StorageTek SL150 Modular Tape Library

Guida per la sicurezza

E40928-03

Giugno 2015

StorageTek SL150 Modular Tape Library
Guida per la sicurezza

E40928-03

Indice

Lista delle tabelle

Prefazione

In questo documento vengono descritte le funzioni di sicurezza di StorageTek SL150 Modular Tape Library di Oracle.

Destinatari

Il presente manuale è rivolto a chiunque sia coinvolto nell'installazione e nella configurazione sicure di StorageTek SL150 Modular Tape Library di Oracle e nell'uso delle relative funzioni di sicurezza.

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

Questa sezione contiene una panoramica su StorageTek SL150 Modular Tape Library di Oracle e una descrizione dei principi generali di sicurezza correlati alla libreria a nastro.

Panoramica sul prodotto

StorageTek SL150 Modular Tape Library è una libreria a nastro automatica modulare installata in rack da 19 pollici, da 3U a 21U, di Oracle Corporation. Questa libreria offre una capacità di storage da 30 a 300 cartucce nastro LTO, da 1 a 20 unità Fibre Channel LTO o SAS e un percorso di controllo della porta Fibre o SAS dell'unità a ponte mediante una delle unità a nastro installate.

Sicurezza

Tutti i prodotti libreria a nastro sono progettati e documentati per l'uso in un ambiente server controllato senza accesso di rete generale o accesso utente. In questo modo è possibile ottenere massima funzionalità e protezione dai pericoli, sia da Internet in generale sia dall'entità interna che utilizza la libreria.

Principi di sicurezza generali

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

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. Di seguito sono elencate le versioni del firmware SL150 rilasciate a partire da aprile 2015.

Giugno 2012 v1.00 (RTA 0.1.0.0.0)
Settembre 2012 v1.03 (RTA 0.1.0.3.0)
Ottobre 2012 v1.50 (RTA 0.1.5.0.0)
Gennaio 2013 v1.82 (RTA 0.1.8.2.0)
Agosto 2013 v2.0 (RTA 0.2.0.0.0)
Ottobre 2013 v2.01(RTA 0.2.0.1.0)
Aprile 2014 v2.25 (RTA 0.2.2.5.0)
Giugno 2015 v2.50 (RTA 0.2.5.0.0)

Limitare l'accesso alla rete

Mantenere la libreria dietro un firewall nel centro dati. Il firewall garantisce che l'accesso a questi sistemi sia limitato a un percorso di rete noto, che è possibile monitorare e limitare, se necessario. Un router dotato di firewall costituisce una valida alternativa a più firewall indipendenti. Si consiglia di identificare gli host a cui è consentito collegarsi alla libreria e bloccare tutti gli altri host, se possibile.

Mantenersi aggiornati sulle ultime informazioni sulla sicurezza

Oracle apporta continui miglioramenti ai prodotti software e alla documentazione. Controllare la presenza di revisioni in questo documento a ogni release.

2

Installazione sicura

In questa sezione viene descritto il processo di pianificazione per un'installazione sicura, vengono illustrate diverse topologie di distribuzione consigliate per i sistemi e viene spiegato come proteggere la libreria.

Informazioni sull'ambiente

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

Quali risorse è necessario proteggere?

Nell'ambiente di produzione è possibile proteggere molte risorse. Identificare le risorse da proteggere quando si stabilisce il livello di sicurezza da impostare.

Da chi è necessario proteggere le risorse?

La libreria deve essere protetto da chiunque navighi su Internet e da utenti non autorizzati che utilizzano la rete Intranet.

Cosa accade in caso di mancata protezione delle risorse strategiche?

In alcuni casi, un errore in uno schema di sicurezza viene rilevato facilmente e considerato semplicemente un inconveniente. In altri casi, un errore può causare un danno grave alle società o ai singoli clienti che utilizzano la libreria. Per proteggere correttamente ogni risorsa, è necessario comprenderne le ramificazioni in termini di sicurezza.

Protezione della libreria

Per impostazione predefinita, la libreria utilizza le porte elencate in Tabella 2.1, «Porte di rete di SL150». È necessario che il firewall sia configurato in modo da consentire al traffico di utilizzare queste porte e bloccare eventuali porte non utilizzate.

Tabella 2.1. Porte di rete di SL150

Porta	Tipo	Descrizione
22	TCP	Accesso CLI SSH - in entrata con conservazione dello stato

Porta	Tipo	Descrizione
		Solo per debug e test dello sviluppo, non disponibile nel campo
25	TCP	SMTP senza autenticazione
67	DHCP	Client - in uscita
68	DHCP	Client - in entrata
80	HTTP	Porta WebLogic per interfaccia utente remota
123	NTP	NTP (Network Time Protocol) (se attivato)
161	UDP	Richieste agente libreria SNMP - in entrata con conservazione dello stato
162	UDP	Trap e notifiche informative libreria SNMP - in uscita senza conservazione dello stato per trap, in uscita con conservazione dello stato per informazioni
465	TCP	SMTP con autenticazione SSL o TLS
443	HTTPS	Porta WebLogic per interfaccia utente remota per HTTPS
546	DHCPv6	Client IPv6 DHCP - in uscita
547	DHCPv6	Client IPv6 DHCP - in entrata
33200-33500	TRACEROUTE	Uso sviluppo software

La selezione di numeri di porta validi per l'uso della libreria è riservata o consigliata per l'elenco riportato nella tabella sopra indicata. I numeri di porta validi iniziano dal numero 1 poiché 0 (zero) non è un numero di porta valido.

Quando si configura SNMP, si consiglia di utilizzare SNMPv3 anziché SNMPv2c a causa delle relative caratteristiche di riservatezza, integrità e autenticazione.

