Oracle® DIVAnet

Guida per la sicurezza

Release 2.0

E74315-01

Marzo 2016

ORACLE®

Oracle® DIVAnet
Guida per la sicurezza

E74315-01

Indice

Prefazione

Nel documento Guida per la sicurezza di Oracle DIVAnet sono incluse informazioni sul prodotto Oracle DIVAnet e vengono descritti i 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 DIVAnet.

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 Oracle DIVAnet 2.0 e vengono descritti i principi generali di sicurezza delle applicazioni.

1.1. Panoramica del prodotto

Oracle DIVAnet offre una vista unificata del contenuto archiviato in più sistemi Oracle DIVArchive distribuiti. Oracle DIVArchive è un sistema scalabile di gestione della memorizzazione del contenuto che supporta l'archiviazione in librerie a nastro e sistemi di dischi. DIVAnet facilita lo spostamento del contenuto tra i siti DIVArchive e dai server e dischi di origine e destinazione del cliente. Esegue task finalizzati al recupero di emergenza, alla distribuzione del contenuto, al controllo dell'accesso, all'ottimizzazione delle prestazioni e della disponibilità del contenuto.

DIVAnet è composto dai principali componenti elencati di seguito.

1.1.1. Servizio DIVAnet ClientAdapter

I client delle applicazioni che desiderano utilizzare l'interfaccia API di DIVArchive o l'interfaccia GUI di DIVAnet, si connettono al **servizio DIVAnet ClientAdapter**. Questo servizio DIVAnet accetta le connessioni Web e socket provenienti dalle applicazioni ed elabora le richieste. Un **ClientAdapter** viene configurato in ogni sito che dispone di applicazioni che sono locali per il sito in cui sono installati DIVArchive e DIVAnet.

1.1.2. Servizio DIVAnet ManagerAdapter

Il **servizio DIVAnet ManagerAdapter** funge da bridge tra DIVAnet e Oracle DIVArchive Manager. Deve essere configurato per fornire accesso remoto tramite altri sistemi DIVAnet.

1.1.3. Servizio DIVAnet DbSync

Il **servizio DIVAnet DbSync** è responsabile della sincronizzazione delle informazioni degli asset presenti in più siti DIVArchive e della memorizzazione delle informazioni nel database DIVAnet. **DbSync** comunica in remoto con i servizi **ManagerAdapter** di più siti per sincronizzare le informazioni degli oggetti archiviati. **DbSync** viene in genere distribuito insieme a **ClientAdapter**. Sia **DbSync** che **ClientAdapter** richiedono l'accesso diretto al database DIVAnet.

1.1.4. Interfaccia utente di DIVAnet (DIVAnetUI)

DIVAnetUI è un'applicazione GUI che consente all'utente di monitorare le richieste DIVAnet e di visualizzare, copiare ed eliminare gli asset DIVAnet (gli oggetti archiviati DIVA) in più siti DIVArchive. È possibile monitorare tutte le richieste a livello di DIVAnet, indipendentemente se effettuate tramite l'interfaccia API o l'interfaccia utente stessa. Inoltre, è possibile visualizzare le informazioni degli asset per tutti i siti DIVArchive configurati, indipendentemente se l'asset sia stato archiviato tramite DIVAnet. **DIVAnetUI** fornisce modalità flessibili di esecuzione di query sulle informazioni riguardanti sia le richieste che gli asset.

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 DIVAnet 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 a servizi fondamentali

Per impostazione predefinita, DIVAnet utilizza le porte TCP/IP riportate di seguito.

- *`tcp/9801`* è la porta **WebService** predefinita usata da DIVAnet **ClientAdapter**.
- *`tcp/7101`* è la porta socket API predefinita usata da DIVAnet **ClientAdapter** (è possibile configurare altre porte).
- *`tcp/9800`* è la porta **WebService** predefinita usata da DIVAnet **ManagerAdapter**.

Nota:

Non è necessario esporre esternamente tutte queste porte e non tutte si basano su configurazione e uso.

1.2.3. Usare il principio di privilegio minimo dove possibile

Non eseguire i servizi DIVAnet come *`admin`* o *`SuperUser`*. L'esecuzione dei servizi con un utente di sistema operativo diverso rispetto a quello utilizzato per amministrare l'applicazione, contribuisce alla sicurezza di tutto il sistema. È necessario che i firewall limitino le porte solo a quelle richieste. DIVAnet dispone di funzioni di controllo dell'accesso, descritte in breve in «Controllo dell'accesso», usate per limitare gli utenti e i sistemi al minimo privilegio possibile.

1.2.4. Monitorare l'attività del sistema

È necessario monitorare l'attività del sistema per stabilire la corretta esecuzione di DIVAnet e l'eventuale presenza di attività anomale. Controllare i file di log presenti nella cartella *$DIVANET_HOME/Program/log/*.

