **storage_location_type** è RPS. La password viene crittografata mediante l'utilità di crittografia d2dutil.

rps_server_protocol

Specifica il protocollo del Recovery Point Server quando il valore di **storage_location_type** è RPS.

rps_server_port

Specifica la porta del Recovery Point Server quando il valore di **storage_location_type** è RPS.

rps_server_datastore

Specifica il nome dell'archivio dati del Recovery Point Server quando il valore di **storage_location_type** è RPS.

encryption_password

Specifica la password di crittografia della sessione. La password viene crittografata mediante l'utilità di crittografia d2dutil.

source_node

Specifica il nome del nodo dell'origine il cui punto di ripristino viene utilizzato per il ripristino.

recovery_point

Selezionare la sessione da ripristinare. Generalmente, una sessione di ripristino presenta il formato seguente: S00000000X, dove X è un valore numerico. Se si desidera ripristinare la sessione più recente, specificare la parola chiave 'last'.

exclude_volumes

Specifica i volumi da escludere per il computer virtuale di destinazione.

Non escludere il volume '/'. Utilizzare ':' per separare più volumi.

include_volumes

Specifica i volumi da includere per il computer virtuale di destinazione.

Includere i volumi seguenti: / , /boot , /boot/efi , /home , /usr , /usr/local. Utilizzare ':' per separare più volumi.

restore_target

Specificare l'indirizzo MAC/IP di destinazione del ripristino.

guest_hostname

Specifica il nome host che si desidera fornire dopo il ripristino del computer virtuale.

guest_network

Specifica il tipo di rete che si desidera configurare. La rete può essere DHCP o statica.

guest_ip

Specifica l'indirizzo IP quando si specifica l'IP statico.

guest_netmask

Specifica la maschera di rete quando si specifica l'IP statico.

guest_gateway

Specifica l'indirizzo gateway quando si specifica l'IP statico.

guest_dns

Specifica l'indirizzo DNS quando si specifica l'IP statico.

guest_reboot

(Facoltativo) Specifica se il computer virtuale di destinazione deve essere riavviato dopo il ripristino. I valori sono Sì e No.

Valore predefinito: No

guest_reset_username

(Facoltativo) Specifica il ripristino della password sul valore fornito nel parametro guest_reset_password.

guest_reset_password

(Facoltativo) Specifica il ripristino della password sul valore specificato. La password viene crittografata mediante l'utilità di crittografia d2dutil.

enable_instant_restore

(Facoltativo) Specifica di abilitare il ripristino immediato. I valori sono Sì e No.

auto_restore_data

(Facoltativo) Specifica di ripristinare i dati automaticamente. I valori sono Sì e No.

script_pre_job_server

(Facoltativo) Specifica lo script da eseguire prima dell'esecuzione del processo sul server.

script_post_job_server

(Facoltativo) Specifica lo script da eseguire dopo l'esecuzione del processo sul server.

script_pre_job_client

(Facoltativo) Specifica lo script da eseguire prima dell'esecuzione del processo sul client.

script_post_job_client

(Facoltativo) Specifica lo script da eseguire dopo l'esecuzione del processo sul client.

script_ready_to_use

(Facoltativo) Specifica lo script da eseguire quando il computer di destinazione è pronto per l'uso e il valore del parametro **enable_instant_restore** è Sì.

force

Specifica se forzare il ripristino del computer virtuale. I valori sono Sì e No.

Valore predefinito: No

4. Salvare e chiudere il modello di configurazione.

   Il modello di configurazione è stato creato correttamente.

5. Inviare un processo tramite il modello d2dbmr utilizzando il seguente comando:

   ./d2dbmr –template=cfg_file_path [--wait]

Nota: Lo switch --wait consente di tornare all'ambiente della shell al termine del processo di ripristino. Se lo switch --wait non è disponibile, tornare immediatamente all'ambiente della shell dopo avere inviato il processo.

Il processo di ripristino viene inoltrato.

Verifica dei prerequisiti di ripristino bare metal

Considerare i seguenti prerequisiti prima di eseguire un ripristino bare metal:

- Si dispone di un punto di ripristino valido e della password di crittografia per il ripristino.
- Si dispone di un computer di destinazione valido per il ripristino bare metal.
- È stato creato Live CD dell'Agente Arcserve UDP (Linux).
- Se si desidera eseguire il ripristino bare metal con l'indirizzo IP, è necessario acquisire l'indirizzo IP del computer di destinazione utilizzando Live CD.
- Se si desidera eseguire il ripristino bare metal PXE con l'indirizzo MAC, è necessario acquisire l'indirizzo MAC del computer di destinazione.
- Se la destinazione di un processo di backup corrisponde all'origine locale, per eseguire un processo di ripristino bare metal dalla destinazione, è necessario esportare la destinazione dell'origine locale tramite NFS o CIFS e specificare il punto di ripristino come disponibile nella condivisione NFS o CIFS.
- È necessario che il punto di ripristino sia creato dal backup basato sull'agente di Linux.
- Il nodo di destinazione e il nodo di origine devono avere le stesse configurazioni firmware. Ad esempio, se si configura il nodo di origine con il firmware BIOS, è necessario configurare il nodo di destinazione solo con il firmware BIOS.
- Esaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Acquisizione dell'indirizzo IP del computer di destinazione con Live CD

Prima di eseguire un ripristino bare metal mediante l'indirizzo IP, è necessario acquisire tale indirizzo del computer di destinazione. Un computer bare metal non è inizialmente associato a nessun indirizzo IP. Pertanto è necessario avviare il computer bare metal mediante il Live CD predefinito, che è il Live CD dell'Agente Arcserve UDP (Linux) o quello basato su CentOS, per ottenere l'indirizzo IP. Dopo aver acquisito l'indirizzo IP del computer di destinazione, è possibile configurarne l'IP statico.

Effettuare le operazioni seguenti:

1. Inserire il Live CD o montare il file .iso del Live CD nell'unità CD-ROM del nodo di destinazione.
2. Avviare il computer di destinazione dal CD-ROM.

   Il computer di destinazione viene avviato nell'ambiente Live CD dell'Agente Arcserve UDP (Linux). Verrà visualizzato l'indirizzo IP del computer di destinazione.

3. Per configurare l'IP statico del computer di destinazione utilizzando il Live CD predefinito, attenersi alla procedura seguente:
   a. Sulla schermata del computer di destinazione, premere Invio per entrare nell'ambiente shell.
   b. Eseguire il comando seguente per configurare l'IP statico:

      ```
      ifconfig <NIC name>  <static IP address> netmask <net-
      mask>
      ```

      ```
      route add default  gw  <gateway IP address> <NIC name>
      ```

      Nota: il nome della scheda di interfaccia di rete (NIC) dipende dall'hardware. Ad esempio, eth0 o em0 sono nomi tipici della scheda NIC.

4. Per configurare l'IP statico del computer di destinazione utilizzando il Live CD basato su CentOS, attenersi alla procedura seguente:
   a. Aprire una finestra del terminale sul computer di destinazione facendo clic su Applicazioni, Strumenti di sistema, Terminale.
   b. Eseguire i comandi seguenti:

      ```
      sudo ifconfig <NIC name>  <static IP address> netmask
      <netmask>
      ```

      ```
      sudo route add default  gw  <gateway IP address> <NIC name>
      ```

Nota: il nome della scheda di interfaccia di rete (NIC) dipende dall'hardware. Ad esempio, eth0 o em0 sono nomi tipici della scheda NIC.

L'IP statico è stato configurato.

L'acquisizione dell'indirizzo IP del computer di destinazione è stata completata.

Importante: Annotare l'indirizzo IP in quanto verrà utilizzato nella **Procedura guidata di ripristino** in fase di indicazione dei dettagli relativi al computer di destinazione.

(Facoltativo) Ripristino dei dati nel volume iSCSI del computer di destinazione

È possibile integrare il volume iSCSI nel computer di destinazione e rendere quel volume parte del computer di destinazione. Quindi, è possibile ripristinare i dati nel volume iSCSI del computer di destinazione. In questo modo, è possibile gestire i dati e trasferirli su una rete.

Importante: Quando si integra il volume iSCSI nel computer di destinazione, tutti i dati esistenti nel volume iSCSI verranno persi.

Effettuare le operazioni seguenti:

1. Inserire il Live CD dell'Agente Arcserve UDP (Linux) o montare il file .iso del Live CD dell'Agente Arcserve UDP (Linux) nell'unità CD-ROM del nodo di destinazione.
2. Avviare il computer di destinazione dal CD-ROM.

   Il computer di destinazione viene avviato nell'ambiente Live CD dell'Agente Arcserve UDP (Linux). Verrà visualizzato l'indirizzo IP del computer di destinazione.
3. Accedere all'ambiente della shell del computer di destinazione.
4. Eseguire il comando seguente per avviare il daemon iniziatore di iSCSI:

   ```
   /etc/init.d/iscsid start
   ```
5. Eseguire uno script di rilevamento per rilevare l'host di destinazione di iSCSI.

   ```
   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>
   ```

   Il valore predefinito della porta dell'host di destinazione di iSCSI è 3260.

   ```
   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>
   ```
6. Prendere nota del nome completo iSCSI (IQN) dell'host di destinazione di iSCSI rilevato dallo script di rilevamento prima di accedere manualmente alla destinazione individuata.
7. Elencare la periferica a blocchi disponibile del nodo di destinazione.

   ```
   #fdisk -l
   ```

8. Accedere alla destinazione rilevata.

   ```
   iscsiadm -m node -T <iSCSI Target IQN name> -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number> -l
   ```

   È possibile visualizzare una periferica a blocchi nella directory /dev del nodo di destinazione.

9. Eseguire il comando seguente per ottenere il nuovo nodo della periferica:

   ```
   #fdisk –l
   ```

   È possibile visualizzare una periferica aggiuntiva chiamata /dev/sd<x> nel nodo di destinazione.

   Il volume iSCSI viene integrato nel volume di destinazione.

(Facoltativo) Ripristino dei dati dal volume iSCSI nel computer di destinazione

Se sono stati archiviati i dati in un volume di destinazione iSCSI, è possibile connettersi al volume iSCSI e ripristinare i dati. Il volume iSCSI consente di gestire i dati e di trasferirli su una rete.

Effettuare le operazioni seguenti:

1. Inserire il Live CD dell'Agente Arcserve UDP (Linux) o montare il file .iso del Live CD dell'Agente Arcserve UDP (Linux) nell'unità CD-ROM del nodo di destinazione.
2. Avviare il computer di destinazione dal CD-ROM.

   Il computer di destinazione viene avviato nell'ambiente Live CD dell'Agente Arcserve UDP (Linux). Verrà visualizzato l'indirizzo IP del computer di destinazione.
3. Accedere all'ambiente della shell del computer di destinazione.
4. Eseguire il comando seguente per avviare il daemon iniziatore di iSCSI:

   ```
   /etc/init.d/iscsid start
   ```
5. Eseguire uno script di rilevamento per rilevare l'host di destinazione di iSCSI.

   ```
   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>
   ```

   Il valore predefinito della porta dell'host di destinazione di iSCSI è 3260.
6. Prendere nota del nome completo iSCSI (IQN) dell'host di destinazione di iSCSI rilevato dallo script di rilevamento prima di accedere manualmente alla destinazione individuata.
7. Elencare la periferica a blocchi disponibile del nodo di destinazione.

   ```
   #fdisk -l
   ```
8. Accedere alla destinazione rilevata.

   ```
   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>
   ```

   È possibile visualizzare una periferica a blocchi nella directory /dev del nodo di destinazione.
9. Eseguire il comando seguente per ottenere il nuovo nome della periferica:

   ```
   #fdisk -l
   ```

È possibile visualizzare una periferica aggiuntiva chiamata /dev/sd<x> nel nodo di destinazione.

Ad esempio, supporre che il nome della periferica sia /dev/sdc. Tale nome della periferica viene utilizzato per creare una partizione e un file system nelle seguenti fasi.

10. Montare il volume iSCSI utilizzando i comandi seguenti:

```
# mkdir /iscsi
```

```
# mkdir /iscsi
```

Nota: Quando si specifica il percorso di sessione nella procedura guidata di ripristino, è necessario selezionare Locale e immette il percorso /iscsi.

Esempio: <path>/iscsi

Il computer di destinazione può connettersi ora al volume iSCSI e può ripristinare i dati in esso contenuti.

Verifica del server di backup

Quando si apre la **Procedura guidata di ripristino**, verificare il server di backup su cui si desidera eseguire l'operazione di ripristino.

Effettuare le operazioni seguenti:

1. Accedere alla procedura guidata di ripristino in uno dei modi seguenti:

   - Da Arcserve UDP:

   a. Fare clic sulla scheda **Risorse**.

   b. Selezionare **Tutti i nodi** nel riquadro sinistro.

      Tutti i nodi Online aggiunti vengono visualizzati nel riquadro centrale.

   c. Nel riquadro centrale, selezionare il nodo e fare clic su **Azioni**.

   d. Fare clic su **Ripristina** dal menu a discesa **Azioni**.

      Viene visualizzata l'interfaccia Web dell'Agente Arcserve UDP (Linux). La finestra di dialogo di selezione del tipo di ripristino viene visualizzata nell'interfaccia utente dell'agente.

   e. Selezionare il tipo di ripristino e fare clic su **OK**.

      Nota: si accede automaticamente al nodo agente e la **Procedura guidata di ripristino** viene visualizzata dal nodo agente.

   - Dall'Agente Arcserve UDP (Linux):

   a. Aprire l'interfaccia Web dell'Agente Arcserve UDP (Linux).

      Nota: durante l'installazione dell'Agente Arcserve UDP (Linux), l'URL per l'accesso e la gestione del server viene fornito all'utente. Accedere ad Agente Arcserve UDP (Linux)

   b. Fare clic su **Ripristino** dal menu **Procedura guidata** e selezionare **Ripristino bare metal (BMR)**.

   Viene visualizzata la pagina **Server di backup** della **Procedura guidata di ripristino - Ripristino bare metal**.

2. Verificare il server nell'elenco a discesa **Server di backup** nella pagina **Server di backup**.

   Non è possibile selezionare alcuna opzione dall'elenco a discesa **Server di backup**.

3. Fare clic su **Avanti**.

   Viene visualizzata la pagina **Punti di ripristino** della finestra di dialogo **Procedura guidata di ripristino - Ripristino bare metal**.

   Viene specificato il server di backup.

Definizione dei punti di ripristino

L'esecuzione di un backup implica la creazione di un punto di ripristino. Specificare le informazioni relative al punto di ripristino della **Procedura guidata di ripristino**, in modo da poter eseguire il ripristino dei dati desiderati. È possibile ripristinare file specifici o tutti i file in base alle proprie esigenze.

Importante: Per eseguire un ripristino bare metal da un punto di ripristino, il volume principale e il volume di avvio devono essere presenti nel punto di ripristino.

Effettuare le operazioni seguenti:

1. Eseguire una delle operazioni riportate di seguito in base all'archiviazione di backup utilizzata.

   - Eseguire le operazioni seguenti per accedere ai punti di ripristino archiviati su una periferica mobile:

   a. Avviare il computer di destinazione utilizzando Live CD.

   b. Accedere all'interfaccia Web dell'Agente Arcserve UDP (Linux) dal Live CD.

   c. Aprire la **procedura guidata di ripristino bare metal**.

   d. Accedere alla pagina **Punti di ripristino**.

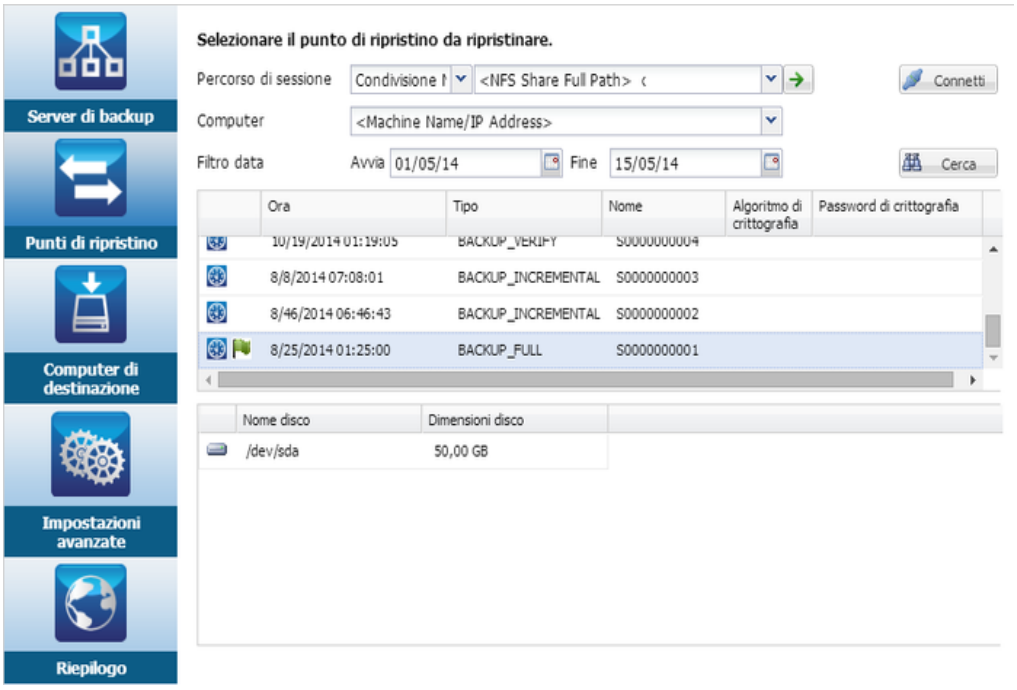
   e. Selezionare **Locale** come **Percorso di sessione** nella pagina **Punti di ripristino** della **procedura guidata di ripristino bare metal**.

   - Eseguire le operazioni seguenti se la posizione di sessione corrisponde a una condivisione NFS o CIFS:

   a. Selezionare una sessione dall'elenco a discesa **Percorso di sessione,** quindi specificare il percorso completo della condivisione.

      Ad esempio, si utilizza il percorso della sessione come condivisione NFD, xxx.xxx.xxx.xxx come indirizzo IP della condivisione NFS e la cartella viene denominata *Data.* Sarà necessario immettere xxx.xxx.xxx.xxx:/Data come percorso di condivisione NFS.

      Nota: se i dati di backup vengono archiviati nell'origine locale, sarà necessario convertire il nodo di origine in un server NFS, quindi condividere il percorso della sessione.



2. Fare clic su **Connetti.**

   Tutti i nodi di cui è stato eseguito il backup per il percorso specificato saranno contenuti nell'elenco a discesa **Computer.**

3. Selezionare il nodo di cui si desidera eseguire il ripristino dall'elenco a discesa **Computer.**

   Verrà creato un elenco contenente tutti i punti di ripristino per il nodo selezionato.

4. Applicare il filtro data per visualizzare i punti di ripristino generati tra le date specificate e fare clic su **Cerca**.

   Valore predefinito: ultime due settimane.

   Vengono visualizzati tutti i punti di ripristino disponibili tra le date specificate.

5. Selezionare il punto di ripristino desiderato.

6. Applicare le impostazioni di filtro del volume per il punto di ripristino selezionato e fare clic su **OK**.

   Vengono visualizzati tutti i volumi disponibili presenti sul nodo. È possibile includere o escludere i volumi in base alle proprie esigenze.

   Nota: non escludere i volumi seguenti: / , /boot, /boot/efi, /home, /usr, /usr/local.

7. Fare clic su **Avanti**.

   Verrà visualizzata la pagina **Computer di destinazione**.

   Il punto di ripristino viene specificato.

Definizione dei dettagli relativi al computer di destinazione

Specificare i dettagli relativi al computer di destinazione in modo che i dati vengano ripristinati su tale computer. Un computer di destinazione è un computer bare metal su cui verrà eseguito un ripristino bare metal. Se si esegue il ripristino mediante l'indirizzo IP, sarà necessario disporre dell'indirizzo IP del computer di destinazione registrato precedentemente all'inizio del processo. Se il ripristino viene eseguito mediante un indirizzo MAC, sarà necessario disporre di tale indirizzo per il computer di destinazione.

Effettuare le operazioni seguenti:

1. Immettere l'indirizzo MAC o IP del computer di destinazione nel campo **Indirizzo MAC/IP**.
2. Specificare un nome per il campo **Nome host**.

   Il computer di destinazione utilizzerà questo nome come nome host al completamento del processo di ripristino.

3. Selezionare una delle opzioni seguenti come rete:

   DHCP

   Configura automaticamente l'indirizzo IP. Questa è l'opzione predefinita. Utilizzare questa opzione se si desidera eseguire il ripristino di un server DHCP (Dynamic Host Configuration Protocol) su una rete DHCP.

   IP statico

   Configura manualmente l'indirizzo IP. Se si seleziona questa opzione, è necessario specificare l'**indirizzo IP**, la **subnet mask** e il **gateway predefinito** del computer di destinazione.

   Importante! Verificare che l'IP statico non sia in uso da altri computer durante il processo di ripristino.

4. (Facoltativo) Selezionare l'opzione **Abilita ripristino bare metal immediato** in modo da poter utilizzare istantaneamente il computer di destinazione.

   Quando si abilita questa opzione, l'Agente Arcserve UDP (Linux) recupera innanzitutto tutti i dati necessari per avviare il computer. Dopo aver avviato il computer di destinazione, i dati rimanenti vengono ripristinati. La connessione di rete deve essere costantemente disponibile durante il ripristino bare metal immediato.

Esempio: se si dispone di 100 GB di dati e si desidera eseguire un ripristino bare metal e *non* si seleziona questa opzione, prima verranno ripristinati tutti i 100 GB di dati, quindi sarà possibile utilizzare il computer di destinazione. Tuttavia, è necessario solo 1 GB di dati circa per avviare il computer. Quando si abilita questa opzione, viene ripristinato innanzitutto 1 GB di dati richiesti in modo che sia possibile avviare e utilizzare il computer. Dopo aver avviato il computer, i rimanenti 99 GB di dati vengono ripristinati automaticamente.

Nota: i dati necessari per avviare il computer dipendono dalla configurazione del sistema operativo. Inoltre, è possibile sospendere o riprendere il ripristino automatico dei dati se l'opzione **Non eseguire il recupero automatico dei dati dopo l'avvio del computer** non è selezionata.

5. (Facoltativo) Selezionare l'opzione **Non eseguire il recupero automatico dei dati dopo l'avvio del computer** per interrompere il ripristino automatico dei dati quando il computer di destinazione viene avviato.

   Quando si seleziona l'opzione **Abilita ripristino bare metal immediato**, il comportamento predefinito prevede innanzitutto il ripristino dei dati necessari e poi l'avvio del computer. Dopo aver avviato il computer, i dati rimanenti vengono ripristinati automaticamente. Se si aggiornano i dati di origine durante il ripristino e poi si seleziona questa opzione, i dati vengono recuperati fino al punto prima dell'aggiornamento.

6. Fare clic su **Avanti**.

   Viene visualizzata la pagina **Impostazioni avanzate**.

   Vengono specificati i dettagli relativi al computer di destinazione.

Definizione delle impostazioni avanzate

Specificare le impostazioni avanzate per eseguire un ripristino bare metal pianificato dei dati. Il ripristino bare metal pianificato garantisce che i dati vengano ripristinati all'ora specificata anche in caso di assenza dell'utente.

Effettuare le operazioni seguenti:

1. Impostare la data e l'ora di inizio selezionando una delle seguenti opzioni:

   Esegui ora

   Avvia il processo di ripristino dopo l'invio del processo.

   Imposta ora speciale

   Avvia il processo di ripristino all'ora specificata dopo l'invio del processo.

2. (Facoltativo) Selezionare uno script dall'opzione **Impostazioni script pre/post backup** per il server di backup e il computer di destinazione.

   Questi script eseguono comandi di script per le azioni da eseguire prima dell'inizio del processo e/o al completamento del processo.

   Nota: i campi **Impostazioni pre/post script** vengono popolati solamente se un file di script è già stato creato e collocato nel percorso seguente:

   `/opt/Arcserve/d2dserver/usr/prepost`

   Nota: per ulteriori informazioni sulla creazione di pre/post script, consultare la sezione *Gestione di pre/post script per l'automazione*.

3. (Facoltativo) Fare clic su **Mostra altre impostazioni** per visualizzare ulteriori impostazioni relative al ripristino bare metal.

4. (Facoltativo) Reimpostare la password per il nome utente specificato per il computer di destinazione di cui è stato eseguito il recupero.

5. (Facoltativo) Immettere il percorso completo del percorso di archiviazione di backup dei punti di ripristino in **Accesso locale al punto di ripristino**.

6. (Facoltativo) Immettere il nome completo del disco nel campo **Dischi** per escludere tali dischi sul computer di destinazione dal processo di recupero.

7. (Facoltativo) Selezionare l'opzione **Abilita riattivazione LAN** se viene eseguito un ripristino bare metal basato su PXE (Preboot Execution Environment).

   Nota: l'opzione **Abilita riattivazione LAN** è applicabile solamente ai computer fisici. Assicurarsi di avere abilitato le impostazioni di riattivazione LAN nelle impostazioni BIOS del computer fisico.

8. (Facoltativo) Selezionare l'opzione di **riavvio** per riavviare automaticamente il nodo di destinazione al completamento del processo di ripristino bare metal.
9. Fare clic su **Avanti**.

   Viene visualizzata la pagina **Riepilogo**.

   Vengono specificate le impostazioni avanzate.

   La presente sezione descrive i seguenti argomenti:

   - (Facoltativo) Gestione di pre/post script per l'automazione

(Facoltativo) Gestione di pre/post script per l'automazione

Gli script di pre/post esecuzione consentono di eseguire regole di business in fasi specifiche di un processo in esecuzione. È possibile specificare quando eseguire gli script nelle **Impostazioni pre/post script** della **Procedura guidata di backup** e della **Procedura guidata di ripristino** dell'interfaccia utente. È possibile eseguire gli script sul server di backup in base alle impostazioni dell'utente.

La gestione del pre/post script è un processo costituito da due passaggi: la creazione del pre/post script e la sua collocazione nella cartella prepost.

Creazione di pre/post script

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Creare un file di script mediante le variabili di ambiente nel linguaggio di scripting preferito.

   Variabili di ambiente del pre/post script

   Per creare lo script, utilizzare le variabili di ambiente seguenti:

   D2D_JOBNAME

   Indica il nome del processo.

   D2D_JOBID

   Identifica l'ID del processo. L'ID di processo è un numero attribuito al processo durante la sua esecuzione. Se si esegue lo stesso processo nuovamente, verrà fornito un nuovo numero di processo.

   D2D_TARGETNODE

   Identifica il nodo di cui viene eseguito il backup o il ripristino.

   D2D_JOBTYPE

   Identifica il tipo di processo in esecuzione. I valori seguenti identificano la variabile D2D_JOBTYPE:

   backup.full

   Identifica il processo come backup completo.

   backup.incremental

   Identifica il processo come backup incrementale.

   backup.verify

Identifica il processo come backup di verifica.

restore.bmr

Identifica il processo come ripristino bare metal (BMR). Si tratta di un processo di ripristino.

restore.file

Identifica il processo come ripristino a livello di file. Si tratta di un processo di ripristino.

D2D_SESSIONLOCATION

Identifica la posizione in cui vengono archiviati i punti di ripristino.

D2D_PREPOST_OUTPUT

Identifica un file temp. Il contenuto della prima linea del file temp viene visualizzato nel registro attività.

D2D_JOBSTAGE

Indica la fase del processo. I valori seguenti identificano la variabile D2D_ JOBSTAGE:

pre-job-server

Identifica lo script eseguito sul server di backup prima dell'avvio del processo.

post-job-server

Identifica lo script eseguito sul server di backup dopo il completamento del processo.

pre-job-target

Identifica lo script eseguito sul computer di destinazione dopo l'avvio del processo.

post-job-target

Identifica lo script eseguito sul computer di destinazione dopo il completamento del processo.

pre-snapshot

Identifica lo script eseguito sul computer di destinazione prima dell'acquisizione della snapshot.

post-snapshot

Identifica lo script eseguito sul computer di destinazione dopo l'acquisizione della snapshot.

D2D_TARGETVOLUME

Identifica il volume di cui viene eseguito il backup durante un processo di backup. Questa variabile è adatta per gli script di snapshot di pre/post automazione per un processo di backup.

D2D_JOBRESULT

Identifica il risultato di uno script del processo di post-esecuzione. I valori seguenti identificano la variabile di D2D_JOBRESULT:

success

Identifica il risultato come corretto.

fail

Identifica il risultato come non corretto.

D2DSVR_HOME

Identifica la cartella in cui è installato il server di backup. È possibile applicare la variabile agli script in esecuzione sul server di backup.

Lo script viene creato.

Nota: per tutti gli script, un valore restituito pari a zero indica un'operazione riuscita, mentre un valore restituito diverso da zero indica la presenza di un errore.

Collocare lo script nella cartella prepost ed eseguire la verifica

Tutti gli script di pre/post per un server di backup sono gestiti centralmente dalla cartella prepost nella posizione seguente:

```
/opt/Arcserve/d2dserver/usr/prepost
```

Effettuare le operazioni seguenti:

1. Collocare il file nella posizione seguente del server di backup:

   ```
   /opt/Arcserve/d2dserver/usr/prepost
   ```

2. Fornire le autorizzazioni di esecuzione per il file di script.
3. Accedere all'interfaccia Web dell'Agente Arcserve UDP (Linux).
4. Aprire la procedura guidata di **backup** o **ripristino** ed accedere alla scheda **Impostazioni avanzate**.
5. Selezionare il file di script nell'elenco del menu a discesa **Impostazioni di pre/post script**, quindi inviare il processo.
6. Fare clic sul **Registro attività** e verificare che lo script venga eseguito per il processo

di backup specificato.

Lo script viene eseguito.

I pre/post script vengono creati correttamente e inseriti nella cartella prevista.

Creazione ed esecuzione del processo di ripristino

Creare e eseguire il processo di ripristino in modo da poter avviare il processo di ripristino bare metal. Prima di eseguire un ripristino bare metal, verificare le informazioni relative al punto di ripristino. Se necessario, è possibile tornare indietro e modificare le impostazioni di ripristino.

Effettuare le operazioni seguenti:

1. Verificare i dettagli relativi al ripristino nella pagina **Riepilogo** della **Procedura guidata di ripristino**.
2. (Facoltativo) Fare clic su **Indietro** per modificare le impostazioni di ripristino da una qualsiasi delle pagine della **Procedura guidata di ripristino**.
3. Immettere un nome per il del processo e fare clic su **Invia**.

   Il campo **Nome processo** è associato a un nome predefinito. È possibile specificare un nuovo nome per il processo ma non è possibile lasciare il campo vuoto.

   La **Procedura guidata di ripristino** viene chiusa. È possibile visualizzare il processo nella scheda **Stato processo.** Se si utilizza l'indirizzo IP per il ripristino bare metal, il computer di destinazione verrà riavviato automaticamente sullo stesso sistema operativo dell'origine di backup al completamento del processo di ripristino bare metal.

   Se si utilizza l'indirizzo MAC per il ripristino bare metal, lo stato della scheda **Stato processo** verrà modificato in *In attesa dell'avvio del nodo di destinazione*.
4. (Facoltativo) Affinché il ripristino bare metal utilizzi l'indirizzo MAC, avviare il computer di destinazione se viene visualizzato il messaggio *In attesa dell'avvio del nodo di destinazione nella scheda* della scheda **Stato processo**.

   Nota: se il computer di destinazione viene avviato prima dell'invio del processo di ripristino, sarà necessario riavviare il computer di destinazione. Verificare che BIOS sia configurato per l'avvio dalla rete.

   Lo stato della colonna **Stato processo** viene modificato in **Ripristino del volume in corso**. Ciò indica che il ripristino è in corso. Al completamento del processo di ripristino, il computer di destinazione verrà riavviato automaticamente con lo stesso sistema operativo dell'origine di backup.

   Il processo di ripristino viene creato ed eseguito correttamente.

   La presente sezione descrive i seguenti argomenti:

   - (Facoltativo) Esecuzione di operazioni successive al ripristino bare metal

(Facoltativo) Esecuzione di operazioni successive al ripristino bare metal

Gli argomenti riportati di seguito fanno riferimento a impostazioni di configurazione facoltative che possono essere eseguite dopo il ripristino bare metal:

Configurazione di X Windows

In caso di ripristino bare metal su hardware diversi, il sistema X Windows del sistema operativo ripristinato non funziona correttamente, pertanto il nodo di destinazione mostra una finestra di dialogo di errore. La finestra di dialogo di errore viene visualizzata a causa della modifica della configurazione di visualizzazione. Per risolvere questo errore, attenersi alle istruzioni riportate nella finestra dialogo di errore per configurare la scheda grafica. Una volta completate tali operazioni, sarà possibile visualizzare l'interfaccia utente X Windows e il desktop.

Configurazione del nome completo di dominio del sistema (FQDN)

Per utilizzare un FQDN, configurare l'FQDN. Il processo di ripristino bare metal non esegue la configurazione automatica dell'FQDN.

Numero massimo di caratteri per FQDN: 63

Attenersi alla procedura seguente per configurare l'FQDN:

1. Modificare il file */etc/hosts* e specificare l'indirizzo IP, il nome FQDN e il nome del server.

   ```
   #vi /etc/hosts

   ip_of_system  servername.domainname.com  servername
   ```

2. Riavviare il servizio di rete.

   ```
   #/etc/init.d/network restart
   ```

3. Verificare il nome host e il nome FQDN.

   ```
   #hostname

   servername

   #hostname -f

   servername.domainname.com
   ```

L'FQDN è stato configurato.

Estensione del volume di dati in seguito al ripristino bare metal su dischi diversi

Se si esegue il ripristino bare metal su un disco di maggiori dimensioni rispetto al disco sul nodo originale, lo spazio su disco non verrà utilizzato completamente. L'operazione di ripristino bare metal non elabora automaticamente lo spazio su disco inutilizzato. È possibile formattare lo spazio su disco su una partizione separata oppure ridimensionare la partizione esistente con lo spazio su disco inutilizzato. Il volume che si desidera ridimensionare deve essere inutilizzato. Si consiglia quindi di non eseguire il ridimensionamento di un volume di sistema. La presente sezione descrive la procedura di estensione di un volume di dati con spazio su disco inutilizzato.

Nota: per evitare la perdita di dati, ridimensionare i volumi immediatamente dopo il ripristino bare metal. Inoltre, è possibile eseguire il backup del nodo prima di avviare il ridimensionamento del volume.

In seguito al corretto riavvio del computer di destinazione dopo il ripristino bare metal, è possibile eseguire l'estensione del volume di dati.

Volume di partizione raw

Ad esempio, il ripristino di un disco da 2GB nella sessione viene eseguito su un disco da 16GB denominato */dev/sdb* con una partizione. La partizione raw */dev/sdb1* viene montata direttamente nella directory */data.*

Questo esempio viene utilizzato per descrivere la procedura di estensione di un volume di partizione raw.

Effettuare le operazioni seguenti:

1. Verificare lo stato del volume /dev/sdb1.

```
# df –h /dev/sdb1
/dev/sdb1              2.0G   40M  1.9G   3% /data
```

2. Smontare il volume /dev/sdb1.

```
# umount /data
```

3. Ridimensionare /dev/sdb1 per occupare tutto lo spazio su disco utilizzando il comando fdisk.

   Per eseguire questa operazione, eliminare la partizione esistente e ricrearla utilizzando lo stesso numero di settore di inizio. L'utilizzo dello stesso numero di settore di inizio consente di evitare la perdita di dati.

```
# fdisk -u /dev/sdb
Command (m for help): p
```

```
Disk /dev/sdb: 17.1 GB, 17179869184 bytes

255 heads, 63 sectors/track, 2088 cylinders, total
33554432 sectors

Units = sectors of 1 * 512 = 512 bytes

Device Boot      Start         End      Blocks   Id
System

/dev/sdb1              63     4192964     2096451
83  Linux

Command (m for help): d

Selected partition 1

Command (m for help): n

Command action

e   extended

p   primary partition (1-4)

p

Partition number (1-4): 1

First sector (63-33554431, default 63):

Using default value 63

Last sector or +size or +sizeM or +sizeK (63-
33554431, default 33554431):

Using default value 33554431

Command (m for help): p

Disk /dev/sdb: 17.1 GB, 17179869184 bytes

255 heads, 63 sectors/track, 2088 cylinders, total
33554432 sectors

Units = sectors of 1 * 512 = 512 bytes

Device Boot      Start         End      Blocks   Id
System

/dev/sdb1              63    33554431    16777184+
83  Linux

Command (m for help): w
```

La partizione adotta lo stesso numero di settore di inizio della partizione originale e il numero di settore di fine è 33554431.

4. Ridimensionare il volume utilizzando il comando resize2fs. Se necessario, eseguire prima il comando e2fsck.

```
# e2fsck -f /dev/sdb1

# resize2fs /dev/sdb1
```

5. Montare il volume sul punto di montaggio e verificare nuovamente lo stato del volume.

```
# mount /dev/sdb1 /data

# df –h /dev/sdb1

/dev/sdb1              16G    43M    16G    1% /data
```

Il volume viene esteso a 16 GB ed è pronto per essere utilizzato.

Volume LVM:

Ad esempio, il ripristino di un disco da 8GB nella sessione viene eseguito su un disco da 16GB denominato */dev/sdb* con una partizione. La partizione raw */dev/sdc1* viene utilizzata come unico volume fisico del volume logic LVM */dev/mapper/VGTest-LVTest* con punto di montaggio */lvm*.

Questo esempio viene utilizzato per descrivere la procedura di estensione di un volume di partizione LVM.

Effettuare le operazioni seguenti:

1. Selezionare lo stato del volume /dev/mapper/VGTest-LVTest.

```
# lvdisplay –m /dev/mapper/VGTest-LVTest

# mount /dev/sdb1 /data

--- Logical volume ---

LV Name                /dev/VGTest/LVTest

VG Name                VGTest

LV UUID                udoBIx-XKBS-1Wky-3FVQ-mxMf-
FayO-tpfPl8

LV Write Access        read/write

LV Status              available
```

```
# open                 1
LV Size                7.88 GB
Current LE             2018
Segments               1
Allocation             inherit
Read ahead sectors     0
Block device           253:2
---Segments---
Logical extent 0 to 2017:
Type                 linear
Physical volume      /dev/sdc1
Physical extents     0 to 2017
```

Il volume fisico è */dev/sdc1*, il gruppo di volume è *VGTest* e il volume logico è */dev/VGTest/LVTest oppure /dev/mapper/VGTest-LVTest*.

2. Smontaggio del volume /dev/mapper/VGTest-LVTest.

   ```
   # umount /lvm
   ```

3. Disabilitare il gruppo di volume in cui risiede il volume fisico /dev/sdc1.

   ```
   # vgchange -a n VGTest
   ```

4. Creare una partizione per occupare lo spazio su disco inutilizzato mediante il comando fdisk.

   ```
   # fdisk -u /dev/sdc

   Command (m for help): pDisk /dev/sdc: 17.1 GB,
   17179869184 bytes

   255 heads, 63 sectors/track, 2088 cylinders, total
   33554432 sectors

   Units = sectors of 1 * 512 = 512 bytes

   Device Boot      Start         End      Blocks   Id
   System
   ```

```
/dev/sdc1              63    16777215     8388576+
83  Linux

Command (m for help): n

Command actione   extended

p   primary partition (1-4)

p

Partition number (2-4): 1

First sector (16777216-33554431, default 16777216):

Using default value 16777216

Last sector or +size or +sizeM or +sizeK (16777216-
33554431, default 33554431):

Using default value 33554431

Command (m for help): p

Disk /dev/sdc: 17.1 GB, 17179869184 bytes

255 heads, 63 sectors/track, 2088 cylinders, total
33554432 sectors

Units = sectors of 1 * 512 = 512 bytes

Device Boot      Start         End      Blocks   Id
System

/dev/sdc1              63    16777215     8388576+
83  Linux

/dev/sdc2        16777216    33554431     8388608
83  Linux

Command (m for help): w
```

La partizione /dev/sdc2 viene creata.

5. Creare un nuovo volume fisico.

```
# pvcreate /dev/sdc2
```

6. Estendere le dimensioni di gruppo del volume.

```
# vgextend VGTest /dev/sdc2
```

7. Abilitare il gruppo di volume disabilitato.

```
# vgchange -a y VGTest
```

8. Estendere le dimensioni del volume logico utilizzando il comando lvextend.

```
# vgchange -a y VGTest# lvextend -L +8G /dev/VGTest/LVTest
```

9. Ridimensionare il volume utilizzando il comando resize2fs. Se necessario, eseguire prima il comando e2fsck.

```
# e2fsck -f /dev/mapper/VGTest-LVTest

# resize2fs /dev/mapper/VGTest-LVTest
```

10. Montare il volume sul punto di montaggio e verificare nuovamente lo stato del volume.

```
# mount /dev/mapper/VGTest-LVTest /lvm

# lvdisplay -m /dev/mapper/VGTest-LVTest

---Logical volume---

LV Name                /dev/VGTest/LVTest

VG Name                VGTest

LV UUID                GTP0a1-kUL7-WUL8-bpbM-9eTR-SVzl-WgA11h

LV Write Access        read/write

LV Status              available

# open                 0

LV Size                15.88 GB

Current LE             4066

Segments               2

Allocation             inherit

Read ahead sectors     0

Block device           253:2

--- Segments ---

Logical extent 0 to 2046:

Type                linear

Physical volume     /dev/sdc1
```

```
Physical extents    0 to 2046

Logical extent 2047 to 4065:

Type                linear

Physical volume     /dev/sdc2

Physical extents    0 to 2018
```

Il volume LVM viene esteso a 16 GB ed è pronto per essere utilizzato.

Verifica del ripristino del nodo di destinazione

Al completamento del processo di ripristino, verificare che il nodo di destinazione sia stato ripristinato e contenga i dati rilevanti.

Effettuare le operazioni seguenti:

1. Accedere al computer di destinazione di cui è stato eseguito il ripristino.
2. Verificare che il computer di destinazione contenga tutte le informazioni di cui è stato eseguito il backup.

   La verifica del computer di destinazione viene eseguita correttamente.

   Il ripristino bare metal è stato eseguito correttamente per i computer Linux.

Esecuzione di un ripristino bare metal per computer Linux in AWS Cloud

Un ripristino bare metal esegue il ripristino del sistema operativo e delle applicazioni software, ed esegue il recupero di tutti i dati sottoposti a backup. Il ripristino bare metal consiste nel ripristino di un sistema del computer avviato a partire da un sistema *bare metal*. Bare metal è un computer senza sistema operativo, driver e applicazioni software. Al completamento del ripristino, il computer di destinazione viene riavviato automaticamente sullo stesso ambiente operativo del nodo di origine del backup e tutti i dati vengono ripristinati.

È possibile eseguire un ripristino bare metal completo poiché quando si esegue un backup di dati, esso acquisisce anche informazioni relative al sistema operativo, alle applicazioni installate, ai driver e così via.

È possibile eseguire un ripristino bare metal utilizzando l'indirizzo IP dell'istanza Linux di destinazione in Amazon EC2. Se si avvia l'istanza Linux di destinazione tramite l'agente Arcserve UDP (Linux) AMI, è possibile ottenere l'indirizzo IP privato dell'istanza.

Il processo per l'esecuzione di un ripristino bare metal per le istanze Linux in Amazon EC2 è praticamente uguale a quello dei computer Linux in locale.

Completare le attività seguenti per eseguire un ripristino bare metal:

- Verifica dei prerequisiti di ripristino bare metal
- Avvio di un'istanza tramite Live CD dell'agente Arcserve UDP
- Revisione dell'istanza del server di backup
- Definizione dei punti di ripristino
- Definizione dei dettagli relativi all'istanza di destinazione
- Definizione delle impostazioni avanzate
- Creazione ed esecuzione del processo di ripristino
- Verifica del ripristino dell'istanza di destinazione

Verifica dei prerequisiti di ripristino bare metal

Prima di eseguire un ripristino bare metal per le istanze Linux in Amazon EC2, tenere presenti le seguenti opzioni:

- Si dispone di un punto di ripristino valido e della password di crittografia per il ripristino.
- Se la destinazione di un processo di backup corrisponde all'origine locale, per eseguire un processo di ripristino bare metal dalla destinazione, è necessario esportare la destinazione dell'origine locale tramite NFS o CIFS e specificare il punto di ripristino come disponibile nella condivisione NFS o CIFS.
- È necessario che il punto di ripristino sia creato dal backup basato su agente Linux.
- Si dispone di un agente Arcserve UDP per l’istanza Linux in Amazon EC2.
- Esaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Avvio di un'istanza tramite Live CD dell'agente Arcserve UDP

Prima di eseguire un ripristino bare metal per le istanze Linux in Amazon EC2, è necessario avviare l'istanza di destinazione di ripristino bare metal tramite Live CD dell'agente Arcserve UDP. Quando l'istanza di ripristino bare metal di destinazione è pronta, è possibile ottenere l'indirizzo IP dell'istanza ed eseguire un processo di ripristino bare metal con l'indirizzo IP.

Effettuare le operazioni seguenti:

1. Accedere alla console di gestione EC2 con il proprio account e selezionare**Avvia istanza**.
2. Selezionare Amazon Machine Image (AMI) nelle AMI della community.

   È possibile eseguire ricerche di AMI con Live CD tramite *Arcserve_UDP_Agent_Linux-LiveCD*nelle AMI della community.

