StorageTek Automated Cartridge System Library Software

Guida per la sicurezza

Release 8.4

E68248-01

Settembre 2015

ORACLE

StorageTek Automated Cartridge System Library Software
Guida per la sicurezza

E68248-01

Indice

Prefazione

In questo documento vengono descritte le funzioni di sicurezza di StorageTek Automated Cartridge System Library Software (ACSLS) e della soluzione ACSLS High Availability (ACSLS HA) di Oracle. Poiché anche ACSLS HA e ACSLS SNMP Agent vengono eseguiti sul server ACSLS, la protezione del server ACSLS implica anche la protezione di ACSLS, ACSLS HA e ACSLS SNMP Agent.

Destinatari

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

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 di ACSLS e vengono descritti i principi generali della sicurezza dell'applicazione.

Nota:

Nel presente documento il prodotto Automated Cartridge System Library Software viene denominato ACSLS, mentre la soluzione ASLS High Availability viene denominata ACSLS HA.

Panoramica del prodotto

ACSLS è il software per server della libreria a nastro di Oracle che controlla una o più librerie a nastro StorageTek per i client dei sistemi aperti. Un sistema di cartucce automatico (ACS, Automated Cartridge System) è una libreria a nastro o un gruppo di librerie a nastro collegate tramite porte pass-thru (PTP, Pass-Thru-Port). ACSLS gestisce uno o più ACS tramite comandi del percorso di controllo inviati in una rete. Il software include un componente di amministrazione del sistema, interfacce per le applicazioni dei sistemi client e funzionalità per la gestione delle librerie.

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. Nel presente documento si presuppone che l'utente utilizzi ACSLS 8.4 o release successive, con tutte le operazioni di manutenzione rilevanti effettuate. L'esecuzione dell'ultima release di ACSLS garantisce la disponibilità dei miglioramenti e delle correzioni più aggiornati.

Applicare tutte le patch di sicurezza significative al sistema operativo e ai servizi installati con il sistema operativo. Applicare tali patch in modo selettivo, in quanto l'applicazione di tutti gli aggiornamenti disponibili potrebbe determinare l'installazione di nuove funzioni e anche di nuove release del sistema operativo non testate con ACSLS e ACSLS HA.

Limitazione dell'accesso di rete ai servizi di importanza critica

Proteggere con un firewall sia ACSLS che le librerie che gestisce. È consigliabile utilizzare una rete privata per le comunicazioni TCP/IP tra ACSLS e le librerie a nastro.

Principio di privilegio minimo

Il principio di privilegio minimo richiede che agli utenti venga assegnata la minore quantità di privilegi per eseguire le operazioni. I privilegi dell'utente devono essere verificati periodicamente per stabilire l'importanza delle responsabilità del lavoro corrente.

In ACSLS questo significa che gli operatori che emettono solo comandi di routine utilizzando cmd_proc devono effettuare il login come utente acssa. Gli amministratori di sistema che effettuano il login come utente acsss devono anche avere accesso a una gamma più vasta di utility e comandi di configurazione. L'uso dell'ID utente acsdb non è necessario per le operazioni normali.

Monitoraggio dell'attività di sistema

La sicurezza del sistema si basa su tre elementi: protocolli di sicurezza validi, configurazione di sistema appropriata e monitoraggio del sistema. Il controllo e l'analisi dei record di controllo soddisfano il terzo requisito. Ciascun componente all'interno di un sistema prevede qualche tipo di funzionalità di monitoraggio. Seguire l'avviso di controllo nel presente documento e monitorare i record di controllo a intervalli regolari

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 e implementazione per un'installazione e una configurazione sicure e vengono illustrate topologie di distribuzione consigliate per ACSLS.

Informazioni sull'ambiente

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

Quali risorse è necessario proteggere?

Le risorse chiave gestite da ACSLS sono librerie a nastro, unità e cartucce. Tali risorse devono essere protette da accessi accidentali o dannosi. È possibile, ad esempio, impedire alle persone di accedere per errore a un server ACSLS diverso da quello desiderato utilizzando password diverse per gli ID utente ACSLS su server diversi.

Da chi è necessario proteggere le risorse?

È possibile proteggere le risorse di storage su nastro dall'accesso non autorizzato sia interno che esterno.

Cosa accade in caso di mancata protezione delle risorse strategiche?

ACSLS può installare le cartucce nelle unità nastro. Se un utente riesce a collegarsi all'unità nastro tramite il percorso dati, potrà leggere i dati sul nastro, se non sono cifrati.

Gli utenti che possono accedere sia ad ACSLS che a una libreria a nastro possono inserire ed espellere le cartucce da una libreria a nastro.

Procedura consigliata per la protezione di ACSLS

Quando si protegge ACSLS e i componenti dell'infrastruttura necessari, seguire questa procedura per accertarsi che ACSLS continui a funzionare dopo avere apportato le modifiche.

- Installare ACSLS.

- Verificare che ACSLS funzioni correttamente. Includere configurazione e controllo delle librerie, installazione e disinstallazione di nastri, inserimento ed espulsione di nastri, nonché backup e ripristino del database.
- Implementare le modifiche per aumentare la sicurezza.
- Verificare che ACSLS funzioni ancora correttamente.

Protezione della comunicazione via Internet di ACSLS

In questa sezione vengono forniti consigli per la distribuzione di ACSLS per un accesso a Internet sicuro.

