StorageTek Enterprise Library Software

Guida per la sicurezza

E63467-01

Marzo 2015

ORACLE

StorageTek Enterprise Library Software
Guida per la sicurezza

E63467-01

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

In questo documento vengono descritte le funzioni di sicurezza di Oracle StorageTek Enterprise Library Software (ELS).

Destinatari

Il presente manuale è rivolto a chiunque sia coinvolto nell'uso delle funzioni di sicurezza nonché nell'installazione e configurazione sicure di StorageTek Enterprise Library Software (ELS).

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

Panoramica

In questa sezione viene fornita una panoramica sulla suite software ELS e vengono descritti i principi generali della sicurezza dell'applicazione.

1.1. Panoramica del prodotto

ELS offre il supporto dell'automazione del nastro per gli ambienti a nastro mainframe di Oracle StorageTek per le piattaforme elencate di seguito.

- Piattaforma IBM z/OS. ELS supporta un'architettura di automazione del nastro client/server TCP/IP che consente di eseguire il software client SMC in una piattaforma z/OS LPAR per comunicare con il software server HSC/VTCS in esecuzione su una piattaforma z/OS LPAR diversa.
- Piattaforma IBM z/OS. Il software client ELS VM per i sistemi z/VM comunica con il software server HSC/VTCS in esecuzione su una piattaforma z/OS LPAR per automatizzare l'elaborazione dei nastri virtuale e fisica per z/VM.
- Piattaforma Fujitsu MSP/EX. È necessario eseguire SMC su ogni host in cui si verifica l'elaborazione del nastro. Il componente server ELS (HSC/VTCS) può essere eseguito sullo stesso host MSP/EX di SMC oppure su un host remoto separato. Se SMC e HSC/VTCS risiedono su host MSP/EX diversi, viene utilizzato il protocollo TCP/IP per inviare richieste dal client host al server host. Per ricevere richieste HTTP da un client SMC remoto, è necessario che il componente HTTP sia attivato sull'SMC in esecuzione sul server host.

La comunicazione client/server di ELS viene utilizzata per emettere le richieste del percorso di controllo, principalmente richieste di installazione/disinstallazione, per i volumi nastro virtuali e fisici. Le informazioni contenute in queste richieste del percorso di controllo sono costituite da informazioni sulla configurazione e i criteri TapePlex, indirizzi dell'unità di trasporto su nastro virtuale/fisico e numeri di serie del volume nastro virtuale/fisico. La comunicazione client/server di ELS, inoltre, non contiene mai dati sul cliente, che vengono sempre trasmessi tramite interfacce per il percorso dati IBM FICON/ESCON che connettono LPAR host ai dispositivi di trasporto su nastro Oracle StorageTek o ai dispositivi a nastro virtuali VSM.

Le informazioni contenute in questa Guida per la sicurezza riguardano tutte le release di ELS. Come illustrato nella Parte 3 di questa Guida, è possibile proteggere le comunicazioni sul percorso di controllo client/server di ELS quando tale protezione è opportuna o necessaria. In questo documento vengono inoltre illustrati gli aspetti correlati alla sicurezza di diverse attività di installazione e post-installazione di ELS.

1.2. Principi di sicurezza generali

I principi riportati di seguito sono fondamentali per l'uso sicuro di qualsiasi prodotto.

1.2.1. Mantenere il software aggiornato

Uno dei principi alla base delle procedure di sicurezza consigliate consiste nel mantenere aggiornate tutte le versioni e le patch del software. L'ultimo bundle di manutenzione cumulativo di ELS, insieme ai singoli PTF e HOLDDATA, è disponibile su My Oracle Support (MOS). I bundle di manutenzione cumulativi vengono aggiornati mensilmente per includere tutti i PTF dall'ultimo ciclo di test di regressione mensile di ELS. Tutti i PTF in un bundle cumulativo sono stati testati insieme come un pacchetto completo. La notifica via e-mail HIPER PTF è disponibile iscrivendosi ai documenti MOS Hot Topics Alert per i prodotti ELS. I clienti sono incoraggiati a mantenere i livelli di manutenzione correnti, mantenere aggiornato HOLDDATA e iscriversi alle notifiche Hot Topics Alerts for HIPER.