   Note:

   - Se PVM corrisponde al nodo di origine di backup che si desidera ripristinare, selezionare l'AMI Arcserve_UDP_Agent_Linux-LiveCD-PVM-UDP$version per avviare l'istanza.
   - Se HVM o un altro computer di destinazione è il nodo di origine di backup che si desidera ripristinare, selezionare l'AMI Arcserve_UDP_Agent_Linux-LiveCD-HVM-UDP$version per avviare l'istanza.
   - Arcserve_UDP_Agent_Linux-LiveCD-PVM-UDP7.1 è applicabile a UDP 8.0.
   - Arcserve_UDP_Agent_Linux-LiveCD-HVM-UDP7.2
   - Arcserve_UDP_Agent_Linux-LiveCD-HVM-UDP8.0
   - Arcserve_UDP_Agent_Linux-LiveCD-HVM-UDP8.1
   - Arcserve_UDP_Agent_Linux-LiveCD-HVM-UDP9.0
3. Dalla procedura guidata di avvio dell'istanza, selezionare il tipo di istanza desiderato.
4. Configurare i dettagli dell'istanza con l'avvio di altre istanze. Ad esempio, includere la rete, la subnet, l'IP pubblico di assegnazione automatica e così via.
5. Aggiungere l'archiviazione per l'istanza attenendosi alla seguente procedura:
   a. Ottenere le informazioni sul disco, compreso il numero del disco e le dimensioni del disco del nodo di origine di backup di cui si desidera eseguire il ripristino. È possibile ottenere le informazioni relative al disco con la selezione del

punto di ripristino nella procedura guidata di ripristino per l'esecuzione di un processo di ripristino bare metal.

b. Estendere la dimensione del volume principale in modo che corrisponda alle dimensioni del disco principale del nodo di origine di backup. È possibile aggiungere altri dischi se il nodo di origine di backup dispone di più dischi.

6. Aggiungere i tag per l'istanza di destinazione del ripristino bare metal.
7. Configurare il gruppo di protezione per l'istanza di destinazione di ripristino bare metal attenendosi alle seguenti procedure:
   a. Creare un nuovo gruppo di protezione per il tipo SSH.
   b. Per rendere l'istanza di destinazione di ripristino bare metal più sicura, selezionare la modalità **Personalizzata** per l'origine che determina il traffico in modo da raggiungere l'istanza di destinazione di ripristino bare metal nella nuova regola creata. Specificare l'origine personalizzata con il formato CIDR in modo che l'istanza di destinazione del ripristino bare metal sia accessibile all'agente Arcserve UDP per il server Linux ma non sia accessibile agli altri computer Internet.

      Ad esempio, se l'indirizzo IP dell'agente Arcserve UDP per il server Linux è 172.31.X.X, specificare l'origine come 172.31.0.0/16 o 172.0.0.0/8.
8. Esaminare i dettagli dell'istanza, quindi fare clic su **Avvia**.

   Viene selezionata la finestra di dialogo di **selezione di una coppia di chiavi esistente o di creazione di una nuova coppia**.
9. Dalla finestra di dialogo, selezionare l'opzione **Procedere senza una coppia di chiavi** e fare clic su **Avvia istanze**.
10. Quando l'istanza di destinazione di ripristino bare metal è pronta all'uso, acquisire l'indirizzo IP privato nella descrizione dell'istanza.

    L'acquisizione dell'indirizzo IP del computer di destinazione è stata completata.

    Importante: Annotare l'indirizzo IP in quanto verrà utilizzato nella **Procedura guidata di ripristino** in fase di indicazione dei dettagli relativi all'istanza di destinazione di ripristino bare metal.

Revisione dell'istanza del server di backup

Quando si apre la **Procedura guidata di ripristino**, verificare l'istanza del server di backup su cui si desidera eseguire l'operazione di ripristino.

Effettuare le operazioni seguenti:

1. Accedere alla procedura guidata di ripristino in uno dei modi seguenti:

   - Da Arcserve UDP:

   a. Fare clic sulla scheda **Risorse**.

   b. Selezionare **Tutti i nodi** nel riquadro sinistro.

      Tutti i nodi Online aggiunti vengono visualizzati nel riquadro centrale.

   c. Nel riquadro centrale, selezionare il nodo e fare clic su **Azioni**.

   d. Fare clic su **Ripristina** dal menu a discesa **Azioni**.

      Viene visualizzata l'interfaccia Web dell'Agente Arcserve UDP (Linux). La finestra di dialogo di selezione del tipo di ripristino viene visualizzata nell'interfaccia utente dell'agente.

   e. Selezionare il tipo di ripristino e fare clic su **OK**.

      Nota: si accede automaticamente al nodo agente e la **Procedura guidata di ripristino** viene visualizzata dal nodo agente.

   - Dall'Agente Arcserve UDP (Linux):

   a. Aprire l'interfaccia Web dell'Agente Arcserve UDP (Linux).

      Nota: durante l'installazione dell'Agente Arcserve UDP (Linux), l'URL per l'accesso e la gestione del server viene fornito all'utente. Accedere ad Agente Arcserve UDP (Linux)

   b. Fare clic su **Ripristino** dal menu **Procedura guidata** e selezionare **Ripristino bare metal (BMR)**.

   Viene visualizzata la pagina **Server di backup** della **Procedura guidata di ripristino - Ripristino bare metal**.

2. Verificare il server nell'elenco a discesa **Server di backup** nella pagina **Server di backup**.

   Non è possibile selezionare alcuna opzione dall'elenco a discesa **Server di backup**.

3. Fare clic su **Avanti**.

   Viene visualizzata la pagina **Punti di ripristino** della finestra di dialogo **Procedura guidata di ripristino - Ripristino bare metal**.

   Viene specificato il server di backup.

Definizione dei punti di ripristino

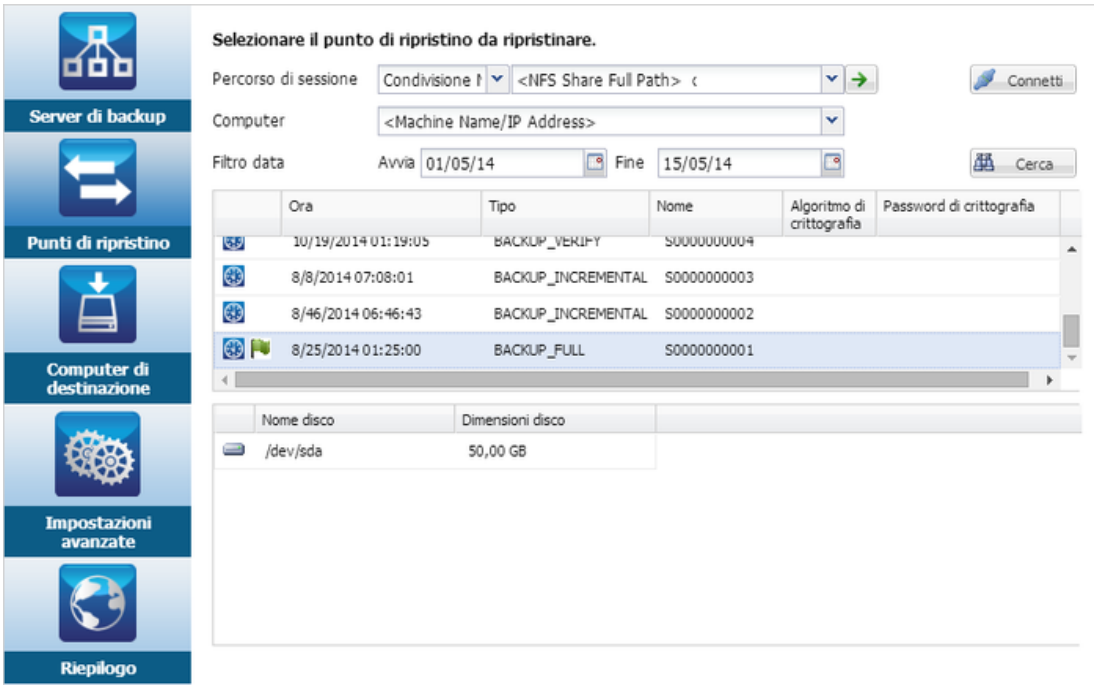
L'esecuzione di un backup implica la creazione di un punto di ripristino. Specificare le informazioni relative al punto di ripristino della **Procedura guidata di ripristino**, in modo da poter eseguire il ripristino dei dati desiderati. È possibile ripristinare file specifici o tutti i file in base alle proprie esigenze.

Importante: Per eseguire un ripristino bare metal da un punto di ripristino, il volume principale e il volume di avvio devono essere presenti nel punto di ripristino.

Effettuare le operazioni seguenti:

1. Selezionare una sessione dall'elenco a discesa **Percorso di sessione,** quindi specificare il percorso completo della condivisione.

   Ad esempio, si utilizza il percorso della sessione come condivisione NFD, xxx.xxx.xxx.xxx come indirizzo IP della condivisione NFS e la cartella viene denominata *Data.* Sarà necessario immettere xxx.xxx.xxx.xxx:/Data come percorso di condivisione NFS.



2. Fare clic su **Connetti.**

   Tutti i nodi di cui è stato eseguito il backup per il percorso specificato saranno contenuti nell'elenco a discesa **Computer.**

3. Selezionare il nodo di cui si desidera eseguire il ripristino dall'elenco a discesa **Computer.**

Verrà creato un elenco contenente tutti i punti di ripristino per il nodo selezionato.

4. Applicare il filtro data per visualizzare i punti di ripristino generati tra le date specificate e fare clic su **Cerca**.

   Valore predefinito: ultime due settimane.

   Vengono visualizzati tutti i punti di ripristino disponibili tra le date specificate.

5. Selezionare il punto di ripristino di cui si desidera eseguire il ripristino e fare clic su **Avanti**.

   Viene visualizzata la pagina **Istanza di destinazione del ripristino bare metal**.

   Il punto di ripristino viene specificato.

Definizione dei dettagli relativi all'istanza di destinazione

Specificare i dettagli dell'istanza di destinazione del ripristino bare metal per ripristinare i dati sul computer. Un'istanza di destinazione è un computer bare metal su cui eseguire un ripristino bare metal. È necessario disporre dell'indirizzo IP dell'istanza di destinazione del ripristino bare metal registrato precedentemente durante la fase iniziale del processo.

Effettuare le operazioni seguenti:

1. Immettere l'indirizzo IP dell'istanza di destinazione del ripristino bare metal nel campo **Indirizzo MAC/IP**.
2. Specificare un nome per il campo **Nome host**.

   L'istanza di destinazione del ripristino bare metal utilizzerà questo nome come nome host al completamento del processo di ripristino.

3. Selezionare una delle opzioni seguenti come rete:

   DHCP

   Configura automaticamente l'indirizzo IP. Questa è l'opzione predefinita. Utilizzare questa opzione se si desidera eseguire il ripristino di un server DHCP (Dynamic Host Configuration Protocol) su una rete DHCP.

   IP statico

   Configura manualmente l'indirizzo IP. Se si seleziona questa opzione, è necessario specificare l'**indirizzo IP**, la **subnet mask** e il **gateway predefinito** del computer di destinazione.

   Importante! Verificare che l'IP statico non sia in uso da altri computer durante il processo di ripristino.

4. (Facoltativo) Selezionare l'opzione **Abilita ripristino bare metal immediato** in modo da poter utilizzare istantaneamente il computer di destinazione.

   Quando si abilita questa opzione, l'Agente Arcserve UDP (Linux) recupera innanzitutto tutti i dati necessari per avviare il computer. Dopo aver avviato il computer di destinazione, i dati rimanenti vengono ripristinati. La connessione di rete deve essere costantemente disponibile durante il ripristino bare metal immediato.

   Esempio: se si dispone di 100 GB di dati e si desidera eseguire un ripristino bare metal e *non* si seleziona questa opzione, prima verranno ripristinati tutti i 100 GB di dati, quindi sarà possibile utilizzare il computer di destinazione. Tuttavia, è

necessario solo 1 GB di dati circa per avviare il computer. Quando si abilita questa opzione, viene ripristinato innanzitutto 1 GB di dati richiesti in modo che sia possibile avviare e utilizzare il computer. Dopo aver avviato il computer, i rimanenti 99 GB di dati vengono ripristinati automaticamente.

Nota: i dati necessari per avviare il computer dipendono dalla configurazione del sistema operativo. Inoltre, è possibile sospendere o riprendere il ripristino automatico dei dati se l'opzione **Non eseguire il recupero automatico dei dati dopo l'avvio del computer** non è selezionata.

5. (Facoltativo) Selezionare l'opzione **Non eseguire il recupero automatico dei dati dopo l'avvio del computer** per interrompere il ripristino automatico dei dati quando il computer di destinazione viene avviato.

   Quando si seleziona l'opzione **Abilita ripristino bare metal immediato**, il comportamento predefinito prevede innanzitutto il ripristino dei dati necessari e poi l'avvio del computer. Dopo aver avviato il computer, i dati rimanenti vengono ripristinati automaticamente. Se si aggiornano i dati di origine durante il ripristino e poi si seleziona questa opzione, i dati vengono recuperati fino al punto prima dell'aggiornamento.

6. Fare clic su **Avanti**.

   Viene visualizzata la pagina **Impostazioni avanzate**.

   Vengono specificati i dettagli dell’istanza di destinazione del ripristino bare metal.

Definizione delle impostazioni avanzate

Specificare le impostazioni avanzate per eseguire un ripristino bare metal pianificato dei dati. Il ripristino bare metal pianificato garantisce che i dati vengano ripristinati all'ora specificata anche in caso di assenza dell'utente.

Effettuare le operazioni seguenti:

1. Impostare la data e l'ora di inizio selezionando una delle seguenti opzioni:

   Esegui ora

   Avvia il processo di ripristino dopo l'invio del processo.

   Imposta ora speciale

   Avvia il processo di ripristino all'ora specificata dopo l'invio del processo.

2. (Facoltativo) Selezionare uno script dall'opzione **Impostazioni script pre/post backup** per il server di backup e l'istanza di destinazione del ripristino bare metal.

   Questi script eseguono comandi di script per le azioni da eseguire prima dell'inizio del processo e/o al completamento del processo.

   Nota: i campi **Impostazioni pre/post script** vengono popolati solamente se un file di script è già stato creato e collocato nel percorso seguente:

   ```
   /opt/Arcserve/d2dserver/usr/prepost
   ```

   Nota: per ulteriori informazioni sulla creazione di pre/post script, consultare la sezione *Gestione di pre/post script per l'automazione*.

3. (Facoltativo) Fare clic su **Mostra altre impostazioni** per visualizzare ulteriori impostazioni relative al ripristino bare metal.

4. (Facoltativo) Reimpostare la password per il nome utente specificato per il computer di destinazione di cui è stato eseguito il recupero.

5. (Facoltativo) Immettere il percorso completo del percorso di archiviazione di backup dei punti di ripristino in **Accesso locale al punto di ripristino**.

6. (Facoltativo) Immettere il nome completo del disco nel campo **Dischi** per escludere tali dischi sull'istanza di destinazione del ripristino bare metal dal processo di recupero.

7. (Facoltativo) Selezionare l'opzione di **riavvio** per riavviare automaticamente il nodo di destinazione al completamento del processo di ripristino bare metal.

8. Fare clic su **Avanti**.

   Viene visualizzata la pagina **Riepilogo**.

   Vengono specificate le impostazioni avanzate.

La presente sezione descrive i seguenti argomenti:

- (Facoltativo) Gestione di pre/post script per l'automazione in AWS Cloud

(Facoltativo) Gestione di pre/post script per l'automazione in AWS Cloud

Gli script di pre/post esecuzione consentono di eseguire regole di business in fasi specifiche di un processo in esecuzione. È possibile specificare quando eseguire gli script nelle **Impostazioni pre/post script** della **Procedura guidata di backup** e della **Procedura guidata di ripristino** dell'interfaccia utente. È possibile eseguire gli script sul server di backup in base alle impostazioni dell'utente.

La gestione del pre/post script è un processo costituito da due passaggi: la creazione del pre/post script e la sua collocazione nella cartella prepost.

Creazione di pre/post script

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Creare un file di script mediante le variabili di ambiente nel linguaggio di scripting preferito.

   Variabili di ambiente del pre/post script

   Per creare lo script, utilizzare le variabili di ambiente seguenti:

   D2D_JOBNAME

   Indica il nome del processo.

   D2D_JOBID

   Identifica l'ID del processo. L'ID di processo è un numero attribuito al processo durante la sua esecuzione. Se si esegue lo stesso processo nuovamente, verrà fornito un nuovo numero di processo.

   D2D_TARGETNODE

   Identifica il nodo di cui viene eseguito il backup o il ripristino.

   D2D_JOBTYPE

   Identifica il tipo di processo in esecuzione. I valori seguenti identificano la variabile D2D_JOBTYPE:

   backup.full

   Identifica il processo come backup completo.

   backup.incremental

   Identifica il processo come backup incrementale.

   backup.verify

Identifica il processo come backup di verifica.

restore.bmr

Identifica il processo come ripristino bare metal (BMR). Si tratta di un processo di ripristino.

restore.file

Identifica il processo come ripristino a livello di file. Si tratta di un processo di ripristino.

D2D_SESSIONLOCATION

Identifica la posizione in cui vengono archiviati i punti di ripristino.

D2D_PREPOST_OUTPUT

Identifica un file temp. Il contenuto della prima linea del file temp viene visualizzato nel registro attività.

D2D_JOBSTAGE

Indica la fase del processo. I valori seguenti identificano la variabile D2D_JOBSTAGE:

pre-job-server

Identifica lo script eseguito sul server di backup prima dell'avvio del processo.

post-job-server

Identifica lo script eseguito sul server di backup dopo il completamento del processo.

pre-job-target

Identifica lo script eseguito sull'istanza di destinazione del ripristino bare metal dopo l'avvio del processo.

post-job-target

Identifica lo script eseguito sull'istanza di destinazione del ripristino bare metal in seguito al completamento del processo.

pre-snapshot

Identifica lo script eseguito sull'istanza di destinazione del ripristino bare metal prima dell'acquisizione della snapshot.

post-snapshot

Identifica lo script eseguito sull'istanza di destinazione del ripristino bare metal dopo l'acquisizione della snapshot.

D2D_TARGETVOLUME

Identifica il volume di cui viene eseguito il backup durante un processo di backup. Questa variabile è adatta per gli script di snapshot di pre/post automazione per un processo di backup.

D2D_JOBRESULT

Identifica il risultato di uno script del processo di post-esecuzione. I valori seguenti identificano la variabile di D2D_JOBRESULT:

success

Identifica il risultato come corretto.

fail

Identifica il risultato come non corretto.

D2DSVR_HOME

Identifica la cartella in cui è installato il server di backup. È possibile applicare la variabile agli script in esecuzione sul server di backup.

Lo script viene creato.

Nota: per tutti gli script, un valore restituito pari a zero indica un'operazione riuscita, mentre un valore restituito diverso da zero indica la presenza di un errore.

Collocare lo script nella cartella prepost ed eseguire la verifica

Tutti gli script di pre/post per un server di backup sono gestiti centralmente dalla cartella prepost nella posizione seguente:

```
/opt/Arcserve/d2dserver/usr/prepost
```

Effettuare le operazioni seguenti:

1. Collocare il file nella posizione seguente del server di backup:

   ```
   /opt/Arcserve/d2dserver/usr/prepost
   ```

2. Fornire le autorizzazioni di esecuzione per il file di script.
3. Accedere all’interfaccia Web dell’Agente Arcserve UDP (Linux).
4. Aprire la procedura guidata di **backup** o **ripristino** ed accedere alla scheda **Impostazioni avanzate**.
5. Selezionare il file di script nell'elenco del menu a discesa **Impostazioni di pre/post script**, quindi inviare il processo.
6. Fare clic sul **Registro attività** e verificare che lo script venga eseguito per il processo

di backup specificato.

Lo script viene eseguito.

I pre/post script vengono creati correttamente e inseriti nella cartella prevista.

Creazione ed esecuzione del processo di ripristino

Creare e eseguire il processo di ripristino in modo da poter avviare il processo di ripristino bare metal. Prima di eseguire un ripristino bare metal, verificare le informazioni relative al punto di ripristino. Se necessario, è possibile tornare indietro e modificare le impostazioni di ripristino.

Effettuare le operazioni seguenti:

1. Verificare i dettagli relativi al ripristino nella pagina **Riepilogo** della **Procedura guidata di ripristino**.
2. (Facoltativo) Fare clic su **Indietro** per modificare le impostazioni di ripristino da una qualsiasi delle pagine della **Procedura guidata di ripristino**.
3. Immettere un nome per il del processo e fare clic su **Invia**.

   Il campo **Nome processo** è associato a un nome predefinito. È possibile specificare un nuovo nome per il processo ma non è possibile lasciare il campo vuoto.

   La **Procedura guidata di ripristino** viene chiusa. È possibile visualizzare il processo nella scheda **Stato processo.** Se si utilizza l'indirizzo IP per il ripristino bare metal, il computer di destinazione verrà riavviato automaticamente sullo stesso sistema operativo dell'origine di backup al completamento del processo di ripristino bare metal.

   Nota: se il computer di destinazione viene avviato prima dell'invio del processo di ripristino, sarà necessario riavviare il computer di destinazione. Verificare che BIOS sia configurato per l'avvio dalla rete.

   Lo stato della colonna **Stato processo** viene modificato in **Ripristino del volume in corso**. Ciò indica che il ripristino è in corso. Al completamento del processo di ripristino, il computer di destinazione verrà riavviato automaticamente con lo stesso sistema operativo dell'origine di backup.

   Il processo di ripristino viene creato ed eseguito correttamente.

   La presente sezione descrive i seguenti argomenti:

   - (Facoltativo) Esecuzione di operazioni successive al ripristino bare metal

(Facoltativo) Esecuzione di operazioni successive al ripristino bare metal

Gli argomenti riportati di seguito fanno riferimento a impostazioni di configurazione facoltative che possono essere eseguite dopo il ripristino bare metal:

Estensione del volume di dati in seguito al ripristino bare metal su dischi diversi

Se si esegue il ripristino bare metal su un disco di maggiori dimensioni rispetto al disco sul nodo originale, lo spazio su disco non verrà utilizzato completamente. L'operazione di ripristino bare metal non elabora automaticamente lo spazio su disco inutilizzato. È possibile formattare lo spazio su disco su una partizione separata oppure ridimensionare la partizione esistente con lo spazio su disco inutilizzato. Il volume che si desidera ridimensionare deve essere inutilizzato. Si consiglia quindi di non eseguire il ridimensionamento di un volume di sistema. La presente sezione descrive la procedura di estensione di un volume di dati con spazio su disco inutilizzato.

Nota: per evitare la perdita di dati, ridimensionare i volumi immediatamente dopo il ripristino bare metal. Inoltre, è possibile eseguire il backup del nodo prima di avviare il ridimensionamento del volume.

In seguito al corretto riavvio dell'istanza di ripristino bare metal di destinazione dopo il ripristino bare metal, è possibile eseguire l'estensione del volume di dati.

Volume di partizione raw

Ad esempio, il ripristino di un disco da 2GB nella sessione viene eseguito su un disco da 16GB denominato */dev/sdb* con una partizione. La partizione raw */dev/sdb1* viene montata direttamente nella directory */data.*

Questo esempio viene utilizzato per descrivere la procedura di estensione di un volume di partizione raw.

Effettuare le operazioni seguenti:

1. Verificare lo stato del volume /dev/sdb1.

```
# df –h /dev/sdb1
/dev/sdb1              2.0G   40M  1.9G   3% /data
```

2. Smontare il volume /dev/sdb1.

```
# umount /data
```

3. Ridimensionare /dev/sdb1 per occupare tutto lo spazio su disco utilizzando il comando fdisk.

   Per eseguire questa operazione, eliminare la partizione esistente e ricrearla utilizzando lo stesso numero di settore di inizio. L'utilizzo dello stesso numero di settore di inizio consente di evitare la perdita di dati.

```
# fdisk -u /dev/sdb

Command (m for help): p

Disk /dev/sdb: 17.1 GB, 17179869184 bytes

255 heads, 63 sectors/track, 2088 cylinders, total
33554432 sectors

Units = sectors of 1 * 512 = 512 bytes

Device Boot      Start         End      Blocks   Id
System

/dev/sdb1              63     4192964     2096451
83  Linux

Command (m for help): d

Selected partition 1

Command (m for help): n

Command action

e   extended

p   primary partition (1-4)

p

Partition number (1-4): 1

First sector (63-33554431, default 63):

Using default value 63

Last sector or +size or +sizeM or +sizeK (63-
33554431, default 33554431):

Using default value 33554431

Command (m for help): p

Disk /dev/sdb: 17.1 GB, 17179869184 bytes
```

```
255 heads, 63 sectors/track, 2088 cylinders, total
33554432 sectors

Units = sectors of 1 * 512 = 512 bytes

Device Boot      Start         End      Blocks   Id
System

/dev/sdb1              63    33554431    16777184+
83  Linux

Command (m for help): w
```

La partizione adotta lo stesso numero di settore di inizio della partizione originale e il numero di settore di fine è 33554431.

4. Ridimensionare il volume utilizzando il comando resize2fs. Se necessario, eseguire prima il comando e2fsck.

```
# e2fsck -f /dev/sdb1

# resize2fs /dev/sdb1
```

5. Montare il volume sul punto di montaggio e verificare nuovamente lo stato del volume.

```
# mount /dev/sdb1 /data

# df -h /dev/sdb1

/dev/sdb1              16G   43M   16G   1% /data
```

Il volume viene esteso a 16 GB ed è pronto per essere utilizzato.

Volume LVM:

Ad esempio, il ripristino di un disco da 8GB nella sessione viene eseguito su un disco da 16GB denominato */dev/sdb* con una partizione. La partizione raw */dev/sdc1* viene utilizzata come unico volume fisico del volume logic LVM */dev/mapper/VGTest-LVTest* con punto di montaggio */lvm*.

Questo esempio viene utilizzato per descrivere la procedura di estensione di un volume di partizione LVM.

Effettuare le operazioni seguenti:

1. Selezionare lo stato del volume /dev/mapper/VGTest-LVTest.

```
# lvdisplay -m /dev/mapper/VGTest-LVTest

# mount /dev/sdb1 /data
```

```
--- Logical volume ---
LV Name                /dev/VGTest/LVTest
VG Name                VGTest
LV UUID                udoBIx-XKBS-1Wky-3FVQ-mxMf-
FayO-tpfPl8
LV Write Access        read/write
LV Status              available
# open                 1
LV Size                7.88 GB
Current LE             2018
Segments               1
Allocation             inherit
Read ahead sectors     0
Block device           253:2
---Segments---
Logical extent 0 to 2017:
Type                linear
Physical volume     /dev/sdc1
Physical extents    0 to 2017
```

Il volume fisico è */dev/sdc1*, il gruppo di volume è *VGTest* e il volume logico è */dev/VGTest/LVTest oppure /dev/mapper/VGTest-LVTest*.

2. Smontaggio del volume /dev/mapper/VGTest-LVTest.

```
# umount /lvm
```

3. Disabilitare il gruppo di volume in cui risiede il volume fisico /dev/sdc1.

```
# vgchange -a n VGTest
```

4. Creare una partizione per occupare lo spazio su disco inutilizzato mediante il comando fdisk.

```
# fdisk -u /dev/sdc
```

```
Command (m for help): pDisk /dev/sdc: 17.1 GB,
17179869184 bytes

255 heads, 63 sectors/track, 2088 cylinders, total
33554432 sectors

Units = sectors of 1 * 512 = 512 bytes

Device Boot      Start         End      Blocks   Id
System

/dev/sdc1              63    16777215     8388576+
83  Linux

Command (m for help): n

Command actione   extended

p   primary partition (1-4)

p

Partition number (2-4): 1

First sector (16777216-33554431, default 16777216):

Using default value 16777216

Last sector or +size or +sizeM or +sizeK (16777216-
33554431, default 33554431):

Using default value 33554431

Command (m for help): p

Disk /dev/sdc: 17.1 GB, 17179869184 bytes

255 heads, 63 sectors/track, 2088 cylinders, total
33554432 sectors

Units = sectors of 1 * 512 = 512 bytes

Device Boot      Start         End      Blocks   Id
System

/dev/sdc1              63    16777215     8388576+
83  Linux

/dev/sdc2        16777216    33554431     8388608
83  Linux

Command (m for help): w
```

La partizione /dev/sdc2 viene creata.

5. Creare un nuovo volume fisico.

```
# pvcreate /dev/sdc2
```

6. Estendere le dimensioni di gruppo del volume.

```
# vgextend VGTest /dev/sdc2
```

7. Abilitare il gruppo di volume disabilitato.

```
# vgchange -a y VGTest
```

8. Estendere le dimensioni del volume logico utilizzando il comando lvextend.

```
# vgchange -a y VGTest# lvextend -L +8G /dev/VGTest/LVTest
```

9. Ridimensionare il volume utilizzando il comando resize2fs. Se necessario, eseguire prima il comando e2fsck.

```
# e2fsck -f /dev/mapper/VGTest-LVTest

# resize2fs /dev/mapper/VGTest-LVTest
```

10. Montare il volume sul punto di montaggio e verificare nuovamente lo stato del volume.

```
# mount /dev/mapper/VGTest-LVTest /lvm

# lvdisplay -m /dev/mapper/VGTest-LVTest

---Logical volume---

LV Name                /dev/VGTest/LVTest

VG Name                VGTest

LV UUID                GTP0a1-kUL7-WUL8-bpbM-9eTR-SVzl-WgA11h

LV Write Access        read/write

LV Status              available

# open                 0

LV Size                15.88 GB

Current LE             4066

Segments               2

Allocation             inherit
```

```
Read ahead sectors     0
Block device           253:2
--- Segments ---
Logical extent 0 to 2046:
Type                linear
Physical volume     /dev/sdc1
Physical extents    0 to 2046
Logical extent 2047 to 4065:
Type                linear
Physical volume     /dev/sdc2
Physical extents    0 to 2018
```

Il volume LVM viene esteso a 16 GB ed è pronto per essere utilizzato.

Verifica del ripristino dell'istanza di destinazione

Al completamento del processo di ripristino, verificare che l'istanza di destinazione sia stata ripristinata e contenga i dati rilevanti.

Effettuare le operazioni seguenti:

1. Accedere all'istanza di destinazione del computer di ripristino di cui è stato eseguito il ripristino.
2. Verificare che l'istanza di destinazione del ripristino bare metal contenga tutte le informazioni di cui è stato eseguito il backup.

   La verifica dell'istanza di destinazione viene eseguita correttamente.

   Nota: quando l'istanza di destinazione del ripristino bare metal è pronta all'uso, è possibile modificare il gruppo di protezione appena creato in base alle proprie necessità aziendali.

   Il ripristino bare metal è stato eseguito correttamente per i computer Linux.

Esecuzione di un ripristino bare metal per i computer Linux in Azure Cloud

Un ripristino bare metal esegue il ripristino del sistema operativo e delle applicazioni software, ed esegue il recupero di tutti i dati sottoposti a backup. Al completamento del ripristino, il computer di destinazione viene riavviato automaticamente sullo stesso ambiente operativo del nodo di origine del backup e tutti i dati vengono ripristinati.

È possibile eseguire un ripristino bare metal completo poiché quando si esegue un backup di dati, esso acquisisce anche informazioni relative al sistema operativo, alle applicazioni installate, ai driver e così via.

È possibile eseguire un ripristino bare metal utilizzando l'indirizzo IP del computer virtuale Linux di destinazione in Microsoft Azure. Il processo per eseguire un ripristino bare metal per istanze Linux in Azure Cloud è leggermente diverso dal processo con computer Linux in locale.

Completare le attività seguenti per eseguire un ripristino bare metal:

- Verifica dei prerequisiti di ripristino bare metal
- Creazione di un nuovo computer su Microsoft Azure come ripristino bare metal di destinazione
- Verifica del computer virtuale del server di backup
- Definizione dei punti di ripristino
- Definizione dei dettagli del computer virtuale di destinazione
- Definizione delle impostazioni avanzate
- Creazione ed esecuzione del processo di ripristino
- Verifica del ripristino dell'istanza di destinazione

Verifica dei prerequisiti di ripristino bare metal

Prima di eseguire un ripristino bare metal per le istanze Linux in Microsoft Azure, tenere presenti le seguenti opzioni:

- Si dispone di un punto di ripristino valido e della password di crittografia per il ripristino.
- Se la destinazione di un processo di backup corrisponde all'origine locale, per eseguire un processo di ripristino bare metal dalla destinazione, è necessario esportare la destinazione dell'origine locale tramite NFS o CIFS e specificare il punto di ripristino come disponibile nella condivisione NFS o CIFS.
- È necessario che il punto di ripristino sia creato dal backup basato su agente Linux.
- Si dispone di un agente Arcserve UDP per l’istanza Linux in Microsoft Azure.
- Il ripristino bare metal sul computer virtuale Linux di destinazione deve disporre dello stesso sistema operativo del nodo Linux di origine.
- Esaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Creazione di un nuovo computer su Microsoft Azure come ripristino bare metal di destinazione

Per il ripristino bare metal su Azure, l'utente può eseguire un ripristino bare metal per il computer virtuale su un computer virtuale Linux con lo stesso sistema Linux su Azure invece di avviare il nodo di destinazione con il Live CD dell'agente Arcserve UDP.

Innanzitutto, creare un nuovo computer virtuale su Azure come nodo di destinazione del ripristino bare metal. Verificare i prerequisiti riportati di seguito.

- Preparare un nuovo computer virtuale con lo stesso sistema operativo del computer virtuale che desidera eseguire un ripristino bare metal.
- Configurare il Tipo di autenticazione come Password per il computer virtuale. Memorizzare il nome utente e la password del computer virtuale.
- Configurare il gruppo di risorse, come ad esempio il gruppo sul server di backup Linux che esegue il ripristino bare metal. In caso contrario, il ripristino bare metal non riuscirà a creare la connessione SSH tra il server di backup Linux e il computer virtuale di destinazione.

Verifica del computer virtuale del server di backup

Per ulteriori informazioni, consultare la sezione Verifica del server di backup.

Definizione dei punti di ripristino

Per ulteriori informazioni, consultare la sezione Definizione dei punti di ripristino

Definizione dei dettagli del computer virtuale di destinazione

Specificare i dettagli del computer virtuale di destinazione del ripristino bare metal per ripristinare i dati su tale computer. Un computer virtuale di destinazione è un computer bare metal su cui eseguire un ripristino bare metal. È necessario disporre dell'indirizzo IP, del nome utente e della password del computer virtuale di destinazione del ripristino bare metal registrato precedentemente durante la fase iniziale del processo.

Effettuare le operazioni seguenti:

1. Dalla schermata della procedura guidata di ripristino bare metal, immettere i seguenti dettagli:
   - Immettere l'indirizzo IP del computer virtuale di destinazione del ripristino bare metal nel campo Indirizzo IP.
   - Immettere il nome utente e la password del computer virtuale di destinazione creato su Azure.
2. Per i dettagli del computer:
   - Specificare un nome per il campo **Nome host**.

     Il computer virtuale di destinazione del ripristino bare metal utilizzerà questo nome come nome host al completamento del processo di ripristino.
   - Verificare che DHCP sia selezionato per impostazione predefinita come Impostazioni di rete.

     Nota: solo DHCP è disponibile su Azure. L'indirizzo IP viene configurato automaticamente.

     DHCP

     Configura automaticamente l'indirizzo IP. Questa è l'opzione predefinita. Utilizzare questa opzione se si desidera eseguire il ripristino di un server DHCP (Dynamic Host Configuration Protocol) su una rete DHCP.
3. (Facoltativo) Selezionare l'opzione **Abilita ripristino bare metal immediato** in modo da poter utilizzare istantaneamente il computer di destinazione.

   Quando si abilita questa opzione, l'Agente Arcserve UDP (Linux) recupera innanzitutto tutti i dati necessari per avviare il computer. Dopo aver avviato il computer di destinazione, i dati rimanenti vengono ripristinati. La connessione di rete deve essere costantemente disponibile durante il ripristino bare metal immediato.

Esempio: se si dispone di 100 GB di dati e si desidera eseguire un ripristino bare metal e *non* si seleziona questa opzione, prima verranno ripristinati tutti i 100 GB di dati, quindi sarà possibile utilizzare il computer di destinazione. Tuttavia, è necessario solo 1 GB di dati circa per avviare il computer. Quando si abilita questa opzione, viene ripristinato innanzitutto 1 GB di dati richiesti in modo che sia possibile avviare e utilizzare il computer. Dopo aver avviato il computer, i rimanenti 99 GB di dati vengono ripristinati automaticamente.

Nota: i dati necessari per avviare il computer dipendono dalla configurazione del sistema operativo. Inoltre, è possibile sospendere o riprendere il ripristino automatico dei dati se l'opzione **Non eseguire il recupero automatico dei dati dopo l'avvio del computer** non è selezionata.

4. (Facoltativo) Selezionare l'opzione **Non eseguire il recupero automatico dei dati dopo l'avvio del computer** per interrompere il ripristino automatico dei dati quando il computer di destinazione viene avviato.

   Quando si seleziona l'opzione **Abilita ripristino bare metal immediato**, il comportamento predefinito prevede innanzitutto il ripristino dei dati necessari e poi l'avvio del computer. Dopo aver avviato il computer, i dati rimanenti vengono ripristinati automaticamente. Se si aggiornano i dati di origine durante il ripristino e poi si seleziona questa opzione, i dati vengono recuperati fino al punto prima dell'aggiornamento.

5. Fare clic su **Avanti**.

   Viene visualizzata la pagina **Impostazioni avanzate**.

   Vengono specificati i dettagli dell’istanza di destinazione del ripristino bare metal.

Definizione delle impostazioni avanzate

Per ulteriori informazioni, consultare la sezione Definizione delle impostazioni avanzate.

Creazione ed esecuzione del processo di ripristino

Per ulteriori informazioni, consultare la sezione Creazione ed esecuzione del processo di ripristino.

Verifica del ripristino del computer virtuale di destinazione

Per ulteriori informazioni, consultare la sezione Verifica del ripristino del computer virtuale di destinazione.

Esecuzione di un ripristino bare metal di migrazione per computer Linux

Il ripristino bare metal di migrazione è un processo composto da due fasi che prevede il ripristino dei dati prima su un computer temporaneo e, quindi, su quello effettivo. Quando è abilitata l'opzione di ripristino bare metal immediato, è possibile recuperare i dati su un computer temporaneo. Il computer temporaneo si può utilizzare finché non è pronto il computer effettivo. Quando è disponibile il computer effettivo, il ripristino bare metal di migrazione permette di trasferire i dati dal computer temporaneo a quello effettivo. Quando si esegue un ripristino bare metal di migrazione, tutti i dati creati sul computer temporaneo vengono trasferiti nel computer effettivo.

Nota: è possibile eseguire un ripristino bare metal di migrazione soltanto con i backup basati su agente. I backup senza agente non supportano il ripristino bare metal di migrazione.

È possibile eseguire un ripristino bare metal mediante l'indirizzo IP o l'indirizzo MAC del computer di destinazione. Se il computer di destinazione viene avviato mediante il sistema Live CD dell'Agente Arcserve UDP (Linux), è possibile ottenere l'indirizzo IP del computer di destinazione.

Nota: è possibile avviare il computer. È stata configurata una sola scheda NIC.

Per effettuare un ripristino bare metal di migrazione, completare le attività seguenti:

- Verifica dei prerequisiti per il ripristino bare metal di migrazione
- Esecuzione di un ripristino bare metal su un computer temporaneo
- Esecuzione del ripristino bare metal di migrazione
- Verifica del ripristino del computer di destinazione

Verifica dei prerequisiti per il ripristino bare metal di migrazione

Prima di eseguire un ripristino bare metal di migrazione, controllare i seguenti punti:

- Si dispone di un punto di ripristino valido e della password di crittografia per il ripristino.
- Si dispone di un computer di destinazione valido per il ripristino bare metal.
- È stato creato Live CD dell'Agente Arcserve UDP (Linux).
- Se si desidera eseguire il ripristino bare metal con l'indirizzo IP, è necessario acquisire l'indirizzo IP del computer di destinazione utilizzando Live CD.
- Se si desidera eseguire il ripristino bare metal PXE con l'indirizzo MAC, è necessario acquisire l'indirizzo MAC del computer di destinazione.
- È necessario che il punto di ripristino sia creato dal backup basato su agente Linux.
- Esaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Esecuzione di un ripristino bare metal su un computer temporaneo

Prima di eseguire un ripristino bare metal di migrazione, è necessario ripristinare i dati dall'origine su un computer temporaneo. Per ripristinare i dati in modo temporaneo, è possibile eseguire il ripristino bare metal sul computer temporaneo. Una volta preparato il computer temporaneo, si può continuare a utilizzarlo.

Quando è pronto il computer effettivo, si può eseguire il ripristino bare metal di migrazione dal computer temporaneo a quello effettivo.

Nota: Per ulteriori informazioni sull'esecuzione del ripristino bare metal, consultare la sezione Esecuzione di un ripristino bare metal (BMR) per computer Linux.

Effettuare le operazioni seguenti:

1. Accedere alla procedura guidata di ripristino in uno dei modi seguenti:

   - Da Arcserve UDP:

   a. Accedere ad Arcserve UDP.

   b. Fare clic sulla scheda **Risorse**.

   c. Selezionare **Tutti i nodi** nel riquadro sinistro.

      Tutti i nodi Online aggiunti vengono visualizzati nel riquadro centrale.

   d. Nel riquadro centrale, selezionare il nodo e fare clic su **Azioni**.

   e. Fare clic su **Ripristina** dal menu a discesa **Azioni**.

      Viene visualizzata l'interfaccia Web dell'Agente Arcserve UDP (Linux). La finestra di dialogo di selezione del tipo di ripristino viene visualizzata nell'interfaccia utente dell'agente.

   f. Selezionare il tipo di ripristino e fare clic su **OK**.

      Nota: si accede automaticamente al nodo agente e la **Procedura guidata di ripristino** viene visualizzata dal nodo agente.

   - Dall'Agente Arcserve UDP (Linux):

   a. Aprire l'interfaccia Web dell'Agente Arcserve UDP (Linux).

      Nota: durante l'installazione dell'Agente Arcserve UDP (Linux), l'URL per l'accesso e la gestione del server viene fornito all'utente.

   b. Accedere all'Agente Arcserve UDP (Linux).

2. Fare clic su **Ripristino** dal menu **Procedura guidata** e selezionare **Ripristino bare metal (BMR)**.

   Viene visualizzata la pagina **Server di backup** della **Procedura guidata di ripristino - Ripristino bare metal**.

3. Inserire i dettagli richiesti nella finestra **Procedura guidata di ripristino - Ripristino bare metal** e salvare.
4. Verificare che sia selezionata la casella di controllo **Abilita ripristino bare metal immediato** nella pagina **Computer di destinazione** della procedura guidata.
5. Verificare che sia selezionata la casella di controllo **Non eseguire il recupero automatico dei dati dopo l'avvio del computer** nella pagina **Computer di destinazione** della procedura guidata.
6. Eseguire il processo di ripristino bare metal.

   Il computer temporaneo viene recuperato utilizzando il ripristino bare metal con l'opzione di ripristino bare metal immediato abilitata. Il computer temporaneo si può utilizzare finché non è pronto il computer effettivo.

Esecuzione del ripristino bare metal di migrazione

Quando il computer effettivo è pronto, è possibile eseguire un ripristino bare metal di migrazione. Il ripristino bare metal di migrazione consente di ripristinare i dati originali dalla sessione di backup e i nuovi dati dal computer temporaneo sul computer effettivo.

Effettuare le operazioni seguenti:

1. Fare clic su **Ripristino** dal menu **Procedura guidata** e selezionare **Ripristino bare metal di migrazione**.

   Viene visualizzata la pagina **Server di backup** della **Procedura guidata di ripristino - Ripristino bare metal di migrazione**.

2. Fornire tutti i dettagli nella **Procedura guidata di ripristino - Ripristino bare metal di migrazione**.

   Nota: Per ulteriori informazioni sull'esecuzione del ripristino bare metal, consultare la sezione Esecuzione di un ripristino bare metal (BMR) per computer Linux.

3. Verificare che nella pagina **Server di Backup** della procedura guidata vengano fornite le seguenti informazioni.

a. Selezionare il processo di ripristino del computer virtuale istantaneo o il processo di ripristino bare metal immediato.

   Server locale

   Indica che il server di backup è gestito localmente. Il processo di ripristino bare metal per il computer temporaneo viene eseguito sul server locale.

   Server remoto

   Indica che il server di backup è gestito in remoto. Il processo di ripristino bare metal per il computer temporaneo viene eseguito sul server remoto. Per la connessione al server remoto, è necessario fornire i dettagli relativi al server interessato.

b. Selezionare il processo di ripristino dall'elenco a discesa Nome processo.

   Una volta pronto per l'uso, nell'elenco viene visualizzato il processo di ripristino di computer virtuale istantaneo o il processo di ripristino bare metal immediato il cui stato è pronto per l'uso o disattivato.

4. Salvare il processo di ripristino bare metal.

   Nella pagina principale, la voce **Fase processo** nella scheda **Stato processo** viene modificata in **Fare clic qui per eseguire la migrazione dei dati**.

5. (Facoltativo) Quando il tipo di processo selezionato è un ripristino bare metal immediato, avviare il computer temporaneo utilizzando un Live CD.

6. Dalla scheda **Stato processo**, selezionare **Fare clic qui per eseguire la migrazione dei dati**.

   La migrazione dei dati viene avviata.

   Il ripristino bare metal di migrazione è stato eseguito correttamente.

Verifica del ripristino del nodo di destinazione

Al completamento del processo di ripristino, verificare che il nodo di destinazione sia stato ripristinato e contenga i dati rilevanti.

Effettuare le operazioni seguenti:

1. Accedere al computer di destinazione di cui è stato eseguito il ripristino.
2. Verificare che il computer di destinazione contenga tutte le informazioni del computer temporaneo, inclusi tutti i nuovi dati creati sul computer temporaneo.