Protezione di ACSLS e delle librerie a nastro tramite un firewall aziendale

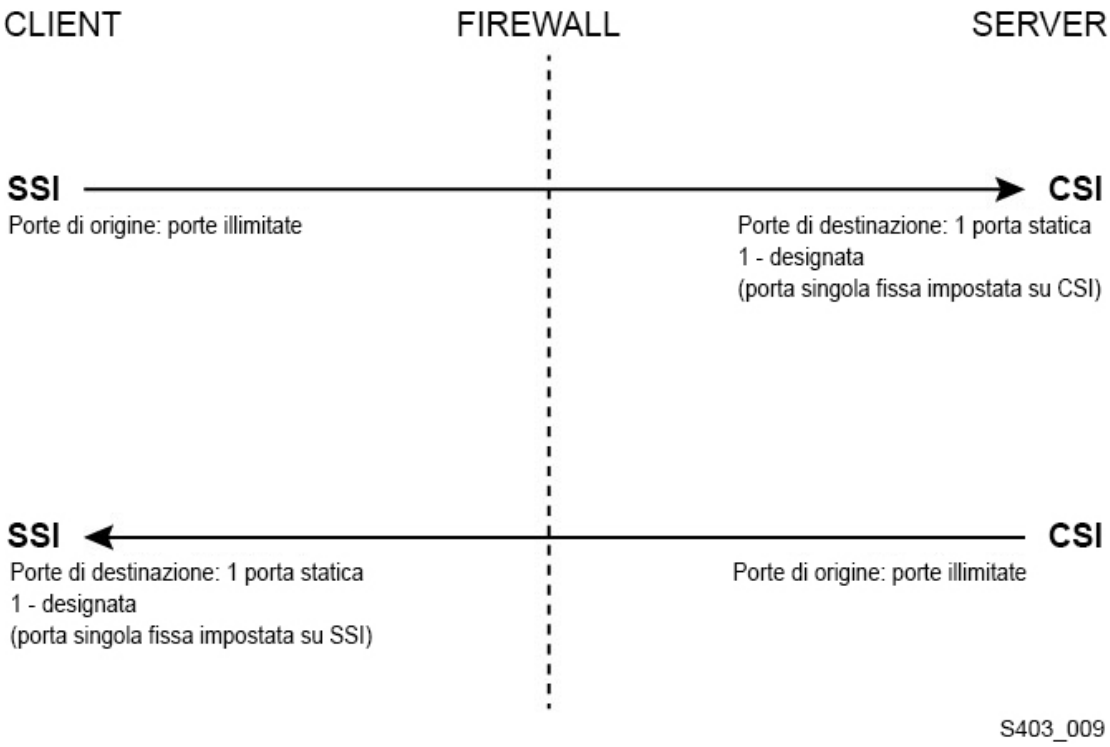
ACSLS e le librerie a nastro che supporta devono essere distribuiti tramite il firewall aziendale. Le persone che lavorano in remoto possono effettuare il login al server ACSLS tramite una VPN.

Nota:

Se si dispone di un firewall perimetrale basato su IPv4, è necessario configurarlo in modo che escluda tutti i pacchetti IPv4 del protocollo 41 in uscita e i pacchetti UDP della porta 3544 per impedire agli host Internet di utilizzare il traffico in tunnelling IPv6 su IPv4 per raggiungere gli host interni.

Opzione di sicurezza del firewall ACSLS

Se le applicazioni client, che utilizzano ACSLS per l'installazione dei nastri e la gestione delle librerie a nastro, sono separate da ACSLS tramite un firewall, è consigliabile abilitare l'opzione di sicurezza del firewall. Anche se le applicazioni client non sono separate da ACSLS tramite un firewall, l'implementazione dell'opzione di sicurezza del firewall offre ulteriore sicurezza ACSLS limitando le porte utilizzate per la comunicazione tra ACSLS e le relative applicazioni client, come mostrato di seguito. Per questi motivi, in ACSLS 8.1 e release successive la variabile statica CSI_FIREWALL_SECURE viene impostata automaticamente su TRUE.



Per informazioni dettagliate, consultare l'appendice ”Firewall Security Option” nel manuale *ACSLS Administrator's Guide*.

Porte Ethernet utilizzate per la comunicazione con ACSLS

- Le porte indicate di seguito vengono utilizzate nel server ACSLS. Assicurarsi che tutti i firewall siano configurati in modo da consentire il traffico su queste porte. Sono inclusi i firewall implementati da ipfilter su Solaris o iptables su Linux.
  - 22: utilizzata in entrambe le direzioni per l'accesso tramite ssh.
  - 111: portmapper, a meno che portmapper non sia stato disabilitato.
  - 115: utilizzata per SFTP (Secure File Transfer Protocol).
  - 161: porta predefinita per l'agente SNMP di ACSLS - preparazione/configurazione/funzionamento.
  - 162: porta predefinita per l'agente SNMP di ACSLS - trap.

    Nota:

    Le porte utilizzate dall'agente SNMP di ACSLS sono configurabili tramite il comando: *`AcslsAgtdSnmpConf [ -p port ] [-t trap port] [-d]`*. L'opzione *`-d`* visualizza l'impostazione corrente. Dopo avere modificato l'impostazione della porta, è necessario riavviare l'agente con il comando *`agentRegister`*.
  - La porta predefinita 5432 per la comunicazione interna da ACSLS al database PostgreSQL (la variabile di ambiente PGPORT per l'ID utente acsss).

Se la porta 5432 è occupata, viene utilizzato il successivo numero di porta superiore disponibile.

