

Oracle® DIVArchive

Guida per la sicurezza

Release 7.3

E70870-01

Dicembre 2015

Oracle® DIVArchive

Guida per la sicurezza

E70870-01

copyright © 2015, Oracle e/o relative consociate. Tutti i diritti riservati.

Il software e la relativa documentazione vengono distribuiti sulla base di specifiche condizioni di licenza che prevedono restrizioni relative all'uso e alla divulgazione e sono inoltre protetti dalle leggi vigenti sulla proprietà intellettuale. Ad eccezione di quanto espressamente consentito dal contratto di licenza o dalle disposizioni di legge, nessuna parte può essere utilizzata, copiata, riprodotta, tradotta, diffusa, modificata, concessa in licenza, trasmessa, distribuita, presentata, eseguita, pubblicata o visualizzata in alcuna forma o con alcun mezzo. La decodificazione, il disassemblaggio o la decompilazione del software sono vietati, salvo che per garantire l'interoperabilità nei casi espressamente previsti dalla legge.

Le informazioni contenute nella presente documentazione potranno essere soggette a modifiche senza preavviso. Non si garantisce che la presente documentazione sia priva di errori. Qualora l'utente riscontrasse dei problemi, è pregato di segnalarli per iscritto a Oracle.

Qualora il software o la relativa documentazione vengano forniti al Governo degli Stati Uniti o a chiunque li abbia in licenza per conto del Governo degli Stati Uniti, sarà applicabile la clausola riportata di seguito.

U.S. GOVERNMENT END USERS: Oracle Programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Il presente software o hardware è stato sviluppato per un uso generico in varie applicazioni di gestione delle informazioni. Non è stato sviluppato né concepito per l'uso in campi intrinsecamente pericolosi, incluse le applicazioni che implicano un rischio di lesioni personali. Qualora il software o l'hardware venga utilizzato per impieghi pericolosi, è responsabilità dell'utente adottare tutte le necessarie misure di emergenza, backup e di altro tipo per garantirne la massima sicurezza di utilizzo. Oracle Corporation e le sue consociate declinano ogni responsabilità per eventuali danni causati dall'uso del software o dell'hardware per impieghi pericolosi.

Oracle e Java sono marchi registrati di Oracle e/o delle relative consociate. Altri nomi possono essere marchi dei rispettivi proprietari.

Intel e Intel Xeon sono marchi o marchi registrati di Intel Corporation. Tutti i marchi SPARC sono utilizzati in base alla relativa licenza e sono marchi o marchi registrati di SPARC International, Inc. AMD, Opteron, il logo AMD e il logo AMD Opteron sono marchi o marchi registrati di Advanced Micro Devices. UNIX è un marchio registrato di The Open Group.

Il software o l'hardware e la documentazione possono includere informazioni su contenuti, prodotti e servizi di terze parti o collegamenti agli stessi. Oracle Corporation e le sue consociate declinano ogni responsabilità ed escludono espressamente qualsiasi tipo di garanzia relativa a contenuti, prodotti e servizi di terze parti se non diversamente regolato in uno specifico accordo in vigore tra l'utente e Oracle. Oracle Corporation e le sue consociate non potranno quindi essere ritenute responsabili per qualsiasi perdita, costo o danno causato dall'accesso a contenuti, prodotti o servizi di terze parti o dall'utilizzo degli stessi se non diversamente regolato in uno specifico accordo in vigore tra l'utente e Oracle.