   La verifica del computer di destinazione viene eseguita correttamente.

   La migrazione del ripristino bare metal è stata eseguita correttamente per i computer Linux basati sull'agente.

Esecuzione di un ripristino bare metal di migrazione per computer Linux da Amazon EC2 sul computer locale

Il ripristino bare metal di migrazione è un processo composto da due fasi che prevede il ripristino dei dati prima su un computer temporaneo e, quindi, su quello effettivo. Quando è abilitata l'opzione di ripristino bare metal immediato, è possibile recuperare i dati su un computer temporaneo. Il computer temporaneo si può utilizzare finché non è pronto il computer effettivo. Quando è disponibile il computer effettivo, il ripristino bare metal di migrazione permette di trasferire i dati dal computer temporaneo a quello effettivo. Quando si esegue un ripristino bare metal di migrazione, tutti i dati creati sul computer temporaneo vengono trasferiti nel computer effettivo.

È possibile che si verifichi un problema di inattività a livello di server Linux locale. È possibile utilizzare una sessione di backup per creare un computer virtuale istantaneo su Amazon EC2 e utilizzare tale server per consentire la continuità dei servizi. Dopo aver risolto il problema a livello locale, la migrazione del ripristino bare metal consente di migrare tutti i dati da Amazon EC2 in locale. Il server locale verrà inoltre ripristinato per fornire nuovamente il servizio richiesto.

Nota: è possibile eseguire un ripristino bare metal di migrazione soltanto con i backup basati su agente. I backup senza agente non supportano il ripristino bare metal di migrazione.

È possibile eseguire un ripristino bare metal mediante l'indirizzo IP o l'indirizzo MAC del computer di destinazione. Se il computer di destinazione viene avviato mediante il sistema Live CD dell'Agente Arcserve UDP (Linux), è possibile ottenere l'indirizzo IP del computer di destinazione.

Nota: è possibile avviare il computer. È stata configurata una sola scheda NIC.

Per effettuare un ripristino bare metal di migrazione, completare le attività seguenti:

- Verifica dei prerequisiti per il ripristino bare metal di migrazione
- Esecuzione del ripristino bare metal di migrazione
- Verifica del ripristino del computer di destinazione

Verifica dei prerequisiti per il ripristino bare metal di migrazione

Prima di eseguire un ripristino bare metal di migrazione, controllare i seguenti punti:

- Si dispone di un punto di ripristino valido e della password di crittografia per il ripristino.
- Si dispone di un computer di destinazione valido per il ripristino bare metal.
- È stato creato Live CD dell'Agente Arcserve UDP (Linux).
- Se si desidera eseguire il ripristino bare metal con l'indirizzo IP, è necessario acquisire l'indirizzo IP del computer di destinazione utilizzando Live CD.
- Se si desidera eseguire il ripristino bare metal PXE con l'indirizzo MAC, è necessario acquisire l'indirizzo MAC del computer di destinazione.
- È necessario che il punto di ripristino sia creato dal backup basato su agente Linux.
- Esaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Esecuzione di un ripristino bare metal di migrazione da Amazon EC2 sul computer locale

Prima di eseguire un ripristino bare metal di migrazione da Amazon EC2, è necessario ripristinare i dati dall'origine su un'istanza EC2. Per ripristinare i dati in modo temporaneo, è possibile eseguire un computer virtuale istantaneo sull'istanza EC2. Una volta preparata l'istanza EC2, si può continuare a utilizzarla.

Quando il computer locale effettivo è pronto, si può eseguire il ripristino bare metal di migrazione dall'istanza Amazon EC2 a tale computer.

Nota: per ulteriori informazioni sull'esecuzione del ripristino bare metal, consultare la sezione Esecuzione di un ripristino bare metal (BMR) per computer Linux.

Effettuare le operazioni seguenti:

1. Accedere alla procedura guidata di ripristino in uno dei modi seguenti:

   - Da Arcserve UDP:

   a. Accedere a Arcserve UDP.

   b. Fare clic sulla scheda **Risorse**.

   c. Selezionare **Tutti i nodi** nel riquadro sinistro.

      Tutti i nodi Online aggiunti vengono visualizzati nel riquadro centrale.

   d. Nel riquadro centrale, selezionare il nodo e fare clic su **Azioni**.

   e. Fare clic su **Ripristina** dal menu a discesa **Azioni**.

      Viene visualizzata l'interfaccia Web dell'Agente Arcserve UDP (Linux). La finestra di dialogo di selezione del tipo di ripristino viene visualizzata nell'interfaccia utente dell'agente.

   f. Selezionare il tipo di ripristino e fare clic su **OK**.

      Nota: si accede automaticamente al nodo agente e la **Procedura guidata di ripristino** viene visualizzata dal nodo agente.

   - Dall'Agente Arcserve UDP (Linux):

   a. Aprire l'interfaccia Web dell'Agente Arcserve UDP (Linux).

      Nota: durante l'installazione dell'Agente Arcserve UDP (Linux), l'URL per l'accesso e la gestione del server viene fornito all'utente.

   b. Accedere all'Agente Arcserve UDP (Linux).

2. Fare clic su **Ripristino** dal menu **Procedura guidata** e selezionare **Ripristino bare metal di migrazione**.

   Viene visualizzata la pagina **Server di backup** della **Procedura guidata di ripristino - Ripristino bare metal di migrazione**.

3. Selezionare le opzioni operazioni e fare clic su **Avanti**:

   a. Selezionare **Server remoto** come posizione del server.

   b. Specificare il server di backup Linux su Amazon EC2 per la connessione al server.

   c. Immettere il nome host, il nome utente, la password, il protocollo e la porta per il server di backup Linux.

   d. Fare clic su **Aggiorna,** , quindi selezionare il processo di ripristino dall'elenco a discesa **Nome processo**.

      Una volta pronto per l'uso, nell'elenco viene visualizzato il processo di ripristino di computer virtuale istantaneo il cui stato è **pronto per l'uso** o **disattivato**.

   Viene visualizzata la sezione Punti di ripristino.

4. Dalla sezione **Punti di ripristino**, attenersi alla seguente procedura, quindi fare clic su **Connetti**.

   - Specificare il **server RPS** creato localmente.
   - Selezionare l'archivio dati corrispondente.

     Il computer viene caricato automaticamente in base al processo del computer virtuale istantaneo.
   - Selezionare la sessione e fare clic su **Avanti**.

   Viene visualizzata automaticamente la scheda **Computer di destinazione.**

5. Nella sezione Computer di destinazione, immettere l'indirizzo MAC/IP, quindi fare clic su **Avanti**.

   Nota: è possibile avviare un computer locale con sistema LiveCD per ottenere l'indirizzo MAC/IP.

   L'utente verrà indirizzato alla seziona Avanzate.

6. Nella sezione **Avanzate**, configurare i pre/post script, quindi fare clic su Avanti.

   Viene visualizzata la sezione **Riepilogo**.

7. Immettere un nome per il processo e fare clic su **Invia**.

Viene eseguito un processo di ripristino bare metal sul computer avviato con il sistema LiveCD.

8. Dalla pagina principale dell'agente di Linux, accedere alla scheda **Stato processo** e fare clic su **Fare clic qui per la migrazione dei dati.**

   I dati sul computer virtuale Amazon EC2 vengono migrati sul computer locale.

   Il ripristino bare metal di migrazione è stato eseguito correttamente.

Verifica del ripristino del nodo di destinazione

Al completamento del processo di ripristino, verificare che il nodo di destinazione sia stato ripristinato e contenga i dati rilevanti.

Effettuare le operazioni seguenti:

1. Accedere al computer di destinazione di cui è stato eseguito il ripristino.
2. Verificare che il computer di destinazione contenga tutte le informazioni del computer temporaneo, inclusi tutti i nuovi dati creati sul computer temporaneo.

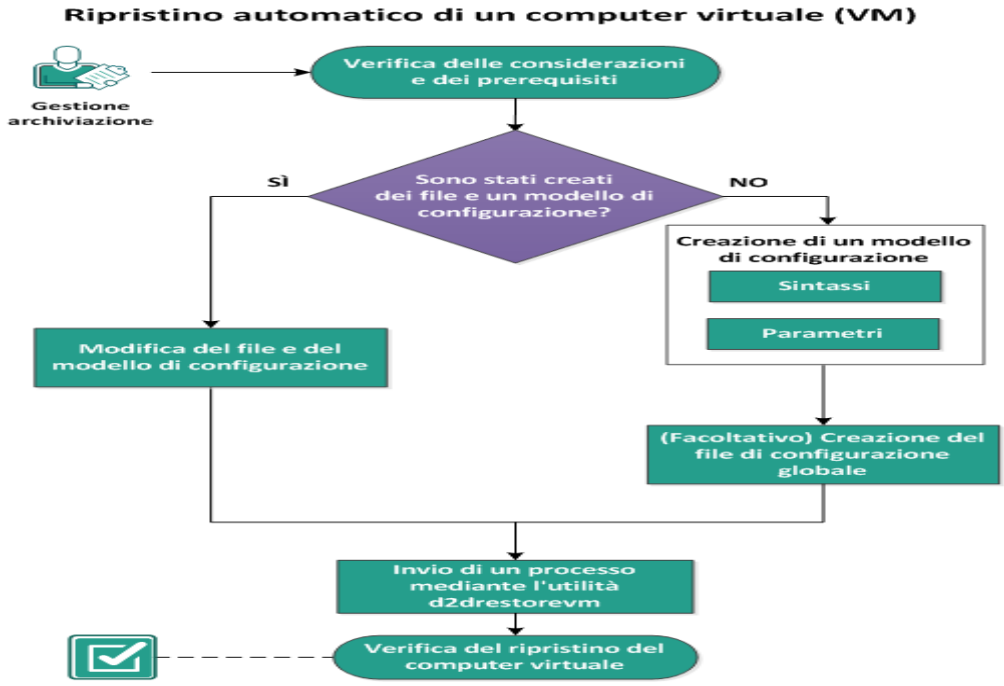
   La verifica del computer di destinazione viene eseguita correttamente.

   La migrazione del ripristino bare metal è stata eseguita correttamente per i computer Linux basati sull'agente.

Ripristino automatico di un computer virtuale

È possibile ripristinare un computer virtuale dalla riga di comando del server di backup mediante l'utilità d2drestorevm. L'utilità d2drestorevm automatizza il processo di esecuzione di un ripristino bare metal semplice o immediato senza dover avviare manualmente il computer virtuale utilizzando un Live CD.

Nel diagramma seguente viene illustrato il processo di ripristino di un computer virtuale dalla riga di comando mediante l'utilità d2drestorevm:



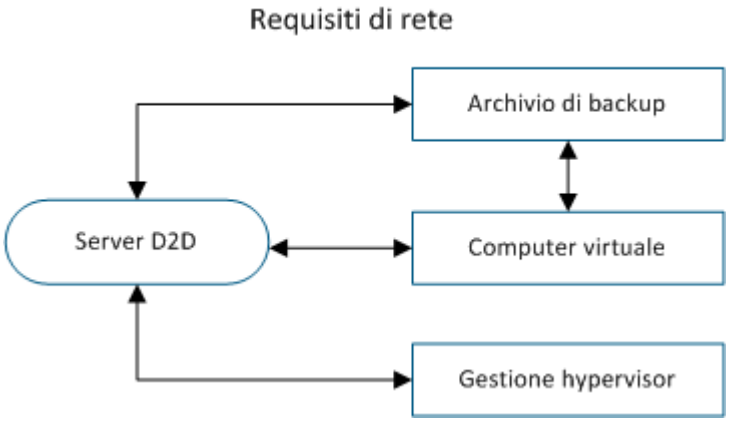
Eseguire queste attività per ripristinare automaticamente un computer virtuale:

- Verifica delle considerazioni e dei prerequisiti
- Creazione di un modello di configurazione
- (Facoltativo) Creazione del file di configurazione globale
- Modifica del file e del modello di configurazione
- Invio di un processo mediante l'utilità d2drestorevm
- Verifica del ripristino del computer virtuale

Verifica delle considerazioni e dei prerequisiti

Verificare i prerequisiti seguenti prima di ripristinare il computer virtuale:

- Sono supportate le seguenti versioni di hypervisor per il ripristino bare metal o il computer virtuale istantaneo tramite l'utilità d2drestorevm:
  - XenServer 6.0 e versioni successive (ripristino del computer virtuale mediante il metodo di ripristino bare metal normale)
  - OVM 3.2 (ripristino del computer virtuale mediante il metodo di ripristino bare metal normale)
  - VMware vCenter/ESX(i) 5.0 o versioni successive (inoltro del processo del computer virtuale istantaneo)
  - Windows Hyper-V Server 2012 o versioni successive (inoltro del processo del computer virtuale istantaneo)
  - Nutanix AHV 5.5.3.1 o versioni successive (inoltro del processo del computer virtuale istantaneo)
- È possibile eseguire l'opzione di ripristino del computer virtuale soltanto dalla riga di comando. Quest'opzione non è disponibile nell'interfaccia utente.
- È possibile utilizzare l'interfaccia utente per monitorare lo stato del processo e i registri delle attività. È possibile utilizzare l'interfaccia utente per sospendere, eliminare ed eseguire nuovamente il processo di ripristino del computer virtuale. Tuttavia, non è possibile modificare il processo di ripristino del computer virtuale.
- Prima del ripristino, è necessario configurare manualmente il computer virtuale su Xen e Oracle Virtual Machine (OVM).
- Quando si ripristinano i computer virtuali Xen e OVM, è necessario che il server NFS sia installato e in esecuzione sul server di backup. Verificare che il firewall non stia bloccando il servizio NFS e che l'hypervisor disponga dell'accesso e dell'autorizzazione corretti per utilizzare il servizio NFS sul server di backup.
- Per eseguire correttamente il ripristino di un computer virtuale, è necessario che sia l'hypervisor, sia il computer virtuale di destinazione dispongano di una connessione di rete valida con il server di backup. Nel diagramma seguente vengono illustrati i requisiti di rete:



- Il server di backup tenta di rilevare e configurare automaticamente una scheda di interfaccia di rete virtuale per il computer virtuale. Tuttavia, talvolta è possibile che non sia stata selezionata una rete valida per la scheda di interfaccia di rete. Il parametro vm_network consente di specificare una certa rete alla quale la scheda di interfaccia di rete dovrebbe essere connessa. Le considerazioni seguenti valgono per diverse piattaforme virtuali:
  - Su XenServer, dopo un'installazione, la rete predefinita viene visualizzata come Network 0 nel XenCenter, che non è la rete effettiva. Tutte le reti con nome Pool-wide network associated with xxx vengono visualizzate come Network 0 in XenCenter. In tali casi, rinominare la rete predefinita e utilizzare il nuovo valore per il parametro vm_network.
  - Su OVM, si consiglia di impostare manualmente il parametro vm_network se è disponibile più di una rete.
- Quando si utilizza la condivisione CIFS come posizione di backup (sessione), considerare i punti seguenti:
  - Utilizzare il carattere / invece di \.
  - I parametri storage_username e storage_password vengono obbligatori per la verifica delle credenziali delle condivisioni CIFS.
- Ai fini del corretto funzionamento di d2drestorevm in caso di ripristino su Xen oppure OVM, è necessario specificare almeno uno dei seguenti parametri:

  `vm_name`

  `vm_uuid`

Se vengono forniti entrambi i parametri, questi devono appartenere allo stesso computer virtuale. Se i parametri appartengono a computer virtuali diversi, verrà visualizzato un errore.

- Esaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Rivedere le considerazioni seguenti prima di ripristinare il computer virtuale:

- Si consiglia di ripristinare le sessioni dalla versione precedente dell'Agente Arcserve UDP (Linux) o di Arcserve UDP per Linux sui computer virtuali originali.
- Quando si ripristina un computer virtuale in un XenServer PV e il computer virtuale ripristinato mostra una schermata vuota ma il servizio SSH e gli altri servizi sono attivi, verificare che il parametro 'console='kernel sia stato impostato correttamente negli argomenti di avvio.
- Le sessioni PV possono essere ripristinate solo su un computer virtuale di destinazione PV su XenServer e OVM.
- I computer con virtualizzazione assistita mediante hardware (HVM) della serie RHEL 6 e i relativi derivati (RHEL 6, CentOS 6 e Oracle Linux6) possono essere ripristinati su un computer virtuale di paravirtualizzazione (PV).

Creazione di un modello di configurazione

Creare un file di configurazione in modo che il comando d2drestorevm possa ripristinare i computer virtuali sulla base dei parametri specificati nel file. Il file d2drestorevm raccoglie tutte le specifiche dal file ed esegue il ripristino in base a tali specifiche.

Sintassi

d2drestorevm --createtemplate=[save path]

L'utilità d2dutil --encrypt crittografa la password e fornisce una password crittografata. È necessario utilizzare questa utilità per crittografare tutte le password. Se si utilizza il parametro --pwdfile=pwdfilepath, occorre crittografare la password. È possibile utilizzare l'utilità con uno dei metodi seguenti:

Metodo 1

```
echo 'string' | ./d2dutil --encrypt
```

string corrisponde alla password specificata.

Metodo 2

Immettere il comando d2dutil –encrypt, quindi specificare la password. Premere Invio: il risultato verrà visualizzato sulla schermata. In questo metodo, la password immessa non viene visualizzata nella schermata.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Creare il modello di configurazione utilizzando il seguente comando:

   ```
   d2drestorevm --createtemplate=[save path]
   ```

   [save path] indica la posizione in cui viene creato il modello di configurazione.
3. Aprire il modello di configurazione e aggiornare i seguenti parametri:

   job_name

   Specifica il nome del processo di ripristino.

   vm_type

   Specifica il tipo di hypervisor in cui viene ripristinato il computer virtuale. I tipi di hypervisor validi sono Xen e OVM.

   vm_server

   Specifica l'indirizzo del server hypervisor. L'indirizzo può essere il nome host o l'indirizzo IP.

   vm_svr_username

Specifica il nome utente dell'hypervisor.

vm_svr_password

Specifica la password dell'hypervisor. La password viene crittografata mediante l'utilità di crittografia d2dutil.

vm_sub_server

Specifica il nome del server ESX durante il ripristino su vCenter o specifica il nome del cluster dell'elemento Prism quando si ripristina a Prism Central.

vm_svr_protocol

Specifica il protocollo dell'hypervisor in caso di ripristino su vCenter/ESX(i) o AHV.

vm_svr_port

Specifica la porta dell'hypervisor in caso di ripristino su vCenter/ESX(i) o AHV.

vm_name

Specifica il nome del computer virtuale di destinazione visualizzato nell'hypervisor.

Importante! Il parametro vm_name non può contenere caratteri speciali tranne spazi vuoti e può includere soltanto i seguenti caratteri: a-z, A-Z, 0-9, - e _.

vm_uuid

Specifica l'UUID del computer virtuale di destinazione.

vm_network

(Facoltativo) Specifica il nome della rete che si desidera utilizzare. Se non si fornisce il nome della rete, viene selezionata automaticamente la rete predefinita.

vm_memory

Specifica la memoria del computer virtuale in MB in caso di ripristino su vCenter/ESX(i) o Hyper-V o AHV.

vm_cpu_count

Specifica il numero di CPU del computer virtuale in caso di ripristino su vCenter/ESX(i) o Hyper-V o AHV.

vm_resource_pool

Specifica il pool di risorse dell'hypervisor in caso di ripristino su vCenter/ESX (i) o AHV.

vm_datastore

Specifica l'archivio dati dell'hypervisor in caso di ripristino su vCenter/ESX(i) o AHV.

storage_location_type

Specifica il tipo di posizione di archiviazione della sessione. La posizione di archiviazione può essere CIFS, NFS o RPS.

storage_location

Specifica la posizione del server di archiviazione della sessione. La posizione di archiviazione può essere CIFS o NFS.

storage_username

Specifica il nome utente quando si utilizza CIFS come posizione di archiviazione.

storage_password

Specifica la password quando si utilizza CIFS come posizione di archiviazione. La password viene crittografata mediante l'utilità di crittografia d2dutil.

rps_server

Specifica il nome del Recovery Point Server quando il valore di **storage_location_type** è RPS.

rps_server_username

Specifica il nome utente del Recovery Point Server quando il valore di **storage_location_type** è RPS.

rps_server_password

Specifica la password del Recovery Point Server quando il valore di **storage_location_type** è RPS. La password viene crittografata mediante l'utilità di crittografia d2dutil.

rps_server_protocol

Specifica il protocollo del Recovery Point Server quando il valore di **storage_location_type** è RPS.

rps_server_port

Specifica la porta del Recovery Point Server quando il valore di **storage_location_type** è RPS.

rps_server_datastore

Specifica il nome dell'archivio dati del Recovery Point Server quando il valore di **storage_location_type** è RPS.

encryption_password

Specifica la password di crittografia della sessione. La password viene crittografata mediante l'utilità di crittografia d2dutil.

source_node

Specifica il nome del nodo dell'origine il cui punto di ripristino viene utilizzato per il ripristino.

recovery_point

Selezionare la sessione da ripristinare. Generalmente, una sessione di ripristino presenta il formato seguente: S00000000X, dove X è un valore numerico. Se si desidera ripristinare la sessione più recente, specificare la parola chiave 'last'.

guest_hostname

Specifica il nome host che si desidera fornire dopo il ripristino del computer virtuale.

guest_network

Specifica il tipo di rete che si desidera configurare. La rete può essere dhcp o statica.

guest_ip

Specifica l'indirizzo IP quando si specifica l'IP statico.

guest_netmask

Specifica la maschera di rete quando si specifica l'IP statico.

guest_gateway

Specifica l'indirizzo gateway quando si specifica l'IP statico.

guest_dns

Specifica l'indirizzo DNS quando si specifica l'IP statico.

guest_reboot

(Facoltativo) Specifica se il computer virtuale di destinazione deve essere riavviato dopo il ripristino. I valori sono Sì e No.

Valore predefinito: No

guest_reset_username

(Facoltativo) Specifica il ripristino della password sul valore fornito nel parametro guest_reset_password.

guest_reset_password

(Facoltativo) Specifica il ripristino della password sul valore specificato. La password viene crittografata mediante l'utilità di crittografia d2dutil.

enable_instant_restore

(Facoltativo) Specifica di abilitare il ripristino immediato. I valori sono Sì e No.

auto_restore_data

(Facoltativo) Specifica di ripristinare i dati automaticamente. I valori sono Sì e No.

script_pre_job_server

(Facoltativo) Specifica lo script da eseguire prima dell'esecuzione del processo sul server.

script_post_job_server

(Facoltativo) Specifica lo script da eseguire dopo l'esecuzione del processo sul server.

script_pre_job_client

(Facoltativo) Specifica lo script da eseguire prima dell'esecuzione del processo sul client.

script_post_job_client

(Facoltativo) Specifica lo script da eseguire dopo l'esecuzione del processo sul client.

script_ready_to_use

(Facoltativo) Specifica lo script da eseguire quando il computer di destinazione è pronto per l'uso e il valore del parametro **enable_instant_restore** è Sì.

force

Specifica se forzare il ripristino del computer virtuale. I valori sono Sì e No.

Valore predefinito: No

exclude_volumes

Specifica i volumi da escludere per il computer virtuale di destinazione.

Non escludere il volume '/'. Utilizzare ':' per separare più volumi.

include_volumes

Specifica i volumi da includere per il computer virtuale di destinazione.

Includere i volumi seguenti: / , /boot , /boot/efi , /home , /usr , /usr/local. Utilizzare ':' per separare più volumi.

4. Salvare e chiudere il modello di configurazione.

   Il modello di configurazione è stato creato correttamente.

(Facoltativo) Creazione di un file di configurazione globale

Il file di configurazione globale (vm.cfg) presenta parametri e valori correlati a posizioni di archiviazione in cui vengono creati i dischi virtuali del computer virtuale. I valori relativi alle posizioni di archiviazione vengono rilevati automaticamente durante il processo di ripristino. Il file vm.cfg sostituisce i valori correlati alle posizioni di archiviazione e ad altri parametri. Se si desidera specificare la propria posizione di archiviazione anziché il valore rilevato automaticamente, è possibile utilizzare il file vm.cfg.

Il file di configurazione globale si trova nella seguente posizione:

```
/opt/Arcserve/d2dserver/configfiles/vm.cfg
```

È possibile configurare i seguenti parametri nel file vm.cfg:

Parametri generali

D2D_VM_PORT

Consente di specificare una porta personalizzata per comunicare con il server dell'hypervisor.

- Per OVM, il comando d2drestorevm richiede l'interfaccia CLI OVM e che la porta predefinita sia 10000.
- Per XenServer, il comando d2drestorevm comunica con il server mediante SSH e la porta predefinita è 22.

Parametri specifici di OVM

OVM_ISO_REPOSITORY

Consente di impostare manualmente il repository per caricare il Live CD dell'Agente Arcserve UDP (Linux).

OVM_ISO_UPLOAD_SERVER

Consente di specificare manualmente il server di repository per caricare il Live CD dell'Agente Arcserve UDP (Linux).

OVM_DISK_REPOSITORY

Consente di utilizzare il repository OVM specifico per creare dischi virtuali.

Nota: L'utilità d2drestorevm utilizza l'ID per i parametri specifici di OVM.

Parametri specifici di Xen

XEN_DISK_SR

Consente di utilizzare un repository di archiviazione Xen specifico per creare dischi virtuali. L'utilità d2drestorevm utilizza il nome file lessicale per i parametri specifici di Xen.

Effettuare le operazioni seguenti:

1. Accedere al server di backup.
2. Creare il file di configurazione globale e denominarlo vm.cfg.
3. Aprire il file di configurazione globale e aggiornare i parametri nel file.
4. Salvare e chiudere il file.
5. Collocare il file nella cartella configfiles:

   `/opt/Arcserve/d2dserver/configfiles/vm.cfg`

   Il file di configurazione globale è stato creato correttamente.

Modifica del file e del modello di configurazione

Se si dispone già del modello di configurazione e del file di configurazione globale, è possibile modificare i file e ripristinare un altro computer virtuale. Non è necessario creare altri modelli e file di configurazione ogni volta che si ripristina un computer virtuale. Quando si invia il processo, viene aggiunto un nuovo processo all'interfaccia utente Web. L'interfaccia utente Web consente di visualizzare i registri delle attività.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Aprire il modello di configurazione dalla posizione in cui è stato salvato il file e modificare i parametri in base ai propri requisiti.
3. Salvare e chiudere il modello di configurazione.
4. (Facoltativo) Aprire il file di configurazione globale dalla seguente posizione e modificare i parametri in base ai propri requisiti:

   ```
   /opt/Arcserve/d2dserver/configfiles/vm.cfg
   ```

5. Salvare e chiudere il file di configurazione globale.

   Il modello e il file di configurazione sono stati modificati correttamente.

Invio di un processo mediante l'utilità d2drestorevm

Eseguire il comando d2drestorevm per ripristinare il computer virtuale. Il comando verifica il computer virtuale di destinazione e invia un processo di ripristino. È possibile visualizzare il processo di ripristino dall'interfaccia utente Web. Durante il processo di ripristino, se uno qualsiasi dei requisiti non viene soddisfatto, verrà visualizzato un errore. Nell'interfaccia utente Web è possibile visualizzare il registro attività.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Inviare il processo di ripristino per il computer virtuale utilizzando il comando seguente:

   ```
   d2drestorevm --template=cfg_file_path [--wait]
   ```

   Nota: Lo switch --wait consente di tornare all'ambiente della shell al termine del processo di ripristino. Se lo switch --wait non è presente, tornare immediatamente all'ambiente della shell dopo avere inviato il processo.

   Il processo di ripristino viene inoltrato.

Verifica del ripristino del computer virtuale

Al completamento del processo di ripristino, verificare che il nodo di destinazione sia stato ripristinato e contenga i dati rilevanti.

Effettuare le operazioni seguenti:

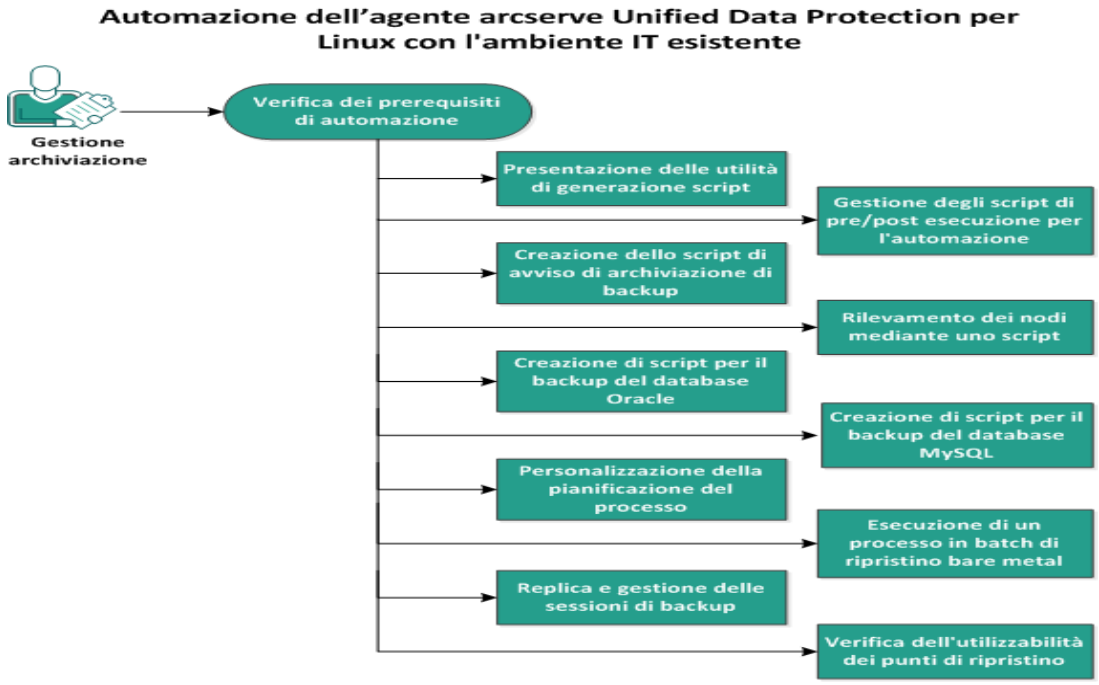
1. Accedere al computer di destinazione di cui è stato eseguito il ripristino.
2. Verificare che il computer di destinazione contenga tutte le informazioni di cui è stato eseguito il backup.

   Il computer virtuale è stato verificato correttamente.

Integrazione e automazione dell'Arcserve UDP per Linux con l'ambiente IT esistente

In qualità di manager dell'archiviazione, è possibile creare script e automatizzare le attività per integrare l'Agente Arcserve UDP (Linux) con l'ambiente IT esistente. Gli script consentono di ridurre l'intervento manuale e diminuiscono la dipendenza sull'interfaccia Web del server di backup per l'esecuzione di qualsiasi attività. L'Agente Arcserve UDP (Linux) fornisce inoltre l'interfaccia e le utilità per l'esecuzione della gestione dei processi, dei nodi e delle attività di gestione del registro attività.

Nel diagramma seguente è possibile visualizzare il processo di integrazione e automatizzazione dell'Agente Arcserve UDP (Linux) nell'ambiente IT esistente:



Eseguire le attività seguenti per automatizzare e gestire l'Agente Arcserve UDP (Linux):

- Verifica dei prerequisiti di automazione
- Presentazione delle utilità di generazione script
- Gestione dei pre/post script per l'automazione
- Creazione dello script di avviso di archiviazione di backup
- Rilevamento dei nodi mediante uno script
- Creazione degli script per l'esecuzione del backup del database Oracle

- Creazione degli script per l'esecuzione del backup del database MySQL
- Utilizzo degli script per il backup e il ripristino del database PostgreSQL
- Personalizzazione della pianificazione del processo
- Esecuzione di un processo in batch di ripristino bare metal
- Replica e gestione delle sessioni di backup
- Verifica dell'utilizzabilità dei punti di ripristino

Verifica dei prerequisiti di automazione

Prima di avviare l'automazione e la gestione dell'Agente Arcserve UDP (Linux) tenere presenti i seguenti requisiti:

- Si dispone delle credenziali di accesso per l'utente root al server di backup.
- Si dispone delle conoscenze necessarie per la generazione di script Linux.
- Si ha una migliore comprensione dell'interfaccia Web dell'Agente Arcserve UDP (Linux).
- Esaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Presentazione delle utilità di generazione script

L'Agente Arcserve UDP (Linux) fornisce delle utilità di generazione script che consentono di creare lo script di automazione. Queste utilità consentono soltanto la generazione di script, pertanto l'output è compatibile con la generazione di script. Le utilità vengono utilizzate per la gestione di nodi e processi, per la replica delle destinazioni di backup e per la gestione dei registri attività.

Tutte le utilità si trovano nella cartella *bin* nel seguente percorso:

```
/opt/Arcserve/d2dserver/bin
```

L'utilità d2dutil --encrypt crittografa la password e fornisce una password crittografata. È necessario utilizzare questa utilità per crittografare tutte le password. Se si utilizza il parametro --pwdfile=pwdfilepath, occorre crittografare la password. È possibile utilizzare l'utilità con uno dei metodi seguenti:

Metodo 1

```
echo "string" | d2dutil --encrypt
```

string corrisponde alla password specificata.

Metodo 2

Immettere il comando d2dutil –encrypt, quindi specificare la password. Premere Invio: il risultato verrà visualizzato sulla schermata. In questo metodo, la password immessa non viene visualizzata nella schermata.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Accedere alla cartella *bin* mediante il seguente comando:

   ```
   # cd /opt/Arcserve/d2dserver/bin
   ```

3. Eseguire i seguenti comandi per gestire i nodi:

   ```
   # ./d2dnode
   ```

   Visualizza un elenco dei comandi disponibili per la gestione di tutti i nodi Linux correlati. Questo comando consente di aggiungere, eliminare, modificare e importare i nodi. È possibile aggiungere i nodi anche mediante le credenziali utente non root.

   Nota: se il server di backup corrisponde a un agente Linux standalone, è possibile utilizzare tutti i parametri del comando d2dnode. Se la gestione del server di backup viene eseguita dalla Console UDP, il comando d2dnode consente di utilizzare unicamente i parametri di elenco, aggiunta, modifica e importazione. I parametri di elenco, aggiunta, modifica e importazione eseguono l'aggiornamento del nodo sulla

Console UDP. Ad esempio, il comando ./d2dnode --list elenca tutti i nodi Linux aggiunti alla Console UDP.

```
# ./d2dnode --list Elenca tutti i nodi gestiti dal server di backup.
```

```
# ./d2dnode --add=nodename/ip --user=username --password=password --description="the description of that node" --attach=jobname --force
```

Aggiunge il nodo specifico al server di backup. Se si è un utente root, utilizzare questo comando per aggiungere i nodi.

Nota: se si modifica il numero di porta del nodo, è necessario specificare il nuovo numero di porta nel parametro --add, così come mostrato nell'esempio seguente.

Esempio: # ./d2dnode –-add=nodename/ip:new_port -–user=username -–password=password -–description="the description of that node" --attach=jobname --force

--attach=jobname

Aggiunge un nuovo nodo a un processo di backup esistente.

--force

Aggiunge il nodo in modo forzato, anche se il nodo è gestito da un altro server di backup. Se il parametro *force* viene rimosso, il nodo non viene aggiunto al server se è gestito da un altro server di backup.

```
# ./d2dnode --add=nodename -- user=username --password=password --rootuser=rootaccount --rootpwd=rootpassword --pwdfile=pwdfilepath --description=description --attach=jobname –force
```

Aggiunge il nodo specifico al server di backup. Se si è un utente non root, utilizzare questo comando per aggiungere i nodi.

Nota: se si modifica il numero di porta del nodo, è necessario specificare il nuovo numero di porta nel parametro --add, così come mostrato nell'esempio seguente.

Esempio: # ./d2dnode --add=nodename/ip:new_port --user=username --password=password --rootuser=rootaccount --rootpwd=rootpassword --pwdfile=pwdfilepath --description=description --attach=jobname –force

-- user=username

Specifica il nome utente dell'utente non root.

-- password=password

Specifica la password dell'utente non root. Se viene fornito il parametro --pwd-file=pwdfilepath, non occorre specificare questo parametro.

--rootuser=rootaccount

Specifica il nome utente dell'utente root.

-- rootpwd=rootpassword

Specifica la password dell'utente root. Se viene fornito il parametro --pwd-file=pwdfilepath, non occorre specificare questo parametro.

--pwdfile=pwdfilepath

(Facoltativo) Specifica la password dell'utente root e dell'utente non root. Questo è un parametro facoltativo che si utilizza se sono state archiviate le password dell'utente root e degli utenti non root in un file separato. Il file di password include i seguenti parametri: password=password e --root-pwd=rootpassword. Per una maggiore protezione, è necessario crittografare la password utilizzando l'utilità d2dutil –encrypt. Dopo avere crittografato la password, sostituire la vecchia password con la password crittografata nel parametro --pwdfile.

```
# ./d2dnode --node=nodename --attach=jobname
```

Aggiunge il nodo specificato a un processo di backup esistente.

```
# ./d2dnode --modify=nodename/ip --user=username --password=newpassword --description=newdescription
```

Modifica il nome utente, la password, o la descrizione del nodo aggiunto. Se si è un utente root, utilizzare questo comando per modificare i nodi.

```
# ./d2dnode --modify=nodename -- user=username --password=newpassword --rootuser=rootaccount --root-pwd=newrootpassword --pwdfile=pwdfilepath --description=newdescription
```

Modifica il nome utente, la password, o la descrizione del nodo aggiunto. Se si è un utente non root, utilizzare questo comando per modificare i nodi.

-- user=username

Specifica il nome utente dell'utente non root.

--password=newpassword

Specifica la nuova password dell'utente non root.

--rootuser=rootaccount

Specifica il nome utente dell'utente root.

--rootpwd=newrootpassword

Specifica la nuova password dell'utente root.

--pwdfile=pwdfilepath

(Facoltativo) Specifica la password dell'utente root e dell'utente non root. Questo è un parametro facoltativo che si utilizza se sono state archiviate le password dell'utente root e degli utenti non root in un file separato. Il file di password include i seguenti parametri: password=newpassword e rootpwd=newrootpassword.

```
# ./d2dnode --delete=nodename1,nodename2,nodename3
```

Elimina i nodi specificati dal server di backup. Per eliminare i nodi multipli, utilizzare una virgola (,) come delimitatore.

```
# ./d2dnode --import=network --help
```

Esegue l'importazione dei nodi dalla rete. Durante l'importazione dei nodi, è necessario configurare le opzioni seguenti:

--netlist

Specifica l'elenco degli indirizzo IP v4. In caso di voci multiple, l'elenco deve essere formato da voci separate da virgola.

Esempio

192.168.1.100: importa il nodo con indirizzo IP 192.168.1.100

192.168.1.100-150: importa tutti i nodi inclusi nell'intervallo tra 192.168.1.100 e 192.168.100.150

192.168.1.100-: importa tutti i nodi che appartengono all'ambito (intervallo) tra 192.168.1.100 e 192.168.1.254. In questo caso non è necessario specificare l'intervallo di fine.

192.168.1.100-150,192.168.100.200-250 : importa nodi multipli inclusi in due intervalli diversi. Il primo ambito (intervallo) tra 192.168.1.100 e 192.168.1.150 e il secondo ambito tra 192.168.100.200 e 192.168.100.250. Ciascuna voce viene separata mediante una virgola.

--joblist

Specifica l'elenco dei nomi di processo. I nomi di processo non devono includere virgole. Una volta completata l'importazione corretta del nodo, il nodo viene aggiunto al processo. In caso di più processi, l'elenco deve essere formato da voci separate da virgola.

Esempio: --joblist=jobA,jobB,jobC

In questo esempio, ciascuna voce di processo è separata da una virgola.

Nota: questa opzione è supportata unicamente nella versione standalone di Agente Arcserve UDP (Linux).

--user

Specifica il nome utente per l'importazione e l'aggiunta dei nodi.

--password

Specifica la password per l'importazione e l'aggiunta dei nodi.

--rootuser

Specifica il nome utente dell'utente root. Se l'utente aggiunto è un utente secondario, utilizzare questo parametro per specificare le credenziali dell'utente root.

--rootpwd

Specifica la password dell'utente root. Se l'utente aggiunto è un utente secondario, utilizzare questo parametro per specificare le credenziali dell'utente root.

--pwdfile

(Facoltativo) Specifica la password dell'utente root e dell'utente non root. Questo è un parametro facoltativo che si utilizza se sono state archiviate le password dell'utente root e degli utenti non root in un file separato. Il file di password include i seguenti parametri: password=newpassword e rootpwd=newrootpassword.

--prefix

Specifica il prefisso assegnato a un nome host. Utilizzare questo parametro per filtrare i nodi che includono il prefisso nel nome host.

--blacklistfile

Specifica un file che include un elenco di nomi host di nodo che non si desidera aggiungere al server di backup. Nel file è necessario specificare un nodo per riga.

--force

Aggiunge il nodo in modo forzato, anche se il nodo è gestito da un altro server di backup. Se il parametro *force* viene rimosso, il nodo non viene aggiunto al server se è gestito da un altro server di backup.

--verbose

Mostra informazioni aggiuntive riguardanti il processo di importazione del nodo. Utilizzare questo parametro per il debug o lo script di automazione.

--help

Visualizza la schermata della Guida in linea.

Note:

- La funzione di importazione utilizza il server SSH per stabilire se si tratta di un nodo Linux. Se il server SSH utilizza una porta non predefinita, configurare il server per l'utilizzo della porta non predefinita. Per ulteriori informazioni sulla configurazione del numero di porta SSH, consultare la sezione Modifica del numero di porta SSH del server di backup.
- Se la password non viene specificata, verrà utilizzato il metodo di autenticazione con chiave SSH.

4. Immettere i comandi seguenti per inoltrare un processo di ripristino file:

   ```
   d2drestorefile --createtemplate=file
   ```

   Specifica di creare un modello. Una volta creato il modello, è possibile modificarlo. Questo modello viene utilizzato dal comando d2drestorefile. È possibile impostare i valori nel modello. Il comando d2drestorefile esegue legge il modello e fornisce il risultato come specificato nel modello.

   ```
   d2drestorefile --template=restore_template [--wait]
   ```

   Specifica di inoltrare il processo di ripristino file. Se si include il parametro [--wait] nel comando, il messaggio di stato viene visualizzato soltanto dopo aver completato il processo di ripristino.

5. Eseguire i seguenti comandi per gestire i processi:

   ```
   # ./d2djob
   ```

   Mostra un elenco di comandi utilizzati per la gestione dei processi. Mediante questo comando, è possibile eseguire, annullare, ed eliminare processi.

   ```
   # ./d2djob --delete=jobname
   ```

   Elimina il processo specificato dalla scheda Stato processo.

   ```
   # ./d2djob --run=jobname --jobtype=1 --recoverysetstart --
   wait
   ```

   Esegue il processo specificato. Il parametro --jobtype è facoltativo. Il comando d2djob identifica automaticamente il tipo di processo dal nome del processo specificato. Se il comando identifica un processo di ripristino, tale processo viene avviato. Se il comando identifica un processo di backup e non si fornisce alcun valore per il parametro --jobtype, allora viene avviato un processo di backup incrementale. Il backup incrementale è il tipo di processo predefinito.

Se si desidera specificare il tipo di processo per un processo di backup, i valori sono 0, 1 e 2, dove 0 indica un processo di backup completo, 1 indica un processo di backup incrementale e 2 indica un processo di backup di verifica.

Il parametro --recoverysetstart è facoltativo. Se questa opzione viene specificata, il backup corrente viene convertito in backup completo e contrassegnato come primo punto di ripristino del set di ripristino se quest'ultimo non è disponibile.

```
# ./d2djob --cancel=jobname --wait
```

Annulla un processo in corso.

Se si include --wait nel comando, lo stato del processo viene visualizzato dopo l'annullamento del processo. Se non si include --wait nel comando, lo stato del processo viene visualizzato immediatamente dopo avere inviato la richiesta di annullamento.

```
# ./d2djob --newrestore=restoreJobName --target=macaddress/ipaddress --hostname=hostname --network=dhcp/staticip --staticip=ipaddress --subnet=subnetMask --gateway=gateway --runnow --wait
```

Esegue un processo di ripristino per un computer di destinazione nuovo basato su un processo di ripristino esistente. Questo comando consente di utilizzare le stesse impostazioni di ripristino del processo di ripristino esistente. Gli unici dati differenti sono i dettagli relativi al computer di destinazione. Se si utilizza questo comando, non sarà necessario creare processi di ripristino multipli per computer di destinazione differenti.

È necessario fornire un valore per *--newrestore*, *--target*, *--hostname* e *--network*.

Se il valore di *--network* è staticip, è necessario fornire un valore per *--staticip*, *--subnet* e *--gateway*. Se il valore di *--network* è dhcp, non è necessario fornire nessun valore per *--staticip, --subnet* e *--gateway*.

Se si include --runnow nel comando, il processo viene eseguito subito dopo l'invio del processo, indipendentemente dalla pianificazione del processo.