> **Nota:**
>
> La porta 5432 deve essere accessibile solo dall'IP localhost (127.0.0.1).

  - 7001 e 7002: utilizzata da WebLogic e dalla GUI di ACSLS.
  - 30031 o la porta di ascolto del CSI di ACSLS, impostata da CSI_INET_PORT.
  - 50003: porta utilizzata per la comunicazione interna dalla GUI di ACSLS e dai componenti Java all'elaborazione ACSLS precedente. Non è configurabile.

- Affinché le applicazioni client possano comunicare con ACSLS tramite ACSAPI, è necessario che le porte indicate di seguito siano aperte.
  - L'applicazione client deve comunicare con la porta di ascolto del CSI di ACSLS. Viene impostata automaticamente la porta predefinita 30031 tramite la variabile statica CSI _INET_PORT.

    È possibile scoprire le porte utilizzate da ACSLS per l'ascolto delle richieste dei client ACSAPI con il seguente comando della shell Unix:

    ```
    rpcinfo -p | egrep "300031 | 536871166"
    ```

    Gli ID delle porte vengono elencati nell'ultimo campo visualizzato.
  - Il client ACSAPI (ad esempio, un server NetBackup o SAM-QFS) imposta la propria porta in entrata fissa utilizzando la variabile di ambiente SSI_INET_PORT. Specificare una porta compresa tra 1024 e 65535, escludendo le porte 50001 e 50004. È necessario che il server ACSLS possa comunicare con questa porta.

    > **Nota:**
    >
    > In un server client ACSAPI le porte 50001 e 50004 vengono utilizzate per la comunicazione IPC del dominio AF_INET con il mini-Logger eventi e dalle applicazioni client all'SSI.

  Per maggiori dettagli sulla comunicazione tra le applicazioni client e ACSLS, consultare l'appendice sull'opzione di sicurezza del firewall nel manuale *ACSLS Administrator's Guide*.

- Se è installato il componente XAPI, il server XAPI utilizza una porta di ascolto fissa per ricevere le richieste TCP in ingresso dai client ELS. La porta di ascolto XAPI è definita dalla variabile statica XAPI_PORT. Il valore predefinito di XAPI_PORT è 50020. Il valore deve essere compreso tra 1024 e 65535 e non può essere in conflitto con alcuna altra porta utilizzata da ACSLS o da altre applicazioni.

  Per maggiori dettagli sulla variabile XAPI_PORT, consultare l'appendice sull'interfaccia client di XAPI Client nel manuale *ACSLS Adiminstrator's Guide*. Questa appendice contiene anche dettagli su come visualizzare e impostare la variabile statica XAPI_PORT.

- Porte che devono essere aperte in una libreria SL8500 o SL3000:

  ACSLS comunica con queste porte sulle connessioni Ethernet 2A e 2B di una libreria SL8500 o SL3000. Se la comunicazione da ACSLS a queste porte è bloccata, ACSLS non può gestire la libreria.
  - 50001: utilizzata per tutte le normali comunicazioni tra ACSLS e la libreria.
  - 50002: utilizzata da ACSLS HA per determinare se il nodo HA alternativo può comunicare con la libreria prima del failover del nodo alternativo.

Configurazione dei firewall sul server ACSLS

Oltre ai firewall esterni, la protezione del firewall può essere implementata sul server ACSLS tramite ipfilter su Solaris o tramite iptables su Linux. Di seguito viene descritto come gestire tali firewall in esecuzione sul server ACSLS.

- Gestione di ipfilter su Solaris:

  Per informazioni dettagliate, consultare le pagine man per ipf e ipfilter.
  - Il firewall ipfilter viene abilitato (disabilitato) dall'utente 'root' mediante il comando:

    ```
    svcadm enable ipfilter (svcadm disable ipfilter)
    ```
  - Per apprendere lo stato corrente di ipfilter:

    ```
    svcs ipfilter
    ```
  - I criteri del firewall sono definiti nel file: /etc/ipf/ipf.conf

    Per consentire una comunicazione libera tra i componenti nell'host locale (ad esempio, tra ACSLS e WebLogic o tra la GUI e il database ACSLS), includere un'istruzione come la seguente:

    ```
    pass in quick from 127.0.0.1 to 127.0.0.1
    ```

    oppure

    ```
    pass in quick from 127.0.0.1 to all
    ```

    È necessario definire criteri che consentano l'accesso a tutte le porte necessarie per ACSLS. Per includere un criterio che consenta ai browser remoti basati sul Web di accedere alla GUI di ACSLS, ad esempio, è necessario aprire le porte 7001 e 7002.

    ```
    pass in quick from any to any port = 7001

    pass in quick from any to any port = 7002
    ```

    Dopo avere rilevato le porte utilizzate da ACSLS per l'ascolto delle richieste dei client ACSAPI, aggiungere le istruzioni 'pass in quick' per ciascuna di queste porte.

Potrebbe essere necessario includere un'istruzione 'pass in quick' per la porta portmapper RPC 111.

L'ultima istruzione nel set di regole proposto, "block in from any", afferma che nessun traffico deve raggiungere l'host, a meno che non sia stato consentito in modo specifico nelle istruzioni precedenti.