1.2.5. Mantenersi aggiornati sulle ultime informazioni sulla sicurezza

È possibile accedere a diverse fonti di informazioni e avvisi sulla sicurezza relativi a un'ampia varietà di prodotti software all'indirizzo:

http://www.us-cert.gov

Il metodo principale per essere sempre aggiornati sulle questioni relative alla sicurezza è quello di utilizzare la release più recente del software DIVAnet.

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 consigliate 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 molte risorse presenti nell'ambiente di produzione. Considerare il tipo di risorse da proteggere quando si stabilisce il livello di sicurezza da fornire.

Quando si utilizza DIVAnet, è necessario proteggere le risorse descritte di seguito.

2.1.1.1. Server DIVAnet

DIVAnet viene installato su un server collegato a uno o più dischi (un disco locale o remoto connesso direttamente al sistema DIVAnet). L'accesso indipendente a questi dischi (non tramite DIVAnet) presenta un rischio per la sicurezza. Questo tipo di accesso esterno potrebbe essere eseguito da un sistema non autorizzato che esegue la lettura o la scrittura di questi dischi oppure da un sistema interno che può accidentalmente fornire accesso a questi dispositivi disco.

2.1.1.2. Database

I sistemi DIVAnet sono costituiti da software di database e da risorse di dati. In genere, i dati si trovano su dischi locali o remoti connessi ai sistemi DIVAnet. L'accesso indipendente a questi dischi (non tramite DIVAnet) presenta un rischio per la sicurezza. Questo tipo di accesso esterno potrebbe essere eseguito da un sistema non autorizzato che esegue la lettura o la scrittura di questi dischi oppure da un sistema interno che può accidentalmente fornire accesso a questi dispositivi disco.

2.1.1.3. Origini e destinazioni DIVArchive e supporti di archiviazione

Per soddisfare i requisiti di sistema, DIVAnet utilizza le origini e le destinazioni DIVArchive e i sistemi di archiviazione DIVA (disco o nastro). L'accesso indipendente non autorizzato

a questi dischi del server e supporti di sistema, che sono in genere controllati dai sistemi DIVArchive, è un rischio per la sicurezza. Le **origini/destinazioni** utilizzate come data store temporanei per le operazioni di copia di DIVAnet dovrebbero essere ad accesso limitato e occorre considerare la possibilità di dedicare tali **origini/destinazioni** esclusivamente alle operazioni DIVAnet, assicurando inoltre che i trasferimenti siano cifrati o avviati su una rete affidabile.

2.1.1.4. File e impostazioni di configurazione

È necessario proteggere le impostazioni di configurazione del sistema DIVAnet dagli utenti senza diritti di amministrazione a livello di sistema operativo. In generale, queste impostazioni sono protette automaticamente dagli utenti con diritti di amministrazione a livello di sistema operativo. 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 non di amministratore su un sistema configurato o da sistemi esterni non autorizzati che possono accedere a queste risorse tramite fabric WAN o FC.

2.1.3. Cosa accade se la protezione delle risorse strategiche fallisce?

Gli errori nella protezione delle risorse strategiche possono comprendere accesso non appropriato (ad esempio, l'accesso ai dati non conforme alle operazioni DIVAdirector ordinarie) e danneggiamento dei dati (eliminazione accidentale di asset o scrittura su disco o nastro non conforme alle autorizzazioni ordinarie).

2.2. Tecnologie di distribuzione consigliate

In questa sezione viene descritta l'installazione e la configurazione di un componente dell'infrastruttura sicura.

Per informazioni sull'installazione di DIVAnet, consultare il documento *Oracle DIVAnet Guide* nella libreria della documentazione di DIVAnet 2.0 all'indirizzo:

`https://docs.oracle.com/en/storage/#csm`

Considerare i seguenti punti quando si installa e configura DIVAnet.

2.2.1. Installazione di DIVAnet

Installare solo i componenti DIVAnet necessari. Ad esempio, se nel sistema si intende eseguire solo **DIVAnetUI**, deselezionare **DIVAnet Services** nell'elenco dei componenti da installare durante l'installazione. I proprietari e le autorizzazioni delle directory di

installazione DIVAnet predefiniti non dovrebbero essere modificati dopo l'installazione senza aver preso in esame le implicazioni di tali modifiche a carico della sicurezza.

2.2.2. Connessione a DIVArchive

Oracle consiglia di installare il componente **ManagerAdapter** nel sistema DIVArchive Manager per migliorare la sicurezza del sistema. Se l'accesso esterno alla porta di DIVArchive Manager non è necessario, si consiglia di bloccare la porta tramite il software firewall. Inoltre, sarà opportuno non consentire spesso l'accesso di rete esterna alla porta **WebService DIVAnet DbSync**.