Se si include il parametro --wait nel comando, il messaggio di stato viene visualizzato dopo il completamento del processo. Se non si include --wait nel comando, il messaggio di stato viene visualizzato immediatamente dopo avere inviato il processo.

```
# ./d2djob <--export=jobname1,jobname2,jobname3> <--file=filepath>
```

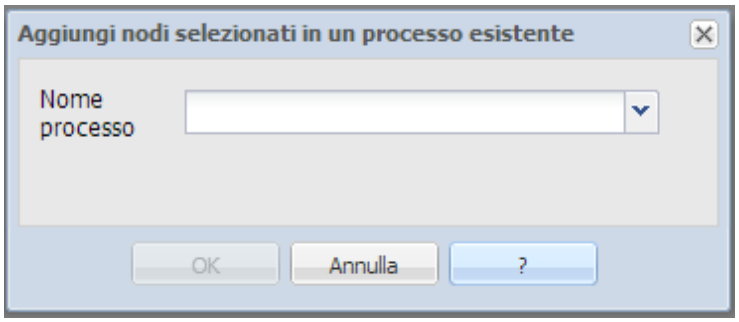
Esporta processi multipli dal server di backup a un file. Se si desidera utilizzare le stesse configurazioni di backup per più server di backup, è possibile esportare i processi di backup in un file, quindi importare il file negli altri server di backup.

Nota: se il server di backup di Linux viene gestito dalla console Arcserve UDP, l'esportazione non è supportata.

```
# ./d2djob <--import=filepath>
```

Importa il file contenente le informazioni sul processo di backup in un server di backup. Se il server di backup è gestito da Arcserve UDP è inoltre possibile importare il file in Arcserve UDP.

Se il processo di backup viene importato in un server di backup, è possibile selezionare il processo dalla finestra di dialogo seguente:



È possibile utilizzare anche l'utilità della riga di comando seguente per aggiungere nodi al processo:

```
./d2dnode -attach=jobname
```

6. Eseguire i comandi riportati di seguito per creare o aggiornare il file di configurazione dei punti di ripristino. L'Agente Arcserve UDP (Linux) utilizza il file di configurazione per gestire e visualizzare i punti di ripristino nell'interfaccia utente.

   ```
   # ./d2drp
   ```

   Crea o aggiorna i file di configurazione dei punti di ripristino in base ai relativi dettagli. Con questo comando è possibile creare o aggiornare i file di configurazione.

   ```
   # ./d2drp --build --storagepath=/backupdestination --node-
   e=node_name
   ```

   Verifica tutti i punti di ripristino appartenenti a *node_name* e aggiornano tutti i file di configurazione dei punti di ripristino. Se i file di configurazione dei punti di ripristino non sono presenti, con questo comando vengono creati in automatico. Il parametro --build crea i file di configurazione dei punti di ripristino.

   ```
   # ./d2drp --build --storagepath=/backupdestination --node-
   e=node_name --rp=recovery_point
   ```

Verifica il nome della sessione specificata e aggiorna tutti i file di configurazione dei punti di ripristino. Se i file di configurazione dei punti di ripristino non sono presenti, con questo comando vengono creati in automatico. Specificare la parola chiave last perché il parametro --rp ottenga il punto di ripristino più recente.

```
# ./d2drp --show --storagepath=path --node=nodeName --rp=r-
recovery_point --user=username --password=password
```

Visualizza le informazioni di sistema relative al punto di ripristino specificato.

--rp=recovery_point

Specifica il punto di ripristino al quale accedere. Specificare la parola chiave last per ottenere il punto di ripristino più recente.

-- user=username

Specifica il nome utente per accedere alla posizione di archiviazione o alla destinazione di backup.

-- password=password

Specifica la password per accedere alla posizione di archiviazione o alla destinazione di backup.

Nota: Per il parametro --build, d2drp non supporta la condivisione NFS o CIFS. Se si desidera utilizzare la condivisione NFS o CIFS, è necessario prima montare la condivisione sull'host locale e poi utilizzare il punto di montaggio come percorso di archiviazione.

7. Eseguire i comandi seguenti per gestire i registri attività:

```
# ./d2dlog
```

Mostra il formato che consente di ottenere i registri attività per l'ID del processo specificato nel formato specificato.

```
# ./d2dlog --show=jobid --format=text/html
```

Mostra il registro attività del processo specificato. Il valore del formato è facoltativo in quanto il valore predefinito è text.

8. Eseguire i comandi seguenti per gestire la cronologia del processo:

```
# ./d2djobhistory
```

Visualizza la cronologia del processo in base ai filtri specificati. È possibile filtrare la cronologia del processo per giorno, settimana, mese e data di inizio e di fine.

```
# ./d2djobhistory --day=n --headers=column_name1,column_
name2,...column_name_n --width=width_value --for-
mat=column/csv/html
```

Visualizza la cronologia del processo recente in base ai giorni specificati.

--headers=column_name1,column_name2,...column_name_n

(Facoltativo) Specifica le colonne che si desidera visualizzare nella cronologia del processo. Questo è un parametro facoltativo. Le colonne predefinite sono ServerName, TargetName, JobName, JobID, JobType, DestinationLocation, EncryptionAlgoName, CompressLevel, ExecuteTime, FinishTime, Throughput, WriteThroughput, WriteData, ProcessedData e Status.

--width=width_value

(Facoltativo) Specifica il numero di caratteri da visualizzare per ciascuna colonna. Questo è un parametro facoltativo. Ciascuna colonna ha la propria larghezza predefinita. È possibile aggiornare il valore relativo alla larghezza per ciascuna colonna, dove ciascun valore di larghezza è separato da una virgola (,).

--format=column/csv/html

Specifica il formato di visualizzazione della cronologia del processo. I formati disponibili sono colonna, csv e HTML. È possibile specificare solamente un formato alla volta.

```
# ./d2djobhistory --week=n --headers=column_name1,column_
name2,...column_name_n --width=width_value --for-
mat=column/csv/html
```

Visualizza la cronologia del processo recente in base ai mesi specificati.

```
# ./d2djobhistory --starttime=yyyymmdd --endtime=yyyymmdd -
-headers=column_name1, column_name2,...column_name_n --wid-
th=width_value --format=column/csv/html
```

Visualizza la cronologia del processo recente in base alla data di inizio e di fine specificata.

```
# ./d2djobhistory --starttime=yyyymmdd --endtime=yyyymmdd -
-headers=column_name1, column_name2,...column_name_n --wid-
th=width_value --format=column/csv/html
```

Le utilità per la generazione di script sono state utilizzate per la gestione di nodi, processi e registri attività.

Gestione dei pre/post script per l'automazione

Gli script di pre/post esecuzione consentono di eseguire regole di business a intervalli specifici di un processo in esecuzione. È possibile specificare quando eseguire gli script nelle **Impostazioni pre/post script** della **Procedura guidata di backup** e della **Procedura guidata di ripristino** nella console. È possibile eseguire gli script sul server di backup in base alle impostazioni dell'utente.

La gestione del pre/post script è un processo costituito da due passaggi: la creazione del pre/post script e la sua collocazione nella cartella prepost.

Creazione di pre/post script

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Creare un file di script mediante le variabili di ambiente nel linguaggio di scripting preferito.

Variabili di ambiente del pre/post script

Per creare lo script, utilizzare le variabili di ambiente seguenti:

D2D_JOBNAME

Indica il nome del processo.

D2D_JOBID

Identifica l'ID del processo. L'ID di processo è un numero attribuito al processo durante la sua esecuzione. Se si esegue lo stesso processo nuovamente, verrà fornito un nuovo numero di processo.

D2D_TARGETNODE

Identifica il nodo di cui viene eseguito il backup o il ripristino.

D2D_JOBTYPE

Identifica il tipo di processo in esecuzione. I valori seguenti identificano la variabile D2D_JOBTYPE:

backup.full

Identifica il processo come backup completo.

backup.incremental

Identifica il processo come backup incrementale.

backup.verify

Identifica il processo come backup di verifica.

restore.bmr

Identifica il processo come ripristino bare metal (BMR). Si tratta di un processo di ripristino.

restore.file

Identifica il processo come ripristino a livello di file. Si tratta di un processo di ripristino.

D2D_SESSIONLOCATION

Identifica la posizione in cui vengono archiviati i punti di ripristino.

D2D_PREPOST_OUTPUT

Identifica un file temp. Il contenuto della prima linea del file temp viene visualizzato nel registro attività.

D2D_JOBSTAGE

Indica la fase del processo. I valori seguenti identificano la variabile D2D_JOBSTAGE:

pre-job-server

Identifica lo script eseguito sul server di backup prima dell'avvio del processo.

post-job-server

Identifica lo script eseguito sul server di backup dopo il completamento del processo.

pre-job-target

Identifica lo script eseguito sul computer di destinazione prima dell'avvio del processo.

post-job-target

Identifica lo script eseguito sul computer di destinazione dopo il completamento del processo.

pre-snapshot

Identifica lo script eseguito sul computer di destinazione prima dell'acquisizione della snapshot.

post-snapshot

Identifica lo script eseguito sul computer di destinazione dopo l'acquisizione della snapshot.

D2D_TARGETVOLUME

Identifica il volume di cui viene eseguito il backup durante un processo di backup. Questa variabile è adatta per gli script di snapshot di pre/post automazione per un processo di backup.

D2D_JOBRESULT

Identifica il risultato di uno script del processo di post-esecuzione. I valori seguenti identificano la variabile di D2D_JOBRESULT:

success

Identifica il risultato come corretto.

fail

Identifica il risultato come non corretto.

D2DSVR_HOME

Identifica la cartella in cui è installato il server di backup. È possibile applicare la variabile agli script in esecuzione sul server di backup.

D2D_RECOVERYPOINT

Identifica il punto di ripristino creato dal processo di backup. Questo valore è applicabile soltanto allo script post-backup.

D2D_RPSSCHEDULETYPE

Identifica il tipo di pianificazione durante il backup in un archivio dati su server RPS. I valori seguenti identificano la variabile di D2D_RPSSCHEDULETYPE:

giornaliero

Identifica la pianificazione come backup giornaliero.

settimanale

Identifica la pianificazione come backup settimanale.

mensile

Identifica la pianificazione come backup mensile.

Lo script viene creato.

Nota: per tutti gli script, un valore restituito pari a zero indica un'operazione riuscita, mentre un valore restituito diverso da zero indica la presenza di un errore.

Collocare lo script nella cartella prepost ed eseguire la verifica

Tutti gli script di pre/post per un server di backup sono gestiti centralmente dalla cartella prepost nella posizione seguente:

```
/opt/Arcserve/d2dserver/usr/prepost
```

Effettuare le operazioni seguenti:

1. Collocare il file nella posizione seguente del server di backup:

   `/opt/Arcserve/d2dserver/usr/prepost`

2. Fornire le autorizzazioni di esecuzione per il file di script.
3. Accedere all'interfaccia Web dell'Agente Arcserve UDP (Linux).
4. Aprire la procedura guidata di **backup** o **ripristino** ed accedere alla scheda **Impostazioni avanzate**.
5. Selezionare il file di script nell'elenco del menu a discesa **Impostazioni di pre/post script**, quindi inviare il processo.
6. Fare clic sul **Registro attività** e verificare che lo script venga eseguito per il processo di backup specificato.

   Lo script viene eseguito.

   I pre/post script vengono creati correttamente e inseriti nella cartella prevista.

   La presente sezione descrive i seguenti argomenti:

   - Esempio di creazione di script definiti dall'utente

Esempio di creazione di script definiti dall'utente

La variabile di ambiente D2D_JOBSTAGE, che dispone di quattro diverse fasi, è molto importante per la scrittura di uno script. Nella fase pre_share, è possibile effettuare alcune operazioni di preparazione implementare il metodo di accesso. La fase post_share consente di implementare il metodo di accesso e di effettuare altre operazioni. La differenza tra le due fasi consiste nel fatto che il percorso indicato D2D_SHARE_PATH è disponibile nella fase post_share. Le fasi pre_cleanup e post_ cleanup offrono la possibilità di liberare risorse allocate o di interrompere le connessioni in un percorso condiviso. La differenza tra le due fasi consiste nel fatto che il percorso indicato D2D_SHARE_PATH è disponibile nella fase pre_cleanup ma non nella fase post_cleanup.

Note:

- È possibile che l'input standard visualizzi la password definita nell'interfaccia utente Web.
- I codici vengono eseguiti da un processo diverso in una fase di diversa. Pertanto, se si desidera condividere i dati in una fase di diversa, è necessario utilizzare risorse globali come un file temporaneo o un database.

Esempio: creazione di script definiti dall'utente

Nota: lo script SFTP viene utilizzato come esempio nella directory examples/sharerp.

```
#!/bin/bash
function pre_sftp_share()
{
local share_path=${D2D_SHARE_PATH}
local user_name=${D2D_SHARE_USER}
local pass_word=""

# Read pass word from standard input.
read -s pass_word

# Check user whether exist.
if grep $user_name /etc/passwd >/dev/null 2>&1; then
    return 1
fi

# Add new user.
```

```
useradd $user_name -d $share_path >/dev/null 2>&1
[ $? -ne 0 ] && return 2

# Set pass word for the user.
echo -e "$pass_word\n$pass_word"|passwd "$user_name" >/dev/null 2>&1
[ $? -ne 0 ] && return 3

return 0
}

function post_sftp_share()
{
return 0
}

function pre_sftp_cleanup()
{
return 0
}

function post_sftp_cleanup()
{
local user_name=${D2D_SHARE_USER}

# Delete the user.
userdel $user_name >/dev/null 2>&1

return 0
}

# Main
################################################################
ret=0
stage=${D2D_JOBSTAGE}
case $stage in
pre_share)
pre_sftp_share
ret=$?
```

```
;;

post_share)
post_sftp_share
ret=$?
;;

pre_cleanup)
pre_sftp_cleanup
ret=$?
;;

post_cleanup)
post_sftp_cleanup
ret=$?
;;
esac

exit $ret
```

Creazione dello script di avviso di archiviazione di backup

Creare lo script di avviso di archiviazione di backup in modo che sia possibile eseguire lo script quando lo spazio per l'archiviazione di backup è inferiore al valore specificato. Quando si aggiunge un percorso di archiviazione di backup nell'interfaccia utente, è possibile selezionare la casella di controllo Esegui script quando lo spazio libero disponibile è inferiore a. Se si seleziona la casella di controllo, l'Agente Arcserve UDP (Linux) controlla lo spazio di archiviazione disponibile con una frequenza di 15 minuti. Ogni volta che lo spazio di archiviazione è inferiore al valore specificato, l'Agente Arcserve UDP (Linux) esegue lo script *backup_storage_alert.sh.* È possibile configurare lo script *backup_storage_alert.sh* per l'esecuzione di qualsiasi attività quando lo spazio di archiviazione di backup è minore.

Esempio 1: È possibile configurare lo script per l'invio automatico di un avviso di posta elettronica sulla diminuzione dello spazio di archiviazione.

Esempio 2: È possibile configurare lo script per l'eliminazione automatica di alcuni dati dallo spazio di archiviazione di backup quando è inferiore rispetto al valore specificato.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Creare lo script *backup_storage_alert.sh* mediante le variabili seguenti:

   backupstoragename

   Definisce il nome del percorso di archiviazione di backup. Ad esempio, NFS o CIFS.

   freesize

   Definisce lo spazio libero disponibile nel percorso di archiviazione di backup.
3. Collocare lo script nel percorso seguente:

   ```
   /opt/Arcserve/d2dserver/usr/alert/backup_storage_
   alert.sh
   ```

   Lo script backup_storage_alert.sh viene creato.

Rilevamento dei nodi mediante uno script

L'Agente Arcserve UDP (Linux) consente di eseguire script per il rilevamento di nodi sulla rete in uso. È possibile scrivere uno script per il rilevamento dei nodi sulla rete e posizionarlo script nella cartella *discovery*.

È possibile configurare le impostazioni di rilevamento dei nodi dall'interfaccia Web e impostare la frequenza di esecuzione dello script. Nello script, è possibile specificare le utilità per il rilevamento di nodi sulla rete. Dopo il rilevamento di un nodo da parte di uno script, utilizzare il comando *d2dnode* per aggiungere il nodo all'Agente Arcserve UDP (Linux). È presente un registro delle attività per ogni esecuzione dello script.

Nota: per tutti gli script, un valore restituito pari a zero indica un'operazione riuscita, mentre un valore restituito diverso da zero indica la presenza di un errore.

Se si desidera stampare informazioni relative allo script di rilevamento nodi del Registro attività, è possibile utilizzare la seguente variabile di ambiente speciale:

```
echo "print something into activity log" > "$D2D_DISCOVER_
OUTPUT"
```

Uno script di esempio viene posizionato nella cartella *discovery* nel seguente percorso, in modo che possa rilevare i nodi Linux della rete secondaria.

```
/opt/Arcserve/d2dserver/examples/discovery
```

È possibile copiare lo script di esempio nel seguente percorso e modificare lo script in base alle proprie esigenze:

/opt/Arcserve/d2dserver/usr/discovery

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Creare uno script di rilevamento dei nodi e posizionare lo script nella cartella *discovery* nel percorso seguente:

   ```
   /opt/Arcserve/d2dserver/usr/discovery
   ```

3. Fornire le autorizzazioni di esecuzione necessarie per il file di script.
4. Accedere all'interfaccia Web dell'.
5. Configurare le impostazioni di rilevamento dei nodi nel menu Nodo per l'esecuzione dello script.
6. Fare clic su Registro attività e verificare che lo script venga eseguito.

   Il Registro attività visualizza un elenco di tutti i nodi rilevati.

I nodi vengono rilevati correttamente mediante lo script.

Creazione degli script per l'esecuzione del backup del database Oracle

È possibile creare script da utilizzare per il backup del database Oracle. Non è necessario interrompere il database per eseguire il backup. Verificare che il database sia in modalità di archiviazione del registro. Se non è nella modalità di archiviazione del registro, modificare il database sulla modalità di archiviazione del registro prima di eseguire il backup del database. Per eseguire il backup del database Oracle, creare i due script seguenti:

- **pre-db-backup-mode.sh**: questo script prepara e mantiene l'intero database in modalità di backup.
- **post-db-backup-mode.sh**: questo script rimuove il database dalla modalità di backup.

Nelle Impostazioni pre/post script della procedura guidata di backup, è possibile specificare gli script da eseguire nei nodi del database Oracle.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Creare lo script *pre-db-backup-mode.sh* mediante il codice seguente:

```
#!/bin/bash

orauser="oracle"

orasid="orcl"

su - ${orauser}   << BOF 2>&1

export ORACLE_SID=$orasid

sqlplus /nolog << EOF 2>&1

connect / as sysdba

alter database begin backup;

exit;

EOF

BOF
```

Nota: specificare il valore delle variabili *orauser* e *orasid* così come definito nel database Oracle.

3. Creare lo script *post-db-backup-mode.sh* mediante il codice seguente:

```
#!/bin/bash

orauser="oracle"

orasid="orcl"

su - ${orauser}   << BOF 2>&1

export ORACLE_SID=$orasid

sqlplus /nolog << EOF 2>&1

connect / as sysdba

alter database end backup;

exit;

EOF

BOF
```

   Nota: specificare il valore delle variabili *orauser* e *orasid* così come definito nel database Oracle.

4. Fornire le autorizzazioni di esecuzione per entrambi gli script.
5. Inserire entrambi gli script nella posizione seguente:

   ```
   /opt/Arcserve/d2dserver/usr/prepost/
   ```

6. Accedere all'interfaccia Web dell'Agente Arcserve UDP (Linux).
7. Aprire la procedura guidata di backup e andare alla scheda Impostazioni avanzate.
8. Nell'opzione Impostazioni pre/post script, selezionare il file di script *pre-db-backup-mode.sh* dall'elenco a discesa Prima dell'acquisizione della snapshot.
9. Nell'opzione Impostazioni pre/post script, selezionare il file di script *post-db-backup-mode.sh* dall'elenco a discesa In seguito all'acquisizione della snapshot.
10. Inoltrare il processo di backup.

    Il processo di backup viene inoltrato.

    Vengono creati gli script per l'esecuzione del backup del database Oracle.

    Nota: Agente Arcserve UDP (Linux) supporta la snapshot a livello di volume. Per assicurare la coerenza dei dati, tutti i file di dati del database devono essere su un solo volume.

    Per ripristinare il database Oracle, consultare la sezione Ripristino di un database Oracle mediante l'Agente Arcserve UDP (Linux).

Creazione degli script per l'esecuzione del backup del database MySQL

È possibile creare script da utilizzare per il backup del database MySQL. Non è necessario interrompere il database per eseguire il backup. Per eseguire il backup del database MySQL, creare i due script seguenti:

- **pre-db-backup-mode.sh**: questo script chiude tutte le tabelle aperte e blocca tutte le tabelle per ogni database con blocco di lettura globale.
- **post-db-backup-mode.sh**: questo script rimuove tutti i blocchi.

Nelle Impostazioni pre/post script della procedura guidata di backup, è possibile specificare gli script da eseguire nei nodi del database MySQL.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Creare lo script *pre-db-backup-mode.sh* mediante il codice seguente:

```
#!/bin/bash#

dbuser=root

dbpwd=rootpwd

lock_mysqldb(){

(

  echo "flush tables with read lock;"

  sleep 5

) | mysql -u$dbuser -p$dbpwd ${ARGUMENTS} }

}

lock_mysqldb &

PID="/tmp/mysql-plock.$!"

touch ${PID}
```

Nota: specificare il valore delle variabili *dbuser* e *dbpwd* così come definito nel database MySQL.

3. Creare lo script *post-db-backup-mode.sh* mediante il codice seguente:

```
#!/bin/bash

killcids(){
```

```
pid="$1"
cids=`ps -ef|grep ${pid}|awk '{if('$pid'==$3){print $2}}'`
for cid in ${cids}
do
        echo ${cid}
        kill -TERM ${cid}
done
echo -e "\n"
}
mysql_lock_pid=`ls /tmp/mysql-plock.* | awk -F . '{print $2}'`
[ "$mysql_lock_pid" != "" ] && killcids ${mysql_lock_pid}
rm -fr /tmp/mysql-plock.*
```

4. Fornire le autorizzazioni di esecuzione per entrambi gli script.
5. Inserire entrambi gli script nella posizione seguente:

   ```
   /opt/Arcserve/d2dserver/usr/prepost/
   ```

6. Accedere all'interfaccia Web dell'Agente Arcserve UDP (Linux).
7. Aprire la procedura guidata di backup e andare alla scheda Impostazioni avanzate.
8. Nell'opzione Impostazioni pre/post script, selezionare il file di script *pre-db-backup-mode.sh* dall'elenco a discesa Prima dell'acquisizione della snapshot.
9. Nell'opzione Impostazioni pre/post script, selezionare il file di script *post-db-backup-mode.sh* dall'elenco a discesa In seguito all'acquisizione della snapshot.
10. Inoltrare il processo di backup.

    Il processo di backup viene inoltrato.

    Vengono creati gli script per l'esecuzione del backup del database MySQL.

    Nota: Agente Arcserve UDP (Linux) supporta la snapshot a livello di volume. Per assicurare la coerenza dei dati, tutti i file di dati del database devono essere su un solo volume.

    La presente sezione descrive i seguenti argomenti:

    - Esecuzione di un ripristino bare metal (BMR) di un server MySQL
    - Esecuzione del ripristino del database MySQL

Esecuzione di un ripristino bare metal (BMR) di un server MySQL

Un ripristino bare metal esegue il ripristino del sistema operativo e delle applicazioni software, oltre ad eseguire il recupero di tutti i dati sottoposti a backup. Il ripristino bare metal consiste nel ripristino di un sistema del computer avviato a partire da un sistema bare metal. Bare metal è un computer senza sistema operativo, driver e applicazioni software. Al completamento del ripristino, il computer di destinazione viene riavviato automaticamente sullo stesso ambiente operativo del nodo di origine del backup e tutti i dati vengono ripristinati.

È possibile eseguire un ripristino bare metal mediante l'indirizzo IP o l'indirizzo MAC del computer di destinazione. Se il computer di destinazione viene avviato mediante il sistema Live CD dell'agente Arcserve UDP per Linux, sarà possibile ottenere l'indirizzo IP del computer di destinazione.

Se il server MySQL è corrotto, è possibile ripristinare il server intero eseguendo un ripristino bare metal.

Per ripristinare un server MySQL, procedere come segue:

1. Accedere alla console del server di backup di Linux come utente root.
2. Eseguire un ripristino bare metal mediante la procedura guidata di ripristino. Per ulteriori informazioni sul processo di ripristino, consultare la sezione Esecuzione di un ripristino bare metal (BMR) per computer Linux.
3. Dopo che il processo di ripristino bare metal è stato completato, accedere al computer di destinazione e verificare che il database sia stato ripristinato.

   Il server MySQL è stato recuperato correttamente.

Esecuzione del ripristino del database MySQL

Se un database MySQL viene perso o è corrotto, è possibile eseguire un ripristino a livello di file per ripristinare il database specifico.

Effettuare le operazioni seguenti:

1. Accedere al computer di destinazione come utente root.
2. Interrompere il servizio MySQL
3. Per effettuare il ripristino sulla posizione originale:
    1. Eliminare file e directory dall'attuale cartella del database MySQL
    2. Ripristinare la cartella del database dal punto di ripristino sulla cartella del database MySQL
4. Avviare il servizio MySQL.

   Il database è stato recuperato correttamente.

Utilizzo degli script per il backup e il ripristino del database PostgreSQL

Per eseguire il backup del database PostgreSQL, è possibile utilizzare i seguenti script. Durante l'esecuzione degli script, non è necessario interrompere il database per eseguire il backup.

- **postgresql_backup_pre. sh**: questo script imposta il database in modalità di backup.
- **postgresql_snapshot_post. sh**: questo script rimuove il database dalla modalità di backup.
- **postgresql_settings**: si tratta di un file di configurazione che potrebbe richiedere l'aggiornamento delle variabili PostgreSQL.
- **postgresql_backup_post. sh**: questo script esegue l'aggiornamento del registro in merito allo stato del backup.

Prerequisiti

Prima di avviare il backup, verificare i seguenti elementi:

- Il livello di WAL è impostato su archiviazione (o hot_standby)
- archive_mode è impostato su attivo
- archive_command deve essere impostato per specificare la posizione di archiviazione

Nota: per applicare le impostazioni, riavviare il server dopo aver configurato queste impostazioni nel file postgresql.conf.

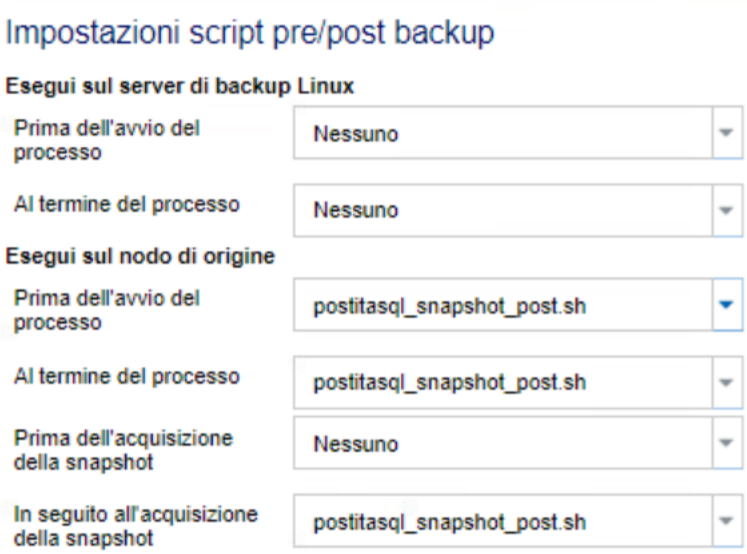
I comandi riportati di seguito consentono di verificare lo stato della modalità di archiviazione dopo il riavvio:

- show archive_mode
- show archive_command
- show WAL level

Applicazione di script

Effettuare le operazioni seguenti:

1. Estrarre il file LinuxPostgres.zip, contenente i quattro file seguenti: postgresql_backup_pre.sh, postgresql_snapshot_post.sh, postgresql_settings, postgresql_backup_post.sh.
2. Copiare i file da from pre/post backup/snapshot nel percorso seguente sul server di backup di Linux /opt/Arcserve/d2dserver/usr/prepost.
3. Copiare il file postgresql_settings nel percorso di origine /root/backup.
4. Verificare che postgresql_settings per tutti i valori sia impostato sulle variabili e apportare le modifiche necessarie per ciascun ambiente.
5. Configurare il piano dalla Console UDP e selezionare il nodo PostgreSQL come origine.



6. Confermare lo stato del backup. Per conoscere lo stato di backup di PostgreSQL, verificare il file arcserve_postgresql_backup_${DATE}.log. Il file di registro viene creato sotto la directory, la quale è impostata dall'utente. Per ulteriori informazioni sulla configurazione della directory, fare riferimento al file postgresql_settings.

Ripristino del database PostgreSQL

Effettuare le operazioni seguenti:

1. Interrompere il server di database.
2. Per eseguire il ripristino nella posizione originale, eseguire le seguenti operazioni:

a. Eliminare i file e le directory dalla cartella /data corrente.

b. Eseguire un ripristino dell'intera cartella /data.

3. Eliminare i file dalle cartelle seguenti dopo il completamento del ripristino dalla cartella /data:
   - pg_dynshmem/
   - pg_notify/
   - pg_serial/
   - pg_snapshots/
   - pg_stat_tmp/
   - pg_subtrans/
   - pg_internal.init
4. Accedere alla cartella configurata per l'archiviazione WAL e procedere come segue:
   a. Eliminare i file presenti nella directory pg_wal ripristinata che contiene le informazioni relative alle transazioni eseguite durante il backup.
   b. A questo punto, copiare i file dalla posizione archiviata definita dall'utente nella cartella pg_wal, con il fine di garantire la conformità dei dati e il ripristino temporizzato.
5. Avviare il server di database.

Ripristino su una posizione alternativa sullo stesso server

1. Interrompere il server di database.
2. Eseguire PGDATA configurandolo su "new_data_directory_path".
3. Avviare il database appena creato utilizzando il comando 'Initdb'.
4. Eliminare i file e le directory dalla cartella /data corrente.
5. Eseguire un ripristino dell'intera cartella /data.
6. Eliminare i file dalle cartelle seguenti dopo il completamento del ripristino dalla cartella /data:
   - pg_dynshmem/
   - pg_notify/
   - pg_serial/
   - pg_snapshots/

- pg_stat_tmp/
- pg_subtrans/
- pg_internal.init

7. Accedere alla cartella configurata per l'archiviazione WAL e procedere come segue:
   a. Eliminare i file presenti nella directory pg_wal ripristinata che contiene le informazioni relative alle transazioni eseguite durante il backup.
   b. A questo punto, copiare i file dalla posizione archiviata definita dall'utente nella cartella pg_wal, con il fine di garantire la conformità dei dati e il ripristino temporizzato.
8. Avviare il server di database.

   Nota: assicurarsi che l'avvio del database venga eseguito nella sessione in cui PGDATA viene aggiornato.

Limitazioni

Gli script precedenti non consentono di eseguire il backup se il database PostgreSQL è configurato con una porta non predefinita. Gli script funzionano solo con il numero di porta predefinito 5432.

Per risolvere il problema, utilizzare i seguenti suggerimenti per modificare manualmente gli script postgresql_backup_pre.sh e postgresql_snapshot_post.sh:

- postgresql_backup_pre.sh:

  Originale: sudo -u ${USERNAME} -H -- psql -c "SELECT pg_start_backup('Arcserve UDP backup - ${DATE} $(timestamp)', true)" >> ${LOG} 2>&1

  Modificato: sudo -u ${USERNAME} -H -- psql -p 5432 -c "SELECT pg_start_backup('Arcserve UDP backup - ${DATE} $(timestamp)', true)" >> ${LOG} 2>&1
- postgresql_snapshot_post.sh:

  Originale: sudo -u ${USERNAME} -H -- psql -c "SELECT pg_stop_backup()" >> ${LOG} 2>&1

  Modificato: sudo -u ${USERNAME} -H -- psql -p 5432 -c "SELECT pg_stop_backup()" >> ${LOG} 2>&1

Personalizzazione della pianificazione del processo

L'Agente Arcserve UDP (Linux) consente di definire la propria pianificazione mediante uno script per l'esecuzione di un processo. Se si desidera eseguire periodicamente un processo e non è possibile eseguirne la pianificazione mediante l'interfaccia utente Web, è possibile creare uno script per la definizione di tale pianificazione. Ad esempio, si desidera eseguire un backup alle 22:00 l'ultimo sabato di ogni mese. Non è possibile definire tale pianificazione mediante l'interfaccia Web, ma è possibile creare uno script per definirla.

È possibile inviare un processo di backup senza specificare nessuna pianificazione (mediante l'opzione Nessuno della pagina Avanzate). Utilizzare l'utilità di pianificazione Cron di Linux per definire la pianificazione personalizzata ed eseguire il comando *d2djob* per l'esecuzione del processo.

Nota: la procedura seguente suppone che si sia inviato un processo di backup senza specificare nessuna pianificazione e si desidera eseguire un backup alle 22:00 l'ultimo sabato di ogni mese.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Creare un file script e immettere il comando seguente per eseguire un backup alle 22:00 l'ultimo sabato di ogni mese:

```
#!/bin/bash#

LAST_SAT=$(cal | awk '$7!=""{t=$7} END {print t}')

TODAY=$(date +%d)

if [ "$LAST_SAT" = "$TODAY" ]; then

            source /opt/Arcserve/d2dserver/bin/setenv

            d2djob --run=your_job_name   --jobtype=your_job_
      type      #run your backup job here

fi
```

Nota: è necessario fornire le autorizzazioni di esecuzione necessarie per il file.

3. Accedere alla cartella crontab e aggiungere il comando seguente al valore crontab del sistema (/etc/crontab):

```
00 22 * * Saturday root runjob.sh
```

Cron esegue lo script runjob.sh alle 22:00 ogni sabato. Viene eseguita una ricerca in runjob.sh al fine di stabilire se oggi è l'ultimo sabato del mese. In caso affermativo, d2djob viene utilizzato per l'esecuzione del processo di backup.

La pianificazione del processo viene personalizzata per eseguire un backup alle 22:00 l'ultimo sabato di ogni mese.

Esecuzione di un processo in batch di ripristino bare metal

Se si desidera eseguire un ripristino bare metal su più computer multipli per poi installare lo stesso ambiente operativo su tutti i computer, è possibile eseguire un ripristino bare metal in batch. Non è necessario creare un processo per ogni processo di ripristino bare metal. Così facendo si risparmia tempo e lavoro ed è possibile ridurre il rischio di errori durante la configurazione dei computer per il ripristino bare metal.

Nota: è necessario disporre di un punto di ripristino valido per il computer di origine da ripristinare. Se non si dispone di un punto di ripristino valido, eseguire prima il backup del computer di origine e, quindi, inviare il processo di ripristino.

Dopo aver definito tutte le impostazioni di ripristino bare metal in un modello di processo BMR, modificare l'indirizzo del computer di destinazione (IP o MAC), il nome host, e la configurazione di rete mediante il comando seguente:

```
d2djob
```

Effettuare le operazioni seguenti:

1. Creare un processo di ripristino bare metal denominato BMR-TEMPLATE ed eseguire il processo per uno dei vari computer.

   Nota: è possibile fornire qualsiasi nome per il processo di ripristino bare metal. Nello script di ripristino bare metal in batch è necessario indicare lo stesso nome del processo.

2. Accedere al server di backup come utente root.
3. Creare uno script di ripristino bare metal in batch in base al processo BMR-TEMPLATE per l'invio automatico di più processi di ripristino bare metal. Utilizzare lo script seguente per crearne uno di ripristino bare metal in batch:

```
#!/bin/sh

prename=lab-server

serverList[0]="<MAC_Address>"

serverList[1]=" <MAC_Address>"

serverList[2]=" <MAC_Address>"

.

.
```

```
.
serverList[300]=" <MAC_Address>"
for((i=0;i<${#serverList[@]};i=i+1))
do
./d2djob --newrestore="BMR-TEMPLATE" --target=${serverList
[i]} --hostname=$prename$i --network=dhcp
done
```

4. Eseguire lo script di ripristino bare metal in batch.

   Lo script viene eseguito. Nell'interfaccia utente vengono creati più processi di ripristino bare metal.

   Viene eseguito un batch per il processo di ripristino bare metal.

Replica e gestione delle sessioni di backup

È possibile creare uno script per replicare le sessioni di backup in modo da ripristinare i dati quando i dati di backup originale sono danneggiati. Le sessioni di backup includono tutti i punti di ripristino sottoposti a backup. È possibile proteggere le sessioni di backup replicandole su una destinazione di replica.

Dopo aver replicato le sessioni di backup, è possibile gestire la destinazione di replica aggiungendola all'interfaccia dell'Agente Arcserve UDP (Linux).

Il processo di replica e gestione delle sessioni di backup comprende tre fasi. Sono incluse le tre fasi seguenti:

- Replica delle sessioni di backup sulla destinazione di replica
- Creazione o aggiornamento dei file di configurazione dei punti di ripristino per la gestione e la visualizzazione nell'interfaccia Web dell'Agente Arcserve UDP (Linux)
- Aggiunta della destinazione di replica all'interfaccia Web dell'Agente Arcserve UDP (Linux)

Replica delle sessioni di backup

È possibile utilizzare la funzionalità Impostazioni pre/post script nella procedura guidata di backup per replicare le sessioni di backup nella destinazione di replica. È possibile scegliere qualsiasi opzione, tra cui File Transfer Protocol (FTP), Secure Copy (SCP) o il comando di cp, per la replica della sessione di backup.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Creare uno script di pre/post esecuzione per replicare le sessioni di backup.
3. Collocare lo script nel percorso seguente:

   ```
   /opt/Arcserve/d2dserver/usr/prepost
   ```

4. Accedere all'interfaccia Web dell'Agente Arcserve UDP (Linux).
5. Aprire la procedura guidata di backup e accedere alla pagina Impostazioni avanzate.
6. Nell'opzione Impostazioni script pre/post backup per Esegui sul server di backup, selezionare lo script di replica dall'elenco a discesa Al termine del processo.
7. Inoltrare il processo di backup.

   La sessione di backup viene replicata nella destinazione di backup.

Creazione o aggiornamento dei file di configurazione dei punti di ripristino

Dopo aver replicato le sessioni di backup, creare e configurare il file di configurazione dei punti di ripristino. Questo file viene utilizzato per identificare i punti di ripristino quando si esegue l'operazione di ripristino dall'interfaccia dell'Agente Arcserve UDP (Linux).

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Accedere alla posizione seguente:

   ```
   /opt/Arcserve/d2dserver/bin
   ```

3. Immettere il comando seguente per creare o aggiornare il file di configurazione dei punti di ripristino:

   ```
   ./d2drp --storagepath=/backupdestination --node=node_name --session=session_name
   ```

   Se si forniscono solo le informazioni *--storagepath* e *--node*, il comando aggiorna tutte le sessioni di backup per il nodo selezionato. Se si forniscono le informazioni *--session,* il comando aggiorna le informazioni di sessioni specifiche.

   Nota: per ulteriori informazioni sul comando d2drp, consultare la sezione *Presentazione delle utilità di generazione script*.

   Il file di configurazione dei punti di ripristino viene creato o aggiornato a seconda dello stato del file.

Aggiunta della destinazione di replica

Aggiungere la destinazione di replica all'interfaccia dell'Agente Arcserve UDP (Linux) per gestire la destinazione. Dopo aver aggiunto la destinazione di replica, è possibile visualizzare lo spazio libero disponibile sulla destinazione e gestire i relativi dati di conseguenza.

Effettuare le operazioni seguenti:

1. Accedere alla destinazione di replica.
2. Creare un file denominato Settings e immettere il codice seguente in questo file:

   ```
   RecoverySetLimit=n
   ```

   n indica il numero di set di ripristino da memorizzare nella destinazione di replica.

3. Collocare il file nella cartella di nodo della destinazione di replica.

   Ad esempio, /backup_destination/node_name/Settings

4. Accedere all'interfaccia Web dell'Agente Arcserve UDP (Linux).

5. Aggiungere la destinazione di replica dal menu Archiviazione di backup.

   La destinazione di replica viene aggiunta all'interfaccia Web dell'Agente Arcserve UDP (Linux).

   Le sessioni di backup sono state replicate e gestite correttamente.

Verifica dell'utilizzabilità dei punti di ripristino

L'utilità d2dverify consente di verificare che i punti di ripristino provenienti da diverse sessioni di backup siano utilizzabili. Generalmente, i processi di backup vengono eseguiti ogni giorno e, quando si hanno più punti di ripristino, può capitare di dubitare che i punti di ripristino siano utilizzabili per il ripristino dei dati durante un errore del sistema. Per evitare tali situazioni, è possibile eseguire periodicamente processi di ripristino bare metal per verificare l'utilizzabilità dei backup. L'utilità d2dverify consente di automatizzare l'attività di verifica dell'utilizzabilità dei punti di ripristino.

Dopo avere configurato i parametri obbligatori, l'utilità d2dverify invia il processo di ripristino bare metal e ripristina i dati nel computer virtuale specificato. Quindi, d2dverify avvia il computer virtuale ed esegue uno script per verificare se le applicazioni nel computer virtuale funzionano correttamente. È anche possibile creare una pianificazione per eseguire periodicamente l'utilità d2dverify mediante l'utilità di sistema, come ad esempio Linux Cron. Ad esempio, è possibile eseguire l'utilità d2dverify dopo l'ultimo backup di un set di ripristino. In questo caso, d2dverify verifica tutti i punti di ripristino in quel set di ripristino.

Nota: Per ulteriori informazioni sulla pianificazione di un processo utilizzando l'utilità di pianificazione Linux Cron, consultare Personalizzazione della pianificazione del processo.

È possibile utilizzare l'utilità d2dverify anche negli scenari seguenti:

- È possibile utilizzare l'utilità d2dverify per eseguire la migrazione dei backup di diversi computer fisici su computer virtuali.
- Al completamento del ripristino di un hypervisor, è possibile utilizzare l'utilità d2dverify per ripristinare tutti i computer virtuali sul nuovo hypervisor.

Considerare i seguenti prerequisiti prima di utilizzare l'utilità d2dverify:

- Identificare i nodi di origine di cui si desidera verificare il backup.
- Identificare un hypervisor in cui verranno creati i computer virtuali.
- Creare computer virtuali per ciascun nodo che si desidera verificare. Assegnare un nome al computer virtuale nel formato seguente:

  `verify_<node name>`

  Nota: Non è necessario allegare dischi rigidi virtuali per questi computer virtuali. Inoltre, è possibile non associare una rete virtuale a questi computer virtuali se si specificano parametri vm_network.

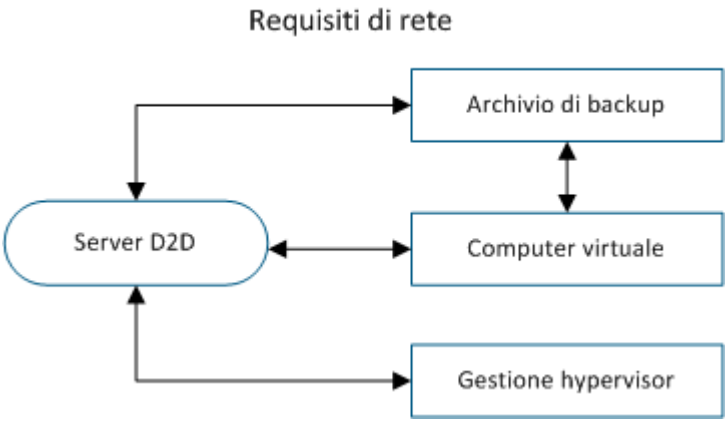
- Verifica dei requisiti di rete
- Identificare una rete a cui verranno connessi i computer virtuali.

  Nota: L'utilità d2dverify supporta solo la rete IP statica.

Importante: Se il database presenta le informazioni sull'account del nodo relative a un utente non root, d2dverify reimposterà la password dell'utente non root su 'CAd2d@2013 per il computer virtuale di destinazione.

Requisiti di rete:

Quando si utilizza d2dverify, si consiglia di tenere i computer virtuali di destinazione in una rete virtuale isolata per evitare eventuali conflitti con l'ambiente di produzione. In tali casi, è necessario connettere i computer virtuali di destinazione sia al server di backup che all'archiviazione di backup.



Supporto dell'hypervisor:

d2dverify dipende dall'utilità d2drestorevm per eseguire il ripristino. d2dverify supporta le versioni seguenti degli hypervisor:

- XenServer 6.0 e successive
- OVM 3.2

Argomenti:

--template

Identifica il modello che include i parametri per eseguire l'utilità d2dverify.

--createtemplate

Crea un modello vuoto che include i parametri per eseguire l'utilità d2dverify.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Creare il modello utilizzato dall'utilità d2dverify mediante il comando seguente:

   ```
   d2dverify --createtemplate=file_path
   ```

3. Aprire il modello e aggiornare i parametri seguenti:

   node_list

   Specifica un elenco di nodi o un criterio di query che interroga le informazioni provenienti dal database del server di backup. Ciascun nodo viene separato da una virgola, ad esempio Node1,Node2,Node3.

   Note: Se il numero di porta SSH non è quello predefinito (22), il formato che consente di specificare ciascun nodo è: Node1:new_port,Node2:new_port,Node3:new_port. Il nome del computer virtuale viene assegnato come verify_<node name>, dove il nome del nodo non include il numero di porta.

   Esempio: Node1:222,Node2:333,Node4:333

   L'elenco seguente è un esempio di criteri di query:

   [node=prefix]

   Trova il nome del nodo contenente il prefisso definito.

   [desc=prefix]

   Trova la descrizione del nodo contenente il prefisso definito.

   guest_ip_list =

   Specifica l'elenco di indirizzi IP applicato rispettivamente a ciascun nodo di destinazione. Ogni indirizzo IP viene separato da una virgola, ad esempio IP1,IP2,IP3. Se è disponibile solamente un indirizzo IP, ma nel parametro node_list sono presenti più nodi, il quarto segmento dell'indirizzo IP viene aumentato di uno per ciascun nodo. L'utilità d2dverify verifica se è stato utilizzato un indirizzo IP. In caso affermativo, quell'indirizzo IP viene ignorato.