Indice

Prefazione	5
Destinatari	5
Accesso facilitato alla documentazione	5
1. Panoramica	7
1.1. Panoramica del prodotto	7
1.1.1. DIVArchive Manager	7
1.1.2. DIVArchive Actor	7
1.1.3. DIVArchive Robot Manager	7
1.1.4. DIVArchive Backup Service	8
1.1.5. Oracle Avid Connectivity	8
1.1.6. DIVArchive Drop Folder Monitor	8
1.1.7. DIVArchive SNMP	9
1.1.8. DIVArchive SPM	9
1.1.9. DIVArchive Migrate Service	9
1.1.10. DIVArchive VACP	9
1.1.11. Interfaccia GUI di controllo di DIVArchive	9
1.1.12. Utility Configuration di DIVArchive	9
1.1.13. Gateway di accesso DIVArchive	9
1.1.14. DIVArchive LynxLocalDelete	10
1.2. Principi di sicurezza generali	10
1.2.1. Mantenere aggiornato il software	10
1.2.2. Limitare l'accesso di rete ai servizi critici	10
1.2.3. Eseguire i servizi come utente DIVA e attenersi al principio di privilegio minimo, ove possibile	10
1.2.4. Monitorare l'attività del sistema	11
1.2.5. Mantenersi aggiornati sulle ultime informazioni sulla sicurezza	11
2. Installazione sicura	13
2.1. Informazioni sull'ambiente	13
2.1.1. Quali risorse è necessario proteggere?	13
2.1.1.1. Disco dati primario	13
2.1.1.2. Dischi di database, di metadati e di backup	13
2.1.1.3. Nastri DIVArchive	13

- 2.1.1.4. Esportazione dei metadati del nastro 14
- 2.1.1.5. File e impostazioni di configurazione 14
- 2.1.2. Da chi è necessario proteggere le risorse? 14
- 2.1.3. Cosa accade in caso di mancata protezione delle risorse strategiche? 14
- 2.2. Topologie di distribuzione raccomandate 14
 - 2.2.1. Rete di metadati distinta 14
 - 2.2.2. Suddivisione in zone FC 15
 - 2.2.3. Protezione dell'accesso alla configurazione dei dischi SAN 15
 - 2.2.4. Installazione del pacchetto DIVArchive 15
 - 2.2.5. Sicurezza dei nastri DIVArchive 15
 - 2.2.6. Backup 15
- 2.3. Configurazione post-installazione 15

- 3. Funzioni di sicurezza 17**
 - 3.1. Modello di sicurezza 17
 - 3.2. Autenticazione 17
 - 3.3. Controllo dell'accesso 17

- A. Lista di controllo per la distribuzione sicura 19**

Prefazione

La Guida per la sicurezza di DIVArchive di Oracle include informazioni relative al prodotto DIVArchive e spiegazioni dei principi generali di sicurezza delle applicazioni.

Destinatari

Il presente manuale è rivolto a chiunque sia coinvolto nell'uso delle funzioni di sicurezza nonché nell'installazione e configurazione sicure di DIVArchive.

Accesso facilitato alla documentazione

Per informazioni sull'impegno di Oracle riguardo l'accesso facilitato, visitare il sito Web Oracle Accessibility Program su <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Accesso al supporto Oracle

I clienti Oracle che hanno acquistato l'assistenza, hanno accesso al supporto elettronico mediante My Oracle Support. Per informazioni, visitare <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> o <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> per i non utenti.

Capitolo 1. Panoramica

In questo capitolo viene fornita una panoramica del prodotto DIVArchive e vengono descritti i principi generali di sicurezza delle applicazioni.

1.1. Panoramica del prodotto

Oracle DIVArchive è un sistema di gestione dello storage del contenuto distribuito. DIVArchive è composto dai principali componenti elencati di seguito.

1.1.1. DIVArchive Manager

DIVArchive Manager è il componente principale di un sistema DIVArchive. Tutte le operazioni di archiviazione sono controllate e gestite da DIVArchive Manager. Le richieste di operazioni vengono inviate da applicazioni responsabili dell'avvio tramite l'interfaccia API del client DIVArchive. Sono inoltre disponibili per l'acquisto le opzioni principale e di backup di DIVArchive Manager. Per ulteriori informazioni sull'installazione di DIVArchive, consultare la libreria della documentazione per i clienti della release software 7.3 di DIVArchive all'indirizzo:

<https://docs.oracle.com/en/storage/#csm>

1.1.2. DIVArchive Actor

DIVArchive Actor consente di spostare i dati tra i dispositivi nel sistema di produzione. Supporta il trasferimento di dati tra molti tipi diversi di dispositivi e gestisce le operazioni di transcodifica con il software di transcodifica del flusso telematico (opzionale).