Quando ci si connette a un'istanza DIVArchive remota su una rete WAN, assicurarsi che la rete sia affidabile. Inoltre, considerare la possibilità di effettuare la connessione al sito utilizzando *SSL/TLS* per la porta di **ManagerAdapter** nel sito remoto.

2.2.3. Protezione dei sistemi di dischi

Utilizzare la suddivisione in zone FC per negare l'accesso ai dischi DIVAnet connessi tramite Fibre Channel a qualsiasi server che non richiede l'accesso ai dischi. È preferibile utilizzare un Fibre Channel switch distinto per eseguire la connessione fisica solo ai server che richiedono l'accesso.

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

2.3. Configurazione postinstallazione

Dopo l'installazione di qualsiasi componente di DIVAnet, andare all'elenco di controllo della sicurezza in Appendice A, *Elenco di controllo per la distribuzione sicura*.

3

Capitolo 3. Funzioni di sicurezza

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

È possibile minimizzare questi rischi per la sicurezza eseguendo una corretta configurazione e consultando l'elenco di controllo postinstallazione in Appendice A, *Elenco 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**: assicura che solo agli utenti autorizzati sia concesso l'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

I servizi DIVAnet possono eseguire l'autenticazione mediante diversi metodi.

- **Certificati SSL/TLS**: DIVAnet consulta un truststore di certificati quando crea una connessione in uscita a un servizio DIVAnet remoto. Ciò consente di assicurare che si sta effettuando la connessione a servizi DIVAnet autentici. Per creare una connessione sicura tra DIVAnet **ClientAdapter** e un'istanza DIVArchive, è necessario connettersi tramite **ManagerAdapter** utilizzando un <*ConnectionType*> identificato come **WebService**.
- **Regole di accesso**: anche se dal punto di vista tecnico si tratta di una forma di controllo dell'accesso, le regole di accesso possono filtrare le connessioni in entrata sull'indirizzo IP in entrata. Questa funzione è necessaria per consentire di assicurare che solo i sistemi approvati dispongono dell'accesso appropriato ai servizi DIVAnet.

AVVERTENZA:

I servizi DIVAnet utilizzano password di database come parte della relativa configurazione. È necessario modificare le password immediatamente dopo l'installazione e in seguito ogni 180 giorni (minimo). Dopo aver effettuato la modifica, conservare le password in un luogo sicuro, non in linea, dove possono essere rese disponibili per il supporto Oracle, se necessario.

3.3. Controllo dell'accesso

È possibile creare regole di accesso per limitare le operazioni che determinati utenti o sistemi possono eseguire nel sistema di archiviazione distribuito. Le regole di accesso possono essere eseguite nelle modalità seguenti:

- **ClientAdapter/modalità MultiDiva**: limita i tipi di richieste DIVAnet che possono essere eseguite.
- **ManagerAdapter**: limita i tipi di richieste DIVArchive che possono essere eseguite per soddisfare una richiesta DIVAnet (possibilmente richiesta da un sistema remoto).

Le regole di accesso possono riguardare le richieste avviate da **DIVAnetUI** o da una connessione socket API (possibilmente avviata da un sistema MAM o di automazione).

Una richiesta DIVAnet può avere accesso alle regole eseguite su di essa a livello DIVAnet o a livello DIVArchive. A livello DIVAnet, **ClientAdapter** elabora la richiesta nel punto in cui questa è stata ricevuta. A livello DIVArchive, un **ManagerAdapter** remoto elabora le richieste DIVArchive effettuate per soddisfare la richiesta DIVAnet.

Oracle consiglia di creare il set di regole più restrittivo possibile che soddisfi i requisiti dell'applicazione. Ad esempio, se solo gli amministratori devono eseguire eliminazioni globali, assicurarsi che ad altre categorie di utenti sia negato l'accesso a tale funzionalità. Se un gruppo di utenti del sistema richiede solo l'accesso a un elenco limitato di origini e destinazioni, assicurarsi che tali utenti possano effettuare richieste solo nei confronti di tali specifiche origini e destinazioni.

Inoltre, considerare i siti usati per soddisfare le richieste. Ad esempio, se gli utenti del sito locale non hanno motivo per eseguire copie dove i siti di origine e destinazione non corrispondono al sito locale (ciò è possibile utilizzando DIVAnet), configurare queste regole nella configurazione di **ClientAdapter**.

Infine, considerare i costrutti specifici nelle richieste che si desidera escludere nella scheda. Ad esempio, se non è necessario fare riferimento agli oggetti solo con il nome oggetto, senza la categoria, escludere tutte le richieste che presentano categorie vuote.

Inoltre, ogni ***`ClientAdapter WorkflowProfile`*** contiene l'elenco dei messaggi validi che possono essere elaborati dalle richieste assegnate a WorkflowProfile. In **modalità MultiDiva**, ciò consente di escludere messaggi specifici dall'elaborazione, inclusi i messaggi informativi.