1.2.2. Limitare l'accesso alla rete

Per motivi di prestazioni e sicurezza, inoltrare le comunicazioni sul percorso di controllo ELS su una rete isolata protetta da un firewall. L'uso di un firewall garantisce che l'accesso ai sistemi ELS sia limitato a una rete nota, che può essere monitorata e limitata, se necessario. L'uso di una rete dedicata per le comunicazioni client/server ELS elimina i conflitti di rete con altre applicazioni e migliora le prestazioni del sistema a nastro.

1.2.3. Mantenersi aggiornati sulle ultime informazioni sulla sicurezza

Oracle apporta continui miglioramenti ai prodotti software e alla documentazione. Verificare a intervalli regolari le revisioni di questa Guida per la sicurezza e della documentazione su tutti gli altri prodotti ELS. Tutta la documentazione su ELS a cui viene fatto riferimento nel presente documento è disponibile nella sezione prodotti di storage a nastro di Oracle Technical Network.

2

Installazione sicura

IBM z/OS System Authorization Facility (SAF) fornisce la protezione essenziale per la maggior parte degli aspetti correlati alla sicurezza di ELS. In genere la funzionalità SAF viene implementata con il pacchetto IBM RACF o con un pacchetto equivalente. In questa sezione viene descritto come utilizzare un ambiente SAF basato su RACF per installare e configurare un'installazione ELS sicura.

2.1. Installazione di ELS

Nel documento di Oracle *StorageTek Enterprise Library Software: Installing ELS* viene descritto come installare e configurare la versione di ELS in uso utilizzando la protezione RACF. Consultare questo documento per ulteriori informazioni sugli argomenti di installazione correlati alla sicurezza indicati di seguito:

- Installazione del software di base e dell'ultimo bundle di manutenzione cumulativo
- Autorizzazione ELS load library APF
- Autorizzazione HSC user exit library APF
- Autorizzazione SMC JES3 load library APF

2.2. Configurazione post-installazione di ELS

Nei documenti di Oracle riportati di seguito vengono descritte le attività di configurazione post-installazione per la versione di ELS in uso:

- *StorageTek Enterprise Library Software: Configuring HSC and VTCS*
- *StorageTek Enterprise Library Software: Configuring and Managing SMC*
- *StorageTek Enterprise Library Software: ELS Programming Reference*

Consultare questi documenti per ulteriori informazioni sugli argomenti di post-installazione correlati alla sicurezza indicati di seguito:

- Definizione della protezione RACF per la sicurezza del set di dati CDS
- Definizione dell'autorità di comando e dell'autorità dell'interfaccia programmatica mediante HSC user exit SLSUX15
- Definizione dell'autorità di accesso al volume per l'installazione e l'espulsione dei volumi mediante HSC user exit SLSUX14
- Definizione dell'autorità volser del pool MVC e del subpool vuoto

- Definizione di un segmento SMC OMVS RACF per la comunicazione con un sottosistema HSC remoto
- Definizione di un segmento SMC OMVS RACF per la comunicazione con un'appliance VLE

3

Funzioni di sicurezza

In questo capitolo vengono descritti i meccanismi di sicurezza specifici offerti da ELS.

3.1. Protezione di ELS solo con AT-TLS – z/OS

La funzionalità IBM z/OS Application Transparent Transport Layer Security (AT-TLS) utilizza la cifratura dei dati SSL per proteggere le applicazioni z/OS TCP/IP. Per ulteriori informazioni su AT-TLS, consultare il manuale *IBM publication z/OS Communications Server: IP Configuration Guide* e vedere le informazioni su AT-TLS Policy Agent nel manuale *IBM publication z/OS Communications Server: IP Configuration Reference*.

La protezione delle comunicazioni client/server ELS tra SMC e HSC/VTCS è descritta nel white paper Oracle *Using AT-TLS with HSC/SMC Client/Server z/OS Solution: Implementation Example*. Questo white paper è disponibile nella sezione dei prodotti di storage a nastro di Oracle Technical Network. Per informazioni dettagliate sulla configurazione, consultare questa pubblicazione.