Quando si configura SMTP, si consiglia di utilizzare l'autenticazione TLS anziché SSL o nessuna opzione di autenticazione.

Configurazione dell'installazione

In questa sezione vengono indicate le modifiche alla configurazione di sicurezza da apportare durante l'installazione.

Assegnazione della password dell'utente (admin)

Alla prima accensione, sul pannello dell'operatore locale viene automaticamente eseguita una procedura di impostazione guidata in cui viene richiesto di specificare le informazioni di configurazione di base. Ciò include il nome utente e la password dell'account di amministratore, le impostazioni di rete e altre impostazioni di base.

La libreria potrà diventare operativa solo una volta completata la procedura di impostazione guidata.

Con la spedizione del prodotto viene fornito un account di login che dovrà essere specificato dal programma di installazione come primo passo della routine di impostazione guidata.

Prima del completamento della procedura di impostazione guidata, l'utente deve immettere una nuova password.

Quando la procedura di impostazione iniziale è stata completata e la libreria è pronta, è possibile eseguire ulteriori modifiche a tutte le impostazioni di configurazione della libreria mediante l'interfaccia utente del browser (BUI).

Applicare la gestione delle password

È necessario applicare a tutte le password le regole base per la gestione delle password, come la lunghezza, la cronologia e la complessità della password. Le password di SL150 devono essere composte da un numero di caratteri compreso tra 8 e 128 e devono contenere almeno un carattere numerico o speciale. La password predefinita deve essere modificata durante l'installazione e non può essere riutilizzata.

Nota:

Il numero di caratteri che appaiano mascherati non indica il numero esatto di caratteri immessi.

Autenticazione dell'interfaccia utente del browser

Limitare le impostazioni del browser utilizzate per accedere all'interfaccia utente remota per continuare a usare TLS 1.0 o versione successiva e limitare l'uso di CVE-2014-3566 per i livelli di firmware inferiori alla versione 2.50. Nella versione 2.50 non verrà eseguita la negoziazione automatica del firmware della libreria fino al livello SSLv3.

3

Funzioni di sicurezza

In questa sezione vengono descritti i meccanismi di sicurezza specifici offerti dal prodotto.

Per la protezione della libreria, è disponibile un firewall interno. La protezione della libreria non dovrebbe essere affidata solo a questa misura di sicurezza. Si consiglia di posizionare la libreria all'interno di un centro dati protetto fisicamente in una rete protetta che consenta l'accesso solo ai server che ne utilizzano la funzionalità. Anche i server e le applicazioni in esecuzione su di esse devono essere protetti.

È necessario limitare gli account utente al ruolo di livello *operatore* anziché concedere a tutti gli utenti il ruolo di livello *amministratore*. L'uso del ruolo utente di *servizio* appropriato deve essere individuato con la pratica. Creare, abilitare o disabilitare gli account del ruolo utente di *servizio* in base alle proprie esigenze. I ruoli utente di servizio prevedono privilegi maggiori rispetto al ruolo *operatore*, quasi pari ai livelli di autorizzazione del ruolo *amministratore*.

Se è necessaria una cronologia dell'attività della libreria a scopo di analisi, è possibile esaminare ed esportare il "log attività" per eseguire un'analisi più approfondita. Il log attività disponibile nell'interfaccia utente può indicare i login dell'utente e le azioni avviate dall'host o dall'interfaccia utente per la registrazione.

4

Ridistribuzione

In questa sezione viene descritto come ripristinare lo stato predefinito di fabbrica della libreria per cancellare i dati dei clienti.

Nel caso in cui il cliente debba decommissionare una libreria, è disponibile una procedura che consente di rimuovere tutte le informazioni di configurazione del cliente e tutti i file di log e di ripristinare lo stato predefinito di fabbrica della libreria. Per richiamare questa procedura, impostare la libreria in modalità di individuazione, quindi tenere premuti contemporaneamente i pulsanti di individuazione anteriore e posteriore per più di 10 secondi, quindi rilasciare entrambi i pulsanti.

Il tempo sufficiente per rilasciare il pulsante di individuazione è indicato dal cambiamento della frequenza di lampeggiamento del LED luminoso da lenta a rapida.

Appendice A

Elenco di controllo per la distribuzione sicura

L'elenco di controllo di sicurezza riportato di seguito include linee guida per la protezione della libreria.

1. Applicare la gestione delle password per tutti gli account utente.
2. Applicare i controlli dell'accesso, utilizzando sia la prossimità fisica che interfacce quali SCSI, interfaccia utente, SNMP e così via.
3. Limitare l'accesso alla rete.
   a. È necessario che sia implementato un firewall.
   b. È necessario che il firewall funzioni correttamente.
   c. È necessario monitorare l'accesso al sistema.
   d. È necessario controllare gli indirizzi IP di rete.
   e. I servizi possono disporre di strumenti che richiedono password appropriate o controlli dell'accesso monitorati, ad esempio SDP-2 per consentire il download automatico delle informazioni di log o un altro tipo di accesso.
4. Se vengono rilevati punti di vulnerabilità nelle librerie a nastro Oracle, contattare Oracle Services, Oracle Tape Library Engineering o il rappresentante dell'account.
5. SMTP deve utilizzare TLS anziché protocolli secondari quali SSL oppure nessuno.
6. SNMP deve essere impostato con il livello V3 anziché V2C o funzionalità secondarie.

Appendice B

Riferimenti

SL150 User Guide disponibile all'indirizzo:

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

Tutta la documentazione relativa a SL150 è disponibile nel set di documenti in linea con il numero parte E35103-07.