

GUI di StorageTek Virtual Storage Manager

Guida per la sicurezza

E79970-01

Luglio 2016

GUI di StorageTek Virtual Storage Manager

Guida per la sicurezza

E79970-01

copyright © 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	5
Destinatari	5
Accessibilità alla documentazione	5
1. Panoramica	7
Panoramica sul prodotto	7
Sicurezza	7
Principi di sicurezza generali	7
Mantenere il software aggiornato	7
Limitare l'accesso alla rete	8
Mantenersi aggiornati sulle ultime informazioni sulla sicurezza	8
2. Installazione sicura	9
Informazioni sull'ambiente	9
Quali risorse è necessario proteggere?	9
Da chi è necessario proteggere le risorse?	9
Cosa accade in caso di mancata protezione delle risorse strategiche?	9
Installazione della GUI di StorageTek VSM	9
Configurazione dopo l'installazione	10
Assegnazione della password dell'utente (admin)	10
Applicazione della gestione delle password	10
3. Funzioni di sicurezza	11
A. Elenco di controllo per la distribuzione sicura	13
B. Riferimenti	15

Prefazione

In questo documento vengono descritte le funzioni di sicurezza della GUI di StorageTek Virtual Storage Manager di Oracle.

Destinatari

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

Accessibilità alla documentazione

Per informazioni sull'impegno di Oracle per l'accessibilità, visitare il sito Web Oracle Accessibility Program all'indirizzo <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Accesso al supporto Oracle

I clienti Oracle che hanno acquistato il servizio di supporto tecnico hanno accesso al supporto elettronico attraverso il portale Oracle My Oracle Support. Per tutte le necessarie informazioni, si prega di visitare il sito <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> oppure <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> per clienti non utenti.

Capitolo 1. Panoramica

Questa sezione contiene una panoramica sulla GUI di StorageTek Storage Manager (VSM) e una descrizione dei principi generali di sicurezza correlati.

Panoramica sul prodotto

La GUI di StorageTek VSM è un prodotto software Oracle che fornisce ai clienti funzioni di reporting e controllo di nastri virtuali per monitorare e gestire in modo efficiente e proattivo le operazioni su nastri virtuali del centro dati.

La GUI di VSM supporta i clienti di ambienti su nastro Enterprise MVS Virtual Storage Manager (VSM) e i clienti che dispongono di tutte le generazioni supportate dei prodotti VSM.

Sicurezza

Fisica

È necessario che la GUI di VSM venga installata su una macchina virtuale di un server Oracle VM o VMware del cliente all'interno del centro dati dell'organizzazione. L'accesso fisico al server sarà regolamentato dai criteri in uso nella società del cliente.

Rete

È necessario che la GUI di VSM venga aggiunta o configurata in una rete interna del cliente protetta da firewall. Questa rete deve disporre dell'accesso TCP/IP a tutte le istanze del server HTTP SMC che generano report sulle risorse dei nastri virtuali.

Accesso dell'utente

L'accesso all'applicazione GUI di VSM è controllato dall'autenticazione tramite nome utente e password. L'autenticazione del nome utente e della password viene eseguita mediante la configurazione dell'applicazione al servizio LDAP dell'utente.

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:

GUI di VSM Release 1.1; luglio 2016

Nota:

La GUI di VSM supporta ELS 7.1, ELS 7.2 e ELS 7.3 e richiede l'applicazione degli ultimi aggiornamenti di manutenzione.

Limitare l'accesso alla rete

Mantenere il server host VSM GUI 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.

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. Problemi specifici correlati alla sicurezza potrebbero essere affrontati anche nelle note di rilascio.

Capitolo 2. Installazione sicura

In questa sezione viene descritto il processo di pianificazione per un'installazione sicura e vengono illustrate diverse topologie di distribuzione consigliate per i sistemi. Nel Manuale dell'utente della GUI di VSM 1.0 vengono descritte in dettaglio le operazioni di installazione, configurazione e amministrazione.

Informazioni sull'ambiente

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

Quali risorse è necessario proteggere?

Per la GUI di VSM è necessario proteggere il server host e la rete associata da qualsiasi accesso non autorizzato.

Da chi è necessario proteggere le risorse?

La GUI di VSM deve essere protetta da chiunque navighi su Internet, da utenti esterni e da utenti interni non autorizzati.

Cosa accade in caso di mancata protezione delle risorse strategiche?

Poiché la GUI di VSM è un'applicazione per il monitoraggio e l'uso di risorse di archiviazione virtuali, l'accesso non autorizzato ad essa può influire sulla disponibilità delle risorse VSM. Lo stato di una risorsa potrebbe essere interessato, ma non i dati delle risorse di archiviazione.

Installazione della GUI di StorageTek VSM

La GUI di VSM deve essere installata solo sui sistemi che si trovano nella stessa infrastruttura di rete protetta (con firewall) delle risorse virtuali monitorate, ovvero VTCS e HSC. Per assicurare che l'accesso all'applicazione sia limitato, applicare i controlli dell'accesso del cliente ai sistemi in cui è installata la GUI di VSM.

Per istruzioni sull'installazione, consultare il *Manuale dell'utente della GUI di VSM*.

Configurazione dopo l'installazione

Non sono previste modifiche alla sicurezza della configurazione da apportare dopo l'installazione. La configurazione viene definita dal cliente durante l'installazione.

Assegnazione della password dell'utente (admin)

La password dell'account di amministrazione del cliente viene impostata dal cliente durante l'installazione.

Applicazione della gestione delle password

È necessario applicare alla password dell'amministratore le regole di gestione delle password aziendali del cliente, come la lunghezza, la cronologia e la complessità della password.

Capitolo 3. Funzioni di sicurezza

In questa sezione vengono descritti i meccanismi di sicurezza specifici offerti dal prodotto. L'applicazione GUI di VSM fornisce agli utenti ruoli con password cifrate per proteggere se stessa. La protezione dell'applicazione non viene affidata solo a questa misura di sicurezza. L'applicazione dovrebbe trovarsi in un centro dati protetto fisicamente e dotato anche di una rete protetta che consenta l'accesso solo agli utenti autorizzati.

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 della libreria.

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 nella GUI di VSM, contattare Oracle Security Products.

Appendice B

Appendice B. Riferimenti

Manuale dell'utente della GUI di VSM