- Gestione di iptables su Linux:
  - Il firewall iptables viene abilitato (disabilitato) dall'utente 'root' mediante il comando:

    ```
    service iptables start (service iptables stop)
    ```
  - Per controllare lo stato di iptables:

    ```
    service iptables status
    ```
  - Il file dei criteri per iptables è /etc/sysconfig/iptables:

    È necessario definire criteri che consentano l'accesso a tutte le porte necessarie per ACSLS. Per includere un criterio che consenta l'accesso remoto tramite http/https alla GUI di ACSLS, ad esempio, è necessario aggiornare tale file in modo che includa le eccezioni per le porte 7001 e 7002 utilizzando istruzioni simili alle seguenti:

    ```
    -A input -p tcp --dport 7001 -j ACCEPT
    ```

    ```
    -A input -p tcp --dport 7002 -j ACCEPT
    ```

    Dopo avere rilevato le porte utilizzate da ACSLS per l'ascolto delle richieste dei client ACSAPI, è necessario aggiungere le eccezioni per ciascuno dei file dei criteri di iptables. Potrebbe essere necessario includere un'istruzione di eccezione per la porta portmapper RPC 111.

Installazione e configurazione di Solaris

In questa sezione viene descritto come installare e configurare Solaris in modo sicuro.

Di seguito sono riportati alcuni suggerimenti.

- Applicare tutte le patch di sicurezza significative al sistema operativo e ai servizi installati con il sistema operativo. Applicare tali patch in modo selettivo, in quanto l'applicazione di tutti gli aggiornamenti disponibili potrebbe determinare l'installazione di nuove funzioni e anche di nuove release del sistema operativo non testate con ACSLS e ACSLS HA.
- Disabilitare telnet e rlogin. Utilizzare piuttosto ssh. Disabilitare anche ftp e utilizzare sftp.

  Disabilitare i servizi telnet, rlogin e ftp emettendo i comandi indicati di seguito come utente root.

  Per visualizzare tutti i servizi:

  ```
  svcs
  ```

Per disabilitare telnet, rlogin e ftp:

```
svcadm disable telnet

svcadm disable rlogin

svcadm disable ftp
```

- Non disabilitare ssh. Si desidera che gli utenti effettuino il login in remoto ad ACSLS utilizzando ssh e non telnet o rlogin. Non disabilitare sftp.
- ACSLS richiede rpc-bind. Non disabilitarlo.

  Se Solaris è installato con l'opzione di protezione predefinita, è necessario modificare la proprietà di configurazione di una rete per rpc-bind per consentire ai client ACSAPI di inviare richieste ad ACSLS.

  Per informazioni dettagliate, consultare la sezione "Installing Solaris" nel capitolo "Installing ACSLS on Solaris" del manuale *ACSLS Installation manual*.
- Per la comunicazione con ACSLS, è necessario che alcune porte Ethernet sul server ACSLS siano aperte. Le applicazioni client utilizzano porte Ethernet specifiche per la comunicazione con ACSLS e ACSLS comunica con porte specifiche sulle librerie a nastro. Per informazioni sulle porte che devono essere disponibili per la comunicazione con ACSLS, vedere Porte Ethernet utilizzate per la comunicazione con ACSLS. Sul server ACSLS accertarsi che ipfilter sia configurato in modo da consentire il traffico alle porte utilizzate da ACSLS.

Determinare i criteri di controllo di Solaris. Per informazioni su quali eventi pianificare per il controllo, dove salvare i log di controllo e come esaminarli, consultare la sezione ”Auditing in Oracle Solaris” in "Oracle System Administration: Security Services".

Installazione e configurazione di Linux

Di seguito sono riportati alcuni suggerimenti per l'installazione e la configurazione sicure di Linux.

- Applicare tutte le patch di sicurezza significative al sistema operativo e ai servizi installati con il sistema operativo. Applicare tali patch in modo selettivo, in quanto l'applicazione di tutti gli aggiornamenti disponibili potrebbe determinare l'installazione di nuove funzioni e anche di nuove release del sistema operativo non testate con ACSLS e ACSLS HA.
- Assicurarsi che telnet e rlogin non siano installati o disabilitati. Utilizzare piuttosto ssh.

  Assicurarsi anche che ftp non sia installato o disabilitato e utilizzare sftp.

  Per visualizzare tutti i servizi, effettuare il login come utente root e immettere:

  ```
  service –-status-all
  ```
- Per eliminare definitivamente i servizi, utilizzare:

```
svccfg delete -f service-name
```

- Non disabilitare ssh. Si desidera che gli utenti effettuino il login in remoto ad ACSLS utilizzando ssh, non telnet né rlogin. Non disabilitare sftp.
- Per consentire la comunicazione con il client ACSLS, è necessario che i servizi di rete siano abilitati, in particolare rpcbind.

  Quando si avvia rpc su Linux, utilizzare il flag –i.
- Per la comunicazione con ACSLS, è necessario che alcune porte Ethernet sul server ACSLS siano aperte. Le applicazioni client utilizzano porte Ethernet specifiche per la comunicazione con ACSLS e ACSLS comunica con porte specifiche sulle librerie a nastro. Per informazioni sulle porte che devono essere disponibili per la comunicazione con ACSLS, vedere Porte Ethernet utilizzate per la comunicazione con ACSLS. Sul server ACSLS accertarsi che iptables sia configurato in modo da consentire il traffico alle porte utilizzate da ACSLS.

Controllo della sicurezza di Linux

Determinare i criteri di controllo di Linux. Per informazioni su quali eventi pianificare per il controllo, dove salvare i log di controllo e come esaminarli, consultare la sezione ”Configuring and Using Auditing” section in *Oracle Linux: Security Guide for Release 6*.