Tutte le operazioni di Actor vengono avviate e coordinate da DIVArchive Manager. È possibile configurare una o più istanze di Actor e controllarle tramite una singola istanza di DIVArchive Manager.

1.1.3. DIVArchive Robot Manager

Sebbene DIVArchive possa essere utilizzato per gestire solo lo storage su disco, è possibile spandere ulteriormente la capacità di storage aggiungendo una o più librerie a nastro. In questi casi il modulo DIVArchive Robot Manager fornisce un livello software intermedio che consente a DIVArchive Manager di interagire con molti tipi diversi di librerie a nastro. È

connesso a DIVArchive Manager tramite TCP/IP. DIVArchive Robot Manager si interfaccia con la libreria utilizzando un'interfaccia diretta alla libreria stessa (mediante SCSI nativa o SCSI su Fiber Channel) o una connessione Ethernet intermedia al software di controllo della libreria del produttore.

1.1.4. DIVArchive Backup Service

Per garantire l'affidabilità e il monitoraggio dei backup sia di Oracle Database che del database di metadati, è stato introdotto DIVArchive Backup Service.

Il componente DIVArchive Backup Service viene installato come parte integrante dell'installazione del sistema DIVArchive standard. In genere il componente viene installato sullo stesso server di DIVArchive Manager e Oracle Database. DIVArchive Backup Service consente la configurazione di backup programmati tramite il file di configurazione. DIVArchive Backup Service gestisce ed esegue il monitoraggio dell'intero processo di backup.

Nella presente release DIVArchive Backup include la possibilità di inviare messaggi di posta elettronica riguardo i problemi derivanti dal processo di backup dei file di Oracle Database e del database di metadati. Per utilizzare questa funzione, è necessario che DIVArchive sia configurato per la connessione a un provider di posta SMTP. Le notifiche tramite posta elettronica vengono configurate mediante la utility Configuration di DIVArchive, nella scheda di impostazioni del Manager.

Per ulteriori informazioni sull'installazione e la configurazione di DIVArchive Backup Service, consultare la libreria della documentazione per i clienti della release software 7.3 di DIVArchive all'indirizzo:

<https://docs.oracle.com/en/storage/#csm>

1.1.5. Oracle Avid Connectivity

Lo scopo di Avid Connectivity con DIVArchive consiste nel trasferire i dati dell'archiviazione da e in DIVArchive in formati video specifici e consentire l'archiviazione e il recupero di singole clip o di sequenze di clip. I componenti correlati ad AMC e TMC vengono installati durante l'installazione di DIVArchive principale. Per alcuni plugin per AMC e TMC è necessaria un'ulteriore installazione.

1.1.6. DIVArchive Drop Folder Monitor

DIVArchive Drop Folder Monitor (DFM) fornisce il monitoraggio automatico dei nuovi file creati in un massimo di 20 cartelle locali o cartelle FTP (o una combinazione di entrambe). Sono supportati uno o più file (in cartelle FTP) per ciascun oggetto DIVArchive. Quando viene identificato un nuovo file (o una nuova cartella FTP), DFM invia automaticamente una richiesta di archiviazione a DIVArchive per archiviare il nuovo file o le nuove cartelle. Una volta completata l'archiviazione, questi file vengono eliminati automaticamente dall'origine.

1.1.7. DIVArchive SNMP

L'agente DIVArchive Simple Network Management Protocol (SNMP) e Management Information Base (MIB) supporta il monitoraggio dello stato e dell'attività di DIVArchive e dei relativi sottosistemi tramite un'applicazione di monitoraggio di terze parti su protocollo SNMP.

1.1.8. DIVArchive SPM

DIVArchive Storage Plan Manager (SPM) fornisce migrazione e ciclo di vita automatici del materiale nell'archivio in base alle regole e ai criteri definiti nella configurazione di SPM.

Il componente SPM viene utilizzato anche per attivare l'eliminazione di materiale dagli array gestiti da SPM (in base ai watermark di spazio su disco).

1.1.9. DIVArchive Migrate Service

DIVArchive include un servizio di migrazione incorporato. Si tratta di un servizio interno (di DIVArchive) nuovo e separato che consente agli utenti di programmare ed eseguire processi per la migrazione di contenuto tra diversi supporti all'interno di un sistema DIVArchive. È possibile utilizzare l'interfaccia GUI di controllo o il client della riga di comando.