   Ad esempio, se si hanno tre nodi, Node 1, Node 2 e Node 3 e un indirizzo IP, xxx.xxx.xxx.xx6, l'indirizzo IP viene applicato così come illustrato nell'elenco seguente:

   Node 1: xxx.xxx.xxx.xx6

   Node 2: xxx.xxx.xxx.xx7

   Node 3: xxx.xxx.xxx.xx8

   vm_type

   Specifica il tipo di hypervisor. Sono validi i seguenti tipi di hypervisor: xen oppure ovm.

vm_server

Specifica il nome host o l'indirizzo IP della gestione hypervisor.

vm_svr_username

Specifica il nome utente della gestione hypervisor.

vm_svr_password

Specifica la password della gestione hypervisor. È necessario crittografare la password mediante l'utilità d2dutil --encrypt.

Per crittografare la password viene utilizzato il seguente comando:

```
echo "password" | d2dutil --encrypt
```

vm_network

Specifica la rete virtuale utilizzata dal computer virtuale di destinazione. Si consiglia di specificare questo parametro se il computer virtuale di destinazione viene connesso a più reti virtuali.

guest_gateway

Specifica il gateway di rete utilizzato dal sistema operativo ospite del computer virtuale di destinazione.

guest_netmask

Specifica la net mask utilizzata dal sistema operativo ospite del computer virtuale di destinazione.

guest_username

Specifica il nome utente utilizzato per connettersi al computer virtuale ripristinato. La password viene reimpostata sulla password specificata nel parametro guest_password. Il parametro guest_username viene ignorato quando si utilizza l'utilità d2dverify per interrogare le informazioni provenienti dal database del server di backup. In tali casi, la password dell'ospite del computer virtuale viene reimpostata sulla password del nodo archiviato nel database.

guest_password

Specifica la password per il parametro guest_username. È necessario crittografare la password mediante l'utilità d2dutil --encrypt. Il parametro guest_password viene ignorato quando si utilizza l'utilità d2dverify per interrogare le informazioni provenienti dal database del server di backup.

storage_location

Specifica il percorso di rete della posizione di archiviazione di backup. Non è necessario specificare la posizione di archiviazione se i nodi nel parametro node_list si trovano nel database del server di backup. Se la posizione di archiviazione è una condivisione CIFS, utilizzare il formato seguente per specificarla:

```
//hostname/path
```

storage_username

Specifica il nome utente per accedere alla posizione di archiviazione di backup. Questo parametro non è richiesto per una condivisione NFS.

Per un utente di dominio Windows, utilizzare il formato seguente per specificare la posizione:

```
domain_name/username
```

storage_password

Specifica la password per accedere alla posizione di archiviazione di backup. È necessario crittografare la password mediante l'utilità d2dutil --encrypt. Questo parametro non è richiesto per una condivisione NFS.

recovery_point = last

Selezionare la sessione da ripristinare. Generalmente, una sessione di ripristino presenta il formato seguente: S00000000X, dove X è un valore numerico. S00000000X è il nome della cartella dei punti di ripristino. Se si desidera ripristinare la sessione più recente, specificare la parola chiave 'last'.

encryption_password

Specifica la password di crittografia per il punto di ripristino. È necessario crittografare la password mediante l'utilità d2dutil --encrypt.

script

Specifica lo script che si desidera eseguire. Lo script viene eseguito sul computer di destinazione dopo un ripristino eseguito correttamente. Se questo parametro non viene fornito, l'utilità d2dverify esegue il comando ls /proc sul computer di destinazione.

email_to_address

Specifica l'indirizzo di posta elettronica dei destinatari che riceveranno i report in un messaggio di posta elettronica. È possibile specificare più di un indirizzo di posta elettronica, separati da una virgola.

email_subject

Specifica l'oggetto del messaggio di posta elettronica.

report_format

Specifica il formato del report che si riceverà in un messaggio di posta elettronica. Il formato potrebbe essere testo (.txt) o HTML.

Valore predefinito: html

node_not_in_db

Specifica i nodi dei parametri node_list che non sono contenuti nel database del server di backup. È necessario specificare i parametri storage_* related.

Valore: Sì

stop_vm_after_recovery

Specifica l'interruzione del computer virtuale di destinazione dopo la corretta esecuzione del ripristino e della verifica. I valori per questo parametro sono Sì e No.

Valore predefinito: Sì

4. Salvare e chiudere il modello.
5. Eseguire l'utilità d2dverify utilizzando il seguente comando:

   ```
   d2dverify --template=file_path
   ```

   Nota: L'utilità d2dverify non riesce se i nodi del parametro node_list vengono aggiunti utilizzando la chiave pubblica/privata. Per risolvere questo problema, configurare la variabile di ambiente export D2D_SSH_IGNORE_PWD=yes nell'ambiente della shell in cui si esegue l'utilità d2dverify.

   L'utilizzabilità dei punti di ripristino è stata correttamente verificata.

Gestione delle impostazioni del server di backup

Per gestire il server di backup, effettuare le operazioni seguenti:

- Configurare la durata del periodo di memorizzazione della cronologia dei processi e dei registri delle attività
- Configurare la durata del periodo di memorizzazione dei registri di debug
- Modifica del numero di porta SSH del server di backup

Per gestire le impostazioni del server di backup, eseguire le attività seguenti:

- Verifica dei prerequisiti per la gestione del server di backup
- Configurazione delle impostazioni di conservazione della cronologia dei processi e dei registri delle attività
- Configurazione delle impostazioni di conservazione del registro di debug
- Configurazione della durata del timeout dell'interfaccia utente
- Modifica del numero di porta SSH del server di backup
- Gestione dei set di ripristino
- Disattivazione dei servizi BOOTPD e TFTPD
- Miglioramento delle prestazioni di query per la cronologia dei processi e il registro attività
- Disabilitazione della verifica dei client CIFS e NFS
- Disabilitazione della convalida CIFS e NFS sul server Linux di backup
- Configurazione della cartella temporanea predefinita
- Configurazione del percorso della snapshot per il nodo di backup
- Configurazione delle informazioni di connessione del server Hyper-V per il computer virtuale istantaneo

Verifica dei prerequisiti per la gestione del server di backup

Considerare i prerequisiti seguenti prima di gestire il server di backup:

- Si dispone delle credenziali di accesso per l'utente root al server di backup.
- Esaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Configurazione delle impostazioni di conservazione della cronologia dei processi e dei registri delle attività

È possibile configurare la durata del periodo di memorizzazione della cronologia dei processi e dei registri delle attività. Se si desidera conservare i registri delle attività e la cronologia dei processi durante un periodo di tempo maggiore, configurare il file server.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Aprire il file server.cfg:

   ```
   /opt/Arcserve/d2dserver/configfiles/server.cfg
   ```

   Nota: se il file non è presente, creare il file server.cfg.
3. Aggiungere la riga seguente nel file server.cfg:

   ```
   job_history_activity_log_keep_day=<numero di giorni>
   ```

   Esempio: per memorizzare la Cronologia processo e il Registro attività per 30 giorni, immettere la riga seguente:

   ```
   job_history_activity_log_keep_day=30
   ```

   Nota: per impostazione predefinita, la Cronologia processo e i Registri attività vengono memorizzati per 90 giorni.

   La Cronologia processo e il Registro attività vengono memorizzati per il tempo specificato.

Configurazione delle impostazioni di conservazione del registro di debug

È possibile configurare la durata del periodo di memorizzazione dei registri di debug. Se si desidera conservare i registri di debug durante un periodo di tempo maggiore, configurare il file server.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Aprire il file server.cfg:

   ```
   /opt/Arcserve/d2dserver/configfiles/server.cfg
   ```

   Nota: per impostazione predefinita, la Cronologia processo e i Registri attività vengono memorizzati per 90 giorni.

3. Aggiungere la riga seguente nel file server.cfg:

   ```
   d2d_log_keep_day =<numero di giorni>
   ```

   Esempio: per memorizzare il registro di debug per 30 giorni, immettere la riga seguente:

   ```
   d2d_log_keep_day =30
   ```

   Nota: per impostazione predefinita, i Registri attività vengono memorizzati per 90 giorni.

   Il registro di debug dell'Agente Arcserve UDP (Linux) viene memorizzato per il periodo specificato.

Configurazione della durata del timeout dell'interfaccia utente

È possibile configurare il file di configurazione del server Web in modo che l'utente venga disconnesso dall'interfaccia utente quando questa non è attiva. Una volta configurato il file, se non si esegue nessuna attività sull'interfaccia utente per la durata specificata, l'utente viene disconnesso automaticamente. È possibile accedere di nuovo e riprendere le attività.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Aprire il file server.cfg dal percorso seguente:

   `/opt/Arcserve/d2dserver/configfiles/server.cfg`

   Nota: se il file server.cfg non è presente, crearlo.

3. Aggiungere la riga seguente nel file server.cfg:

   `ui_timeout=<value>`

   Esempio:

   Il valore deve essere specificato in minuti. Il valore massimo di timeout dell'interfaccia utente è pari a 60.

   `ui_timeout=40`

   L'esempio indica che se il server di backup non rileva alcuna attività sull'interfaccia utente per 40 minuti, l'utente viene disconnesso.

4. Aggiornare il browser Web per implementare le modifiche.

   La durata del timeout dell'interfaccia utente è configurata.

Modifica del numero di porta SSH del server di backup

Il server di backup utilizza la porta SSH predefinita (22) per connettersi ai nodi. Se si desidera modificare la porta predefinita con una porta diversa, è possibile configurare il file server.env per specificare la nuova porta.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Aprire il file server.env.

   ```
   /opt/Arcserve/d2dserver/configfiles/server.env
   ```

   Nota: Se il file non è presente, creare il file server.env.

3. Aggiungere la seguente riga al file server.env e salvarlo:

   ```
   export D2D_SSH_PORT=new_port_number
   ```

   new_port_number deve essere un valore numerico.

4. Riavviare il server di backup.

   Dopo avere configurato il file server.env, tutti i processi, tranne il processo di ripristino bare metal, utilizzano il nuovo numero di porta per connettersi al nodo di destinazione. Il processo di ripristino bare metal utilizza la porta predefinita.

   Il numero di porta SSH del server di backup è stato modificato correttamente.

Gestione dei set di ripristino

La gestione dei set di ripristino comprende la loro eliminazione. È opportuno gestire regolarmente i set di ripristino per rendersi conto dello spazio libero disponibile. Di conseguenza, è possibile pianificare l'archiviazione dei set di ripristino. Ci sono due modi per gestire i set di ripristino:

- **Metodo 1:** Gestione mediante un'archiviazione di backup dedicata. In questo metodo, l'archiviazione di backup gestisce i set di ripristino ogni 15 minuti. È possibile gestire solo le archiviazioni di backup a cui il server di backup può accedere. Se si sceglie l'origine locale come destinazione di backup, è necessario condividere la cartella locale.
- **Metodo 2:** Gestione mediante un processo di backup. In questo metodo, il processo di backup gestisce i set di ripristino. I set di ripristino vengono gestiti dopo che il processo di backup è terminato. È possibile gestire i set di ripristino archiviati nell'origine locale.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Aprire il file server.cfg.

   ```
   /opt/Arcserve/d2dserver/configfiles/server.cfg
   ```

   Nota: se il file non è presente, creare il file server.cfg.
3. Aggiungere la seguente riga al file server.cfg e salvarlo:

   ```
   manage_recoveryset_local=0 or 1
   ```

   Il valore 0 indica che il file utilizza il metodo 1.

   Il valore 1 indica che il file utilizza il metodo 2.
4. Riavviare il server di backup.

   I set di ripristino vengono gestiti dalla riga di comando del server di backup.

Disattivazione dei servizi BOOTPD e TFTPD

È possibile disattivare i servizi BOOTPD e TFTPD se la funzione di ripristino bare metal PXE non è necessaria.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Aprire il file server.env.

   ```
   /opt/Arcserve/d2dserver/configfiles/server.env
   ```

   Nota: se il file server.env non è presente, creare il file.
3. Aggiornare il seguente parametro nel file server.env e salvarlo:

   ```
   export D2D_DISABLE_PXE_SERVICE=yes
   ```
4. Riavviare il server di backup.

   ```
   /opt/Arcserve/d2dserver/bin/d2dserver restart
   ```

   I servizi BOOTPD e TFTPD sono stati disattivati correttamente.

Miglioramento delle prestazioni di query per la cronologia dei processi e il registro attività

Se si dispone di un file di database di dimensioni più grandi, l'interrogazione della cronologia del processo e del registro attività richiede molto tempo. È possibile migliorare il tempo di query per la cronologia del processo e il registro attività utilizzando switch specifici. In questo modo, sarà possibile ricevere l'output in breve tempo.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Aprire il file server.cfg:

   ```
   /opt/Arcserve/d2dserver/configfiles/server.cfg
   ```

   Nota: se il file non è presente, creare il file server.cfg.

3. Aggiungere le seguenti righe al file server.cfg:
   - Per migliorare le prestazioni di query della cronologia del processo, aggiungere la seguente riga:

     ```
     skip_getting_job_history_count=true
     ```

   - Per migliorare le prestazioni di query del registro attività, aggiungere la seguente riga:

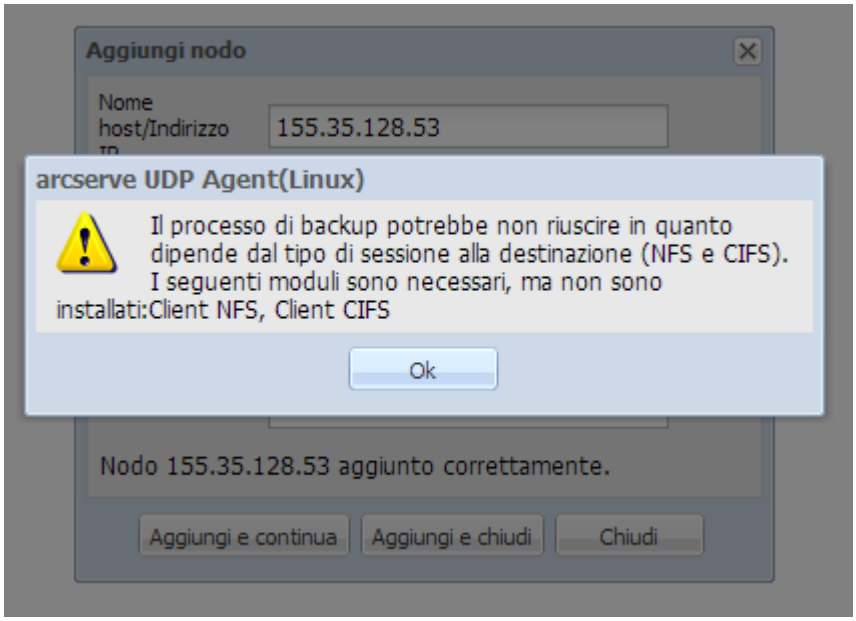
     ```
     skip_getting_activity_log_count=true
     ```

4. Salvare il file server.cfg.

   Il tempo di query per la cronologia del processo e il registro attività è stato migliorato correttamente.

Disabilitazione della verifica dei moduli CIFS e NFS

Durante l'aggiunta o la modifica di un nodo, il server di backup verifica i moduli CIFS e NFS sul nodo di destinazione. Se tali moduli non sono stati installati, viene visualizzato un messaggio di avviso. È possibile nascondere questa finestra di dialogo configurando il file server.cfg.



Effettuare le operazioni seguenti:

1. Accedere al server di backup.
2. Aprire il file server.cfg:

   `/opt/Arcserve/d2dserver/configfiles/server.cfg`

3. Aggiungere i seguenti parametri:

   `skip_client_check=nfs,cifs`

   L'esempio fornito consente di ignorare la verifica dei moduli NFS e CIFS sul nodo di destinazione. Specificare entrambi i moduli per non eseguire la verifica di tali moduli. Specificare un solo modulo per non eseguire la verifica del modulo specificato.

4. Salvare il file server.cfg.

   La verifica viene ignorata per i moduli CIFS e NFS.

Disabilitazione della convalida CIFS e NFS sul server Linux di backup

Quando si aggiunge o si modifica l'archiviazione del server di backup, esso esegue la convalida se è possibile accedere a CIFS o NFS sul server Linux di backup. Se si desidera ignorare la convalida sul server di backup Linux, è possibile configurare il file server.env.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Aprire il file server.env:

   ```
   /opt/Arcserve/d2dserver/configfiles/server.env
   ```

   Nota: Se il file non è presente, creare il file server.env.
3. Aggiungere la riga seguente nel file server.env:

   ```
   export skip_validate_backup_storage_on_server=true
   ```
4. Riavviare il server di backup.

Configurazione della cartella temporanea predefinita

Durante il backup dei nodi Linux, viene utilizzata la cartella predefinita **/tmp** per archiviare i registri binari, dei dati di snapshot temporanei e quelli di debug necessari. La cartella /tmp deve disporre di spazio libero sufficiente e delle autorizzazioni necessarie per eseguire i file binari. Per modificare il percorso predefinito sui nodi Linux, configurare il file server.env e indicare i nuovi percorsi.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Aprire il file server.env:

   ```
   /opt/Arcserve/d2dserver/configfiles/server.env
   ```

   Nota: Se il file non è presente, creare il file server.env.

3. Per configurare il percorso di esecuzione dell'agente per un nodo Linux, aggiungere la riga seguente nel file server.env:

   ```
   export TARGET_BOOTSTRAP_DIR=<path>
   ```

   Esempio: Per effettuare la distribuzione dell'agente Linux al percorso **/d2dagent**, immettere la riga seguente:

   ```
   export TARGET_BOOTSTRAP_DIR=/d2dagent
   ```

   Nota: Per impostazione predefinita, l'agente viene distribuito ed eseguito nella cartella /tmp.

4. Per configurare il registro di debug del nodo Linux e il percorso di archiviazione dei registri di debug, aggiungere la riga seguente nel file server.env:

   ```
   export TARGET_ WORK_DIR=<path>
   ```

   Esempio: per configurare i registri di debug e i dati di snapshot temporanea nel percorso **d2dagentlogs**, immettere la riga seguente:

   ```
   export TARGET_WORK_DIR=/d2dagentlogs
   ```

   Nota: per impostazione predefinita, l'agente viene distribuito ed eseguito nella cartella /tmp.

5. Riavviare il server di backup.

   ```
   /opt/Arcserve/d2dserver/bin/d2dserver restart
   ```

   La cartella temporanea predefinita è stata configurata.

Configurazione del percorso della snapshot per il nodo di backup

Durante il backup dei nodi Linux, viene utilizzata la cartella predefinita **/tmp** per archiviare il file di snapshot del disco. La cartella **/tmp** deve disporre di spazio libero sufficiente. Per modificare il percorso della snapshot sui nodi Linux, configurare un file specifico per il nodo e indicare il nuovo percorso.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Accedere alla cartella **node**:

   `/opt/Arcserve/d2dserver/configfiles/node`

   Nota : se la cartella non è presente, è necessario crearla.

   La cartella **node** contiene il file <node_name>.cfg. È previsto un file .cfg per ogni nodo.

3. Per configurare il percorso di snapshot di un nodo Linux, aggiungere la riga seguente nel file <node_name>.cfg specifico:

   `target_snapshot_dir=<path>`

   Nota : se il file <node_name>.cfg non è presente, è necessario crearlo.

   Esempio: se il nome del nodo è **d2dbackupnode** e si desidera archiviare la snapshot nel percorso **/d2dsnapshot**, aprire il seguente file .cfg:

   `/opt/Arcserve/d2dserver/configfiles/node/d2dbackupnode.cfg`

   Aggiungere la riga seguente:

   `target_snapshot_dir=/d2dsnapshot`

   La cartella della snapshot sul nodo di destinazione è stata configurata.

Configurazione delle informazioni di connessione del server Hyper-V per il computer virtuale istantaneo

Quando vengono inviati i processi del computer virtuale istantaneo per i nodi Linux, il server di backup tenta di rilevare automaticamente il server Hyper-V. Tuttavia, se il processo non riesce, è possibile verificare che siano state utilizzate le informazioni corrette per la connessione al server Hyper-V.

Il computer virtuale istantaneo di Linux supporta Hyper-V con SMB 2.0 (o versioni successive) per evitare le vulnerabilità di SMB 1.0.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Accedere alla seguente cartella Hyper-V:

   `/opt/Arcserve/d2dserver/configfiles/hyperv`

   Nota : se la cartella non è presente, è necessario crearla. La cartella Hyper-V contiene il file <upper_case_hyperv_server_name>.cfg. Ogni server Hyper-V dispone del proprio file cfg.

3. Per configurare le informazioni di connessione Hyper-V, aggiungere le seguenti righe al file <upper_case_hyperv_server_name>.cfg specifico:

   protocol=<HTTP|HTTPS>

   port=<number>

   Nota: se il file <upper_case_hyperv_server_name>.cfg non è presente, è necessario crearlo.

   Per il numero di porta e protocollo, accedere al server di destinazione Hyper-V mediante la seguente riga di comando:

   winrm enumerate winrm/Config/Listener

   Ad esempio, il nome del server Hyper-V di destinazione è ivm-hyperv e WinRM sul server Hyper-V è configurato come HTTPS in attesa sulla porta 5986. Aprire quindi il seguente file cfg:

   /opt/Arcserve/d2dserver/configfiles/hyperv/IVM-HYPERV.cfg

   Aggiungere le righe seguenti:

   protocol=HTTPS

   port=5986

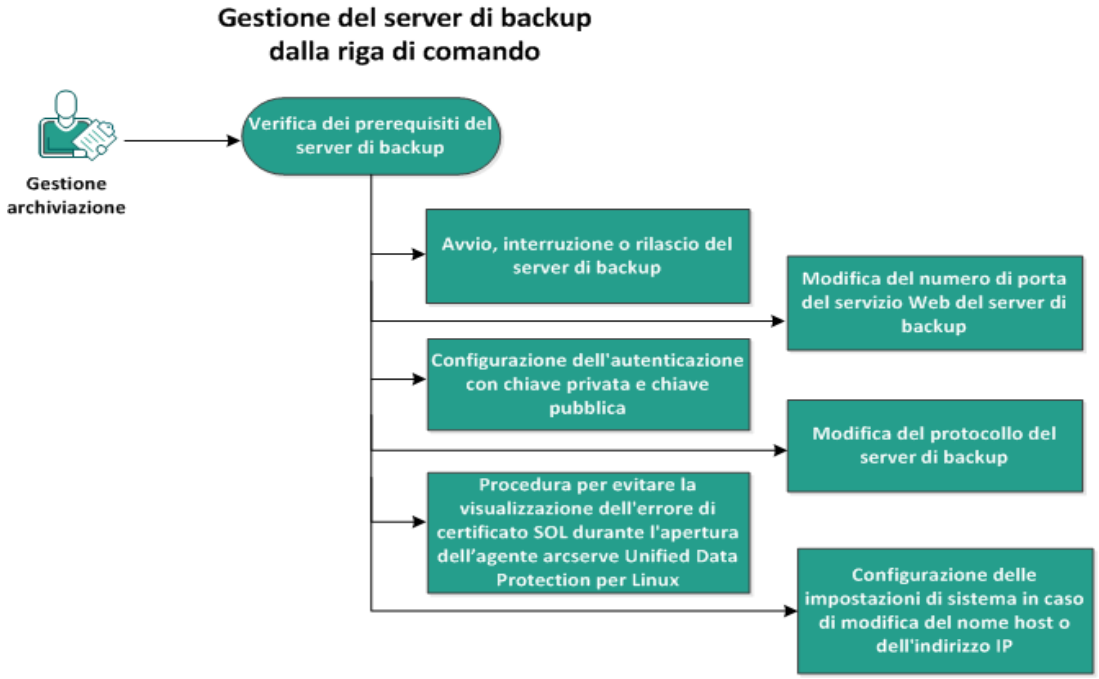
Le informazioni di connessione per il server Hyper-V sono configurate.

Gestione del server di backup Linux dalla riga di comando

Il server di backup Linux esegue tutte le attività di elaborazione dell'Agente Arcserve UDP (Linux). Per corretto funzionamento dell'Agente Arcserve UDP (Linux), è necessario verificare che il server di backup sia sempre in esecuzione. È possibile accedere al server di backup e gestire il server mediante alcuni comandi.

Ad esempio, se si desidera accedere all'interfaccia Web dell'Agente Arcserve UDP (Linux), è necessario accertarsi che il server Web sia in esecuzione. È possibile verificare lo stato di esecuzione del server Web dal server di backup e verificare il corretto funzionamento dell'Agente Arcserve UDP (Linux).

Nel diagramma seguente è possibile visualizzare il processo per la gestione del server di backup dalla riga di comando:



Per gestire il server di backup, eseguire le attività seguenti:

- Verifica dei prerequisiti del server di backup
- Avvio, interruzione o rilascio del server di backup
- Modifica del numero di porta del servizio Web del server di backup
- Configurazione dell'autenticazione con chiave privata e chiave pubblica
- Modifica del protocollo del server di backup

- Blocco della visualizzazione dell'errore di certificato SSL all'apertura dell'Agente Arcserve UDP (Linux)
- Configurazione delle impostazioni di sistema in caso di modifica del nome host o dell'indirizzo IP

Verifica dei prerequisiti del server di backup

Considerare i prerequisiti seguenti prima di gestire il server di backup:

- Si dispone delle credenziali di accesso per l'utente root al server di backup.
- Esaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Avvio, interruzione o rilascio del server di backup

Gestire il server di backup per conoscere lo stato di esecuzione del server di backup. È possibile verificare se il server di backup è stato interrotto o è ancora in esecuzione, quindi gestire il server di conseguenza. Agente Arcserve UDP (Linux) supporta le funzioni della riga di comando seguenti:

- Avvio del server di backup
- Interruzione del server di backup
- Rilascio del server di backup

Effettuare le operazioni seguenti:

1. Accedere alla cartella bin mediante il seguente comando:

   ```
   # cd /opt/Arcserve/d2dserver/bin
   ```

   Accedere alla cartella bin.

2. Dalla cartella bin, eseguire i comandi seguenti in base all'attività che si desidera eseguire sul server:

   Nota: in caso di errore di un comando, verrà visualizzato un messaggio di errore contenente la spiegazione corrispondente.

   ```
   # ./d2dserver start
   ```

   Avvia il server di backup.

   Se l'operazione viene eseguita correttamente, viene visualizzato un messaggio che informa l'utente circa l'avvio del server.

   ```
   # ./d2dserver stop
   ```

   Interrompe il server di backup.

   Se l'operazione viene eseguita correttamente, viene visualizzato un messaggio che informa l'utente circa l'interruzione del server.

   ```
   # ./d2dserver restart
   ```

   Riavvia il server di backup.

   Se l'operazione viene eseguita correttamente, viene visualizzato un messaggio che informa l'utente circa il riavvio del server.

   ```
   # ./d2dserver status
   ```

   Visualizza lo stato del server di backup.

```
# /opt/Arcserve/d2dserver/bin/d2dreg --release
```

Rilascia i server di backup rimanenti che vengono gestiti dal server principale.

Ad esempio, se il server di backup A gestisce altri due server, ovvero il server di backup B e il server di backup C, quando si disinstalla il server di backup A non è possibile accedere al server di backup B e al server di backup C. È possibile rilasciare il server di backup B e il server di backup C mediante questo script e accedere ai server.

Il server di backup è gestito correttamente dalla riga di comando.

Modifica del numero di porta del servizio Web del server di backup

L'Agente Arcserve UDP (Linux) utilizza la porta 8014 per impostazione predefinita. Se il numero di porta 8014 è utilizzato da altre applicazioni, l'Agente Arcserve UDP (Linux) non funziona correttamente. In questo caso, è necessario modificare il numero di porta predefinito dell'Agente Arcserve UDP (Linux) con un numero di porta differente.

Effettuare le operazioni seguenti:

1. Aprire il file server.xml dal percorso seguente:

   ```
   /opt/Arcserve/d2dserver/TOMCAT/conf/server.xml
   ```

2. Cercare la stringa seguente nel file e sostituire il numero di porta 8014 con il numero di porta desiderato:

   ```
   <Connector port="8014" protocol="HTTP/1.1" SSLEnabled="true"
   maxThreads="150" scheme="https" secure="true" clien-
   tAuth="false" sslProtocol="TLS" key-
   storeFile="${catalina.home}/conf/server.keystore"
   keystorePass="LinuxD2D"/>
   ```

3. Eseguire il comando seguente per riavviare il server di backup:

   ```
   /opt/Arcserve/d2dserver/bin/d2dserver restart
   ```

   Il numero di porta predefinito viene sostituito dal numero di porta desiderato.

Configurazione dell'autenticazione con chiave privata e chiave pubblica

La chiave pubblica e la chiave privata consentono di connettersi ai nodi in modalità protetta nei casi in cui non venga fornita la password. Ogni volta che il server di backup crea una connessione SSH con i nodi, il server di backup verifica la chiave pubblica e la chiave privata per i rispettivi nodi. Se le chiavi non coincidono, viene visualizzato un messaggio di errore.

Nota:

- Solo gli utenti che dispongono dell'autorizzazione root possono utilizzare l'autenticazione con la chiave pubblica e la chiave privata. Non è necessario che il nome utente sia root. Gli utenti non root non possono utilizzare l'autenticazione con la chiave pubblica e la chiave privata. Gli utenti non root devono fornire l'autenticazione con nome utente e password.
- L'autenticazione con chiave pubblica e chiave privata può essere utilizzata nei casi in cui non viene fornita la password. Il nome utente è comunque obbligatorio e deve corrispondere al proprietario della chiave.
- Quando si utilizza l'autenticazione sudo, consultare la sezione How to Configure Sudo User Account for Linux Nodes (Come configurare un account utente sudo per i nodi Linux) per informazioni sulla configurazione specifica.
- Verrà richiesto un piano per aggiungere un nodo Linux per l'autenticazione della chiave SSH, che presenta una serie di modifiche relative alla configurazione sia nel server di backup di Linux sia nel computer virtuale di origine.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Generare una chiave pubblica/privata mediante il seguente comando ssh-keygen:

   ```
   ssh-keygen -t rsa -f server
   ```

   Nota: è possibile generare una chiave pubblica/privata per Rhel/alma/rocky/orel 9.x e Debian 12.x utilizzando il seguente comando:

   ```
   ssh-keygen -t ecdsa -f server
   ```

   Vengono generati due file, ovvero server.pub e server.
3. Copiare il file della chiave pubblica server.pub nella seguente posizione:

   ```
   /opt/Arcserve/d2dserver/configfiles/server_pub.key
   ```

4. Copiare il file server della chiave privata nella seguente posizione:

   ```
   /opt/Arcserve/d2dserver/configfiles/server_pri.key
   ```

5. (Facoltativo) Eseguire il comando seguente se è stata fornita la passphrase durante la generazione delle chiavi pubbliche e private:

   ```
   echo "passphrase" | ./d2dutil --encrypt > /op-
   t/Arcserve/d2dserver/configfiles/key.pass
   ```

6. Modificare l'autorizzazione per il file key.pass mediante il comando seguente:

   ```
   chmod 600 /opt/Arcserve/d2dserver/configfiles/key.pass
   ```

7. Accedere al nodo di origine.
8. Copiare il contenuto dal file server_pub.key situato nel server di backup nella seguente posizione nel nodo:

   ```
   /<user_home>/.ssh/authorized_keys
   ```

   Esempio: per backup_admin, user_home corrisponde a */home/backup_admin*

   Esempio: /home/backup_admin/.ssh/authorized_keys

9. (Facoltativo) Eseguire il seguente comando nel nodo se SELinux blocca l'autenticazione:

   ```
   restorecon /<user_home>/.ssh/authorized_keys
   ```

   La chiave privata e la chiave pubblica sono state configurate correttamente. Mediante la chiave pubblica e la chiave privata, è possibile connettersi ai nodi di origine.

Modifica del protocollo del server di backup

L'Agente Arcserve UDP (Linux) viene installato con il protocollo https. È possibile modificare il protocollo se non si desidera trasferire i dati con crittografia. Si consiglia di utilizzare il protocollo HTTPS perché tutti i dati trasferiti tramite questo protocollo vengono crittografati. I dati trasferiti tramite il protocollo HTTP dispongono di testo non crittografato.

Effettuare le operazioni seguenti:

1. Aprire il file server.xml dal percorso seguente:

   ```
   /opt/Arcserve/d2dserver/TOMCAT/conf/server.xml
   ```

2. Cercare la stringa seguente nel file server.xml:

   ```
   <!--<Connector connectionTimeout="180000" port="8014" pro-
   tocol="HTTP/1.1"/>-->
   ```

3. Rimuovere i caratteri di stringa **<!--** e **-->** come mostrato nell'esempio seguente:

   Esempio: la stringa seguente è l'output desiderato dopo la rimozione dei caratteri di stringa **<!--** e **-->**:

   ```
   <Connector connectionTimeout="180000" port="8014" pro-
   tocol="HTTP/1.1"/>
   ```

4. Cercare la stringa seguente nel file server.xml:

   ```
   <Connector port="8014" protocol="HTTP/1.1" SSLEnabled="true"
   maxThreads="150" scheme="https" secure="true" clien-
   tAuth="false" sslProtocol="TLS" key-
   storeFile="${catalina.home}/conf/server.keystore"
   keystorePass="LinuxD2D"/>
   ```

5. Aggiungere i caratteri di stringa **<!--** e **-->** come mostrato nell'esempio seguente:

   Esempio: la stringa seguente è l'output desiderato dopo l'aggiunta dei caratteri di stringa **<!--** e **-->** :

   <!--
   ```
   <Connector port="8014" protocol="HTTP/1.1" SSLE-
   nabled="true" maxThreads="150" scheme="https" secure="true"
   clientAuth="false" sslProtocol="TLS" key-
   storeFile="${catalina.home}/conf/server.keystore" key-
   storePass="LinuxD2D"/>
   ```
   -->

6. Eseguire il comando seguente per riavviare il server di backup:

   ```
   /opt/Arcserve/d2dserver/bin/d2dserver restart
   ```

Il protocollo del server di backup viene modificato da https a http.

Blocco della visualizzazione dell'errore di certificato SSL all'apertura dell'Agente Arcserve UDP (Linux)

Per evitare la visualizzazione dell'errore di certificato quando si apre l'interfaccia Web dell'Agente Arcserve UDP (Linux), rimuovere il certificato SSL personalizzato. Una volta configurato il certificato SSL, non si riceverà più l'errore di certificato.

Effettuare le operazioni seguenti:

- Utilizzare il certificato generato dall'Agente Arcserve UDP (Linux) per il browser Firefox.

  1. Aprire l'Agente Arcserve UDP (Linux) in Firefox.
  2. Fare clic su Sono consapevole dei rischi e fare clic su Aggiungi eccezione.

     Viene visualizzata la finestra di dialogo Aggiungi eccezione di sicurezza.
  3. Fare clic su Visualizza per visualizzare il certificato.

     Verrà visualizzata la finestra di dialogo del visualizzatore di certificati.
  4. Verificare i dettagli del certificato e fare clic su Chiudi.

     Non è necessario effettuare alcuna operazione nella finestra del visualizzatore di certificati.
  5. Nella finestra di dialogo Aggiungi eccezione di sicurezza, selezionare la casella di controllo Salva eccezione in modo permanente.
  6. Fare clic su Conferma eccezione di sicurezza.

     Il certificato viene aggiunto.

- Utilizzare il certificato generato dall'Agente Arcserve UDP (Linux) per i browser Internet Explorer (IE) o Chrome.

  1. Aprire l'Agente Arcserve UDP (Linux) in IE o Chrome.
  2. Fare clic su Continuare con il sito Web (scelta non consigliata).

     La barra degli indirizzi viene mostrata in rosso e viene visualizzato un messaggio di errore del certificato nella barra Stato protezione.
  3. Fare clic su Errore certificato.

     Viene visualizzata la finestra di dialogo Certificato non attendibile.

4. Fare clic su Visualizza certificati.

   Viene visualizzata la finestra di dialogo Certificato.

5. Nella scheda Generale, fare clic su Installa certificato.

   Viene visualizzata l'Importazione guidata certificati.

6. Fare clic su Avanti.
7. Nella pagina Archivio certificati, selezionare Colloca tutti i certificati nel seguente archivio e fare clic su Sfoglia.
8. Selezionare Autorità di certificazione fonti attendibili e fare clic su OK.

   Viene visualizzata la pagina Archivio certificati dell'Importazione guidata certificati.

9. Fare clic su Avanti, quindi su Fine.

   Viene visualizzata la finestra di dialogo Avviso di protezione.

10. Fare clic su Sì.
11. Riavviare IE o Chrome.

    Il certificato viene aggiunto.

    Nota: dopo aver aggiunto il certificato, il browser di Chrome mostra l'icona di errore per il certificato SSL nella barra degli indirizzi. Si tratta di un promemoria sulle autorità di certificazione che non identificano il certificato. Tuttavia, il certificato viene considerato attendibile da Chrome e tutti i dati trasferiti alla rete vengono crittografati.

- Eseguire le operazioni seguenti per utilizzare un certificato firmato:

  1. Utilizzare il certificato firmato da un'autorità di certificazione.
  2. Importare il certificato firmato utilizzando il comando keytool.

     Il certificato viene aggiunto.

L'errore del certificato SSL viene risolto.

Configurazione delle impostazioni di sistema in caso di modifica del nome host o dell'indirizzo IP

In caso di modifica del nome host o dell'indirizzo IP del server di backup o del nodo client (nodo di backup), è necessario configurare le impostazioni di sistema. La configurazione delle impostazioni di sistema consente di:

- Garantire la corretta comunicazione tra il server centrale e il server membro. Un server membro è un server di backup gestito dall'utente dal server di backup centrale. Per gestire il server membro dall'interfaccia utente del server centrale, aggiungere il server membro all'interfaccia utente del server centrale.
- Garantire la corretta esecuzione del backup del nodo client in seguito alla modifica del nome host o dell'indirizzo IP del nodo client.

Modifica del nome host del server di backup centrale

In caso di modifica del nome host del server di backup centrale, è necessario configurare il server in modo da poter utilizzare l'Agente Arcserve UDP (Linux) correttamente.

Effettuare le operazioni seguenti:

1. Accedere al server di backup centrale come utente root.
2. Per aggiornare il nome host e le informazioni di licenza, immettere i comandi seguenti:

   ```
   source /opt/Arcserve/d2dserver/bin/setenv
   ```

   ```
   /opt/Arcserve/d2dserver/sbin/sqlite3 /opt/Arcserve/d2dserver/data/ARCserveLinuxD2D.db "update D2DServer set Name='New_Hostname' where IsLocal=1"
   ```

   ```
   /opt/Arcserve/d2dserver/sbin/sqlite3 /opt/Arcserve/d2dserver/data/License.db "update LicensedMachine set ServerName ='New_Hostname' where ServerName ='Old_Hostname'"
   ```

3. Rinominare il file keystore:

   ```
   mv /opt/Arcserve/d2dserver/TOMCAT/conf/server.keystore /opt/Arcserve/d2dserver/TOMCAT/conf/server.keystore.old
   ```

4. Creare un file keystore utilizzando il comando Java keytool.

   ```
   keytool -genkey -alias tomcat -keyalg RSA -keypass <YOUR_VALUE> -storepass <YOUR_VALUE> -keystore
   ```

```
/opt/Arcserve/d2dserver/TOMCAT/conf/server.keystore -validity
3600 -dname "CN=<New Hostname>"
```

Nota: aggiornare il campo YOUR_VALUE in base alle proprie necessità. Generalmente, viene utilizzata la password utente.

Esempio:

```
keytool -genkey -alias tomcat -keyalg RSA -keypass LinuxD2D -
storepass LinuxD2D -keystore /op-
t/Arcserve/d2dserver/TOMCAT/conf/server.keystore -validity
3600 -dname "CN=New Hostname"
```

5. Aprire il file di configurazione TOMCAT server.xml e modificare il valore keystoreFile e il valore keystorePass in base al file keystore creato:

```
<Connector port="8014" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true" clien-
tAuth="false" sslProtocol="TLS" key-
storeFile="${catalina.home}/conf/server.keystore"
keystorePass="YOUR_VALUE"/>
```

Esempio:

```
<Connector port="8014" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true" clien-
tAuth="false" sslProtocol="TLS" key-
storeFile="${catalina.home}/conf/server.keystore"
keystorePass="LinuxD2D"/>
```

6. Riavviare il server di backup centrale.

```
/opt/Arcserve/d2dserver/bin/d2dserver restart
```

Il server di backup centrale è configurato.

Modifica del nome host o dell'indirizzo IP del server membro

In caso di modifica del nome host o dell'indirizzo IP del server di backup membro, configurare il server membro per la gestione dal server centrale. In caso contrario, non sarà possibile gestire il server membro dal server centrale e si verificherà un errore. Un server membro è un server aggiunto all'interfaccia Web del server di backup centrale.

Effettuare le operazioni seguenti:

1. Accedere al server di backup centrale come utente root:
2. Per modificare il nome host, immettere i comandi seguenti:

```
source /opt/Arcserve/d2dserver/bin/setenv
```

```
/opt/Arcserve/d2dserver/sbin/sqlite3 /opt/Arcserve/d2dser-
ver/data/ARCserveLinuxD2D.db "update D2DServer set Name='New_
Hostname' where IsLocal=1"
```

3. Rinominare il file keystore:

```
mv /opt/Arcserve/d2dserver/TOMCAT/conf/server.keystore
/opt/Arcserve/d2dserver/TOMCAT/conf/

server.keystore.old
```

4. Creare un file keystore utilizzando il comando Java keytool.

```
keytool -genkey -alias tomcat -keyalg RSA -keypass LinuxD2D -
storepass LinuxD2D -keystore /opt/Arcserve/d2dser-
ver/TOMCAT/conf/server.keystore -validity 3600 -dname "CN=New
Hostname"
```

Nota: aggiornare il campo YOUR_VALUE in base alle proprie necessità. Generalmente, viene utilizzata la password utente.

Esempio:

```
keytool -genkey -alias tomcat -keyalg RSA -keypass LinuxD2D -
storepass LinuxD2D -keystore /op-
t/Arcserve/d2dserver/TOMCAT/conf/server.keystore -validity
3600 -dname "CN=New Hostname"
```

5. Aprire il file di configurazione TOMCAT server.xml e cambiare il valore keystoreFile e il valore keystorePass in base al file keystore.

```
<Connector port="8014" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true" clien-
tAuth="false" sslProtocol="TLS" key-
storeFile="${catalina.home}/conf/server.keystore"
keystorePass="YOUR_VALUE"/>
```

Esempio:

```
<Connector port="8014" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true" clien-
tAuth="false" sslProtocol="TLS" key-
storeFile="${catalina.home}/conf/server.keystore"
keystorePass="LinuxD2D"/>
```

6. Riavviare il server di backup membro.

```
/opt/Arcserve/d2dserver/bin/d2dserver restart
```

7. Accedere all'interfaccia Web centrale di Arcserve UDP per Linux.
8. Dal riquadro del server di backup, selezionare il server nome host precedente.
9. Dal menu Server di backup, fare clic su Elimina.
10. Nella finestra di dialogo Elimina, fare clic su OK.

    Il server dei nomi host precedente viene eliminato.

11. Dal menu Server di backup, fare clic su Aggiungi.

    Viene visualizzata la finestra di dialogo Aggiungi server.

12. Immettere i dettagli del nuovo nome host nella finestra di dialogo e fare clic su OK.

    La finestra di dialogo Aggiungi server viene chiusa e il server membro con il nuovo nome host viene aggiunto all'interfaccia utente.

13. Effettuare l'accesso al server di backup centrale che gestisce il server di backup membro.
14. Per aggiornare le informazioni di licenza, immettere i comandi seguenti:

    ```
    source /opt/Arcserve/d2dserver/bin/setenv
    ```

    ```
    /opt/Arcserve/d2dserver/sbin/sqlite3 /opt/Arcserve/d2dser-
    ver/data/License.db "update LicensedMachine set ServerName
    ='New_Hostname' where ServerName ='Old_Hostname'"
    ```

    Il server di backup membro è configurato.

Modifica del nome host o dell'indirizzo IP del nodo client

In caso di modifica del nome host o dell'indirizzo IP di un nodo, è possibile configurare il nome host o l'indirizzo IP nelle impostazioni di sistema per eseguire il backup del nodo senza nessun errore.

Effettuare le operazioni seguenti:

1. Accedere alla destinazione di backup.
2. Individuare la cartella denominata **Old_Hostname** nella destinazione di backup del nodo e rinominarla in **New_Hostname**.

   Ad esempio, il nome host precedente per node1 è First_Node. La destinazione di backup per node1 è //Backup_Destination/LinuxBackup. In seguito al corretto completamento del primo backup, una cartella denominata First_Node viene creata in //Backup_Destination/LinuxBackup. Il nome host originale viene modificato in Second_Node. Individuare la cartella First_Node in //Backup_Destination/LinuxBackup e rinominare la cartella in Second_Node.

3. Accedere al server di backup come utente root.

4. Per aggiornare il nome host, immettere i comandi seguenti:

   ```
   source /opt/Arcserve/d2dserver/bin/setenv
   ```

   ```
   /opt/Arcserve/d2dserver/bin/d2drp --storagepath=Backup Destination --node=New_Hostname
   ```

   ```
   /opt/Arcserve/d2dserver/sbin/sqlite3 /opt/Arcserve/d2dserver/data/ARCserveLinuxD2D.db "update TargetMachine set Name='New_Hostname' where Name='Old_Hostname'"
   ```

   ```
   /opt/Arcserve/d2dserver/sbin/sqlite3 /opt/Arcserve/d2dserver/data/ARCserveLinuxD2D.db "update JobQueue set TargetName='New_Hostname' where JobType in (1,3,4,5) and TargetName='Old_Hostname'"
   ```

   Nota: se si utilizza una condivisione NFS o CIFS come destinazione di backup, montarla sulla condivisione Locale.

