

StorageTek T10000D

Guida per la sicurezza

E50327-04

Agosto 2016

StorageTek T1000D

Guida per la sicurezza

E50327-04

copyright © 2014-2016, 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	7
Destinatari	7
Accesso facilitato alla documentazione	7
1. Panoramica	9
Panoramica sul prodotto	9
Capacità e prestazioni di T10000D	9
Sicurezza	9
Principi di sicurezza generali	9
Mantenere il software aggiornato	10
Limitare l'accesso alla rete	10
Mantenersi aggiornati sulle ultime informazioni sulla sicurezza	10
2. Installazione sicura	11
Informazioni sull'ambiente	11
Quali risorse è necessario proteggere?	11
Da chi è necessario proteggere le risorse?	11
Cosa accade in caso di mancata protezione delle risorse strategiche?	11
Protezione dell'unità nastro	11
Installazione dell'applicazione Virtual Operator Panel (VOP)	12
Configurazione dopo l'installazione	12
Assegnazione della password dell'utente (admin)	12
Applicazione della gestione delle password	13
3. Funzioni di sicurezza	15
A. Elenco di controllo per la distribuzione sicura	17
B. Riferimenti	19

Lista delle tabelle

2.1. Porte di rete utilizzate	11
-------------------------------------	----

Prefazione

In questo documento vengono descritte le funzioni di sicurezza di StorageTek T10000D di Oracle.

Destinatari

Il presente manuale è rivolto a chiunque sia coinvolto nell'uso delle funzioni di sicurezza nonché nell'installazione e configurazione sicure di StorageTek T10000D.

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

Questa sezione contiene una panoramica sulle unità nastro StorageTek T10000D e una descrizione dei principi generali di sicurezza correlati.

Panoramica sul prodotto

La famiglia di unità nastro Enterprise T10000D supporta sia la tecnologia SCSI su protocollo Fibre Channel per sistemi aperti sia la tecnologia mainframe su protocollo FICON. Le unità nastro T10000D trasferiscono i dati verso e da un host e li memorizzano su un supporto magnetico removibile. Le unità nastro T10000D intendono innanzitutto fornire funzionalità di elevata affidabilità, backup ad alta capacità, archiviazione ed elaborazione dati per clienti aziendali che richiedono elevato duty cycle e affidabilità. Il prodotto offre la cifratura dei dati opzionale. Il cliente può decidere se abilitare o meno la funzione di cifratura. Il prodotto unità nastro è stato migliorato in termini di capacità e velocità del nastro nativo. Nel corso delle diverse release sono state inoltre aggiunte funzioni di gestione dei dati.

Capacità e prestazioni di T10000D

L'unità nastro T10000D ha una capacità pari a 8,5 TB e una velocità del nastro nativo di 252 MB al secondo.

Sicurezza

L'unità nastro T10000D è progettata e documentata per l'uso in un ambiente hardware controllato. Le unità nastro si trovano sempre all'interno di un centro dati controllato e in genere sono posizionate all'interno di una libreria a nastro. In alcuni rari casi il cliente utilizza una versione con installazione in rack. Il centro dati controllato si trova a sua volta in un firewall protetto dalle norme di sicurezza del cliente. In questo modo è possibile ottenere la massima funzionalità e protezione dai pericoli, sia da Internet in generale sia dall'entità interna che utilizza l'unità nastro.

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. Questo documento riguarda i seguenti livelli software:

T10000D 4.XX.1XX

Limitare l'accesso alla rete

Mantenere l'unità nastro 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 all'unità nastro 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.

Capitolo 2. Installazione sicura

In questa sezione viene descritto il processo di pianificazione e implementazione per un'installazione e una configurazione sicure, vengono illustrate diverse topologie di distribuzione consigliate per i sistemi e viene spiegato come proteggere una libreria a nastro.

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?

L'unità nastro deve essere protetta da chiunque navighi su Internet. Stabilire tuttavia se l'unità nastro deve essere protetta anche dai dipendenti che utilizzano la rete Intranet aziendale.

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 l'unità nastro. Per proteggere correttamente ogni risorsa, è necessario comprenderne le ramificazioni in termini di sicurezza.