1.1.10. DIVArchive VACP

VACP (Video Archive Command Protocol) è un protocollo sviluppato da Harris Automation per l'interfaccia con un sistema di archiviazione. DIVArchive dispone della propria interfaccia API per la comunicazione con DIVArchive Manager, non compatibile con VACP.

1.1.11. Interfaccia GUI di controllo di DIVArchive

L'interfaccia GUI (Graphical User Interface) di controllo di DIVArchive consente di monitorare, controllare e supervisionare le operazioni in DIVArchive. È possibile che più interfacce GUI di DIVArchive siano in esecuzione e connesse allo stesso sistema DIVArchive nello stesso momento.

1.1.12. Utility Configuration di DIVArchive

La utility Configuration di DIVArchive viene utilizzata per configurare un sistema DIVArchive. Sebbene venga utilizzata principalmente per la configurazione di DIVArchive, dalla utility Configuration vengono eseguite anche alcune funzioni operative.

1.1.13. Gateway di accesso DIVArchive

Il gateway di accesso consente il funzionamento e l'interazione di più sistemi DIVArchive indipendenti da un singolo computer. Si tratta della soluzione globale per la distribuzione di contenuto. La replica dei file automatica per il mirroring dei siti offre un metodo facile e pulito per la distribuzione locale, il backup e il ripristino di emergenza con sicurezza,

controllo della larghezza di banda e verifica checksum. Le reti vengono monitorate e DIVAnet garantisce la consegna finale di contenuto.

1.1.14. DIVArchive LynxLocalDelete

LYNXLocalDelete è un servizio di monitoraggio delle funzioni di replica degli oggetti tra un sistema DIVArchive locale (ad esempio, LYNXlocal) e uno o più sistemi DIVArchive remoti (ad esempio, LYNXdr). Una volta completata la replica dell'oggetto nel sistema DIVArchive remoto, questo viene contrassegnato come idoneo per l'eliminazione dal sistema DIVArchive locale.

1.2. Principi di sicurezza generali

Nelle sezioni successive vengono descritti i principi fondamentali necessari per utilizzare in maniera sicura qualsiasi applicazione.

1.2.1. Mantenere aggiornato il software

Mantenere aggiornata la versione di DIVArchive in esecuzione. È possibile trovare versioni correnti del software da scaricare sul sito Oracle Software Delivery Cloud:

<https://edelivery.oracle.com/>

1.2.2. Limitare l'accesso di rete ai servizi critici

DIVArchive utilizza le seguenti porte TCP/IP:

- tcp/8500 viene utilizzata da DIVArchive Robot Manager
- tcp/9000 viene utilizzata da DIVArchive Manager
- tcp/9300 viene utilizzata da DIVArchive Backup Service
- tcp/9500 viene utilizzata da DIVArchive Access Gateway
- tcp/9900 viene utilizzata da DIVArchive Actor
- tcp/9191 viene utilizzata da DIVArchive Migrate Service

1.2.3. Eseguire i servizi come utente DIVA e attenersi al principio di privilegio minimo, ove possibile

Tutti i servizi DIVArchive devono essere eseguiti come utente DIVA. L'interfaccia GUI di controllo di DIVArchive fornisce tre profili utente fissi (Administrator, Operator e User). Per ottenere l'accesso agli account Administrator e Operator, è necessaria una password. Il sistema DIVArchive viene installato con password predefinite che possono essere modificate in qualsiasi momento utilizzando la utility Configuration di DIVArchive. Se le password predefinite non vengono modificate, il sistema DIVArchive rimane accessibile a possibili attività dannose. **Le password predefinite devono essere modificate subito dopo l'installazione e la configurazione degli account Administrator e Operator e, in seguito, almeno ogni 180 giorni. Una volta apportata la modifica, è necessario archiviare le**

password in una posizione sicura, offline, in cui possano essere rese disponibili per il supporto Oracle, se necessario.