   Esempio: il punto di montaggio utilizzato è /mnt/backup_destination.

   ```
   /opt/Arcserve/d2dserver/bin/d2drp --storagepath=<mount point> --node=New_Hostname
   ```

   Nota: se si utilizza la condivisione Locale, utilizzare il comando:

   ```
   /opt/Arcserve/d2dserver/bin/d2drp --storagepath=<local path> --node=New_Hostname
   ```

5. Accedere al server di backup centrale come utente root.
6. Per aggiornare le informazioni di licenza, immettere il comando seguente:

   ```
   /opt/Arcserve/d2dserver/sbin/sqlite3 /opt/Arcserve/d2dserver/data/License.db "update LicensedMachine set MachineName ='New_Hostname' where MachineName ='Old_Hostname'"
   ```

   Il nome host viene configurato per eseguire il backup senza errori.

   ### Quando il computer virtuale LBS viene clonato in un ambiente virtuale.

   Quando il computer virtuale LBS viene clonato in un ambiente virtuale, contiene lo stesso UUID del modello clonato. Pertanto, viene richiesto di rigenerare l'UUID.

   Effettuare le operazioni seguenti:

1. Accedere al server di backup di Linux come utente root.
2. Aprire il prompt sqlite.

   ```
   /opt/Arcserve/d2dserver/sbin/sqlite3 /opt/Arcserve/d2dserver/data/ARCserveLinuxD2D.db
   ```

3. Ottenere l'UUID dal database sqlite.

```
sqlite> select uuid from D2DServer;

702ab046-3b70-493d-a2e2-ef3ff3b4dc52
```

4. Eliminare l'UUID esistente dal database sqlite.

```
sqlite> delete from D2DServer where UUID="702ab046-3b70-493d-
a2e2-ef3ff3b4dc52";
```

5. Riavviare i servizi UDP per rigenerare un nuovo UUID.

```
opt/Arcserve/d2dserver/bin # ./d2dserver restart
```

Aggiunta di un utente alla Console del server di backup Linux mediante la riga di comando

Tramite l'agente Arcserve UDP per Linux e la riga di comando, è possibile creare un utente in grado di fungere da sostituito dell'utente root sul server Linux. È possibile utilizzare la riga di comando: d2duser per aggiungere un utente in grado di fungere al posto dell'utente root in caso di disattivazione.

L'utente root è disabilitato a causa di varie ragioni. Ad esempio, quando si crea il computer virtuale su EC2 AWS, per impostazione predefinita la directory principale è disabilitata.

- Verifica dei prerequisiti
- Aggiunta di un utente alla Console del server di backup Linux mediante la riga di comando

Verifica dei prerequisiti

Prima di aggiungere un utente, tenere presenti i seguenti prerequisiti:

- Si dispone delle credenziali di accesso per l'utente root al server di backup.
- Solo l’utente root può eseguire la riga di comando: d2duser.

Aggiunta di un utente alla Console del server di backup Linux mediante la riga di comando

Per aggiungere un utente in grado di sostituire l'utente root, se necessario, è possibile utilizzare la riga di comando d2duser.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Accedere a /opt/Arcserve/d2dserver/configfiles e aprire il file: server.cfg.

   Nota: se non esiste un file con il nome specificato, creare un nuovo file con lo stesso nome e aggiungere il contenuto seguente al file:

   ui_login_use_udp_user = true | false

   Consente di creare l'utente che funge da utente predefinito in assenza dell'utente root durante l'accesso al server. È possibile selezionare **true** per questa opzione.

   ui_login_user_password_min_length = 6

   Consente di definire la lunghezza minima della password. È possibile modificare il valore predefinito di 6, se necessario.

   login_failure_time_to_lock_user = 9

   Consente di stabilire quando bloccare l'account utente in seguito a un numero prestabilito di errori di accesso. È possibile modificare il valore predefinito di 9, se necessario.
3. Accedere a */opt/Arcserve/d2dserver/bin*, quindi individuare la riga di comando d2duser.
4. Immettere ./d2duser per visualizzare l'utilizzo per la riga di comando:

   ```
   d2duser --action=<add|delete|lock|unlock|passwd> --user-
   name=<username>
   ```
5. Immettere i seguenti dettagli nella riga di comando d2duser:

   d2duser --action=add --username=arcserve

   Consente di aggiungere un utente denominato arcserve. Dopo aver premuto Invio, viene richiesta l'immissione di una password e di riconfermare la password appena immessa.

   d2duser --action=delete --username=arcserve

   Consente di eliminare l'utente arcserve.

   d2duser --action=lock --username=arcserve

Consente di bloccare l'utente arcserve.

d2duser --action=unlock --username=arcserve

Consente di sbloccare l'utente arcserve.

d2duser --action=passwd --username=arcserve

Consente di modificare la password per l'utente arcserve.

d2duser --action=list

Consente di visualizzare l'elenco di tutti gli utenti.

6. Dal browser, aprire la pagina della Console del server di backup Linux.
7. Verificare se l'utente predefinito visualizzato è quello appena aggiunto.
8. Effettuare l'accesso tramite nome utente e password.

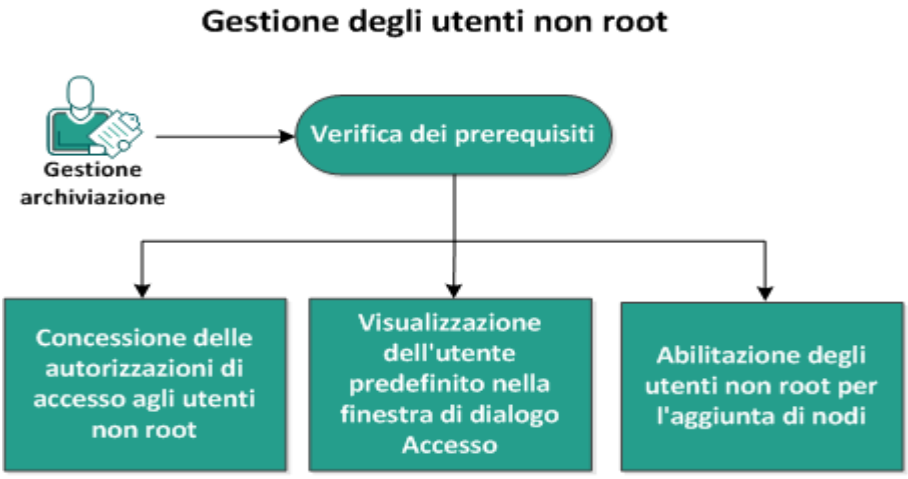
   Verrà visualizzato il messaggio di conferma relativo alla creazione dell'utente.

Gestione degli utenti non root

È possibile gestire tutti gli utenti non root che accedono all'Agente Arcserve UDP (Linux) e definire le autorizzazioni di tali utenti in modo da limitare il loro livello di accesso all'Agente Arcserve UDP (Linux). È possibile gestire gli utenti non root modificando il file di configurazione del server Web (file server.cfg).

Nota: Se il nodo di origine di backup viene configurato con pam_wheel, utilizzare allora l'opzione use_uid per configurare pam_wheel. Per ulteriori informazioni su pam_wheel, vedere la pagina principale di pam_wheel.

Il diagramma seguente mostra il processo di gestione degli utenti non root:



Eseguire queste attività per gestire gli utenti non root:

- Verifica dei prerequisiti
- Concessione delle autorizzazioni di accesso agli utenti non root
- Visualizzazione dell'utente predefinito nella finestra di dialogo Accedi
- Abilitazione degli utenti non root per l'aggiunta di nodi

Verifica dei prerequisiti

Considerare i prerequisiti seguenti prima di gestire gli utenti non root:

- Si dispone delle credenziali di accesso per l'utente root al server di backup.
- Esaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Concessione delle autorizzazioni di accesso agli utenti non root

Un utente root può concedere delle autorizzazioni agli utenti non root per l'accesso al server di backup. Se gli utenti non root ottengono l'autorizzazione per l'accesso al server di backup, possono utilizzare l'Agente Arcserve UDP (Linux) per eseguire tutte le attività di protezione e ripristino di dati.

Nota: Per concedere le autorizzazioni di accesso agli utenti non root, connettersi al server di backup come utente root mediante la connessione SSH.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Aprire il file server.cfg dal percorso seguente:

   ```
   /opt/Arcserve/d2dserver/configfiles/server.cfg
   ```

   Nota: se il file server.cfg non è presente, crearlo.

3. Aggiungere il codice seguente nel file server.cfg:

   ```
   allow_login_users=user1 user2
   ```

   Nota: utilizzare gli spazi vuoti per distinguere più utenti.

   Il codice viene aggiunto.

4. Verificare che l'utente non root possa connettersi al server di backup mediante la connessione SSH.

   L'autorizzazione di accesso viene concessa agli utenti non root per accedere al server di backup.

Visualizzazione dell'utente predefinito nella finestra di dialogo Accedi

È possibile gestire gli utenti e modificare il nome visualizzato nella finestra di dialogo di accesso dell'Agente Arcserve UDP (Linux). L'utente predefinito visualizzato nella finestra di dialogo di accesso è l'utente root. Se non si dispone di utenti root che accedono al prodotto, è possibile sostituire il nome predefinito con qualsiasi nome utente non root. A tal fine è necessario modificare il file server.cfg situato nel server di backup.

Nota: Per modificare il file server.cfg, connettersi al server di backup come utente root mediante la connessione SSH.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Aprire il file server.cfg dal percorso seguente:

   `/opt/Arcserve/d2dserver/configfiles/server.cfg`

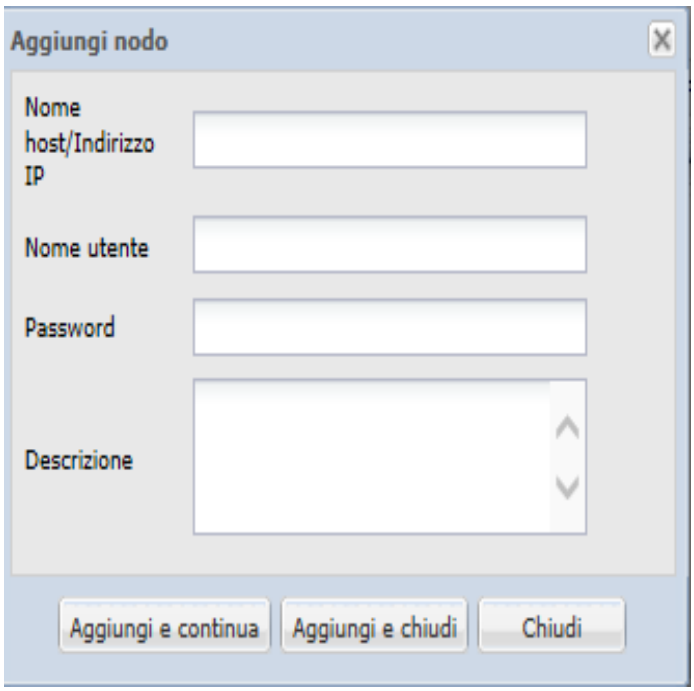
   Nota: se il file server.cfg non è presente, crearlo.
3. Aggiungere il codice seguente nel file server.cfg: show_default_user_when_login=false|true
4. Accedere all'interfaccia Web dell'Agente Arcserve UDP (Linux).
   - Se è stato aggiunto il comando *allow_login_users*,la finestra di dialogo di accesso mostra il primo utente aggiunto nel comando *allow_login_users.*
   - Se non è stato aggiunto il comando *allow_login_users*,la finestra di dialogo di accesso mostra l'utente root.

   L'utente predefinito viene visualizzato nella finestra di dialogo di accesso dell'Agente Arcserve UDP (Linux).

Abilitazione degli utenti non root per l'aggiunta di nodi

Se il Server SSH disattiva l'accesso dell'utente root, è possibile abilitare l'accesso dell'utente non root per l'aggiunta di nodi. Quando si abilitano le credenziali di accesso dell'utente non root, la finestra di dialogo Aggiungi nodo cambia e viene visualizzata l'opzione delle credenziali root.

Nota: in caso di modifica delle credenziali del nodo client da utente root a un utente non root, si consiglia di cancellare la cartella */tmp* sul nodo client prima di eseguire il processo di backup.



Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Aprire il file server.cfg dal percorso seguente:

   `/opt/Arcserve/d2dserver/configfiles/server.cfg`

   Nota: se il file server.cfg non è presente, crearlo.

3. Aggiungere la riga seguente nel file server.cfg per abilitare la funzione dell'utente non root:

   `enable_non_root_user=true`

   La funzione dell'utente non root è abilitata.

4. (Facoltativo) Aggiungere la riga seguente nel file server.cfg per disabilitare la funzione dell'utente non root:

   ```
   enable_non_root_user=false
   ```

   La funzione dell'utente non root è disabilitata.

   Gli utenti non root sono abilitati per l'aggiunta di nodi.

   Nota: se si modifica la password dell'utente root o dell'utente non root e si modifica il nodo, è necessario immettere entrambe la password (utente root e non root) nel campo corrispondente della finestra di dialogo Modifica Nodo.

   Nota: gli utenti non root non possono gestire i nodi utilizzando il comando *d2dnode* dalla riga di comando.

Modalità di configurazione dell'account utente sudo per i nodi Linux

È possibile utilizzare sudo per configurare gli account utente regolari per l'esecuzione di attività di backup e ripristino. Per gli account sudo, tutte le configurazioni sono relative ai nodi Linux. Se l'account sudo è configurato correttamente, è possibile utilizzarlo come se si trattasse di un account root normale per tutte le interfacce utente. Tramite l'account sudo è possibile eseguire attività quali l'aggiunta, il backup e il ripristino dei nodi. Configurare l'account sudo in base al documento specifico di distribuzione di Linux.

Eseguire queste attività per gestire gli utenti sudo:

- Verifica dei prerequisiti
- Modifica delle impostazioni sudo predefinite in SUSE
- Configurazione del comando sudo in Debian
- Configurazione del comando sudo in Ubuntu
- Configurazione del comando sudo per l'autorizzazione senza password durante l'utilizzo dell'autenticazione con chiave pubblica SSH
- Configurazione di Sudo per consentire soltanto il processo dell'agente di backup

Verifica dei prerequisiti

Considerare i prerequisiti seguenti prima di gestire gli utenti non root:

- Si dispone delle credenziali di accesso per l'utente root per il nodo Linux.
- Le autorizzazioni sudo sono state configurate correttamente per l'utente in questione.
  - Verificare che l'utente Sudo disponga delle autorizzazioni necessarie per eseguire i seguenti programmi: d2d_ea e ln. Ad esempio, se il nome utente è backupadmin, l'esempio di configurazione di Sudo sarà: *backupadmin ALL=(ALL) /usr/bin/d2d_ea,/usr/bin/ln*.
  - Verificare che l'utente Sudo disponga delle autorizzazioni necessarie per conservare almeno le seguenti variabili di ambiente:

HOSTNAME	USERNAME	LANG	LC_ADDRESS
LC_CTYPE	LC_COLLATE	LC_ IDENTIFICATION	LC_ MEASUREMENT
LC_MESSAGES	LC_MONETARY	LC_NAME	LC_NUMERIC
LC_TIME	LC_ALL LANGUAGE	SSH_ CONNECTION	CRE_ROOT_ PATH
CRE_LOG_BASE_ DIR	TARGET_BOOTSTRAP_ DIR	TARGET_ WORK_ DIR	jobID

    Ad esempio, se il nome utente è backupadmin, gli esempi di configurazione di Sudo saranno i seguenti:

    Impostazione predefinita: backupadmin env_keep += "HOSTNAME USERNAME LANG LC_ADDRESS LC_CTYPE"

    Impostazione predefinita: backupadmin env_keep += "LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT"

    Impostazione predefinita: backupadmin env_keep += "LC_MESSAGES LC_MONETARY LC_NAME LC_NUMERIC LC_TIME LC_ALL LANGUAGE"

    Impostazione predefinita: backupadmin env_keep += "SSH_ CONNECTION CRE_LOG_BASE_DIR jobID TARGET_BOOTSTRAP_DIR CRE_ROOT_PATH TARGET_WORK_DIR"

- Esaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Modifica delle impostazioni sudo predefinite in SUSE

Per impostazione predefinita, SUSE richiede una password root anziché la password dell'utente per fornire l'autorizzazione. L'autenticazione sudo non funziona con il server di backup Linux in quanto il server di backup utilizza le credenziali utente per l'autorizzazione. È possibile modificare le impostazioni sudo predefinite per autorizzare l'utilizzo delle credenziali utente.

Effettuare le operazioni seguenti:

1. Accedere al nodo Linux come utente root.
2. Aprire il file **/etc/sudoer** o eseguire il comando *visudo*.
3. Immettere un commento nelle impostazioni come mostrato nell'esempio seguente:

   Esempio:

   ```
   #Defaults targetpw # richiede la password dell'utente di
   destinazione, ad esempio root

   #ALL ALL=(ALL) ALL # WARNING! Utilizzare l'opzione soltanto
   se congiuntamente con 'Defaults targetpw'!
   ```

4. Verificare che la riga di comando sudo richieda una password utente anziché la password root per fornire l'autorizzazione.

   Le impostazioni sudo predefinite sono state modificate correttamente.

Configurazione del comando sudo in Debian

Per impostazione predefinita, l'account principale non è abilitato per l'accesso a Debian. Di conseguenza, è necessaria un'autenticazione sudo quando si aggiunge Debian Linux come nodo Linux.

Effettuare le operazioni seguenti:

1. Accedere al nodo Linux e passare alla directory principale utilizzando il comando *su*.
2. Se il pacchetto sudo non è installato, utilizzare il comando seguente per installarlo:

   ```
   apt-get install sudo
   ```

3. Aggiungere un utente esistente con id=user a group=sudo:

   Esempio:

   ```
   adduser user sudo
   ```

   oppure creare un nuovo utente con sudo

   ```
   adduser user
   ```

   ```
   adduser user sudo
   ```

4. Accedere alla shell utente e digitare il seguente comando per verificare che l'utente disponga delle autorizzazioni necessarie:

   ```
   sudo -v
   ```

   L'autenticazione sudo è stata configurata correttamente in Debian.

   Nota: per Debian 12.x, dopo aver eseguito i passaggi precedenti, aprire il file **/etc/sudoers** dalla directory principale, aggiungere un commento alla riga seguente nel file *sudoers*, quindi salvare il file *sudoers*:

   ```
   Il valore predefinito è use_pty
   ```

Configurazione del comando sudo in Ubuntu

Questa sezione fornisce informazioni sulla configurazione del file *sudoers* in Ubuntu 22.

Per effettuare la configurazione, attenersi alla procedura seguente:

1. Accedere al nodo Linux come utente root.
2. Creare un nuovo utente sudo utilizzando il seguente comando:

   ```
   adduser user
   ```

3. Aprire il file **/etc/sudoers** dalla directory principale e aggiungere un commento alla riga seguente nel file *sudoers*.

   ```
   Il valore predefinito è use_pty
   ```

4. Salvare il file *sudoers*.

Sudo è stato configurato correttamente in Ubuntu 22.

Configurazione di sudo per l'autorizzazione senza password durante l'utilizzo dell'autenticazione con chiave pubblica SSH

Con l'utilizzo dell'autenticazione con chiave pubblica SSH, il server di backup Linux non memorizza le credenziali utente. È possibile configurare sudo per consentire l'autorizzazione senza password.

Effettuare le operazioni seguenti:

1. Accedere al nodo Linux come utente root.
2. Aprire il file **/etc/sudoer** o eseguire *visudo* per modificare il file di configurazione.
3. Accedere alla riga di configurazione per l'utente specificato e aggiungere l'opzione 'NOPASSWD'.

   Ad esempio, se il nome utente è backupadmin, aggiungere l'opzione 'NOPASSWD' come illustrato nell'esempio seguente:

   Esempio: backupadmin ALL=(ALL) NOPASSWD: /usr/bin/d2d_ea,/user/bin/ln
4. Accedere alla shell utente e digitare il comando seguente per verificare che l'autorizzazione non richieda alcuna password:

   ```
   sudo -v
   ```

   Sudo è stato configurato correttamente per l'autorizzazione senza password durante l'utilizzo della configurazione della chiave pubblica SSH.

Configurazione di Sudo per consentire soltanto il processo dell'agente di backup

Se l'utente può utilizzare soltanto i comandi limitati di Sudo, è necessario effettuare l'installazione manuale del programma dell'agente di backup. Per l'esecuzione dei processi di backup, è necessario disporre delle autorizzazioni Sudo per il processo *d2d_ea*.

Effettuare le operazioni seguenti:

1. Accedere al nodo Linux come utente root.
2. Aprire il file **/etc/sudoer** o eseguire *visudo* per modificare il file di configurazione.
3. Accedere alla riga di configurazione per l'utente specificato e aggiungere '/usr/-bin/d2d_ea' all'elemento di configurazione dei comandi consentiti.

   Ad esempio, se il nome utente è backupadmin, aggiungere '/usr/bin/d2d_ea' come illustrato nell'esempio seguente:

   Esempio: backupadmin ALL=(ALL) /usr/bin/d2d_ea
4. Determinare se il nodo di origine di backup è a 32 o a 64 bit e individuare il file binario corretto sul server dell'agente di backup:
5. Copiare il file binario determinato dal passaggio 4 nel nodo di origine di backup come d2d_ea e posizionarlo in '/usr/bin/d2d_ea'.

   ```
   Per 32 bit: /opt/Arcserve/d2dserver/sbin/ea.32
   ```

   ```
   Per 64 bit: /opt/Arcserve/d2dserver/sbin/ea.64
   ```
6. Eseguire il comando seguente per verificare le autorizzazioni di esecuzione:

   ```
   chmod +x /usr/bin/d2d_ea
   ```

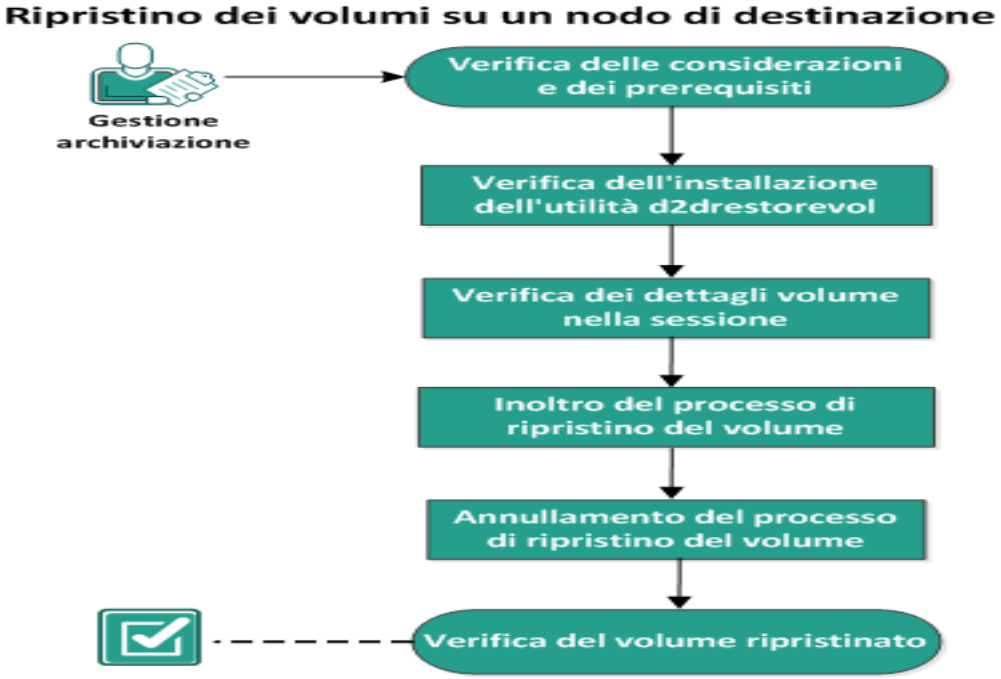
   Sudo è stato configurato correttamente per consentire soltanto il processo dell'agente di backup.

Ripristino dei volumi su un nodo di destinazione

È possibile ripristinare singoli volumi sul nodo di destinazione senza eseguire un ripristino bare metal completo. Il nodo di destinazione può essere un server di backup o un nodo protetto.

Il ripristino di singoli volumi utilizza meno risorse e fornisce prestazioni migliori.

Nel diagramma seguente è possibile visualizzare il processo per ripristinare i volumi:



Per eseguire il ripristino dei volumi, procedere come segue:

- Verifica delle considerazioni e dei prerequisiti
- Verifica dell'installazione dell'utilità d2drestorevol
- Verifica dei dettagli volume nella sessione
- Inoltro del processo di ripristino del volume
- Annullamento del processo di ripristino del volume
- Verifica del volume ripristinato

Verifica delle considerazioni e dei prerequisiti

Rivedere i prerequisiti seguenti prima di ripristinare i volumi:

- Si dispone di una sessione di backup valida per eseguire un ripristino.
- Il ripristino del volume supporta una sessione generata dai piani o dai processi basati sull'agente di Linux.
- È necessario accedere alle sessioni di backup localmente sul nodo di destinazione. Se la posizione della sessione è sul volume locale del nodo di destinazione, utilizzare il percorso esatto della directory come posizione della sessione. Se la posizione della sessione è su una condivisione di rete, montare innanzitutto la condivisione di rete su un punto di montaggio locale, quindi utilizzare il percorso del punto di montaggio come posizione della sessione. Se il backup della sessione viene eseguito in un archivio dati RPS, è necessario individuare il percorso condiviso nei dettagli dell'archivio dati. Montare quindi il percorso condiviso in un punto di montaggio locale e utilizzare il percorso del punto di montaggio come percorso della sessione.
- I volumi di destinazione che si desidera ripristinare devono essere non montanti, a tal fine utilizzare il comando umount:

  ```
  Esempio: umount /dev/sda2
  ```

- Il volume di destinazione deve essere uguale o più grande del volume di origine.
- Esaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Rivedere le considerazioni seguenti prima di ripristinare i volumi:

- Quando si esegue il ripristino, qualsiasi dato esistente sul volume di destinazione viene eliminato. Eseguire un backup dei dati esistenti dal volume di destinazione prima di ripristinare.

Verifica dell'installazione dell'utilità d2drestorevol

L'utilità d2drestorevol ripristina il volume sul nodo di destinazione. Il nodo di destinazione può essere un server di backup o un altro nodo di Linux (client). Se l'utilità restorevol non è installata sul nodo di destinazione, va installata manualmente.

Ripristino su un server di backup

Se il nodo di destinazione è un server di backup, l'utilità è installata con il pacchetto di installazione. Verificare se l'utilità è presente alla cartella *bin.*

Effettuare le operazioni seguenti:

1. Accedere al server di backup.
2. Verificare che l'utilità si trovi nella posizione seguente:

   ```
   /opt/Arcserve/d2dserver/bin/d2drestorevol
   ```

   L'utilità viene installata e verificata.

Ripristino su un client

L'utilità non è già installata su un nodo client. Si deve installare manualmente l'utilità sul client.

Importante: È necessario scaricare l'utilità dal server di backup come descritto nei passaggi seguenti. Se si copia manualmente l'utilità da un server di backup a un client, l'utilità potrebbe non funzionare correttamente.

Effettuare le operazioni seguenti:

1. Accedere al client.
2. Individuare il percorso di download dell'utilità d2drestorevol dalla riga di comando.

   ```
   http[s]://[Backup-Server-address]:[port]/d2drestorevol
   ```

3. Scaricare lo script mediante uno strumento della riga di comando, come wget.

   ```
   wget http://192.168.1.1:8014/d2drestorevol -O d2drestorevol
   ```

   Nota: se il file server.cfg non è presente, crearlo.

   ```
   wget https://192.168.1.1:8014/d2drestorevol -O d2drestorevol
   --no-check-certificate
   ```

4. Fornire l'autorizzazione di esecuzione all'utilità mediante il comando seguente:

   ```
   chmod +x d2drestorevol
   ```

   L'autorizzazione viene fornita.

   L'utilità d2drestorevol viene installata e verificata.

Verifica dei dettagli volume nella sessione

Verificare i dettagli volume nella sessione che si desidera ripristinare. È possibile visualizzare il volume di origine, il file system, le dimensioni file e le informazioni di montaggio nell'output.

Effettuare le operazioni seguenti:

1. Accedere al nodo di destinazione.
2. Se i punti di ripristino si trovano in una cartella condivisa o locale, utilizzare il comando seguente per verificare le informazioni sul volume:

   ```
   d2drestorevol --command=info --storage-path=<local_path> --
   node=<node_name> --rp=<recovery_point>
   ```

   --command=info

   Specifica la visualizzazione dei dettagli volume della sessione.

   --storage-path

   Specifica il percorso determinato nell'argomento Prerequisiti. Per ulteriori informazioni, consultare l'argomento Verifica delle considerazioni e dei pre-requisiti.

   --node

   Specifica il nodo di origine di cui si è stato eseguito il backup.

   --rp

   Specifica il punto di ripristino o la sessione di ripristino che si desidera ripristinare. Generalmente, un punto di ripristino presenta il formato seguente: S00000000X, dove X è un valore numerico.

   L'output viene visualizzato.

3. Se i punti di ripristino si trovano in un archivio dati RPS, utilizzare il comando seguente per verificare le informazioni sul volume:

   ```
   d2drestorevol --command=info --storage-path=<rps_path> --node-
   e="<node_name>[UUID_number]" --rp=<recovery_point> --rps-host-
   t=<host_name> --rps-user=<user_name> --rps-pw=<rps_password>
   --rps-protocal=<internet_secutity_protocol> --rps-port=<port_
   number> --rps-dedup
   ```

   Il comando riportato di seguito è un esempio per un archivio dati abilitato per la deduplicazione:

```
d2drestorevol --command=info --storage-path=/root/rpsshare --
node="xx.xx.xx.xx[11111aa-22bb-33cc-yyyy-4c4c4c4c]" --rp=V-
VStore/S0000000001 --rps-host=machine_name --rps-use-
r=administrator --rps-pw******** --rps-protocol=https --rps-
port=8014 --rps-dedup
```

--command=info

Specifica la visualizzazione dei dettagli volume della sessione.

--storage-path

Specifica il percorso determinato nell'argomento Prerequisiti. Per ulteriori informazioni, consultare l'argomento Verifica delle considerazioni e dei pre-requisiti.

--node

Specifica il nodo di origine di cui è stato eseguito il backup nel formato seguente:

<node name>[<uuid>]

--rp

Specifica il punto di ripristino o la sessione di ripristino che si desidera ripristinare da un archivio dati RPS. In genere, è necessario specificare una sessione del punto di ripristino da un archivio dati RPS nel formato seguente:

VStore/S00000000X, dove X è un valore numerico.

--rps-host

Specifica il nome host del server RPS in cui sono memorizzate le sessioni di ripristino.

--rps-user

Specifica il nome utente per accedere all'host RPS.

--rps-pw

Specifica la password per accedere all'host RPS.

--rps-protocol

Specifica il protocollo per l'host RPS. Può trattarsi del protocollo http o https.

--rps-port

Specifica il numero di porta dell'host RPS.

--rps-dedup

Specifica che la deduplicazione è abilitata per l'archivio dati. Questo parametro è obbligatorio solo se la deduplicazione è abilitata per l'archivio dati.

--ds-share-folder

Specifica il percorso condiviso dell'archivio dati. Questo parametro è obbligatorio solo se la deduplicazione è disabilitata per l'archivio dati.

--ds-user

Specifica il nome utente per l'accesso al percorso condiviso dell'archivio dati.

--ds-user-pw

Specifica il nome utente per l'accesso al percorso condiviso dell'archivio dati.

--ds-pw

Specifica la password di crittografia dei dati se per l'archivio dati è abilitata anche la crittografia.

L'output viene visualizzato.

I dettagli volume vengono verificati.

Inoltro del processo di ripristino del volume

Inoltrare il processo di ripristino del volume per iniziare a ripristinare il volume sul nodo di destinazione.

Effettuare le operazioni seguenti:

1. Accedere al nodo di destinazione.
2. Se i punti di ripristino si trovano in una cartella locale o in una rete condivisa, è possibile inoltrare il processo di ripristino utilizzando il comando seguente:

```
d2drestorevol --command=restore  --storage-path=<local_
path> --node=<node_name> --rp=<recovery_point> --
source-volume=<source_volume> --target-volume=<target_
volume> [--encryption-password=<encryption_password>]
[--mount-target=<mount_point> [--quick-recovery]]
```

-command=restore

Specifica l'invio del processo di ripristino del volume.

--storage-path

Specifica il percorso determinato nell'argomento Prerequisiti. Per ulteriori informazioni, consultare l'argomento Verifica delle considerazioni e dei prerequisiti.

--node

Specifica il nodo di origine di cui si è stato eseguito il backup.

--rp

Specifica il punto di ripristino o la sessione di ripristino che si desidera ripristinare. Generalmente, un punto di ripristino presenta il formato seguente: S00000000X, dove X è un valore numerico.

--encryption-password

Specifica la password della sessione. Questa opzione è necessario se la sessione è crittografata. Se la sessione è crittografata ma questa opzione non è presente, viene richiesto di inserire la password dal terminale.

--source-volume

Specifica il volume di origine. È possibile ottenere il volume di origine mediante il parametro *command=info* come descritto nell'argomento Verifica dei dettagli volume nella sessione o il volume di origine può essere il punto di montaggio dal sistema di origine.

--target-volume

Specifica il percorso file della periferica del nodo di destinazione.

Esempio: /dev/sda2

--mount-target

Specifica il punto di montaggio del volume ripristinato.

Esempio: /mnt/volrestore

--quick-recovery

Se utilizzato con il comando --mount-target, il volume di destinazione viene montato il prima possibile. Durante il ripristino dei dati è possibile utilizzare i dati sul volume di destinazione.

Una volta completato, il processo di ripristino viene chiuso automaticamente ed è possibile utilizzare i dati senza alcuna interruzione.

Nota: in caso di esecuzione simultanea di un processo di ripristino e di backup:

- Se si utilizza il comando --quick-recovery, il processo (backup o rispristino del volume) avviato più tardi non viene eseguito.
- Se il comando --quick-recovery non viene utilizzato, viene eseguito unicamente il backup dei volumi non ripristinati.

Il processo di ripristino viene inoltrato e si apre una schermata che visualizza il progresso. Se si desidera inoltrare altri processi, è possibile attendere il completamento del processo corrente o premere Q per uscire dalla schermata e inoltrare un nuovo processo.

3. Se i punti di ripristino si trovano in un archivio dati RPS, è possibile inoltrare il processo di ripristino utilizzando il comando seguente:

```
d2drestorevol --command=restore --storage-path=<local_path> --node=<node_name> --rp=<recovery_point> --source-volume=<source_volume> --target-volume=<target_volume> [--encryption-password=<encryption_password>] [--mount-target=<mount_point> [--quick-recovery]]
```

--command=restore

Specifica che il processo di ripristino del volume è stato inoltrato.

--storage-path

Specifica il percorso determinato nell'argomento Prerequisiti. Per ulteriori informazioni, consultare l'argomento Verifica delle considerazioni e dei prerequisiti.

--node

Specifica il nodo di origine di cui è stato eseguito il backup nel formato seguente:

<node name>[<uuid>]

--rp

Specifica il punto di ripristino o la sessione di ripristino che si desidera ripristinare da un archivio dati in RPS. In genere, è necessario specificare una sessione del punto di ripristino da un archivio dati RPS nel formato seguente:

VStore/S00000000X, dove X è un valore numerico.

--source-volume

Specifica il volume di origine. È possibile ottenere il volume di origine mediante il parametro *command=info* come descritto nell'argomento Verifica dei dettagli volume nella sessione o il volume di origine può essere il punto di montaggio dal sistema di origine.

--target-volume

Specifica il percorso file della periferica del nodo di destinazione.

Esempio: /dev/sda2

--rps-host

Specifica il nome host del server RPS in cui sono memorizzate le sessioni di ripristino.

--rps-user

Specifica il nome utente per accedere all'host RPS.

--rps-pw

Specifica la password per accedere all'host RPS.

--rps-protocol

Specifica il protocollo per l'host RPS. Può trattarsi del protocollo http o https.

--rps-port

Specifica il numero di porta dell'host RPS.

--rps-dedup

Specifica che la deduplicazione è stata abilitata per l'archivio dati. Questo parametro è obbligatorio solo se la deduplicazione è abilitata per l'archivio dati.

--ds-share-folder

Specifica il percorso condiviso dell'archivio dati. Questo parametro è obbligatorio solo se la deduplicazione è disabilitata per l'archivio dati.

--ds-user

Specifica il nome utente per l'accesso al percorso condiviso dell'archivio dati.

--ds-user-pw

Specifica la password per l'accesso al percorso condiviso dell'archivio dati.

--ds-pw

Specifica la password di crittografia dei dati se per l'archivio dati è abilitata anche la crittografia.

Il processo di ripristino viene inoltrato e si apre una schermata che visualizza il progresso. Se si desidera inoltrare altri processi, è possibile attendere il completamento del processo corrente o premere Q per uscire dalla schermata e inoltrare un nuovo processo.

4. (Facoltativo) Utilizzare il comando seguente per verificare il progresso del processo di ripristino del volume:

   ```
   d2drestorevol --command=monitor
   ```

   I dettagli sul progresso, come il nome del volume, il tempo trascorso, il progresso, la velocità, lo stato e il tempo rimanente vengono visualizzati su una schermata.

   La schermata si chiude al completamento del processo. È anche possibile premere Q per uscire manualmente dalla schermata. Uscendo manualmente la schermata non si interrompe il processo di ripristino in esecuzione.

   Il processo di ripristino del volume viene inoltrato.

Annullamento del processo di ripristino del volume

È possibile annullare il processo di ripristino del volume dalla riga di comando del nodo di destinazione. Utilizzare il comando seguente per annullare il processo di ripristino del volume.

```
d2drestorevol --command=cancel --target-volume=<target_
volume>
```

--command=cancel

Specifica l'annullamento del processo di ripristino di volume.

--target-volume

Specifica il percorso file della periferica del nodo di destinazione. Il valore deve essere identico al valore utilizzato per inoltrare il processo di ripristino.

Importante: Annullando un processo di ripristino del volume il volume di destinazione diventa inutilizzabile. In tali casi è possibile riprovare a eseguire il processo di ripristino del volume oppure ripristinare i dati persi, se si dispone di un backup.

Verifica del volume ripristinato

Verificare i dati quando il volume viene ripristinato.

Effettuare le operazioni seguenti:

1. Accedere al nodo di destinazione.
2. Verificare la schermata di progresso per verificare lo stato di completamento.
3. (Facoltativo) Verificare il file *d2drestvol_activity_[target volume].log* per visualizzare tutti i registri del processo di ripristino.
4. Montare il volume ripristinato e verificare che i dati siano stati ripristinati.

Il processo di ripristino del volume viene verificato.

Il volume viene ripristinato correttamente.

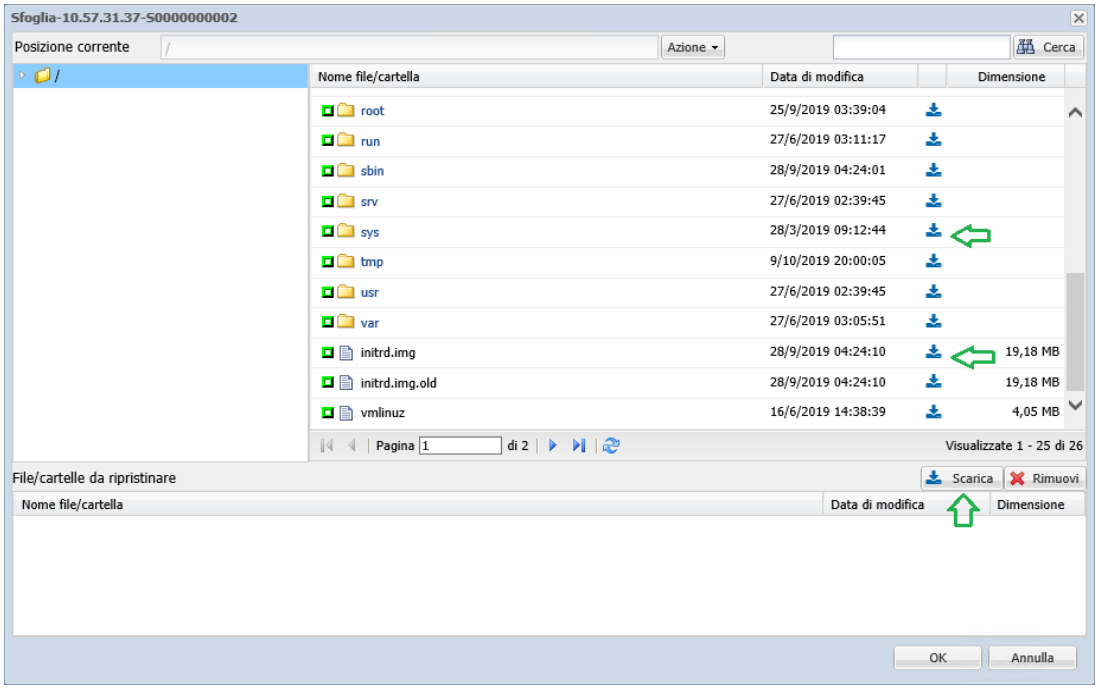
Download di file e cartelle senza ripristino per i nodi Linux

[[[Undefined variable Variables.AUDP]]] consente di scaricare un file o una cartella completa senza doverli inviare per il ripristino. Dalla procedura guidata di ripristino, la schermata Sfoglia punti di ripristino consente di scaricare direttamente qualsiasi file o cartella completa contenente tutti i file. L'esecuzione del download prima del ripristino consente di effettuare una breve ricerca dei file per impedire il ripristino dei file non desiderati.

Un singolo file viene scaricato direttamente nello stesso formato, mentre una cartella viene scaricata come file .zip. Il nome del formato del file .zip è il seguente:

[nodename]_[sessionid]_[timestamp].zip

Per eseguire il download, è sufficiente accedere alla schermata Sfoglia punti di ripristino nella procedura guidata di ripristino. La seguente schermata illustra la procedura di download di un file o di una cartella per i nodi Linux:

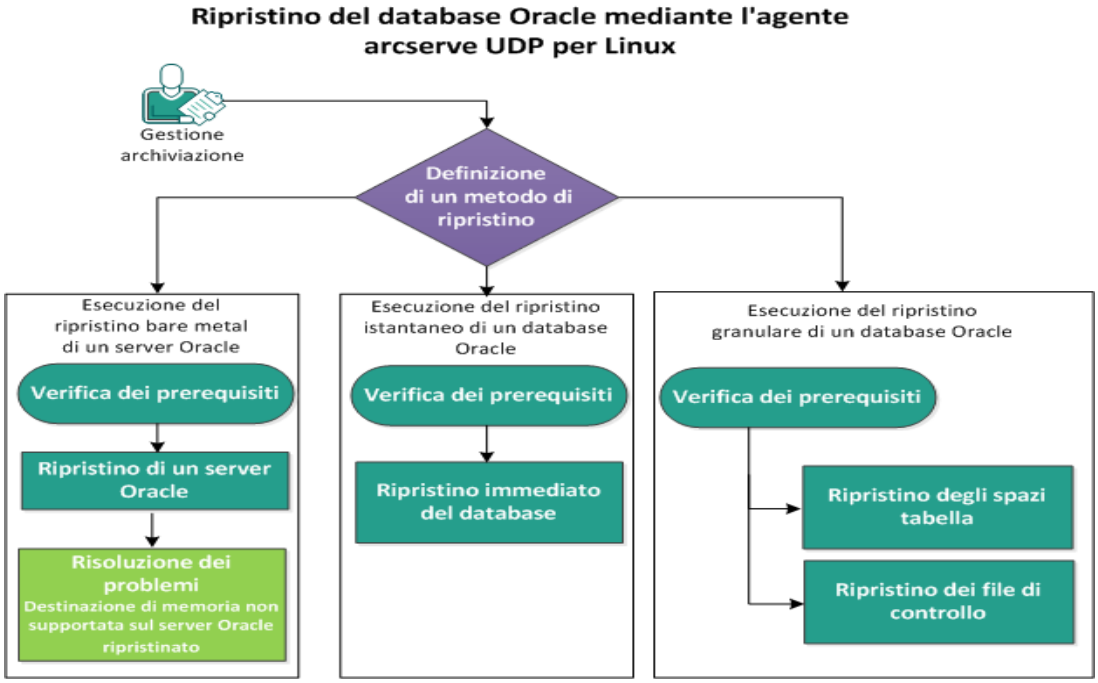


Per aprire i file scaricati, utilizzare gli strumenti zip, ad esempio WinZip, WinRAR, 7-Zip e così via.

Ripristino di un database Oracle mediante l'Agente Arcserve UDP (Linux)

È possibile ripristinare l'intero database Oracle o ripristinare file specifici dal database. È possibile, inoltre, eseguire un ripristino bare metal (BMR) di un server Oracle quando il server di origine non funziona correttamente. Se si è perso il database e si desidera averlo immediatamente disponibile, è possibile eseguire un ripristino istantaneo. Prima di avviare il processo di ripristino, leggere i prerequisiti per ciascun tipo di ripristino.