Di seguito sono riportati alcuni log e comandi utili per il controllo della sicurezza di Linux.

- Visualizzare var/log/secure come utente root per controllare la cronologia dei tentativi di login e altri messaggi correlati all'accesso.
- Il comando 'last | more' fornisce una cronologia degli utenti che hanno eseguito il login.
- In /var/log/audit/audit.log.[0-9] viene salvato un log dei tentativi di accesso negati da SE Linux. Per visualizzare questi dati è necessario accedere come utente root.

Sicurezza SELinux

ACSLS 8.4 è progettato per essere eseguito in ambienti Security Enhanced Linux opzionali. SELinux fornisce il controllo dell'accesso a file, directory e altre risorse di sistema che non rientrano nello standard di protezione tradizionale disponibile negli ambienti Unix. Oltre all'accesso su autorizzazione del proprietario/del gruppo/pubblica, SELinux include il controllo dell'accesso basato su ruolo, dominio e contesto dell'utente. L'agente che applica il controllo dell'accesso su tutte le risorse di sistema è il kernel Linux.

L'utente root in un sistema Linux può attivare o disattivare l'applicazione mediante il comando `setenforce`.

```
setenforce [Enforcing | Permissive | 1 | 0 ]
```

Utilizzare `Enforcing` o 1 per impostare SELinux in modalità di applicazione. Utilizzare `Permissive` o 0 per impostare SELinux in modalità permissiva.

Per visualizzare lo stato di applicazione del sistema corrente, utilizzare il comando *getenforce*.

Quando si installa ACSLS, nel kernel vengono caricati tre moduli di criteri SELinux: allowPostgr, acsdb e acsdb1. Questi moduli offrono le definizioni e le eccezioni di applicazione necessarie affinché ACSLS acceda ai propri database e ad altre risorse di sistema mentre l'applicazione di SELinux è attiva. Con questi moduli installati, è possibile eseguire le normali operazioni di ACSLS, incluse le operazioni di database, come bdb.acsss, rdb.acsss, db_export.sh e db_import.sh senza dover disabilitare l'applicazione di SELinux.

Per ulteriori informazioni, consultare la sezione su SELinux nell'Appendice ”Troubleshooting” del manuale *StorageTek ACSLS 8.4 Administrator’s Guide*.

Installazione e configurazione di ACSLS

In questa sezione viene descritto come installare ACSLS in sicurezza.

Esecuzione di un'installazione di ACSLS standard

L'esecuzione di un'installazione di ACSLS standard garantisce la disponibilità di tutti i componenti necessari.

Se si esegue la migrazione a una release di ACSLS successiva da una release di ACSLS precedente, analizzare le impostazioni per le variabili dinamiche e statiche per verificare se si desidera utilizzare più opzioni sicure, in particolare per quanto riguarda l'opzione di sicurezza del firewall.

Uso di password sicure per gli ID utente di ACSLS

ACSLS richiede gli ID utente di ACSLS acsss, acssa e acsdb. Scegliere password sicure per questi ID e modificarle a intervalli regolari.

Limitazione dell'accesso ai file di ACSLS

In genere l'accesso ai file di ACSLS è limitato al solo gruppo acsls, che include gli ID utente acsss, acssa, acsdb e root. Alcuni file diagnostici e di database sono accessibili solo da un singolo ID utente acsls. ACSLS viene eseguito con umask impostato su 027.

L'accesso pubblico ai file di ACSLS non deve essere disponibile né in lettura né in scrittura. La limitazione dell'accesso oltre le impostazioni predefinite dell'installazione, tuttavia, può causare il malfunzionamento delle funzioni di ACSLS.

Impostazione di ’root’ come ID utente effettivo per i tre file di ACSLS

Lo script di installazione avvisa i clienti che è necessario impostare l'ID utente effettivo di 'root' (setuid) in tre file eseguibili nel file system /export/home/ACSSS:

- *acsss* (questo file binario deve essere eseguito con privilegi 'root' in quanto viene utilizzato per l'avvio e l'arresto dei servizi di sistema richiesti dall'applicazione ACSLS).
- *db_command* (questo file binario avvia e arresta il motore di database PostgreSQL che controlla e gestisce il database ACSLS).
- *get_diags* (questo file binario viene richiamato da un cliente per raccogliere le informazioni diagnostiche complete sul sistema che possono essere necessarie durante una chiamata al servizio di assistenza).

Durante l'installazione di ACSLS con pkgadd, ai clienti viene chiesto se desiderano *Installare i file come setuid/setgid*. Se si risponde *y* al prompt, si consente agli utenti nel gruppo acsls di eseguire questi tre comandi, anche se le utility eseguono determinate operazioni di sistema che richiedono privilegi root.

Analisi delle impostazioni per le variabili statiche e dinamiche di ACSLS

Le variabili statiche e dinamiche di ACSLS controllano il comportamento di molte funzioni di ACSLS. Impostare queste variabili utilizzando la utility *acsss_config*. Proteggere le impostazioni per molte di queste variabili come indicato nel presente documento. Quando le opzioni per una variabile sono presentate da *acsss_config*, se si risponde con un punto di domanda (?), viene visualizzata una spiegazione dettagliata della variabile. Queste informazioni sono disponibili anche nel capitolo ”Setting Variables that Control ACSLS Behavior” del manuale *ACSLS Administrator's Guide*.

Configurazione di WebLogic

ACSLS 8.1 e release successive utilizza WebLogic per il server Web. WebLogic viene installato con ACSLS.