1.2.4. Monitorare l'attività del sistema

Monitorare l'attività del sistema per stabilire la corretta esecuzione di DIVArchive e la presenza di attività anomale. Controllare i file di log posizionati nella directory di installazione sotto /Program/log/.

1.2.5. Mantenersi aggiornati sulle ultime informazioni sulla sicurezza

È possibile accedere a diverse fonti di informazioni di sicurezza. Per avvisi e informazioni sulla sicurezza relativi a un'ampia varietà di prodotti software, vedere:

<http://www.us-cert.gov>

Il metodo principale per essere sempre aggiornati sulle questioni relative alla sicurezza è quello di utilizzare la versione più aggiornata del software DIVArchive.

Capitolo 2. Installazione sicura

In questo capitolo viene presentato il processo di pianificazione di un'installazione sicura e sono descritte alcune topologie di distribuzione raccomandate per i sistemi.

2.1. Informazioni sull'ambiente

Per comprendere meglio le esigenze di sicurezza, è necessario rispondere alle domande riportate di seguito:

2.1.1. Quali risorse è necessario proteggere?

È possibile proteggere tutte le risorse presenti nell'ambiente di produzione. Considerare il tipo di risorse che si desidera proteggere quando si stabilisce il livello di sicurezza da fornire.

Quando si utilizza DIVArchive, proteggere le seguenti risorse:

2.1.1.1. Disco dati primario

Sono disponibili risorse disco dati e disco cache utilizzate per generare i sistemi DIVArchive. In genere si tratta di dischi locali o remoti connessi ai sistemi DIVArchive. L'accesso indipendente a questi dischi (non tramite DIVArchive) presenta un rischio per la sicurezza. Questo tipo di accesso esterno potrebbe essere eseguito da un sistema non autorizzato che esegue lettura o scrittura di questi dischi oppure da un sistema interno che può accidentalmente fornire accesso a questi dispositivi disco.

2.1.1.2. Dischi di database, di metadati e di backup

Sono disponibili risorse disco di database, di metadati e di backup utilizzate per generare i sistemi DIVArchive con oggetti complessi. In genere si tratta di dischi **locali o remoti** connessi ai sistemi DIVArchive. L'accesso indipendente a questi dischi (non tramite DIVArchive) presenta un rischio per la sicurezza. Questo tipo di accesso esterno potrebbe essere eseguito da un sistema non autorizzato che esegue lettura o scrittura di questi dischi oppure da un sistema interno che può accidentalmente fornire accesso a questi dispositivi disco.

2.1.1.3. Nastri DIVArchive

La concessione dell'accesso indipendente ai nastri, in genere in una libreria a nastro controllata da sistemi DIVArchive in cui vengono scritti i dati, rappresenta un rischio per la sicurezza.

2.1.1.4. Esportazione dei metadati del nastro

I dump dei metadati del nastro creati dall'operazione di esportazione contengono dati e metadati. Questi dati e metadati dovrebbero essere protetti dall'accesso eseguito da utenti diversi dall'amministratore del sistema operativo nel corso di un'attività di esportazione o importazione di routine.

2.1.1.5. File e impostazioni di configurazione

Le impostazioni di configurazione del sistema DIVArchive devono essere protette dagli utenti senza diritti di amministrazione a livello di sistema operativo. In generale queste impostazioni sono protette automaticamente dagli utenti amministrativi a livello di sistema operativo. Tenere presente che rendere i file di configurazione modificabili da parte di utenti del sistema operativo senza diritti di amministrazione costituisce un rischio per la sicurezza.

2.1.2. Da chi è necessario proteggere le risorse?

In generale, le risorse descritte nella sezione precedente devono essere protette da tutti gli accessi di utenti senza diritti di amministrazione su un sistema configurato o da un sistema esterno non autorizzato con accesso a queste risorse mediante fabric WAN o FC.

2.1.3. Cosa accade in caso di mancata protezione delle risorse strategiche?

Gli errori nella protezione delle risorse strategiche possono comprendere accesso non appropriato (accesso ai dati non conforme alle operazioni DIVArchive ordinarie) e danneggiamento dei dati (scrittura su disco o nastro non conforme alle autorizzazioni ordinarie).