Il diagramma seguente illustra la procedura per ripristinare il database Oracle tramite l'Agente Arcserve UDP (Linux):



Eseguire i passaggi seguenti per ripristinare un database Oracle mediante l'Agente Arcserve UDP (Linux):

- Esecuzione di un ripristino bare metal di un server Oracle
- Esecuzione di un ripristino istantaneo di un database Oracle
- Esecuzione del ripristino granulare di un database Oracle

Esecuzione di un ripristino bare metal (BRM) di un server Oracle

Un ripristino bare metal esegue il ripristino del sistema operativo e delle applicazioni software, ed esegue il recupero di tutti i dati sottoposti a backup. Il ripristino bare metal consiste nel ripristino di un sistema del computer avviato a partire da un sistema bare metal. Bare metal è un computer senza sistema operativo, driver e applicazioni software. Al completamento del ripristino, il computer di destinazione viene riavviato automaticamente sullo stesso ambiente operativo del nodo di origine del backup e tutti i dati vengono ripristinati.

È possibile eseguire un ripristino bare metal mediante l'indirizzo IP o l'indirizzo MAC del computer di destinazione. Se il computer di destinazione viene avviato mediante il sistema Live CD dell'Agente Arcserve UDP (Linux), è possibile ottenere l'indirizzo IP del computer di destinazione.

La presente sezione descrive i seguenti argomenti:

- Verifica dei prerequisiti
- Ripristino di un server Oracle
- Destinazione di memoria non supportata sul server Oracle ripristinato

Verifica dei prerequisiti

Verificare i prerequisiti seguenti prima di ripristinare il database Oracle:

- Si dispone di un punto di ripristino valido e della password di crittografia per il ripristino.
- Si dispone di un computer di destinazione valido per il ripristino bare metal.
- È stato creato il Live CD di dell'Agente Arcserve UDP (Linux) (Linux).
- Se si desidera eseguire il ripristino bare metal con l'indirizzo IP, è necessario acquisire l'indirizzo IP del computer di destinazione utilizzando Live CD.
- Se si desidera eseguire il ripristino bare metal PXE con l'indirizzo MAC, è necessario acquisire l'indirizzo MAC del computer di destinazione.
- Verificare i file system supportati per i backup basati su agente UDP per Linux. I file system ASM (Automatic Storage Management), ACFS e Oracle Cluster File System (OCFS / OCFS2) non sono supportati per i backup basati su agente UDP per Linux. Per proteggere i dati su questi file system, utilizzare i backup UDP Oracle RMAN.
- Esaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Ripristino di un server Oracle

Se il server Oracle è corrotto, è possibile ripristinare il server intero eseguendo un ripristino bare metal.

Effettuare le operazioni seguenti:

1. Accedere alla console del server di backup di Linux come utente root.
2. Eseguire un ripristino bare metal mediante la procedura guidata di ripristino. Per ulteriori informazioni sul processo di ripristino, consultare la sezione Esecuzione di un ripristino bare metal (BMR) per computer Linux.
3. Dopo che il processo di ripristino bare metal è stato completato, accedere al computer di destinazione e verificare che il database sia stato ripristinato.

   Il server Oracle è stato recuperato correttamente.

Destinazione di memoria non supportata sul server Oracle ripristinato

Sintomo

È stato eseguito un ripristino bare metal di un server Oracle. La dimensione di memoria del computer di destinazione è minore rispetto al server Oracle di origine e il database Oracle utilizza AMM (Gestione di memoria automatica). Dopo il ripristino bare metal, all'avvio dell'istanza del database Oracle si ottiene il seguente errore:

SQL> startup

ORA-00845: MEMORY_TARGET not supported on this system (SQL> startup ORA-00845: MEMORY_TARGET non supportato su questo sistema)

Soluzione

Per risolvere questo errore, aumentare la dimensione del file system virtuale della memoria condivisa.

Effettuare le operazioni seguenti:

1. Accedere al computer di destinazione come utente root.
2. Aprire il prompt dei comandi e verificare la dimensione del file system virtuale della memoria condivisa.

   ```
   # df -k /dev/shm

   Filesystem 1K-blocks Used Available Use% Mounted on tmpfs
   510324 88 510236 1% /dev/shm
   ```

3. Immettere il comando seguente e specificare la dimensione necessaria della memoria condivisa:

   ```
   # mount -o remount,size=1200m /dev/shm
   ```

4. Accedere alla cartella "/etc/fstab" e aggiornare l'impostazione tmpfs:

   ```
   tmpfs /dev/shm tmpfs size=1200m 0 0
   ```

   Nota: La dimensione del file system virtuale della memoria condivisa dovrebbe essere grande abbastanza per ospitare i valori MEMORY_TARGET e MEMORY_MAX_TARGET . Per ulteriori informazioni sulle variabili, fare riferimento alla documentazione di Oracle.

Esecuzione di un ripristino istantaneo di un database Oracle

È possibile recuperare istantaneamente un database Oracle senza eseguire un ripristino bare metal completo. È possibile recuperare il database usando comandi specifici dalla riga di comando.

La presente sezione descrive i seguenti argomenti:

- Verifica dei prerequisiti
- Ripristino istantaneo del database

Verifica dei prerequisiti

Verificare i prerequisiti seguenti prima di ripristinare il database Oracle:

- Si dispone di un punto di ripristino valido e della password di crittografia per il ripristino.
- È necessario accedere alle sessioni di backup localmente sul nodo di destinazione. Se la posizione della sessione è sul volume locale del nodo di destinazione, utilizzare il percorso esatto della directory come posizione della sessione. Se la posizione della sessione è su una condivisione di rete, montare innanzitutto la condivisione di rete su un punto di montaggio locale, quindi utilizzare il percorso del punto di montaggio come posizione della sessione.
- I volumi di destinazione che si desidera ripristinare non possono essere un volume root e devono essere smontati mediante il comando umount.

  Esempio: umount /dev/sda1
- Il volume di destinazione deve essere uguale o più grande del volume di origine.
- Verificare i file system supportati per i backup basati su agente UDP per Linux. I file system ASM (Automatic Storage Management), ACFS e Oracle Cluster File System (OCFS / OCFS2) non sono supportati per i backup basati su agente UDP per Linux. Per proteggere i dati su questi file system, utilizzare i backup UDP Oracle RMAN.
- Esaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Ripristino istantaneo del database

Quando si recupera il database istantaneamente, quest'ultimo è disponibile per l'uso immediato. Tuttavia, il processo di ripristino viene eseguito nel back-end e tutti i file sono disponibili solamente dopo che il database è stato recuperato completamente.

Nota: Per ulteriori informazioni sul ripristino del volume, consultare Ripristino dei volumi su un nodo di destinazione.

Effettuare le operazioni seguenti:

1. Accedere al computer di destinazione come utente root.
2. Aprire un prompt dei comandi come utente root.
3. Verificare che il volume di destinazione /dev/sdb1 non sia montato.

   ```
   # df | grep 'target_volume'
   ```

   Esempio: # df | grep '/dev/sdb1'

4. Montare la condivisione NFS remota sul percorso locale.

   ```
   #mount <nfs_session_path>:/nfs <session_location_on_local>
   ```

   Esempio: #mount xxx.xxx.xxx.xxx:/nfs /CRE_ROOT

5. Immettere il seguente comando per avviare il programma di ripristino:

   ```
   #. /d2drestorevol --command=restore --storage-path=<session_
   location_on_local> --node=<oracle_server> --rp=last --source-
   volume=<mount_point_for_oracle_data_volume> --target-volu-
   me=<restore_target_volume_name> --mount-target=<mount_point_
   for_oracle_data_volume> --quick-recovery
   ```

   Esempio: #. /d2drestorevol --command=restore --storage-path=/CRE_ROOT --node-e=rh63-v2 --rp=last --source-volume=/opt/oracle --target-volume=/dev/sdb1 --mount-target=/opt/oracle --quick-recovery

   È possibile avviare il database Oracle immediatamente dopo l'avvio del processo di ripristino. Non è necessario attendere il completamento del recupero del database.

6. Aprire un altro prompt dei comandi e accedere con il nome utente e la password di Oracle.

   ```
   $sqlplus / as sysdba

   SQL> startup;
   ```

Esempio: #. /d2drestorevol --command=restore --storage-path=/CRE_ROOT --node-e=rh63-v2 --rp=last --source-volume=/opt/oracle --target-volume=/dev/sdb1 --mount-target=/opt/oracle --quick-recovery

Il database Oracle si apre ed è possibile eseguire le normali operazioni del database come quelle relative alle query, all'inserimento, all'eliminazione, all'aggiornamento dei dati e così via.

Il database Oracle viene recuperato istantaneamente.

Esecuzione del ripristino granulare di un database Oracle

È possibile recuperare file specifici relativi al database Oracle. Questi file possono essere file di controllo o file di dati degli spazi tabella.

La presente sezione descrive i seguenti argomenti:

- Verifica dei prerequisiti
- Ripristino degli spazi tabelle
- Ripristino dei file di controllo

Verifica dei prerequisiti

Verificare i prerequisiti seguenti prima di ripristinare il database Oracle:

- Si dispone di un punto di ripristino valido e della password di crittografia.
- Si dispone di un nodo di destinazione valido per il recupero dei dati.
- Si è verificato che il server di backup di Linux supporta il file system che si desidera ripristinare.
- Verificare i file system supportati per i backup basati su agente UDP per Linux. I file system ASM (Automatic Storage Management), ACFS e Oracle Cluster File System (OCFS / OCFS2) non sono supportati per i backup basati su agente UDP per Linux. Per proteggere i dati su questi file system, utilizzare i backup UDP Oracle RMAN.
- Esaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Ripristino degli spazi tabelle

Se uno spazio tabella di database viene perso o corrotto, è possibile ripristinarlo eseguendo un ripristino a livello del file. Dopo che il ripristino a livello del file è stato completato correttamente, è necessario recuperare manualmente lo spazio tabella.

Effettuare le operazioni seguenti:

1. Accedere al computer di destinazione come utente root.
2. Assicurarsi che il database sia disponibile.
3. Prendere lo spazio di tabella necessario in modalità non in linea.

   Esempio: Considerare che il nome dello spazio tabella sia MYTEST_DB. Immettere il comando seguente per prendere lo spazio tabella in modalità non in linea:

   ```
   $ sqlplus "/ as sysdba"

   SQL> alter tablespace MYTEST_DB offline;
   ```

4. Elencare tutti i file di dati per lo spazio tabella MYTEST_DB specificato.

   ```
   SQL> select file_name, tablespace_name from dba_data_files
   where tablespace_name='MYTEST_DB';

   FILE_NAME

   ----------------------------------------------------------------
   ------------------

   TABLESPACE_NAME

   ------------------------------

   /opt/oracle/oradata/lynx/MYTEST_DATA01.dbf

   MYTEST_DB
   ```

5. Ripristinare i file di dati degli spazi tabella mediante la procedura guidata di ripristino. Per ulteriori informazioni sul processo di ripristino, vedere Esecuzione di un ripristino a livello di file sui nodi Linux.
6. Specificare le informazioni seguenti sulla procedura guidata di ripristino e inoltrare il processo:

a. Quando si selezionano i file e le cartelle, immettere il nome del file di dati obbligatorio dello spazio tabella e avviare la ricerca.

Esempio: Immettere "MYTEST_DATA01.dbf" dello spazio tabella "MYTEST_DB" e cercare.

b. Sulla pagina del computer di destinazione, immettere le informazioni seguenti:
   - Selezionare Ripristina in posizione originale.
   - Immettere il nome host o l'indirizzo IP del server Oracle di destinazione.
   - Immettere il nome utente root e la password del server Oracle di destinazione.
   - Selezionare Sovrascrivi i file esistenti per l'opzione Risoluzione conflitti.

7. Dopo che i file di dati sono stati ripristinati, recuperare lo spazio tabella del database Oracle.

   ```
   SQL>recover tablespace MYTEST_DB;

   Specify log: {<RET>=suggested | filename | AUTO | CANCEL}

   Automatico
   ```

8. Creare lo spazio tabella specificato in modalità in linea.

   ```
   SQL>alter tablespace MYTEST_DB online;
   ```

   Lo spazio tabella è stato recuperato correttamente.

Ripristino dei file di controllo

Se i file di controllo di un database sono persi o corrotti, è possibile ripristinarli eseguendo un ripristino a livello del file. Dopo che il ripristino a livello del file è stato completato correttamente, è necessario recuperare manualmente i file di controllo.

Effettuare le operazioni seguenti:

1. Accedere al computer di destinazione come utente root.
2. Chiudere l'istanza Oracle.

   ```
   SQL>shutdown abort
   ```

3. Avviare il database nello stato nomount.

   ```
   SQL>startup nomount
   ```

4. Elencare il percorso per tutti i file di controllo.

   ```
   SQL> show parameter control_files;

   NAME            TYPE             VALUE

   -------------- -------- -------------

   control_files string /opt/oracle/oradata/lynx/control01.ctl,
   /opt/oracle/flash_recovery_area/lynx/control02.ctl
   ```

5. Ripristinare i file di controllo mediante la procedura guidata di ripristino. Per ulteriori informazioni sul processo di ripristino, vedere Esecuzione di un ripristino a livello di file sui nodi Linux.
6. Specificare le informazioni seguenti sulla procedura guidata di ripristino e inoltrare il processo:
   a. Quando si selezionano i file e le cartelle, immettere il nome del file di controllo obbligatorio e avviare la ricerca. Ripetere questo passaggio finché tutti i file di controllo sono stati selezionati.

      Esempio: Immettere "control01.ctl " e avviare la ricerca.

   b. Sulla pagina del computer di destinazione, immettere le informazioni seguenti:
      - Selezionare Ripristina in posizione originale.
      - Immettere il nome host o l'indirizzo IP del server Oracle di destinazione.

- Immettere il nome utente root e la password del server Oracle di destinazione.
- Selezionare Sovrascrivi i file esistenti per l'opzione Risoluzione conflitti.

7. Dopo il ripristino di tutti i file di controllo, installare il database e aprirlo.

```
$sqlplus / as sysdba

SQL>alter database mount;
```

8. Recuperare il database con il comando RECOVER e aggiungere la clausola USING BACKUP CONTROLFILE.

```
SQL> RECOVER DATABASE USING BACKUP CONTROLFILE
```

9. Applicare i registri archiviati richiesti.

   Nota: se il registro archiviato richiesto non è disponibile, significa che nei registri di ripristino in linea è contenuto il record di ripristino necessario. Questa situazione si verifica quando nei registri in linea sono presenti modifiche non archiviate in seguito a un errore dell'istanza. È possibile specificare il percorso completo di un file del registro di ripristino in linea, quindi premere Invio. Per trovare il registro corretto, è possibile che si debba ripetere questa operazione più volte.

   Esempio:

```
SQL> RECOVER DATABASE USING BACKUP CONTROLFILE

ORA-00279: change 1035184 generated at 05/27/2014
18:12:49 needed for thread 1

ORA-00289: suggestion :

/opt/oracle/flash_recovery_area/LYNX/archivelog/2014_05_
27/o1_mf_1_6_%u_.arc

ORA-00280: change 1035184 for thread 1 is in sequence #6

Specify log: {<RET>=suggested | filename | AUTO | CANCEL}

/opt/oracle/oradata/lynx/redo03.log

Log applied.
```

10. Media recovery complete.
11. Aprire il database con la clausola RESETLOGS una volta completato il processo di ripristino.

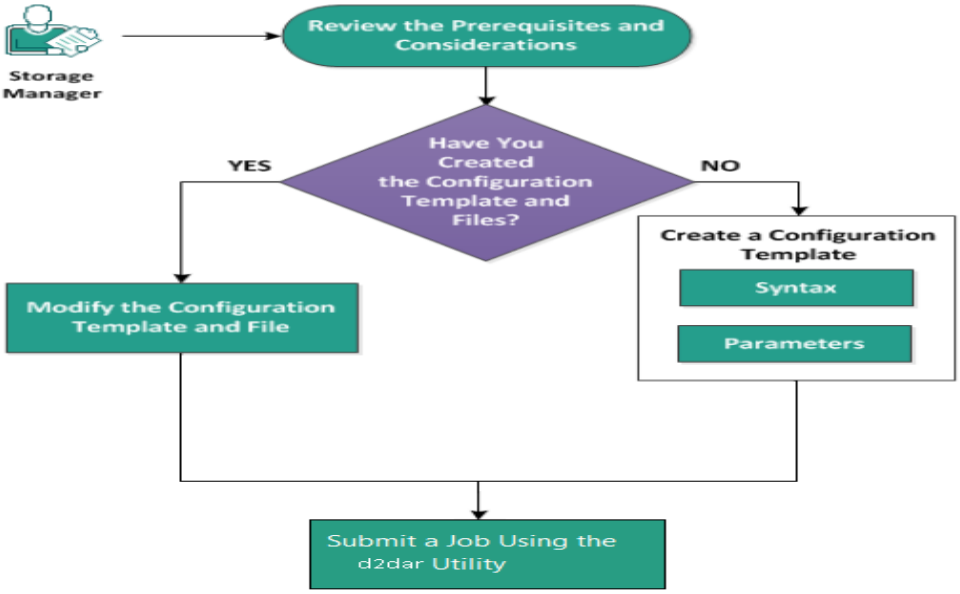
```
SQL> alter database open resetlogs;
```

I file di controllo sono stati recuperati correttamente.

Esecuzione della verifica Assured Recovery dalla riga di comando

È possibile eseguire la verifica Assured Recovery dalla riga di comando del server di backup mediante l'utilità d2dar. L'utilità d2dar automatizza il processo di esecuzione di una verifica Assured Recovery per le sessioni di backup specificate.

Nel diagramma seguente viene illustrato il processo di esecuzione di una verifica Assured Recovery dalla riga di comando tramite l'utilità d2dar:



Eseguire queste attività per l'esecuzione della verifica Assured Recovery:

- Verifica delle considerazioni e dei prerequisiti
- Creazione di un modello di configurazione
- Modifica del file e del modello di configurazione
- Inoltro di un processo mediante l'utilità d2dar

Verifica delle considerazioni e dei prerequisiti

Tenere presenti le seguenti considerazioni prima di eseguire la verifica di Assured Recovery:

- Sono supportate le seguenti versioni di hypervisor per la verifica Assured Recovery tramite l'utilità d2dar:
  - VMware vCenter/ESX(i) 5.0 o versioni successive
  - Hyper-V Server 2012 o versioni successive

    Nota: per ulteriori informazioni sui computer virtuali Linux supportati su Hyper-V, fare clic sul seguente collegamento.
- La verifica Assured Recovery viene eseguita soltanto dalla riga di comando. Questa opzione non è disponibile nell'interfaccia utente.

Creazione di un modello di configurazione

È possibile creare un file di configurazione in modo che il comando d2dar possa eseguire la verifica Assured Recovery in base ai parametri specificati nel file.

Sintassi

d2dar –createtemplate=<cfg_file_path>

L'utilità *d2dutil --encrypt* crittografa la password e fornisce una password crittografata. È necessario utilizzare questa utilità per crittografare tutte le password.

Metodo 1

echo 'string' | ./d2dutil --encrypt

string corrisponde alla password specificata.

Metodo 2

Immettere il comando *d2dutil –encrypt*, quindi specificare la password. Premere **Invio** per visualizzare i risultati sulla schermata. In questo metodo, la password immessa non viene visualizzata nella schermata.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Accedere alla cartella bin di installazione dell'agente Arcserve Unified Data Protection per Linux immettendo il seguente comando:

   #cd /opt/Arcserve/d2dserver/bin
3. Creare il modello di configurazione utilizzando il seguente comando:

   #./d2dar --createtemplate=<cfg_file_path>

   <cfg_file_path> indica la posizione in cui viene creato il modello di configurazione.
4. Aprire il modello di configurazione e aggiornare i seguenti parametri:

   job_name

   Specifica il nome del processo Assured Recovery.

   vm_name_prefix

   Specifica il prefisso per il computer virtuale creato per il processo Assured Recovery. Il nome del computer virtuale Assured Recovery è vm_ name_prefix + nome nodo + indicatore data/ora.

   vm_type

Specifica il tipo di hypervisor per l'esecuzione della verifica di Assured Recovery. I tipi di hypervisor validi sono Hyper-V , ESX e AHV.

vm_server

Specifica l'indirizzo del server hypervisor. L'indirizzo può essere il nome host o l'indirizzo IP.

vm_svr_username

Specifica il nome utente dell'hypervisor.

vm_svr_password

Specifica la password dell'hypervisor. La password viene crittografata mediante l'utilità di crittografia d2dutil.

vm_svr_protocol

Specifica il protocollo dell'hypervisor nel caso in cui venga eseguito Assured Recovery su vCenter/ESX(i) o AHV.

vm_svr_port

Specifica la porta dell'hypervisor nel caso in cui venga eseguito Assured Recovery su vCenter/ESX(i) o AHV.

vm_sub_server

Specifica il nome del server ESX quando si esegue Assured Recovery su vCenter o Specifica il nome del cluster dell'elemento Prism quando si esegue Assured Recovery su Prism Central.

vm_datastore

Specifica la posizione di archiviazione per il computer virtuale utilizzata per la verifica di Assured Recovery. Quando si esegue la verifica di Assured Recovery su vCenter/ESXI(i), la posizione corrisponde all'archivio dati sul server ESX (i). La posizione dovrebbe essere il percorso locale sul server Hyper-V quando si esegue Assured Recovery on Hyper-V. La posizione è il contenitore_di_memorizzazione sul cluster AHV quando si esegue Assured Recovery on AHV.

vm_resource_pool

Specifica il nome del Pool di risorse nel caso in cui venga eseguito Assured Recovery su vCenter/ESX(i).

timeout

Specifica il tempo per il processo Assured Recovery durante il riavvio fino all'utilizzo del computer virtuale. L'unità di tempo è espressa in secondi.

vm_memory

Specifica la dimensione di memoria del computer virtuale. La dimensione dell'unità è espressa in MB, in multipli di 4.

vm_cpu_count

Specifica il numero di CPU del computer virtuale.

run_after_backup

Specifica che il processo Assured Recovery verrà eseguito una volta oppure sempre per il processo di backup definito dal parametro backup_job_name. Il processo Assured Recovery verrà eseguito immediatamente per il processo di backup specificato se impostato su **no. Verrà inoltre eseguito ad ogni completamento del processo di backup specificato se impostato su sì**.

Valore predefinito: No

backup_job_name

Specifica il nome del processo di backup dei nodi per l'esecuzione del processo Assured Recovery.

storage_type

Specifica il tipo di archiviazione per la sessione di backup. I tipi di archiviazione validi sono cifs, nfs e rps.

storage_location

Specifica la posizione NFS o CIFS.

storage_username

Specifica il nome utente della posizione CIFS.

storage_password

Specifica la password della posizione CIFS. La password viene crittografata mediante l'utilità di crittografia d2dutil.

rps_protocol

Specifica il protocollo del Recovery Point Server quando si esegue il processo Assured Recovery per le sessioni nel Recovery Point Server.

rps_hostname

Specifica il nome host del Recovery Point Server. L'indirizzo può essere il nome host o l'indirizzo IP.

rps_username

Specifica il nome utente del Recovery Point Server.

rps_password

Specifica la password del Recovery Point Server. La password viene crittografata mediante l'utilità di crittografia d2dutil.

rps_port

Specifica la porta del Recovery Point Server.

Valore predefinito: 8014.

rps_datastore

Specifica il nome dell'archivio dati sul Recovery Point Server.

encryption_password

Specifica la password della sessione crittografata. La password viene crittografata mediante l'utilità di crittografia d2dutil.

node_name_list

Specifica il nome de nodi di cui viene eseguita la verifica di Assured Recovery. I nomi vengono separati dal simbolo ‘;’. Se il nome non viene specificato o viene lasciato vuoto, tutti i nodi con lo stesso nome per il processo di backup o contenuti nello stesso percorso eseguiranno la verifica di Assured Recovery.

recovery_point_date_filter

Specifica la data del punto di ripristino. La verifica di Assured Recovery verrà eseguita per l'ultimo punto di ripristino precedente alla data specificata. Se la data non viene specificata o viene lasciata vuota, l'ultima sessione di backup eseguirà la verifica di Assured Recovery.

gateway_vm_network

Specifica la rete del computer virtuale per il server gateway. Il computer virtuale e il server di backup si trovano sulla stessa rete.

gateway_guest_network

Specifica il tipo di indirizzo IP di rete per il server gateway. La rete può essere dhcp o statica.

gateway_guest_ip

Specifica l'indirizzo IP del server gateway quando si specifica l'IP statico.

gateway_guest_netmask

Specifica la netmask del server gateway quando si specifica l'IP statico.

gateway_guest_gateway

Specifica il gateway del server gateway quando si specifica l'IP statico.

script_post_job_server

(Facoltativo) Specifica lo script da eseguire dopo il completamento del processo sul server di backup.

script_ready_to_use

(Facoltativo) Specifica lo script da eseguire quando il computer di destinazione è pronto per l'uso sul computer virtuale di Assured Recovery.

run_script_ready_to_use_timeout

Specifica il tempo per l'esecuzione dello script pronto all'uso dell'utente specificato da script_ready_to_use. L'unità di tempo è espressa in secondi.

Nota: i parametri delle informazioni relative alla sessione, compresi *storage_type, storage_location, storage_username, storage_password, rps_protocol, rps_hostname, rps_username, rps_password, rps_port e rps_datastore* sono obbligatori solo se il parametro *backup_job_name* non viene specificato.

5. Fare clic su **Salva** e chiudere il modello di configurazione.

   Il modello di configurazione è stato creato correttamente.

Modifica del file e del modello di configurazione

Se si dispone già del file del modello di configurazione, è possibile modificare il file ed eseguire la verifica di Assured Recovery con una configurazione differente. Non è necessario creare un altro modello di configurazione. Quando si invia il processo, viene aggiunto un nuovo processo all'interfaccia Web. Nell'interfaccia Web è possibile visualizzare i registri attività.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Aprire il modello di configurazione dalla posizione in cui è stato salvato il file e modificare i parametri in base ai propri requisiti.
3. Fare clic su **Salva** e chiudere il modello di configurazione.
4. Fare clic su **Salva** e chiudere il file di configurazione globale.

Il modello di configurazione è stato modificato correttamente.

Inoltro di un processo mediante l'utilità d2dar

È possibile utilizzare il comando d2dar per eseguire la verifica Assured Recovery per le sessioni sottoposte a backup. Dopo l'invio, è possibile visualizzare il processo dall'interfaccia Web. Durante il processo di Assured Recovery, se uno qualsiasi dei requisiti non viene soddisfatto, la riga di comando visualizza un errore. Nell'interfaccia Web è inoltre possibile visualizzare il registro attività.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Inviare il processo Assured Recovery utilizzando il comando seguente:

   #./d2dar --template=cfg_file_path

Montaggio dei punti di ripristino

Il montaggio dei punti di ripristino può condividere i file in un punto di ripristino tramite NFS o WebDAV. È inoltre possibile accedere ai file montando la posizione sul server Linux.

Per il montaggio del punto di ripristino, eseguire le seguenti attività:

- Verifica dei prerequisiti
- Definizione del punto di ripristino per il montaggio del punto di ripristino
- Definizione delle impostazioni per il montaggio del punto di ripristino
- Creazione ed esecuzione del processo di montaggio del punto di ripristino
- Montaggio della condivisione NFS o WebDAV su server Linux

Verifica dei prerequisiti

Considerare i prerequisiti seguenti prima di procedere con il montaggio dei punti di ripristino:

- Si dispone di un punto di ripristino valido e della password di crittografia.
- Se si desidera eseguire il montaggio del punto di ripristino tramite WebDAV, accertarsi che il pacchetto davfs2 sia stato installato sul server Linux.
- Esaminare la Matrice di compatibilità che fornisce i sistemi operativi, i database e i browser supportati.

Definizione del punto di ripristino per il montaggio del punto di ripristino

L'esecuzione di un backup implica la creazione di un punto di ripristino. Specificare le informazioni relative al punto di ripristino della Procedura guidata di ripristino, in modo da poter eseguire il ripristino dei dati desiderati. È possibile ripristinare file specifici o tutti i file in base alle proprie esigenze.

Effettuare le operazioni seguenti:

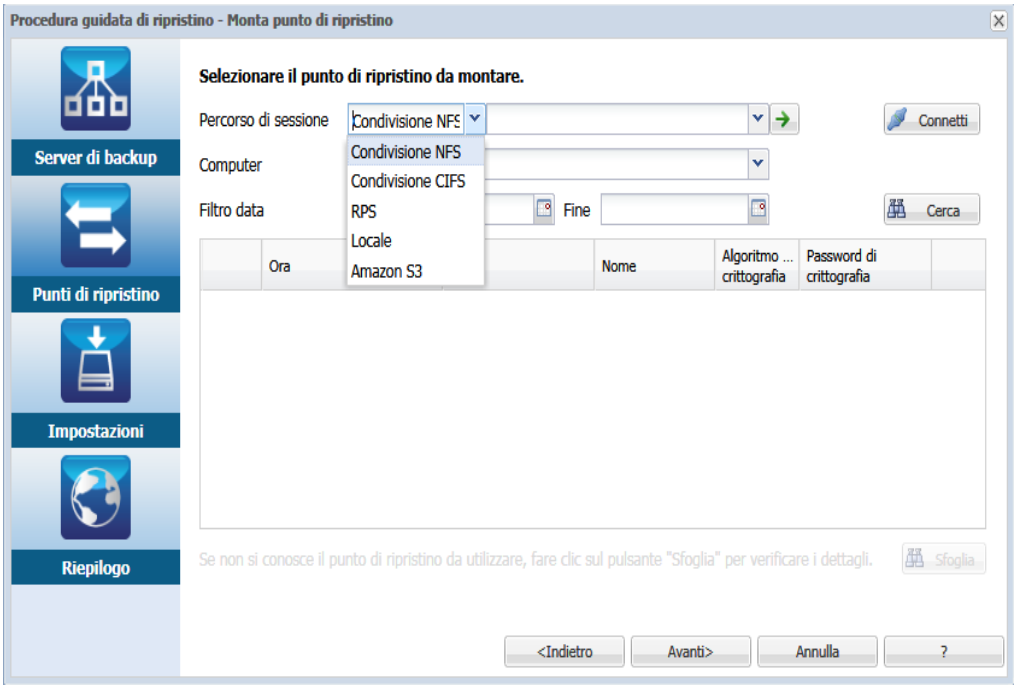
1. Aprire l'interfaccia Web dell'agente Arcserve UDP (Linux).
2. Fare clic su **Ripristino** dal menu **Procedura guidata** e selezionare **Monta punto di ripristino.**

   Viene visualizzata la **Procedura guidata di ripristino** – **Monta punto di ripristino**.

   È possibile visualizzare il **server di backup** selezionato nella pagina Server di backup della **procedura guidata di ripristino**. Non è possibile selezionare alcuna opzione dall'elenco a discesa **Server di backup**.

3. Fare clic su **Avanti**.

   Viene visualizzata la pagina **Punti di ripristino** della **Procedura guidata di ripristino**.



4. Selezionare uno dei seguenti elementi **condivisione CIFS/condivisione NFS/-condivisione RPS/Locale** dall'elenco a discesa Percorso di sessione.
5. Eseguire una delle operazioni riportate di seguito in base al percorso di sessione:

   Per condivisione CIFS/condivisione NFS/Locale

   Specificare il percorso completo della condivisione CIFS/condivisione NFS/Locale e fare clic su **Connetti**.

   Tutti i computer vengono elencati nell'elenco a discesa **Computer**.

   Nota: se si seleziona l'opzione di condivisione CIFS, specificare il nome utente e la password.

   Per il server RPS

   a. Selezionare il server RPS e fare clic su **Aggiungi**.

      Viene visualizzata la finestra di dialogo **Informazioni sul server del punto di ripristino**.

   b. Fornire i dettagli RPS e fare clic sul pulsante **Carica.**

   c. Selezionare l'archivio dati dall'elenco a discesa e fare clic su **Sì**.

      La finestra di dialogo Informazioni sul server del punto di ripristino viene chiusa e viene visualizzata la procedura guidata.

   d. Fare clic su **Connetti.**

      Tutti i computer vengono elencati nell'elenco a discesa Computer.

   e. Selezionare il computer dall'elenco a discesa.

      Tutti i punti di ripristino del computer selezionato vengono visualizzati sotto l'opzione **Filtro data**.

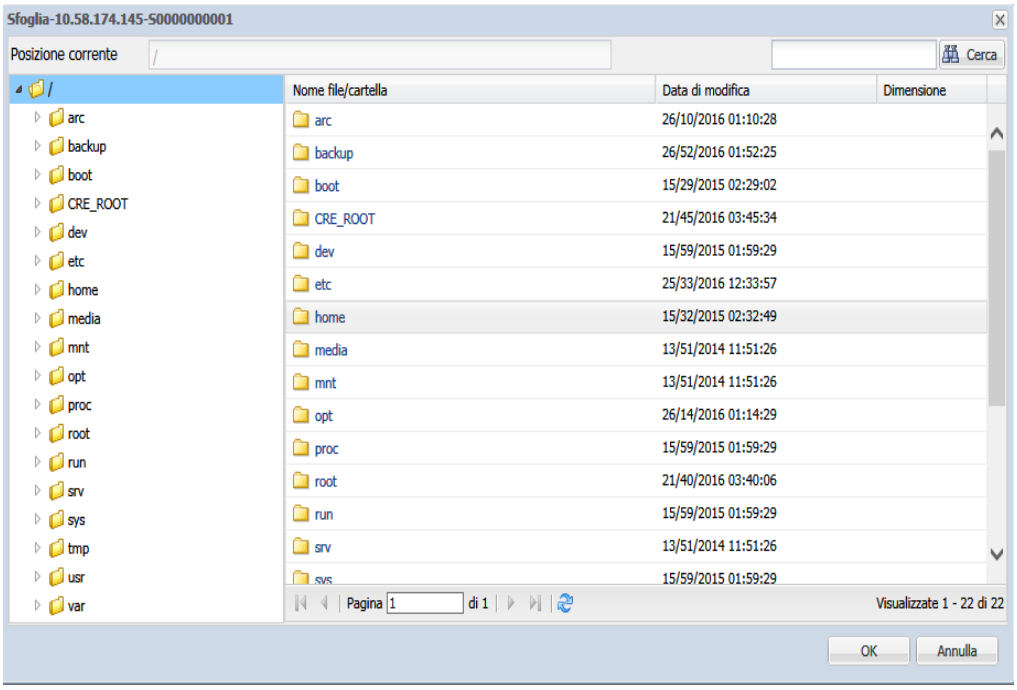
6. Applicare il filtro data per visualizzare i punti di ripristino generati tra le date specificate e fare clic su **Cerca**.

   Valore predefinito: ultime due settimane.

   Vengono visualizzati tutti i punti di ripristino disponibili tra le date specificate.

7. Fare clic su Sfoglia per visualizzare il punto di ripristino.

   Viene visualizzata la finestra di dialogo **Sfoglia-<nome nodo>-<numero sessione>**.



Nota: se si esegue la ricerca di un file o una cartella mediante il campo **Cerca**, accertarsi di selezionare la cartella più elevata nella gerarchia. La ricerca viene condotta in tutte le cartelle figlie della cartella selezionata.

8. Fare clic su **OK**.

   La finestra di dialogo **Sfoglia <nome nodo>-<numero sessione>** viene chiusa e si verrà reindirizzati alla pagina Punti di ripristino.

9. Fare clic su **Avanti**.

   Vengono visualizzate le **Impostazioni** della pagina Monta punto di ripristino.

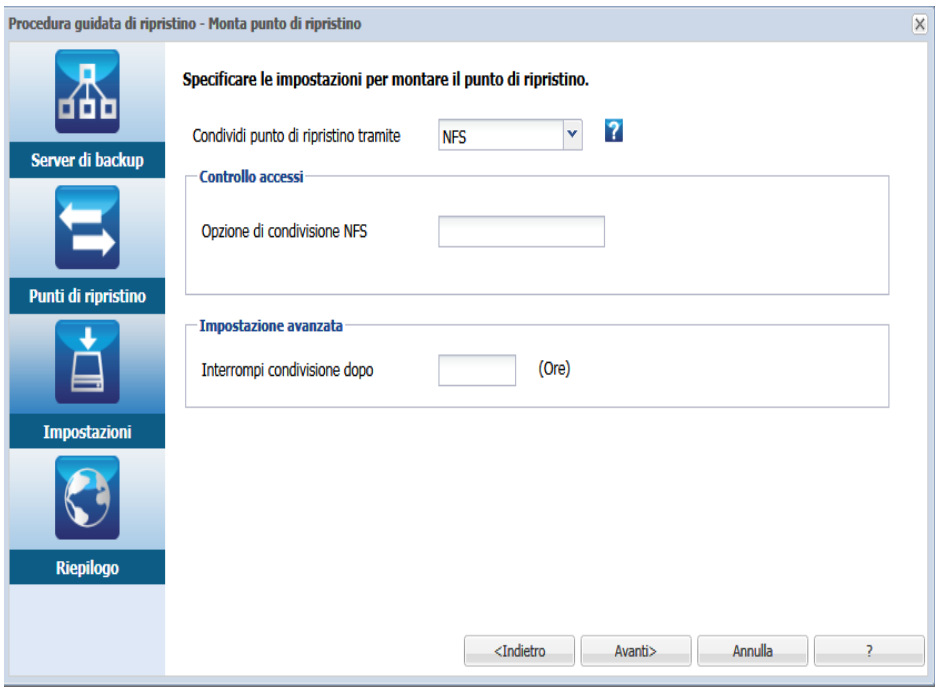
Definizione delle impostazioni per il montaggio del punto di ripristino

Specificare le impostazioni per il montaggio del punto di ripristino per la scelta del metodo di condivisione appropriato.

Effettuare le operazioni seguenti:

1. Per montare il punto di ripristino tramite NFS, procedere come segue:
   a. Selezionare **NFS** dall'elenco a discesa del metodo di condivisione.

      I file nel punto di ripristino verranno condivisi tramite NFS. È inoltre possibile montare la condivisione NFS su qualsiasi computer con accesso al server di backup Linux.



   b. (Facoltativo) Immettere le **opzione di condivisione NFS** in base ai propri requisiti.

      Consultare la pagina principale per le esportazioni, le opzioni candidate e i formati validi. Lasciare il campo vuoto se non è necessario disporre del controllo dell'accesso.

   c. Immettere **Ora** per il tempo la cui condivisione scadrà in seguito al raggiungimento dell'orario specificato.

Se si immette 0 in questo campo, è possibile che la condivisione venga abilitata in modo permanente.

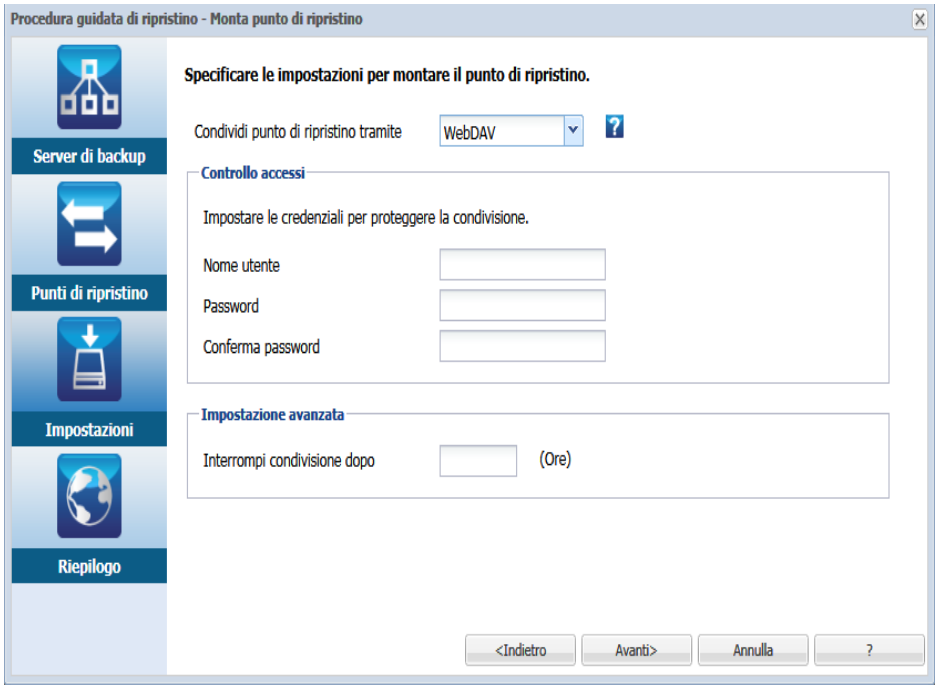
d. Fare clic su **Avanti**.

Viene visualizzata la pagina del processo di montaggio del punto di ripristino.

2. Nella sezione Montaggio del punto di ripristino tramite WebDAV, eseguire la procedura riportata di seguito:

a. Selezionare **WebDAV** dall'elenco a discesa del metodo di condivisione.

I file nel punto di ripristino verranno condiviso tramite WebDAV. È inoltre possibile montare la condivisione WebDAV mediante mount.davfs. Si tratta del metodo consigliato quando è necessario accedere alla condivisione tramite Internet.



b. Immettere **Nome utente**, **Password**, quindi immettere nuovamente la password nel campo **Conferma password** per Access Control.

Annotare il nome utente e la password poiché verranno richiesti nuovamente per accedere al punto di ripristino di cui è stato eseguito il montaggio.

c. Immettere **Ora** per il tempo la cui condivisione scadrà in seguito al raggiungimento dell'orario specificato.

Se si immette 0 in questo campo, è possibile che la condivisione venga abilitata in modo permanente.

Se viene raggiunta l'ora specificata, non sarà possibile accedere al punto di ripristino di cui è stato eseguito il montaggio.

d. Fare clic su **Avanti**.

Viene visualizzata la pagina di riepilogo del processo di montaggio del punto di ripristino.

Creazione ed esecuzione del processo di montaggio del punto di ripristino

È possibile creare ed eseguire il processo di montaggio del punto di ripristino in modo da poter accedere ai file nel punto di ripristino specificato. Verificare le informazioni di configurazione prima di inoltrare il processo. Se necessario, è possibile tornare indietro e modificare le impostazioni della procedura guidata.

Effettuare le operazioni seguenti:

1. Verificare i dettagli di montaggio del punto di ripristino dalla pagina **Riepilogo**.
2. (Facoltativo) Fare clic su **Indietro** per modificare le informazioni immesse in una pagina qualsiasi della Procedura guidata di ripristino.
3. Immettere un nome per il del processo e fare clic su **Invia**.

   Il campo **Nome processo** è associato a un nome predefinito. È possibile specificare un nuovo nome per il processo ma non è possibile lasciare il campo vuoto.

   La **Procedura guidata di ripristino** viene chiusa. È possibile visualizzare lo stato del processo dalla scheda **Stato processo**.

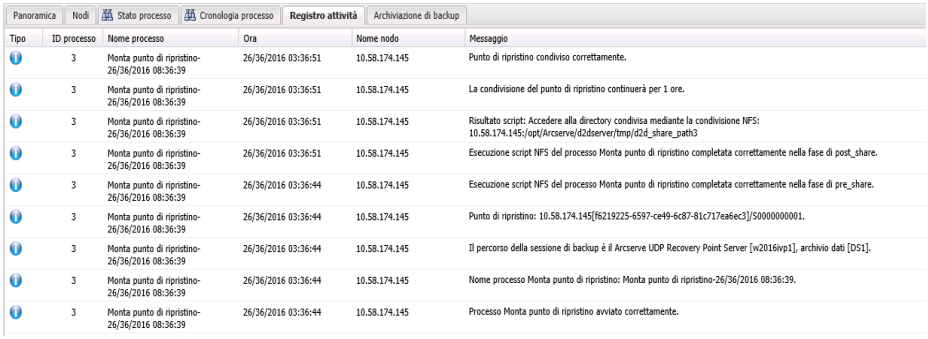
   Il processo di montaggio del punto di ripristino è stato creato ed eseguito correttamente.

Montaggio della condivisione NFS o WebDAV su server Linux

È possibile accedere al punto di ripristino montato dopo che la **Fase processo** della scheda **Stato processo** corrisponde a **Punto di ripristino di condivisione.**

Effettuare le operazioni seguenti:

1. Acquisire l'**ID processo / Nome processo** del processo Monta punto di ripristino nella scheda **Stato processo**.
2. Filtrare i registri attività per processo Monta punto di ripristino per **ID processo / Nome processo** nella pagina **Registro attività** tramite gli strumenti **Filtro**.



3. Individuare la directory condivisa per il punto di ripristino montato visualizzato nel registro attività.

   Formato della directory per il montaggio via NFS:

   < d2dserver >:/opt/Arcserve/d2dserver/tmp/d2d_share_path<jobid>

   È possibile accedere ai file nel punto di ripristino tramite il montaggio della directory.

   Esempio:

   mount *< d2dserver >:/opt/Arcserve/d2dserver/tmp/d2d_share_path<jobid> /mnt*

   Formato della directory per il montaggio via WebDAV:

   https://<d2dserver>:8014/share/<User Name>/

   È possibile accedere ai file nel punto di ripristino con browser Web o tramite il montaggio della directory.

   Esempio:

   mount.dafs https://<d2dserver>:8014/share/<User Name>/ /mnt

4. Immettere il nome utente e la password forniti durante l'inoltro del processo di montaggio del punto di ripristino.

La presente sezione descrive i seguenti argomenti:

- Installazione del pacchetto davfs su server Linux

Installazione del pacchetto davfs sul server Linux

È possibile installare il pacchetto davfs sul server Linux.

- Per Red Hat Linux, Linux CentOS oppure Oracle Linux

  Effettuare le operazioni seguenti:

  1. Ottenere pacchetti aggiuntivi per Enterprise Linux (EPEL) per il server Linux con la versione corrispondente all'indirizzo http://fedoraproject.org/wiki/EPEL#How_can_I_use_these_extra_packages.3F
  2. Copiare il pacchetto EPEL scaricato sul server Linux di destinazione.
  3. Installare il pacchetto EPEL utilizzando il comando seguente.