Per informazioni sulle opzioni di protezione di un server WebLogic e sulle possibilità di audit trail con WebLogic, consultare *Oracle Fusion Middleware; Understanding Security for Oracle WebLogic Server 11g Release 1 (10.3.6).*

Uso della utility userAdmin.sh di ACSLS per creare e gestire gli utenti della GUI di ACSLS

La utility basata sui menu *userAdmin.sh* consente di amministrare le password degli utenti della GUI di ACSLS. È possibile aggiungere, rimuovere ed elencare gli utenti, nonché modificarne le password. Per usufruire di questa utility, è necessario che WebLogic sia in esecuzione. In caso contrario, questa utility avvia WebLogic e verifica che sia online prima di visualizzare il menu.

La utility *userAdmin.sh* deve essere eseguita dall'utente root e richiede l'autenticazione acsls_admin. L'account utente acsls_admin viene configurato durante l'installazione di ACSLS.

Uso della GUI di ACSLS

Per utilizzare la GUI di ACSLS, è necessario installare l'ultima versione di JRE e accedere alla GUI tramite un browser.

Installazione dell'ultima versione di JRE sui sistemi client della GUI

Accertarsi che sui sistemi che dovranno utilizzare la GUI per accedere ad ACSLS sia installato Java Runtime Environment (JRE).

Accesso alla GUI di ACSLS

Aprire un browser e immettere un URL con il nome host o l'indirizzo IP del server nel seguente formato:

`https://myAcslsHostName.myDomainName:7002/SlimGUI/faces/Slim.jsp` oppure *`https://127.99.99.99:7002/SlimGUI/faces/Slim.jsp`*

È preferibile utilizzare il nome host completo o l'indirizzo IP del computer host. Se WebLogic non riesce a risolvere completamente l'URL, è possibile che alcune pagine, incluse le pagine della Guida di ACSLS, non vengano visualizzate correttamente.

Se si utilizza http con la porta 7001, WebLogic reindirizza automaticamente su https sulla porta 7002.

Poiché WebLogic utilizza il protocollo sicuro https, è possibile che il browser visualizzi un avviso che indica che il certificato di sicurezza del sito non è stato registrato e pertanto non è sicuro. Se si è certi che l'URL corrisponde a quello del computer ACSLS locale, è possibile continuare in sicurezza. A questo punto, dovrebbe essere visualizzata la schermata di login.

Uso della GUI di ACSLS

L'accesso a AcslsDomain in WebLogic viene eseguito utilizzando il protocollo di sicurezza, https. Questo protocollo utilizza la comunicazione cifrata tra browser e server con chiavi private e certificati digitali. Di seguito sono riportate le opzioni per ottenere un certificato digitale.

Certificato demo ACSLS

ACSLS include un cosiddetto certificato 'demo'. Tale certificato offre un livello minimo di sicurezza di cifratura e consente agli utenti di iniziare a utilizzare l'interfaccia GUI di ACSLS senza dover eseguire ulteriori operazioni di configurazione. Nei casi in cui l'interazione del cliente con la libreria ACSLS si svolge interamente in una intranet protetta, questo metodo di certificazione demo è in genere sufficiente. Questo metodo, tuttavia, utilizza una chiave di cifratura a 512 bit non supportata in alcuni browser, in particolare Internet Explorer e FireFox Versione 39 e successive.

Configurazione di un certificato digitale autofirmato

Il manuale ACSLS Installation Guide offre agli amministratori ACSLS un metodo dettagliato per configurare un certificato digitale autofirmato della lunghezza di 2048 bit. Nella sezione 'Configuring an SSL Encryption Key', questo metodo offre un certificato supportato su tutti i browser. Si consiglia agli utenti che accedono a un sito https con un certificato autofirmato di non procedere nell'esplorazione del sito se non si è personalmente certi della sicurezza della risorsa Web. Nel contesto degli utenti ACSLS e del server di controllo della libreria, questo livello di sicurezza è in genere ben noto e, nella maggior parte dei casi, non è necessario ottenere una prova dell'integrità del sito tramite la verifica della firma di terze parti.

Certificati digitali firmati da un'apposita autorità di terze parti

È responsabilità dell'utente stabilire per ciascun sito se è necessario fornire l'autenticazione del certificato mediante un'autorità di firma di terze parti come Verisign o Entrust.net. La procedura di generazione di un certificato digitale firmato di questo tipo è descritta nel documento online di Oracle, Configuring Identity and Trust all'indirizzo:

http://docs.oracle.com/cd/E13222_01/wls/docs92/secmanage/identity_trust.html

Installazione di ACSLS HA

Se si utilizza la soluzione High Availability di ACSLS, seguire le istruzioni nel cluster ACSLS-HA per l'installazione, la configurazione e l'uso.

3

Funzioni di sicurezza

In questa sezione vengono descritti i meccanismi di sicurezza specifici offerti da ACSLS.

Modello di sicurezza

I requisiti di sicurezza di ACSLS sorgono dall'esigenza di proteggere i dati: in primo luogo da perdita e danni accidentali e in secondo luogo da tentativi deliberati non autorizzati di accesso o modifica di tali dati. La seconda preoccupazione include la protezione da ritardi indesiderati nell'accesso o nell'uso dei dati o persino da interferenze fino al punto di negazione del servizio.

Di seguito sono elencate le funzioni di sicurezza di importanza critica che offrono questa protezione.