2.2. Topologie di distribuzione raccomandate

In questa sezione viene descritto come installare e configurare un componente dell'infrastruttura in modo sicuro. Per informazioni sull'installazione di DIVArchive, consultare la libreria della documentazione per i clienti della release software 7.3 di DIVArchive all'indirizzo:

<https://docs.oracle.com/en/storage/#csm>

Considerare i seguenti punti quando si installa e configura DIVArchive:

2.2.1. Rete di metadati distinta

Per la connessione tra i diversi componenti dei servizi DIVArchive, la connessione al database di metadati e la connessione dai relativi client, fornire una rete TCP/IP distinta e un hardware switch non connesso ad alcuna rete WAN. Poiché il traffico dei metadati è implementato mediante TCP/IP, un attacco esterno ai danni di questo traffico è teoricamente

possibile. La configurazione di una rete di metadati separata consente di ridurre i rischi e ottenere prestazioni migliori. Se non è possibile ottenere una rete separata, bloccare il traffico alle porte DIVArchive dalla rete WAN esterna e da qualsiasi host non sicuro sulla rete. Vedere [Sezione 1.2.2, «Limitare l'accesso di rete ai servizi critici»](#).

2.2.2. Suddivisione in zone FC

Utilizzare la suddivisione in zone FC per negare l'accesso ai dischi DIVArchive connessi tramite Fiber Channel da qualsiasi server che non richiede l'accesso ai dischi. È preferibile utilizzare un Fibre Channel switch separato per eseguire il collegamento fisico solo ai server che necessitano di accesso.

2.2.3. Protezione dell'accesso alla configurazione dei dischi SAN

In genere è possibile accedere ai dischi RAID SAN per scopi di amministrazione mediante TCP/IP o più specificatamente mediante HTTP. È necessario proteggere i dischi dagli accessi esterni limitando l'accesso per scopi amministrativi ai dischi RAID SAN ai soli sistemi con un dominio attendibile. Modificare inoltre la password predefinita negli array del disco.

2.2.4. Installazione del pacchetto DIVArchive

Installare in primo luogo solo i servizi DIVArchive necessari. Se ad esempio non si intende eseguire l'interfaccia GUI o la utility Configuration da un sistema, deselezionarle nell'elenco di componenti da includere nell'installazione. I proprietari e le autorizzazioni delle directory di installazione DIVArchive predefiniti non dovrebbero essere modificati dopo l'installazione senza aver preso in esame le implicazioni di tali modifiche a carico della sicurezza.

2.2.5. Sicurezza dei nastri DIVArchive

Impedire l'accesso esterno ai nastri DIVArchive all'interno della libreria a nastro controllata dal sistema DIVArchive. Accessi non autorizzati ai nastri DIVArchive possono compromettere o distruggere i dati dell'utente.

2.2.6. Backup

Impostare ed eseguire i backup del database utilizzando DIVArchive Backup Service. Limitare l'accesso al dump di backup solo agli utenti di tipo amministratore a livello di sistema operativo.

2.3. Configurazione post-installazione

Dopo aver installato i pacchetti DIVArchive, consultare la lista di controllo di sicurezza in [Appendice A, Lista di controllo per la distribuzione sicura](#).

Capitolo 3. Funzioni di sicurezza

Per evitare potenziali minacce alla sicurezza, gli utenti di DIVArchive devono preoccuparsi dell'autenticazione e dell'autorizzazione del sistema.

È possibile minimizzare questi rischi per la sicurezza eseguendo una corretta configurazione e consultando la lista di controllo in seguito all'installazione in [Appendice A, Lista di controllo per la distribuzione sicura](#).

3.1. Modello di sicurezza

Di seguito sono elencate le funzioni di sicurezza fondamentali per la protezione dai rischi.

- Autenticazione: garantisce che solo gli utenti autorizzati abbiano accesso al sistema e ai dati.
- Autorizzazione: controllo dell'accesso a dati e privilegi di sistema. Questa funzione si basa sull'autenticazione per garantire che le persone ottengano solo il livello di accesso appropriato.

