Oracle® DIVAdirector

Guida per la sicurezza

Release 5.3

E71132-01

Dicembre 2015

ORACLE®

Oracle® DIVAdirector
Guida per la sicurezza

E71132-01

Indice

Prefazione

La Guida per la sicurezza di DIVAdirector di Oracle include informazioni relative al prodotto DIVAdirector e spiegazioni dei principi generali di scurezza 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 DIVAdirector.

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 udenti.

1

Capitolo 1. Panoramica

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

1.1. Panoramica del prodotto

Oracle DIVAdirector è uno strumento di interazione con i sistemi Oracle DIVArchive esistenti. L'interfaccia utente è disponibile in forma grafica tramite un browser Web. DIVAdirector è composto dai principali componenti elencati di seguito.

1.1.1. DIVAdirector Server

DIVAdirector Server fornisce interfacce con DIVArchive mediante l'API C++ per tutte le operazioni richieste da DIVAdirector Web. Inoltre sincronizza le informazioni sull'oggetto rilevato archiviate in DIVArchive con quelle nel proprio database. Esegue il monitoraggio delle cartelle di destinazione configurate per proxy, metadati e operazioni e gestisce la cronologia di tutte le cartelle di destinazione e le operazioni dell'interfaccia utente.

1.1.2. DIVAdirector Web

Il modulo Web di DIVAdirector offre un'interfaccia utente basata sul Web che consente agli utenti di cercare oggetti rilevati in DIVArchive, amministrare i diritti di accesso degli utenti, aggiungere metadati per asset, eseguire proxy di oggetti ed effettuare operazioni (ad esempio ripristino, ripristino parziale ed eliminazione) su elementi aggiunti a raccoglitori o elenchi di riprese. Consente inoltre agli utenti di sfogliare i file in locale e archiviare contenuto nel sistema DIVArchive.

1.1.3. DIVAdirector Database

DIVAdirector utilizza PostgreSQL per archiviare tutte le informazioni sugli asset, i metadati, le informazioni proxy, le informazioni sugli utenti, la cronologia delle operazioni e le impostazioni di configurazione di DIVArchive.

1.1.4. DIVAdirector Transcoder Service

DIVAdirector Transcoder Service è un servizio separato richiamato da DIVAdirector per la transcodifica di clip ad alta risoluzione in proxy a bassa risoluzione e la successiva visualizzazione nell'interfaccia utente di DIVAdirector Web.

1.1.5. DIVAdirector Task Manager Service

DIVAdirector Task Manager Service è un'applicazione di un servizio di Windows visibile nella finestra di dialogo standard di Services Control Manager. Questa applicazione è responsabile dell'esecuzione di task potenzialmente lunghi in un processo in background.

1.1.6. DIVAdirector API Service

Questo servizio espone gli endpoint per la funzionalità di DIVAdirector comune. Inizialmente questo servizio conterrà solo un piccolo sottoinsieme della logica di DIVAdirector. Gli endpoint esposti tramite questo servizio continueranno a crescere con la graduale migrazione della funzionalità da DIVAdirector Web.

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 DIVAdirector 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

DIVAdirector utilizza le seguenti porte TCP/IP:

- tcp/7680 per i comandi dell'interfaccia utente
- tcp/8080 per il server HTTP

Per le release di DIVAdirector successive la 5.3.0, sono necessarie le tre porte aggiuntive elencate di seguito.

- tcp/9763: integrazione di DIVArchiveWS Service.
- tcp/9876: integrazione di DIVAtranscode Service.
- tcp/6543: integrazione di DIVAdirector API Service.

Nota:

I numeri di porta elencati in precedenza sono quelli correnti, ma è possibile che vengano modificati in futuro.

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

In DIVAdirector è disponibile un utente Super Admin predefinito la cui password deve essere modificata dopo il primo login. Questo utente potrà quindi creare altri utenti con autorizzazioni di gruppo diverse per l'accesso e le operazioni consentite.

Se la password predefinita non viene modificata, il sistema rimane accessibile a possibili attività dannose. La password predefinita deve essere modificata subito dopo l'installazione e la configurazione dell'account Super Admin 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

È possibile monitorare l'attività del sistema per stabilire la corretta esecuzione di DIVAdirector. I log si trovano in C:/Program Files (x86)/DIVAdirector 5/cmg-server and C:/Program Files (x86)/DIVAdirector 5/www/logs.

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 DIVAdirector.

2

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 DIVAdirector, proteggere le risorse riportate di seguito.

2.1.1.1. Disco dati primario

Sono disponibili cartelle proxy contenenti clip a bassa risoluzione. Si tratta principalmente di dischi locali o remoti connessi al sistema DIVAdirector. L'accesso indipendente a questi dischi (non tramite DIVAdirector) 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 e di backup

Sono disponibili risorse disco di database e di backup utilizzate per generare DIVAdirector. In genere si tratta di dischi locali o remoti connessi ai sistemi DIVAdirector. L'accesso indipendente a questi dischi (non tramite DIVAdirector) 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. File e impostazioni di configurazione

Le impostazioni di configurazione del sistema DIVAdirector 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. I file sensibili includono tutti i file di configurazione delle applicazioni contenuti nella directory di installazione, tra cui i seguenti:

- www/Web.config
- Api/Oracle.DIVAdirector.Api.exe.config
- TaskManager/Oracle.DIVAdirector.TaskManager.exe.config
- cmgserver/cmgserver.ini

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 DIVAdirector ordinarie) e danneggiamento dei dati (scrittura su disco o nastro non conforme alle autorizzazioni ordinarie).

3

Capitolo 3. Funzioni di sicurezza

Per evitare potenziali minacce alla sicurezza, gli utenti di DIVAdirector 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.

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 o DIVAdirector.
2. Non utilizzare account del sistema operativo amministratore locale, assegnare piuttosto ruoli quando necessario ad altri account utente.
3. Impostare una password sicura per l'utente Administrator di DIVAdirector. Modificare subito la password installata predefinita con una password sicura. È possibile eseguire questa operazione dalla schermata di impostazioni **Admin**, **Personal** di DIVAdirector.
4. Installare un firewall nel sistema e applicare le regole per la porta DIVAdirector predefinite.
5. Installare gli aggiornamenti del sistema operativo e DIVAdirector a intervalli regolari in quanto questi includono patch di sicurezza.
6. Installare l'antivirus ed escludere i processi e lo storage DIVAdirector per motivi correlati alle prestazioni.