- Autenticazione: garantisce che solo le persone autorizzate ottengano l'accesso al sistema e ai dati.
- Autorizzazione: fornisce il controllo dell'accesso ai privilegi di sistema e ai dati. Si basa sull'autenticazione per garantire che le persone ottengano solo il livello di accesso appropriato.
- Controllo: consente agli amministratori di rilevare i tentativi di violazione del meccanismo di autenticazione e i tentativi o le violazioni al controllo dell'accesso.

Configurazione e uso dell'autenticazione

Per impostazioni predefinita, in Linux o Solaris gli utenti di ACSLS vengono autenticati da PAM (Pluggable Authentication Modules). Consultare le pagine man Solaris o il manuale *Linux-PAM System Administrators Guide*.

Gli utenti dell'interfaccia GUI di ACSLS vengono autenticati dal server LDAP incorporato in WebLogic. Consultare il documento Managing the Embedded LDAP Server:

`http://docs.oracle.com/cd/E13222_01/wls/docs81/secmanage/ldap.html`

Autenticazione degli utenti di ACSLS da parte dei sistemi operativi Solaris o Linux

Gli utenti di ACSLS acsss e acssa devono effettuare il login a Solaris o Linux ed essere autenticati dal sistema operativo prima di utilizzare cmd_proc o, per l'utente acsss, eseguire

le utility e i comandi di configurazione di ACSLS. L'ID utente acsdb viene utilizzato anche per le operazioni correlate al database. Come parte del processo di installazione di ACSLS, i clienti devono impostare le password per questi ID al primo login. Per informazioni dettagliate, consultare il manuale *ACSLS Installation Guide*.

Autenticazione dell'utente della GUI di ACSLS da parte di WebLogic

Gli utenti della GUI di ACSLS devono eseguire il login ed essere autenticati da WebLogic. acsls_admin viene creato durante l'installazione di ACSLS e i clienti devono impostarne la password. I clienti possono aggiungere tutti gli utenti della GUI desiderati utilizzando la utility `userAdmin.sh`. Per informazioni dettagliate, consultare il manuale *ACSLS Installation Guide* e la sezione su `userAdmin.sh` nel capitolo ”Utilities” del manuale *ACSLS Administrator’s Guide*.

Considerazioni sul controllo

Di seguito sono riportate considerazioni generali sul controllo valide per ACSLS.

Come garantire la gestibilità delle informazioni controllate

Sebbene il controllo non comporti praticamente alcun costo, è opportuno limitare il più possibile il numero di eventi controllati. In tal modo si riduce l'impatto sulle prestazioni dell'esecuzione delle istruzioni controllate e la dimensione dell'audit trail, semplificandone l'analisi, la comprensione e la gestione.

Per delineare una strategia di controllo, attenersi alle regole generali indicate di seguito.

Valutazione dello scopo del controllo

Dopo avere compreso chiaramente i motivi del controllo, è possibile delineare una strategia di controllo appropriata ed evitare controlli non necessari.

Controllo consapevole

Controllare il numero minimo di istruzioni, utenti o oggetti necessari per ottenere le informazioni desiderate.

Configurazione e uso dei log di controllo di ACSLS

ACSLS dispone di diversi log di informazioni che consentono di registrare ed esaminare l'attività di ACSLS.

- La maggior parte dei log può essere visualizzata utilizzando vi e altri editor. Gli eventi di sistema possono essere visualizzati solo utilizzando la GUI di ACSLS.

- La maggior parte di questi log può essere archiviata automaticamente quando raggiunge una dimensione definita dal cliente. Verrà conservato solo un numero di log specificato dal cliente. Per evitare di riempire il file system di ACSLS, è previsto un limite configurabile al numero di log che verranno conservati. Se si desidera conservare un numero maggiore di questi file di log o conservarli su un altro sistema, è necessario sviluppare una procedura personalizzata per archiviarli in un'ubicazione dove è presente spazio sufficiente.
- La dimensione, il numero di log archiviati da conservare e altre caratteristiche di questi file sono definite dalle variabili dinamiche e statiche di ACSLS.

Directory di log di ACSLS

La directory di log di ACSLS è controllata dalla variabile statica LOG_PATH. Il valore predefinito è la directory $ACS_HOME/log. Questa directory include i log elencati di seguito.

acsss_event.log
Registra i messaggi per eventi di sistema, eventi della libreria ed errori significativi di ACSLS.

Quando acsss_event.log raggiunge una dimensione limite definita dalla variabile dinamica LOG_SIZE, viene copiato in event0.log e cancellato. Durante il processo di copia, i log degli eventi conservati vengono copiati nei log conservati con numero maggiore e i log conservati con numero superiore vengono sovrascritti. Ad esempio: event8.log viene copiato in event9.log, event7.log viene copiato in event8.log, …, event0 .log viene copiato in event1.log, acsss_event.log viene copiato in event0.log e acsss _event.log viene cancellato. Questa operazione è controllata dalle variabili indicate di seguito.

- *EVENT_FILE_NUMBER* specifica il numero di log degli eventi da conservare.
- *LOG_SIZE* specifica la dimensione limite raggiunta la quale il log degli eventi viene copiato in un log degli eventi conservato e viene troncato.

Utilizzare la utility *`greplog`* per filtrare il log acsss_event in modo che includa o escluda i messaggi contenenti parole chiave specifiche. Per ulteriori dettagli, consultare la sezione su greplog nel capitolo ”Utilities” del manuale *ACSLS Administrator's Guide*.