Oracle consiglia di eseguire l'avvio con le regole predefinite stabilite nel file *`AccessRules.xml.ini`* anche se non si definiscono regole di accesso proprie. Per ulteriori informazioni sulle funzioni di controllo dell'accesso di DIVAnet, consultare il documento *Oracle DIVAnet Guide* all'indirizzo:

`https://docs.oracle.com/en/storage/#csm`

3.4. Configurazione di SSL/TLS

In DIVAnet, i dati del certificato sono contenuti in due posizioni: in un *keystore privato*, usato per i servizi Web ospitati nel sistema locale, e in un *keystore pubblico*, usato per verificare i servizi Web richiamati in remoto. È possibile usare la **utility Keytool di Java** per modificare la password del keystore, nonché aggiungere ed eliminare certificati.

Per ulteriori informazioni sulla creazione dei keystore, fare riferimento all'indirizzo:

http://docs.oracle.com/javase/8/docs/technotes/guides/security/jsse/JSSERefGuide.html#CreateKeystore

Solo le connessioni dei servizi Web DIVAnet utilizzano *SSL/TLS*. In questa release, la connessione a DIVArchive o DIVAnet tramite una connessione socket API DIVArchive non utilizzerà *SSL/TLS*.

3.4.1. Keystore privato

I dati del certificato della chiave privata di DIVAnet sono memorizzati nella seguente directory:

$DIVANET_HOME/Program/divanet/lib/diva129.jks

In questo keystore deve essere presente un solo certificato. Tale certificato viene usato per i servizi Web ospitati dai servizi che vengono eseguiti in questa directory *$DIVANET_HOME*. Si consiglia di sostituire il certificato fornito con il prodotto con un nuovo certificato e di usare un certificato diverso per ogni sito DIVAnet presente nella rete.

È necessario modificare la password di questo keystore. Memorizzare le informazioni della password in un nuovo file denominato *$DIVANET_HOME/Program/divanet/lib/diva129.properties* e rendere il file leggibile per i servizi DIVAnet ma non per utenti occasionali del sistema. Per il file utilizzare il seguente formato:

keystorePassword=[newpassword]

3.4.2. Keystore pubblico

Denominato anche *truststore*, i relativi dati si trovano nella seguente directory:

$DIVANET_HOME/Java/lib/security/cacerts2

Questi dati del certificato vengono utilizzati nelle chiamate in uscita ai servizi Web, incluso **DIVAnetUI**. In questo keystore è possibile caricare più chiavi pubbliche.

Se nel keystore privato di DIVAnet è stato aggiunto un nuovo certificato con firma automatica, esportare il certificato utilizzando la utility Keytool. Tutte le applicazioni

(servizi DIVAnet, DIVAnetUI e così via) che richiamano **WebService** in questo sito devono aggiungere il certificato esportato nel proprio keystore pubblico.

Appendice A

Appendice A. Elenco di controllo per la distribuzione sicura

1. Impostare password sicure per l'amministratore e qualsiasi altro account del sistema operativo che dispone di un amministratore DIVAnet o di ruoli servizio assegnati. Sono inclusi:
   - *divanet*, ID utente Oracle se utilizzati;
   - qualsiasi account amministrativo di dischi.
2. Non usare un account di amministratore locale del sistema operativo, ma assegnare i ruoli necessari ad altri account utente.
3. Usare certificati specifici per ogni installazione DIVAnet e definire una password sicura per il database Oracle e il keystore privato. Impostare una password sicura per il login dell'utente al database Oracle.
4. Installare il software firewall in ogni sistema DIVAnet e applicare le regole di porta DIVAnet predefinite. Limitare l'accesso al socket API DIVAnet API (*tcp 7101*) agli IP che richiedono l'accesso utilizzando le regole del firewall. Eseguire questo passo con le regole di accesso di DIVAnet.
5. Installare regolarmente gli aggiornamenti del sistema operativo e di DIVAnet poiché includono le patch di sicurezza.
6. Installare l'antivirus ed escludere i processi DIVAdirector e la memorizzazione per non influire sulle prestazioni.
7. Nelle procedure consigliate viene suggerita la separazione dei dischi FC e delle unità nastro FC a livello fisico oppure tramite la suddivisione in zone FC, in modo che i dischi e le unità nastro non condividano la stessa porta HBA. In questo modo si previene la perdita di dati provocata dalla sovrascrittura accidentale di dati importanti.
8. Configurare un set appropriato di backup per la configurazione e il database DIVAnet. I backup sono fondamentali per la sicurezza e forniscono una soluzione per il ripristino di dati persi in modo accidentale o violati. Il backup dovrebbe includere alcuni criteri durante il trasporto in un'altra posizione. È necessario proteggere i backup allo stesso livello dei dischi DIVAnet.