Protezione dell'unità nastro

Per impostazione predefinita, l'unità nastro utilizza le porte elencate nella tabella riportata di seguito. È necessario che il firewall sia configurato in modo da consentire al traffico di utilizzare queste porte e bloccare eventuali porte non utilizzate. Le unità nastro supportano IPv6 e IPv4.

Tabella 2.1. Porte di rete utilizzate

Porta	T10000D
22 tcp - SSH VOP	X

Porta	T10000D
22 tcp - SFTP	X
161 udp - richieste agente unità nastro SNMPV1 - in entrata con conservazione dello stato	X
162 udp - notifiche informative e di interrupt unità nastro SNMPV1 - in uscita senza conservazione dello stato per interrupt, in uscita con conservazione dello stato per informazioni	X
23 tcp - TELNET	
21 tcp - FTP	
9842 tcp - EPT	
3331 OKM - servizio challenge e root CA	X
3332 OKM - Iscrizione. Energia cibernetica: AES256	X
3334 OKM - Cambio chiave di cifratura. Energia cibernetica: AES256	X
3335 OKM - Ricerca automatica cluster. Energia cibernetica: AES256	X

Le porte 21 e 23 saranno disabilitate per i clienti per T10000D. Se un cliente richiede l'accesso tramite TELNET o FTP non protetto, o entrambi, è disponibile un'opzione di configurazione di VOP.

Installazione dell'applicazione Virtual Operator Panel (VOP)

VOP deve essere installato solo nei sistemi inclusi nella stessa infrastruttura di rete protetta dell'unità nastro. Per garantire un accesso limitato all'unità nastro, applicare i controlli dell'accesso del cliente ai sistemi in cui è installato VOP. Per un elenco delle porte utilizzate da VOP, vedere [Tabella 2.1, «Porte di rete utilizzate»](#).

Per istruzioni sull'installazione di VOP per l'avvio Web, consultare il manuale dell'utente riportato di seguito.

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

Configurazione dopo l'installazione

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

Assegnazione della password dell'utente (admin)

La password dell'account admin del cliente deve essere modificata dal cliente sul sito ed è di proprietà del cliente. La sicurezza della password è conforme agli standard Oracle. È disponibile un numero infinito di password da utilizzare durante il ciclo di vita dell'unità nastro. Se si dimentica la password dell'account admin, è possibile reimpostarla. La prima password è la password predefinita inviata con l'unità nastro.

Applicazione della gestione delle password

È necessario applicare alla password dell'amministratore le regole base per la gestione delle password, come la lunghezza e la complessità della password.

Le regole di gestione delle password richiedono l'applicazione di almeno una delle regole elencate di seguito.

- Deve essere composta da 8 - 16 caratteri
- Deve includere caratteri minuscoli (a-z)
- Deve includere caratteri maiuscoli (A-Z)
- Deve includere cifre decimali (0-9)
- Deve includere caratteri speciali (.?;"'{}[])!@#\$%&, ...)

Capitolo 3. Funzioni di sicurezza

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

L'unità nastro T10000D comunica su un canale sicuro con Oracle Key Management System. L'unità nastro T10000D comunica tramite SSH e SFTP con Virtual Operator Panel, mentre TELNET e FTP rimarranno disabilitati per i clienti. La protezione dell'unità nastro non dovrebbe essere affidata solo a questa misura di sicurezza. In teoria, le unità nastro dovrebbero trovarsi in un centro dati protetto fisicamente e dotato anche di 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. Il cliente, inoltre, può innalzare il livello di sicurezza dell'unità nastro. Una delle opzioni disponibili è la cifratura dei dati.

Appendice A

Appendice A. Elenco di controllo per la distribuzione sicura

L'elenco di controllo di sicurezza riportato di seguito include linee guida per la protezione dell'unità nastro.

1. Applicare la gestione delle password.
2. Applicare i controlli dell'accesso.
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.
4. Se vengono rilevati punti di vulnerabilità nelle unità nastro Oracle, contattare Oracle Services, Oracle Tape Library Engineering o il rappresentante dell'account.

Appendice B

Appendice B. Riferimenti

È possibile accedere al manuale dell'utente di VOP al seguente indirizzo:

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