Per proteggere ELS con AT-TLS, Oracle consiglia di utilizzare uno dei seguenti algoritmi di cifratura SSL:

- Famiglia SHA-2 (SHA-256, SHA-384, SHA-512)
- AES >= 128 bit
- RSA >= 2048 bit
- Diffie-Hellman (DH) >= 2048 bit
- ECC >= 256 bit

Qualsiasi altro algoritmo di cifratura SSL fornisce una protezione più debole e pertanto non deve essere utilizzato con ELS.

Nota:

L'appliance StorageTek Virtual Library Extension (VLE) per VSM attualmente non supporta le comunicazioni AT-TLS. Non proteggere le comunicazioni ELS VLE con AT-TLS.

3.2. Uso della funzione di sicurezza ELS XAPI

ELS 7.3 introduce una nuova funzione di sicurezza XAPI per la comunicazione tra client e server, abilitata per impostazione predefinita nel server HTTP SMC. La funzione di sicurezza XAPI fornisce ulteriori funzionalità di autenticazione dell'utente come parte del

protocollo XAPI completamente interne a ELS. Per utilizzare la funzione di sicurezza XAPI, è necessario definire credenziali di sicurezza (ID utente e password) per i client e i server ELS. Le operazioni TapePlex di ELS 7.3 utilizzano queste credenziali di sicurezza per proteggere le transazioni XAPI (installazione, disinstallazione, ricerca del volume, creazione di unità provvisorie e così via). L'uso delle credenziali di sicurezza XAPI è completamente trasparente e non richiede ulteriori interventi da parte dell'utente o dell'operatore. Per ulteriori informazioni sulla configurazione della funzione di sicurezza XAPI, consultare *Configuring and Managing SMC 7.3*.

Il metodo preferito per proteggere le transazioni XAPI per i TapePlex su cui risiedono solo le applicazioni client ELS (client SMC e VM) consiste nell'utilizzare le funzionalità AT/TLS come descritto in Sezione 3.1, «Protezione di ELS solo con AT-TLS – z/OS». AT/TLS è una funzionalità a livello di trasporto esterna e trasparente a ELS.

Utilizzare la funzione di sicurezza XAPI di ELS 7.3 per proteggere i TapePlex su cui risiedono client non ELS (client di sistemi aperti) o un misto di client ELS (client SMC e VM) e non ELS. In questi ambienti è possibile utilizzare AT-TLS in aggiunta alla funzione di sicurezza XAPI di ELS 7.3, ma le transazioni XAPI per i client non ELS non verranno protette.

4

Considerazioni sulla sicurezza per gli sviluppatori

Nel documento di Oracle *StorageTek Enterprise Library Software: ELS Programming Reference* sono descritte le interfacce API di ELS disponibili per gli sviluppatori di applicazioni. L'interfaccia programmatica per ELS utilizza l'interfaccia UUI (Unified User Interface), che si avvale dell'uscita di sicurezza del comando HSC SLSUX15 per gestire l'accesso alle relative funzioni in base all'autorizzazione RACF (o a un'autorizzazione equivalente). Per ulteriori informazioni sulla protezione di SLSUX15 con RACF, vedere Sezione 2.2, «Configurazione post-installazione di ELS».

Appendice A

Elenco di controllo per la distribuzione sicura

1. Utilizzare la protezione RACF (o una protezione equivalente) come descritto nella presente Guida per la sicurezza.
2. Limitare l'accesso alla rete. ELS e le librerie a nastro che gestisce devono essere protetti dal firewall aziendale.
3. Se necessario, proteggere il traffico di rete di ELS con la funzionalità IBM AT-TLS o la funzione di sicurezza ELS XAPI.
4. Applicare tutti i PTF e HOLDDATA di ELS.
5. Se vengono rilevati punti di vulnerabilità nel software Oracle ELS, rivolgersi al supporto software Oracle all'indirizzo `http://www.myoraclesupport.com/`.

Appendice B

Riferimenti

La documentazione su ELS viene salvata in librerie organizzate in base alla release di ELS. Accedere a tale documentazione dalla pagina Tape Storage Documentation.

http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html