3.2. Autenticazione

L'interfaccia GUI di controllo di DIVArchive fornisce tre profili utente fissi (Administrator, Operator e User). Per ottenere l'accesso agli account Administrator e Operator, è necessaria una password. Il sistema DIVArchive viene installato con password predefinite che possono essere modificate in qualsiasi momento mediante la utility Configuration di DIVArchive. Se le password predefinite non vengono modificate, il sistema DIVArchive rimane accessibile a possibili attività dannose. **Le password predefinite devono essere modificate subito dopo l'installazione e la configurazione degli account Administrator e Operator e, in seguito, almeno ogni 180 giorni. Una volta apportata la modifica, è necessario archiviare le password in una posizione sicura, offline, in cui possano essere rese disponibili per il supporto Oracle, se necessario.**

3.3. Controllo dell'accesso

Il controllo dell'accesso in DIVArchive è suddiviso nei tre profili riportati di seguito.

User: una volta stabilita la connessione a DIVArchive Manager, l'interfaccia GUI di controllo consente solo all'utente di monitorare le operazioni di DIVArchive e di recuperare i dati dal database. Questo profilo è denominato profilo User. Non tutte le funzioni che inviano

comandi a DIVArchive sono accessibili in modalità profilo User. In questo modo è possibile gestire le situazioni in cui è necessario il monitoraggio ma non è consentito inviare comandi a DIVArchive.

Administrator: per inviare richieste a DIVArchive, ad esempio richieste di archiviazione o ripristino, o per espellere un nastro da una libreria, è necessario passare al profilo Administrator. Il profilo Administrator è protetto da password. La password predefinita per questo profilo è diva, ma è possibile modificarla nella utility Configuration. Per ulteriori informazioni, consultare la libreria della documentazione per i clienti della release software 7.3 di DIVArchive all'indirizzo:

<https://docs.oracle.com/en/storage/#csm>

Operator: oltre alle autorizzazioni del profilo User, il profilo Operator consente di accedere alla utility Object Transfer e richiede di inserire la stessa password del profilo Administrator.

Appendice A

Appendice A. Lista di controllo per la distribuzione sicura

1. Impostare password sicure per l'account Administrator e qualsiasi altro account del sistema operativo a cui è assegnato un ruolo di amministratore o di servizio DIVArchive, inclusi quelli elencati di seguito.
 - DIVA, ID utente Oracle (se utilizzati)
 - Qualsiasi account amministrativo array di dischi
2. Non utilizzare account del sistema operativo amministratore locale, assegnare piuttosto ruoli quando necessario ad altri account utente.
3. Impostare password sicure per gli account Administrator e Operator per l'interfaccia GUI di controllo. Modificare subito la password installata predefinita con una password sicura. È possibile eseguire questa operazione dalla utility Configuration sotto Tools.
4. Impostare una password sicura per il login al database Oracle. Modificare le password degli utenti del database oracle rispetto a quelle installate per impostazione predefinita.
5. Installare il firewall su ciascun sistema e applicare le regole per la porta DIVArchive predefinite. Limitare l'accesso all'interfaccia API DIVArchive (tcp 9000) agli indirizzi IP che richiedono l'accesso mediante regole di firewall.
6. Installare gli aggiornamenti del sistema operativo e DIVArchive a intervalli regolari in quanto questi includono aggiornamenti di sicurezza.
7. Installare l'antivirus ed escludere i processi e lo storage DIVArchive per motivi correlati alle prestazioni.
8. Per risultati ottimali, separare i dischi FC e le unità nastro FC fisicamente o tramite la suddivisione in zone FC, in modo che i dischi e le unità nastro non condividano la stessa porta HBA. Per il disco gestito, solo gli attori DIVArchive dovrebbero avere accesso al disco e anche alle unità nastro. In questo modo si previene la perdita di dati provocata dalla sovrascrittura accidentale di nastri o dischi.
9. Impostare un set di backup appropriato della configurazione e del database DIVArchive. I backup sono fondamentali per la sicurezza e forniscono una soluzione per il ripristino dei dati accidentalmente smarriti o violati. Il backup dovrebbe includere alcuni criteri durante il trasporto in un'altra posizione. È necessario proteggere i backup allo stesso livello di dischi e nastri DIVArchive.