     # yum install <package_path>/epel-release-<version_information>.rpm
  4. Installare il pacchetto davfs2 utilizzando il comando seguente.

     # yum install davfs2

- Per SuSE Linux 12 SP1

  Effettuare le operazioni seguenti:

  1. Accedere al server Linux.
  2. Installare il pacchetto davfs2 utilizzando il comando seguente.

     # zypper addrepo

     # zypper refresh

     # zypper install davfs2

  Per ulteriori informazioni, fare clic sul seguente collegamento.

Attivazione del supporto per i kernel Linux più recenti di RHEL, OEL (kernel RHEL), Debian, SUSE e Ubuntu

RHEL, OEL (kernel RHEL), Debian, SUSE e Ubuntu aggiornano i propri kernel regolarmente. Pertanto, i driver inviati non risultano aggiornati. Inoltre, il processo di aggiornamento automatico del kernel elimina la necessità di compilare manualmente un nuovo pacchetto di driver da parte di CFT per ogni nuovo kernel. Sebbene la disattivazione del processo di aggiornamento automatico del kernel di questi sistemi consenta di risolvere il problema, Arcserve offre inoltre supporto per i kernel aggiornati (se richiesto).

Importante: nonostante il massimo impegno per supportare i kernel RHEL, OEL (kernel RHEL), Debian, SUSE e Ubuntu più recenti, le modifiche kernel principali potrebbero ancora ritardare o annullare i driver corrispondenti.

I manager dell'archiviazione possono esaminare gli scenari seguenti per abilitare l'utilizzo dell'agente Arcserve UDP (Linux) con i kernel RHEL, OEL (kernel RHEL), Debian, SUSE e Ubuntu più recenti:

- Se il server dell’agente Arcserve UDP (Linux) dispone di una connessione Internet attiva, i driver aggiornati vengono scaricati e distribuiti in modo automatico. È possibile utilizzare il software senza ulteriori sforzi.
- Se il server dell’agente Arcserve UDP (Linux) non dispone dell’accesso a Internet, è possibile scaricare e distribuire manualmente il pacchetto del driver aggiornato.
- Se si dispone di più server dell’agente Arcserve UDP (Linux), è possibile distribuire il pacchetto del driver aggiornato su un server, quindi configurare l’altro server affinché venga utilizzato come server di gestione temporanea.

Per distribuire il pacchetto del driver aggiornato, procedere come segue:

- Verifica dei prerequisiti
- Distribuzione manuale del pacchetto di driver RHEL, OEL (kernel RHEL), Debian, SUSE e Ubuntu aggiornati
- (Facoltativo) Utilizzo del server di gestione temporanea per l’aggiornamento dei driver
- (Facoltativo) Configurazione del proxy HTTP

Verifica dei prerequisiti

Tenere presente i seguenti prerequisiti:

- Le credenziali di accesso root sono disponibili per l'accesso al server di backup.
- È necessario aver installato curl o wget sul server di backup.
- È necessario aver installato gpg sul server di backup.

Distribuzione manuale del pacchetto di driver RHEL, OEL (kernel RHEL), Debian, SUSE e Ubuntu aggiornati

Se il server dell'agente Arcserve UDP (Linux) non dispone dell'accesso a Internet, è possibile aggiornare i driver scaricandoli e distribuendoli manualmente.

Effettuare le operazioni seguenti:

1. Scaricare il pacchetto driver e il file di firma. Per ottenere il collegamento per il download, contattare il Supporto tecnico di Arcserve.

   Nota: collocare il file di firma scaricato e il pacchetto del driver nel formato *.tar.gz nel percorso della cartella di destinazione. Non estrarre i file.

2. Accedere al server di backup come utente root.

3. Accedere al percorso contenente il pacchetto scaricato e avviare la distribuzione utilizzando i seguenti comandi:

   # source /opt/Arcserve/d2dserver/bin/setenv

   # /opt/Arcserve/d2dserver/bin/d2dupgradetool deploy <folder containing the downloaded package>

   Il pacchetto driver aggiornato è stato distribuito correttamente.

(Facoltativo) Utilizzo del server di gestione temporanea per l'aggiornamento dei driver

Se si dispone di più server dell'agente Arcserve UDP (Linux) che richiedono il supporto per i kernel più recenti di RHEL, OEL (kernel RHEL), Debian, SUSE e Ubuntu, è possibile configurarli per utilizzarne uno come server di gestione temporanea. Assicurarsi che il driver aggiornato sia già stato distribuito sul server di gestione temporanea tramite la connessione Internet attiva, oppure che si attenga alle istruzioni riportate nell'attività Distribuzione manuale del pacchetto driver dei kernel RHEL, OEL (kernel RHEL), Debian, SUSE e Ubuntu aggiornati. È possibile configurare ogni server di backup che necessita del pacchetto del driver RHEL, OEL (kernel RHEL), Debian, SUSE e Ubuntu aggiornato.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Aprire e modificare il file di configurazione:

   # /opt/Arcserve/d2dserver/configfiles/auto_upgrade.cfg
3. Modificare gli elementi di configurazione seguenti:

   scheme=<http o https>

   Host=<indirizzo del server di gestione temporanea>

   Port=<porta del server dell'agente, solitamente 8014>

   L'aggiornamento del pacchetto del driver automatizzato è stato configurato correttamente.

(Facoltativo) Configurazione del proxy HTTP

È possibile configurare il proxy per l'agente Arcserve UDP (Linux) per accedere a Internet.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Aprire e modificare il file di configurazione:

   # /opt/Arcserve/d2dserver/configfiles/auto_upgrade.cfg
3. Modificare gli elementi di configurazione seguenti:

   # /opt/Arcserve/d2dserver/configfiles/auto_upgrade.cfg

   http_proxy=<proxy address>

   proxy_user=<username>

   proxy_password=<password>

   Il proxy è stato configurato correttamente.

Disattivazione del bit SUID durante l'esecuzione del processo di ripristino del file

Durante l'esecuzione del processo di ripristino del file mediante le credenziali dell'utente sudo (non root) del nodo di destinazione, il bit SUID viene impostato per il file binario d2dtar in modo da sfruttarne l'utilizzo. Il file binario d2dtar viene eseguito sul nodo di destinazione durante il processo di ripristino del file. In alcuni ambienti, l'utilizzo del bit SUID è disattivato per la protezione dei dati. Questa sezione fornisce informazioni su come disabilitare il bit SUID per il file binario d2dtar.

La presente sezione descrive i seguenti argomenti:

Verifica dei prerequisiti

Tenere presente i seguenti prerequisiti:

- Si dispone delle credenziali di accesso root per accedere al server di backup Linux.
- Si dispone delle credenziali di accesso root del nodo di destinazione per modificare il file *sudoers*.

Configurazione delle impostazioni nel server di backup Linux

Questa sezione fornisce informazioni su come configurare le impostazioni nel server di backup Linux.

Effettuare le operazioni seguenti:

1. Accedere al server di backup Linux utilizzando le credenziali root.
2. Accedere al file */opt/Arcserve/d2dserver/configfiles/server.env*, quindi aggiungere la riga seguente:

   "export FLR_DISABLE_SUID=1"

   Nota: se il file *server.env* non esiste in */opt/Arcserve/d2dserver/configfiles*, creare il file *server.env*, quindi aggiungere la riga precedente al file *server.env*.
3. Per riavviare d2dserver, eseguire il seguente comando:

   # /opt/Arcserve/d2dserver/bin/d2dserver restart

Configurazione di sudo per autorizzare il file binario d2dtar nel nodo di destinazione

Questa sezione fornisce informazioni su come configurare sudo per autorizzare il file binario d2dtar nel nodo di destinazione.

Effettuare le operazioni seguenti:

1. Accedere al nodo di destinazione utilizzando le credenziali root.
2. Per modificare il file di configurazione, aprire il file */etc/sudoer* utilizzando il comando *visudo*.
3. Aggiungere la riga seguente:

   <sudo-user> ALL=(ALL) NOPASSWD: /home/<sudo-user>/.d2drestorefile/d2dtar.64,/tmp/d2dtar.64

   Esempio: se udplinux è un utente sudo, aggiungere la seguente riga al file /etc/sudoers:

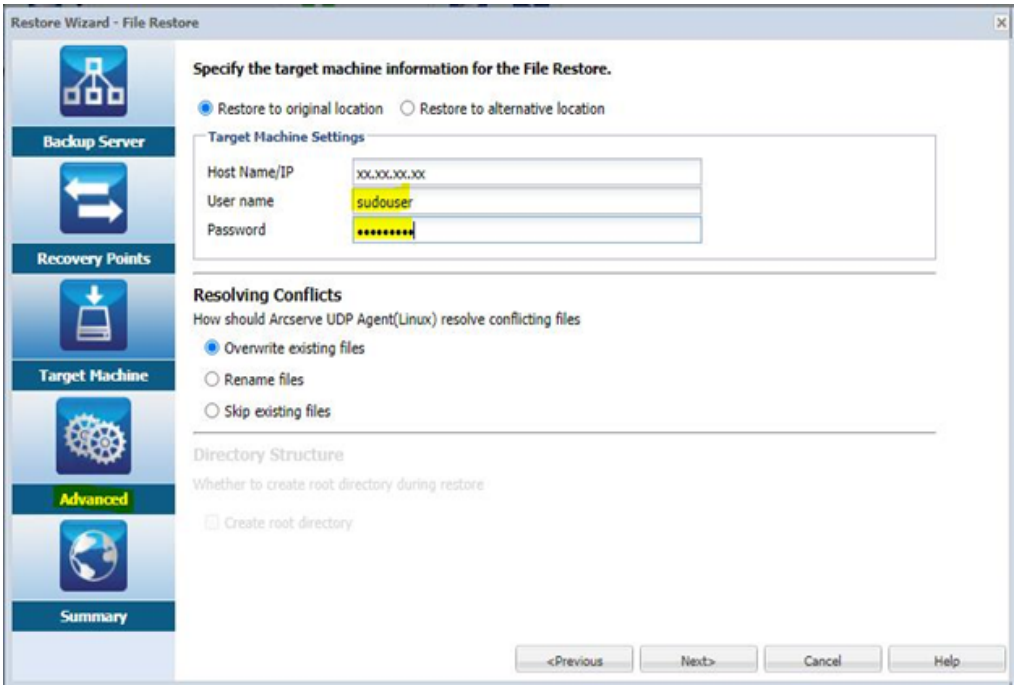
   udplinux ALL=(ALL) NOPASSWD: /home/udplinux/.d2drestorefile/d2dtar.64,/tmp/d2dtar.64

Esecuzione del processo di ripristino dei file utilizzando le credenziali dell'utente sudo del nodo di destinazione

In questa sezione vengono fornite informazioni su come eseguire il processo di ripristino dei file utilizzando le credenziali utente sudo.

Effettuare le operazioni seguenti:

1. Aprire la procedura guidata di ripristino dei file, quindi inserire i dettagli necessari.
2. Nella pagina Avanzate, in Impostazioni computer di destinazione, fornire le credenziali dell'utente sudo, quindi eseguire il processo di ripristino del file.



Il bit SUID è disattivato per il file binario d2dtar nel nodo di destinazione durante l'esecuzione del processo di ripristino del file.

Chapter 5: Risoluzione dei problemi

La presente sezione descrive i seguenti argomenti:

Mancata installazione dell'Agente Arcserve UDP (Linux) sui server supportati 407

Errore di timeout dell'operazione visualizzato dall'Agente Arcserve UDP (Linux) 409

Il backup dell'agente Arcserve UDP per Linux potrebbe non riuscire quando si passa dal backup senza agente al backup basato sull'agente 410

Errore dei processi pianificati in caso di modifica dell'ora di sistema su un valore precedente all'ora corrente 411

Mancato montaggio dell'Agente Arcserve UDP (Linux) sulle periferiche Linux Software RAID 412

Errore di download e distribuzione dei driver Ubuntu aggiornati su SLES 11 e RHEL 6 da parte di Agente Arcserve UDP (Linux) 413

Se avviato mediante Live CD, il computer paravirtuale (PVM) visualizza una schermata nera nella finestra del client Virtual Network Computing (VNC). 414

Errore di raccolta delle informazioni di ripristino bare metal durante il processo di backup o errore di creazione del layout del disco durante il processo di ripristino bare metal 416

Errore del processo di backup su RHEL7.0 come server di backup Linux e RPS su Windows Server 2019 417

Controllo della sequenza di avvio del disco dopo un ripristino bare metal su Oracle VM Server 418

Ripristino della versione precedente del server di backup 420

Backup delle istanze Debian 9.X EC2 in AWS Cloud 421

Errore di avvio del nodo di destinazione dopo l'esecuzione del processo di ripristino bare metal di migrazione per i nodi Debian 10.8 e 10.10 422

Il computer virtuale produce un errore di avvio per il processo IVM/AR al server ESXi 423

Il Computer virtuale non si avvia quando si utilizza la scheda di rete e1000e sul nodo ESXi 424

IVM su Hyper-V non viene avviato correttamente per i nodi di origine Debian 10.x 424

IVM su Hyper-V non viene avviato correttamente per il nodo di origine RHEL 8.0 424

I processi basati sull'agente Linux non riescono occasionalmente 426

I processi d2drestorevm e d2dverify non vengono completati correttamente su Oracle VM Server 427

Errore di avvio del computer virtuale ESXi dopo il ripristino bare metal da un computer fisico 428

Impossibile montare CIFS sul server o sul nodo di destinazione 429

Errore di ripristino a livello di file in un computer virtuale Linux basato su host causato da un file system non supportato 431

Impossibile ripristinare il volume di sistema di SUSE15 con file system XFS 431

Impossibile accedere all'URL di montaggio del punto di ripristino condiviso da WebDAV 432

Errore di distribuzione dei driver Ubuntu mediante il comando d2dupgradetool in Ubuntu20.04 LBS 432

Mancata installazione dell'Agente Arcserve UDP (Linux) sui server supportati

Valido su CentOS 6.x, Red Hat Enterprise Linux (RHEL) 6.x, Suse Linux Enterprise Server (SLES) 11 SP3/SP4 e server Oracle Linux 6.x

Sintomo

Quando si installa l'Agente Arcserve UDP (Linux), l'installazione non riesce con i messaggi di avviso di Linux seguenti:

```
mkisofs                Treate Live CD image

mount.nfs             Montaggio del file system di con-
divisione NFS

come destinazione di backup e origine di ripristino

mount.cifs             Montaggio del file system di con-
divisione CIFS come destinazione di backup e origine di ripri-
stino

I seguenti processi devono essere in esecuzione

Processi inattivi                              Funzione inte-
ressata

rpc.statd               La funzionalità di blocco del file
NFS non è funzionante
```

Soluzione

All'inizio dell'installazione, l'Agente Arcserve UDP (Linux) verifica se il sistema operativo Linux soddisfa i requisiti del server di backup. Se il sistema operativo Linux non soddisfa i requisiti minimi, l'Agente Arcserve UDP (Linux) visualizza un messaggio di avviso per informare l'utente del problema. Il messaggio include l'elenco di tutti i pacchetti richiesti per il server di backup.

Per risolvere questo problema di installazione dell'Agente Arcserve UDP (Linux), eseguire i passaggi seguenti:

1. Installare i pacchetti seguenti mediante il comando *yum:*
   - genisoimage
   - nfs-utils
   - cifs-utils
2. Eseguire i due comandi seguenti:

   ```
   service rpcbind start
   ```

```
service nfs start
```

3. Eseguire il comando seguente per verificare se *rpc.statd* è in esecuzione:

   ```
   ps -ef|grep rpc.statd
   ```

4. Reinstallare l'Agente Arcserve UDP (Linux).

   L'Agente Arcserve UDP (Linux) viene installato correttamente.

Errore di timeout dell'operazione visualizzato dall'Agente Arcserve UDP (Linux)

Valido su CentOS 6.x, Red Hat Enterprise Linux (RHEL) 6.x, Suse Linux Enterprise Server (SLES) 11 SP3/SP4 e server Oracle Linux 6.x

Sintomo

Viene visualizzato il messaggio seguente:

Timeout dell'operazione. È stato superato il tempo di completamento massimo per l'operazione. Riprovare.

Questo messaggio viene visualizzato frequentemente durante il ripristino a livello di file e se si accede a punti di ripristino contenenti più di 1000 punti di ripristino incrementali.

Soluzione

Il valore predefinito di timeout è pari a 3 minuti. È possibile risolvere questo problema aumentando il valore di timeout.

Per aumentare il valore di timeout, effettuare le operazioni seguenti:

1. Accedere al server di backup come un utente root.
2. Aggiungere la seguente variabile di ambiente di sistema:

   `D2D_WEBSVR_TIMEOUT`

   Il valore della variabile di ambiente corrisponde a un numero. Tale numero deve essere maggiore di 3. L'unità del valore è espressa in minuti.
3. Riavviare il server di backup.

   Il valore di timeout viene aumentato correttamente.

Il backup dell'agente Arcserve UDP per Linux potrebbe non riuscire quando si passa dal backup senza agente al backup basato sull'agente

Sintomo

Se è già stato eseguito il backup del computer virtuale Linux utilizzando il backup senza agente di UDP (mediante il proxy Windows) e si passa al backup basato sull'agente UDP (Linux), il processo di backup potrebbe non riuscire.

Soluzione

Per risolvere il problema, prima di passare dal backup senza agente al backup basato sull'agente, procedere come segue:

1. Aprire il computer virtuale Linux di destinazione, accedere alla cartella ***/tmp*** o al percorso configurato come directory di lavoro.
2. Verificare l'esistenza del file *checkmachine.output.txt*. Se il file esiste, eliminarlo.
3. Eseguire nuovamente il processo di backup di Linux.

Il backup di Linux è stato eseguito correttamente.

Errore dei processi pianificati in caso di modifica dell'ora di sistema su un valore precedente all'ora corrente

Valido su CentOS 6.x, Red Hat Enterprise Linux (RHEL) 6.x, Suse Linux Enterprise Server (SLES) 11 SP3/SP4 e server Oracle Linux 6.x

Sintomo

Se l'ora di sistema viene impostata su un valore precedente all'ora corrente, tale modifica viene applicata a tutti i processi pianificati. Si verifica un errore di esecuzione dei processi pianificati in seguito all'impostazione dell'ora di sistema su un orario precedente all'ora corrente.

Soluzione

Dopo avere modificato l'ora di sistema, riavviare il servizio BACKUP.

Eseguire le operazioni seguenti per riavviare il servizio BACKUP:

1. Accedere al server di backup come utente root.
2. Accedere alla cartella bin:

   ```
   /opt/Arcserve/d2dserver/bin/
   ```

3. Riavviare il server di backup utilizzando il comando seguente:

   ```
   d2dserver restart
   ```

   Il server di backup viene riavviato.

   Tutti i processi pianificati vengono eseguiti in base alla pianificazione.

Mancato montaggio dell'Agente Arcserve UDP (Linux) sulle periferiche Linux Software RAID

Valido su CentOS 6.x, Red Hat Enterprise Linux (RHEL) 6.x, Suse Linux Enterprise Server (SLES) 11 SP3/SP4 e server Oracle Linux 6.x

Sintomo

Si verifica un errore di montaggio delle periferiche Linux Software RAID in seguito al riavvio del computer di destinazione.

Soluzione

Per risolvere questo problema, riavviare il computer di destinazione.

Errore di download e distribuzione dei driver Ubuntu aggiornati su SLES 11 e RHEL 6 da parte di Agente Arcserve UDP (Linux)

Valido per alcune versioni obsolete di SUSE Linux Enterprise Server (SLES) 11 e Red Hat Enterprise Linux (RHEL) 6

Sintomo

Quando desidera eseguire il backup del nodo Ubuntu con la versione del kernel aggiornata, il processo di backup produce un errore e il messaggio del registro attività indica un errore di download e distribuzione dei driver Ubuntu.

Soluzione

Aggiornare i pacchetti di sistema e verificare che curl o wget dispongano della versione più recente.

Effettuare le operazioni seguenti:

1. Riavviare il computer di destinazione.
2. Eseguire il seguente comando:

   Su SUSE: zypper update wget curl

   Su RHEL: yum update wget curl
3. Eseguire nuovamente il processo di backup non riuscito sul nodo Ubuntu.

Il driver Ubuntu è stato aggiornato correttamente.

Se avviato mediante Live CD, il computer paravirtuale (PVM) visualizza una schermata nera nella finestra del client Virtual Network Computing (VNC).

Valido per computer paravirtuali (PVM) su Oracle VM Server.

Sintomo

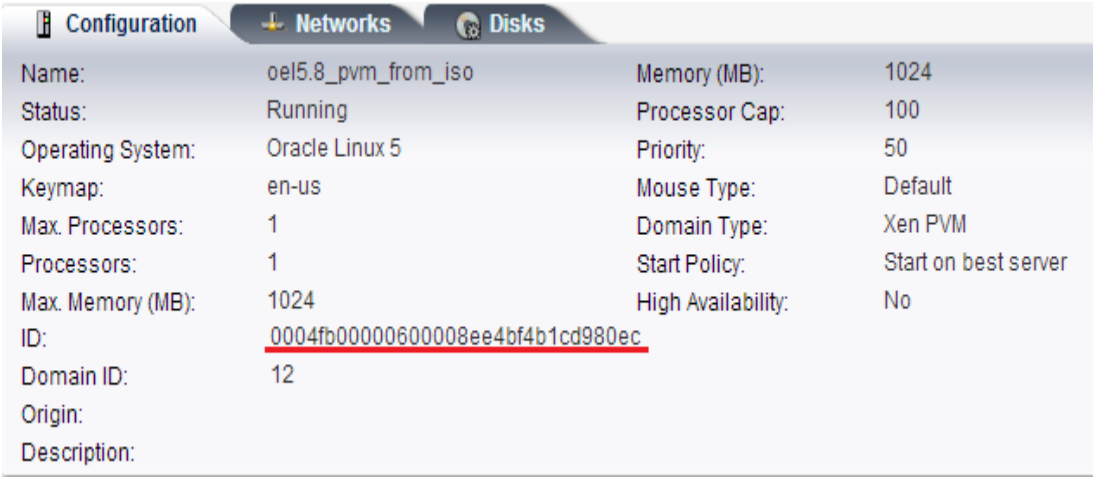
Quando si procede all'avvio del computer paravirtuale (PVM) su Oracle VM Server mediante Live CD, viene visualizzata una schermata nera nella finestra del client VNC.

Soluzione

Per risolvere il problema, accedere alla console Live CD dal backend.

Effettuare le operazioni seguenti:

1. Avviare il computer virtuale mediante Live CD.
2. Annotare l'ID del computer virtuale disponibile in Oracle VM Manager.



3. Mediante Secure Shell (SSH), accedere al server Oracle VM su cui il computer virtuale è in esecuzione.
4. Eseguire il comando *xm console $ID* come illustrato a continuazione:

```
[root@                ~]# xm console 0004fb00000600008ee4bf4b1cd980ec
```

5. (Facoltativo) Quando richiesto, premere Invio per confermare l'operazione.
6. Live CD avvierà e visualizzerà la console del computer paravirtuale Xen.
7. Configurare la rete.
8. Uscire dalla console utilizzando i comandi ctrl+] oppure ctrl+5.

Il problema verrà così risolto.

Errore di raccolta delle informazioni di ripristino bare metal durante il processo di backup o errore di creazione del layout del disco durante il processo di ripristino bare metal

Valido su Oracle VM Server per HVM con volume LVM

Sintomo

Durante il processo di backup HVM con volumi LVM su Oracle VM Server, le informazioni relative al ripristino bare metal non vengono raccolte. Inoltre, durante il ripristino bare metal per un computer HVM con volumi LVM su Oracle VM Server, il layout del disco non viene creato.

Soluzione

Per risolvere il problema, disabilitare i driver paravirtualizzati del nodo di origine di backup.

Effettuare le operazioni seguenti:

1. Aprire la finestra del prompt dei comandi sul nodo di origine di backup e immettere il seguente comando:

   ```
   sfdisk –s
   ```

2. Verificare se lo stesso disco viene visualizzato due volte nell'elenco dei risultati.

   Ad esempio, xvdX e hdX sono lo stesso disco. Verificare se entrambi i dischi compaiono nei risultati.

3. In tal caso, procedere come segue:

a. Aggiungere la seguente linea al file */etc/modprobe.d/blacklist* sul nodo di origine di backup:

   ```
   blacklist xen_vbd
   ```

b. Riavviare il nodo di origine di backup, quindi eseguire nuovamente il processo di backup.

   Il processo di backup viene eseguito.

4. In caso contrario, contattare il Supporto tecnico di Arcserve.

   Il problema verrà così risolto.

Errore del processo di backup su RHEL7.0 come server di backup Linux e RPS su Windows Server 2019

Sintomo

I processi di backup non vengono eseguiti correttamente quando si installa RPS su Windows Server 2019 e RHEL7.0 sull'agente Linux, il quale utilizza il protocollo SMB1 durante il montaggio di CIFS e che è disattivato in Windows Server 2019.

Soluzione

Per eseguire correttamente il processo di backup, è necessario abilitare il protocollo SMB1 su Windows Server 2019.

Effettuare le operazioni seguenti:

1. Per abilitare il protocollo SMB1 su Windows Server 2019, eseguire il comando seguente:

   Enable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

2. Riavviare il server.

Il processo di backup viene eseguito correttamente.

Controllo della sequenza di avvio del disco dopo un ripristino bare metal su Oracle VM Server

Valido per Oracle VM Server

Sintomo

Quando viene eseguito il ripristino bare metal su un nodo di destinazione collocato su Oracle VM Server, il registro attività restituisce il seguente avviso:

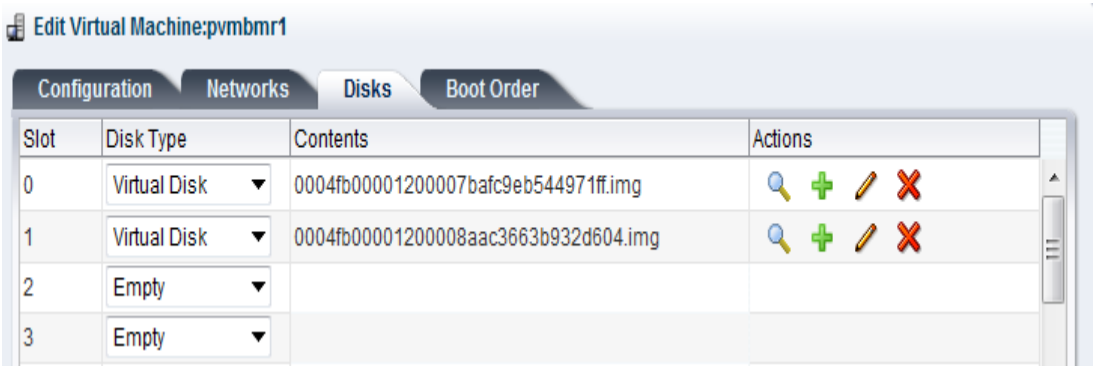
```
Il volume di avvio è stato ripristinato sul disco /dev/xxx.
Modificare la sequenza di avvio del disco nel BIOS per ese-
guire l'avvio da /dev/xxx.
```

Soluzione

Per evitare questo problema, invertire la sequenza di avvio del disco del nodo di destinazione del ripristino bare metal.

Effettuare le operazioni seguenti:

1. Modificare il nodo di destinazione del ripristino bare metal da Oracle VM Manager, quindi fare clic sulla scheda Disks.

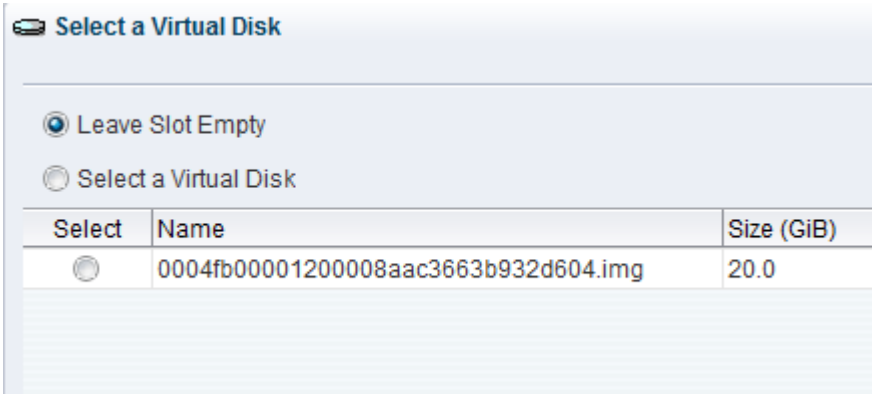


2. Selezionare Slot N come disco di avvio.
3. Annotare il nome del disco e il numero di slot N.

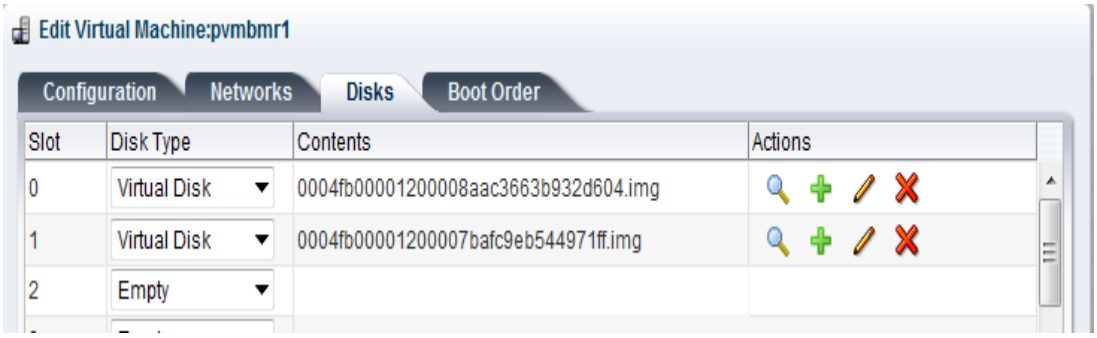
   Tali dati saranno necessari nelle fasi successive.

4. Dalla colonna Actions, selezionare il pulsante Virtual Machine Disk.

5. Selezionare l'opzione Leave Slot Empty e fare clic su Save.



6. Selezionare Slot 0 Disk e annotare il nome del disco.
7. Dalla colonna Actions, selezionare il pulsante Virtual Machine Disk.
8. Selezionare l'opzione Leave Slot Empty e fare clic su Save.
9. Allegare l'immagine del disco di avvio selezionato allo Slot 0 e riassegnare allo Slot N l'immagine originariamente assegnata allo Slot 0.



10. Avviare il nodo di destinazione del ripristino bare metal.

    La sequenza di avvio del disco verrà modificata con successo.

Ripristino della versione precedente del server di backup

Valido su Red Hat Enterprise Linux (RHEL) 6.x e CentOS 6.x per il server di backup

Sintomo

Durante un tentativo di aggiornamento del server di backup si è verificato un errore. Il server di backup non funziona nel modo previsto. Si desidera ripristinare la versione precedente del server di backup.

Soluzione

Quando si esegue l'aggiornamento a una nuova versione, il server di backup crea una cartella di backup contenente tutti i file di configurazione e i file di database precedenti provenienti dalla versione installata in precedenza. La cartella si trova nella posizione seguente:

```
/opt/Arcserve/d2dserver.bak
```

Effettuare le operazioni seguenti:

1. Disinstallare il server di backup esistente utilizzando il comando seguente:

   ```
   /opt/Arcserve/d2dserver/bin/d2duninstall
   ```

2. Installare la versione precedentemente installata del server di backup.
3. Interrompere il server di backup utilizzando il comando seguente:

   ```
   /opt/Arcserve/d2dserver/bin/d2dserver stop
   ```

4. Copiare i file di configurazione e i file di database precedenti nella cartella d2dserver utilizzando il comando seguente:

   ```
   cp –Rpf /opt/Arcserve/d2dserver.bak/* /opt/Arcserve/d2dserver/
   ```

5. Avviare il server di backup utilizzando il comando seguente:

   ```
   /opt/Arcserve/d2dserver/bin/d2dserver start
   ```

   La versione precedentemente installata del server di backup è stata ripristinata correttamente.

Backup delle istanze Debian 9.X EC2 in AWS Cloud

Sintomo

Quando viene eseguito un backup per le istanze Debian 9.X EC2 in AWS Cloud, il processo di backup non riesce e non vengono visualizzati messaggi di errore specifici.

Soluzione

Quando vengono create e aggiunte istanze Debian 9.X in AWS Cloud per la protezione, l'assenza dei moduli Perl potrebbe comportare l'insorgere di un errore. Per risolvere il problema, installare i pacchetti mediante i comandi seguenti:

sudo apt update

sudo apt install apt-file

sudo apt-file update

Errore di avvio del nodo di destinazione dopo l'esecuzione del processo di ripristino bare metal di migrazione per i nodi Debian 10.8 e 10.10

Sintomo

Quando il processo di ripristino bare metal di migrazione viene eseguito con un computer istantaneo virtuale, il nodo di destinazione non viene avviato e viene visualizzato il seguente messaggio di errore, quindi viene eseguito l'accesso alla shell di ripristino *initramfs*:

Errore di danneggiamento del filesystem root

Soluzione

Per risolvere il problema, procedere come segue:

1. Per controllare e riparare il volume di avvio, eseguire il seguente comando fsck:

   (initramfs) fsck -yf /dev/sdX

2. Per uscire dalla shell di ripristino *initramfs*, eseguire il seguente comando:

   (initramfs) exit

Il nodo di destinazione viene avviato correttamente.

Il computer virtuale produce un errore di avvio per il processo IVM/AR al server ESXi

Sintomo

Quando viene eseguito un processo di computer virtuale IVM/AR al server ESXi utilizzando la sessione di backup senza agente e il nodo di origine è il server ESXi, il computer virtuale non si avvia correttamente nel sistema.

Soluzione

Nel computer virtuale potrebbe essere necessario l'inserimento del driver. È possibile impostare una variabile di ambiente per l'abilitazione.

Effettuare le operazioni seguenti:

1. Accedere al server di backup come utente root.
2. Aprire il seguente file .env di server:

   ```
   /opt/Arcserve/d2dserver/configfiles/server.env
   ```

3. Aggiornare il seguente parametro nel file server.env e salvarlo:

   ```
   esportare HBBU_VM_RESTORE_DISABLE=1
   ```

4. Riavviare il server di backup utilizzando il comando seguente:

   ```
   /opt/Arcserve/d2dserver/bin/d2dserver restart
   ```

Il Computer virtuale non si avvia quando si utilizza la scheda di rete e1000e sul nodo ESXi

Sintomo

Quando viene eseguito un processo di computer virtuale IVM mediante la scheda di rete e1000e sul nodo ESXi, il computer virtuale potrebbe non avviarsi correttamente nel sistema.

Soluzione

È possibile eseguire un processo del computer virtuale IVM utilizzando le altre schede di rete disponibili, ma non con e1000e NIC.

IVM su Hyper-V non viene avviato correttamente per i nodi di origine Debian 10.x

Sintomo

Se si seleziona l'opzione **Server con GUI** durante l'installazione di uno qualsiasi di questi nodi di origine, ad esempio Debian 10.x su ESXI e si esegue il processo da IVM su Hyper-V, l'avvio del nodo di destinazione generato su Hyper-V non viene eseguito correttamente. Sebbene i registri mostrino l'esito positivo del processo IVM, questo non viene avviato correttamente.

Soluzione

Una volta che il nodo di destinazione è stato creato sulla piattaforma Hyper-V e lo stato / i registri del processo da "IVM a Hyper-V" mostra il completamento corretto, riavviare il nodo di destinazione manualmente. Dopo il riavvio, il nodo di destinazione apre la GUI prevista.

IVM su Hyper-V non viene avviato correttamente per il nodo di origine RHEL 8.0

Sintomo

Se si seleziona l'opzione **Server con GUI** durante l'installazione di RHEL 8.0 su ESXI e si esegue il processo IVM su Hyper-V, il nodo di destinazione generato su Hyper-V non viene avviato correttamente. Sebbene i registri mostrino l'esito positivo del processo IVM, l'avvio non riesce.

Nota: questo problema è relativo a Redhat 8.0 su piattaforma Hyper-V. Per ulteriori informazioni su questo problema di Redhat 8.0, consultare il portale Redhat.

A differenza della serie RHEL 7.x, quando si seleziona l'opzione **Server con GUI** per l'installazione di RHEL 8.0, i seguenti driver non vengono installati per impostazione predefinita:

- xorg-x11-drv-fbdev
- xorg-x11-drv-vesa
- xorg-x11-drv-vmware

Soluzione 1

Come soluzione alternativa, attenersi alle seguenti istruzioni:

1. Dopo aver installato il nodo di origine RHEL 8.0 su ESXI, installare i seguenti pacchetti sul nodo:

   yum install xorg-x11-drv-fbdev xorg-x11-drv-vesa xorg-x11-drv-vmware -y
2. Eseguire un backup.
3. Utilizzare la stessa sessione di backup da RPS ed eseguire il processo IVM su Hyper-V.

Soluzione 2

Utilizzare questa soluzione alternativa se il backup non è stato eseguito dopo aver installato i seguenti driver:

- xorg-x11-drv-fbdev
- xorg-x11-drv-vesa
- xorg-x11-drv-vmware

Come soluzione alternativa, attenersi alle seguenti istruzioni:

1. Dopo aver eseguito IVM su Hyper-V per RHEL 8.0 presente su ESXI o dopo aver installato RHEL 8.0 su Hyper-V, dalla scheda **Rete** di Hyper-V, ottenere l'indirizzo IP.

   Nota: in questo stato, la GUI non è disponibile sul nodo IVM.
2. Connettere il computer virtuale tramite l'applicazione ssh (ad esempio putty) utilizzando l'indirizzo IP.
3. Installare i seguenti pacchetti sul nodo.

   yum install xorg-x11-drv-fbdev xorg-x11-drv-vesa xorg-x11-drv-vmware -y
4. Riavviare il nodo.

I processi basati sull'agente Linux non riescono occasionalmente

Sintomo

Quando vengono aggiunti più di 200 nodi Linux a un piano, in lacuni casi i processi basati sull'agente Linux non riescono e si verifica il seguente errore:

Impossibile connettersi al server delle licenze.

Soluzione

Per risolvere il problema, ridurre il numero di processi simultanei. Ad esempio, se il numero di processi simultanei è impostato su 48, ridurlo a 30 e verificare che l'errore sia stato risolto. L'impostazione dei processi simultanei dipende dalle risorse ambientali, quali I/O del disco, memoria, CPU sul server della console UDP e LBS. È necessario impostare il numero di processi simultanei in base a ciascun ambiente. Inoltre, potrebbe essere necessario aggiungere più nodi LBS per dividere i piani e ridurre il carico.

I processi d2drestorevm e d2dverify non vengono completati correttamente su Oracle VM Server

Valido per Oracle VM Server

Sintomo

All'avvio dei processi d2drestorevm e d2dverify su Oracle VM Server, tutti i processi non vengono completati correttamente. Viene visualizzato il seguente messaggio di errore nel registro attività:

```
Impossibile importare l'immagine ISO all'hypervisor. Per ulteriori informazioni, consultare la console di gestione dell'hypervisor o il registro di debug.
```

Soluzione

Verificare se Oracle VM Server si è bloccato.

Effettuare le operazioni seguenti:

1. Accedere alla console di Oracle VM Server e passare alla scheda Processi.
2. Trovare tutti i processi con stato In corso..., quindi interromperli.
3. Avviare nuovamente il processo d2drestorevm o d2dverify.

   Se il processo d2drestorevm o d2dverify non riesce nuovamente e viene visualizzato lo stesso messaggio di errore, accedere alla console Oracle VM Server e verificare l'eventuale presenza di processi con stato In corso... Se sono presenti processi con stato In corso..., riavviare Oracle VM Server.

   I processi d2drestorevm e d2dverify vengono eseguiti correttamente.

Errore di avvio del computer virtuale ESXi dopo il ripristino bare metal da un computer fisico

Sintomo

Viene eseguito un ripristino bare metal mediante i punti di ripristino di un computer fisico su un computer virtuale ESXi. Il computer fisico utilizza un BIOS meno recente. Il ripristino bare metal viene completato correttamente ma il computer virtuale ESXi non si avvia correttamente.

Soluzione

Modificare il tipo di controller SCSI del computer virtuale ESXi di destinazione e inoltrare nuovamente il processo di ripristino bare metal.

Effettuare le operazioni seguenti:

1. Accedere al server ESX.
2. Fare clic con il tasto destro del mouse sul computer virtuale ESXi di destinazione e selezionare Modifica impostazioni.
3. Dalla scheda Hardware, selezionare Controller SCSI 0 e fare clic sul pulsante Change Type (Modifica tipo).

   Viene visualizzata la finestra di dialogo Change SCSI Controller Type (Modifica tipo di controller SCSI).
4. Selezionare LSI Logic SAS e salvare le impostazioni.
5. Inoltrare un processo di ripristino bare metal al computer virtuale.

   Il computer virtuale si avvia correttamente dopo il processo di ripristino bare metal.

Impossibile montare CIFS sul server o sul nodo di destinazione

Sintomo

Non è possibile montare CIFS sul server o sul nodo di destinazione quando si tenta di eseguire il backup o il ripristino mediante CIFS.

Soluzione

È necessario soddisfare alcuni requisiti durante il montaggio di CIFS su un computer Linux.

Effettuare le operazioni seguenti:

1. Utilizzare il comando di montaggio sul server o sul nodo di destinazione per verificare l'errore.
2. Verificare che durante l'utilizzo di un percorso condiviso esportato da sistemi diversi da Windows, le lettere maiuscole/minuscole del percorso condiviso corrispondano a quelle del percorso originale.
3. Se il comando di montaggio restituisce un errore, verificare che l'ora sul server o sul nodo di destinazione sia sincronizzata con il server CIFS.
4. Se non si riesce a individuare l'errore, aggiungere alcuni opzioni al comando di montaggio e riprovare.

   Ad esempio, aggiungere "sec=ntlm" quando viene restituito l'errore di autorizzazione negata.

5. Quando si esegue la diagnosi dell'errore, procedere come segue:

   Se non è possibile montare il modulo CIFS sul server

   1. Aprire il file server.env dal percorso seguente:

      /opt/Arcserve/d2dserver/configfiles/server.env

   2. Aggiungere tutte le opzioni al file mediante il comando seguente:

      export D2D_MOUNTOPTION=<options>

   c. Salvare il file e riavviare il servizio.

   Se non è possibile montare il modulo CIFS sul nodo di destinazione

   1. Aprire il file .bashrc dal percorso della directory principale dell'utente.

      Esempio: il percorso di un utente è */home/user/* e quello della directory principale è */root/*.

2. Aggiungere tutte le opzioni al file mediante il comando seguente:

   export D2D_MOUNTOPTION=<options>

c. Salvare il file.

   Nota: Il file .bashrc è consigliato in questo esempio, ma è possibile modificare anche altri file, come /ect/profile, /etc/bashrc, e così via.

6. Verificare che durante l'utilizzo di un percorso condiviso esportato da sistemi diversi da Windows, le lettere maiuscole/minuscole del percorso condiviso corrispondano a quelle del percorso originale.

Errore di ripristino a livello di file in un computer virtuale Linux basato su host causato da un file system non supportato

Sintomo

Quando viene eseguito un ripristino a livello di file per un computer virtuale Linux basato su host, la procedura guidata di ripristino visualizza il seguente messaggio di errore:

Non supportato: file system reiserfs

L'errore è dovuto al ripristino di un file system non supportato.

Soluzione

È possibile ripristinare il computer virtuale Linux basato su host utilizzando uno dei seguenti metodi:

- Utilizzare il sistema Live CD dell'Agente Arcserve UDP (Linux) per il ripristino a livello di file, in quanto il Live CD supporta tutti i tipi di file system. Si tratta di una soluzione conveniente ma temporanea. È possibile eseguire il ripristino tramite un sistema Live CD se non viene eseguito il ripristino frequente del nodo.
- Un altro metodo permanente consiste nell'installazione obbligatoria del file system corretto per il supporto di reiserfs o per l'attivazione del driver corrispondente già installato sul server di backup.

Impossibile ripristinare il volume di sistema di SUSE15 con file system XFS

Sintomo

Quando viene eseguito un processo di ripristino tramite il punto di ripristino SUSE15 con file system XFS, il processo di ripristino non riesce poiché il volume di sistema non è installato e viene visualizzato il seguente messaggio di avviso nel registro attività: *Impossibile montare il volume di sistema. Il sistema potrebbe non riuscire ad avviarsi dopo il ripristino.*

Soluzione

Creare un Live CD CentOS 7.5 e utilizzare il Live CD per eseguire il ripristino bare metal/istantaneo BMR.sudo apt apt-file di installazione

Impossibile accedere all'URL di montaggio del punto di ripristino condiviso da WebDAV

Sintomo

Durante l'esecuzione del montaggio del punto di ripristino condiviso da WebDAV a cui accedono più utenti mediante lo stesso server di backup Linux, soltanto l'accesso al primo URL avrà esito positivo, mentre l'accesso agli altri produrrà un errore.
Questo errore si verifica perché Arcserve non supporta l'accesso agli URL condivisi da più utenti dallo stesso browser.

Soluzione

Utilizzare browser diversi per accedere agli URL, oppure cancellare i cookie e riprovare.

Errore di distribuzione dei driver Ubuntu mediante il comando d2dupgradetool in Ubuntu20.04 LBS

Sintomo

Durante il download dell'archivio dei driver e dei file di firma, il comando curl genera il seguente errore:

cURL error 35: error:1414D172:SSL routines:tls12_check_peer_sigalg:wrong signature type

Soluzione

Aggiornare OpenSSL 1.1.1f a OpenSSL 1.1.1g in Ubuntu20.04 LBS.