Log di configurazione
Sono disponibili due log in cui vengono registrati i dettagli quando ACSLS aggiorna la configurazione della libreria archiviata nel database ACSLS. Le modifiche alla configurazione apportate tramite *`acsss_config`* e *`Dynamic Config`* (utility *`config`*) vengono registrate in questi log.

acsss_config.log
Registra i dettagli di tutte le configurazioni o riconfigurazioni delle librerie supportate da ACSLS. L'ultima modifica alla configurazione viene aggiunta al record delle configurazioni precedenti.

acsss_config_event.log
Registra gli eventi durante il processo di configurazione o riconfigurazione.

rpTrail.log
Registra la risposta a tutte le richieste per ACSLS dai client ACSAPI o cmd_proc, nonché tutte le richieste alla GUI o all'interfaccia client SCSI alle librerie logiche, ad eccezione delle query di database. Le informazioni registrate includono il richiedente, la richiesta e la data e l'ora della richiesta.

rpTrail.log è gestito dalle variabili indicate di seguito.

- *LM_RP_TRAIL* abilita questo audit trail di eventi ACSLS. Il valore predefinito è TRUE.
- *RP_TRAIL_LOG_SIZE* specifica la dimensione limite raggiunta la quale rpTrail.log viene compresso e archiviato.
- *RP_TRAIL_FILE_NUM* specifica il numero di log rpTrail archiviati da conservare.
- *RP_TRAIL_DIAG* specifica se i messaggi rpTrail devono includere informazioni di diagnostica aggiuntive. Il valore predefinito è FALSE.

Statistiche sui volumi della libreria
Registra tutti gli eventi che riguardano i volumi (cartucce) in una libreria a nastro, ad esempio se un volume viene installato, disinstallato, spostato, inserito, espulso o trovato dal controllo o dal recupero cartucce. Se le statistiche sui volumi della libreria sono abilitate, queste informazioni vengono registrate in acsss_stats.log.

Le statistiche sui volumi della libreria sono gestite dalle variabili indicate di seguito.

- *LIB_VOL_STATS* abilita le statistiche sui volumi della libreria. Il valore predefinito è OFF.
- *VOL_STATS_FILE_NUM* specifica il numero di file acsss_stats.log archiviati da conservare.
- *VOL_STATS_FILE_SIZE* specifica la dimensione limite raggiunta la quale il file acsss _stats.log viene archiviato.

Directory Log/sslm di ACSLS

Nella directory dei log di ACSLS le informazioni sulla GUI di ACSLS e sull'interfaccia client SCSI per le librerie logiche vengono registrate nella directory sslm. Questa directory include collegamenti ai log di controllo di WebLogic. La directory sslm include i log indicati di seguito.

slim_event.g#.log[.pp#]
Registra sia gli eventi della GUI di ACSLS che quelli dell'interfaccia client SCSI. Include messaggi di modifica alla configurazione della libreria logica ed eventi del client SCSI.

- .g# indica il numero di generazione di questo log.
- .pp# indica il numero di processo parallelo di questo log. In caso di registrazione di più processi allo stesso tempo, ai log dei processi aggiuntivi verrà assegnato un numero di processo parallelo.

smce_trace.log
Tiene traccia dell'attività dei client SCSI per le librerie logiche ACSLS utilizzando l'emulazione dell'interfaccia SMC.

guiAccess.log
Si tratta di un collegamento al file access.log di WebLogic. Vedere Configurazione e uso dei log di controllo di WebLogic.

AcslsDomain.log
Si tratta di un collegamento al file AcslsDomain.log di WebLogic. Vedere Configurazione e uso dei log di controllo di WebLogic.

AdminServer.log
Si tratta di un collegamento al file AdminServer.log di WebLogic. Vedere Configurazione e uso dei log di controllo di WebLogic.

Visualizzazione degli audit trail di ACSLS dal Visualizzatore log della GUI

Accedere al Visualizzatore log dalla sezione di configurazione e amministrazione della struttura di navigazione della GUI. Il Visualizzatore log mostra le informazioni combinate di ???TITLE??? e ???TITLE???.

Visualizzazione degli eventi di sistema dalla GUI

È anche possibile visualizzare gli eventi di sistema dalla sezione di configurazione e amministrazione della struttura di navigazione della GUI. Nel log degli eventi di sistema vengono registrate tutte le operazioni della libreria discreta. Ciascun record in questo log contiene la data e l'ora, il tipo e una descrizione di un evento.

Configurazione e uso dei log di controllo di Solaris

Determinare i criteri di controllo di Solaris. Per informazioni su quali eventi pianificare per il controllo, dove salvare i log di controllo e come esaminarli, consultare la sezione sul controllo in Oracle Solaris in *Oracle System Administration: Security Services*.

Se non sono stati abilitati gli audit trail personalizzati di Solaris, sono disponibili gli audit trail dei login e dei comandi Unix emessi dagli utenti acsss, acsdb e acssa elencati di seguito.

- Gli utenti attualmente iscritti a Unix vengono registrati in utmpx di Unix e il precedente accesso degli utenti viene registrato nel database wtmpx.
- Utilizzare il comando `last` per visualizzare tutti gli accessi di un ID utente (ad esempio `last acsss`). Per ulteriori informazioni, consultare le pagine man per: wtmpx, `last` e getutxent.
- I comandi emessi da un utente vengono registrati nei file .*_history (ovvero [dot]*_history) nella directory home di tale utente.

  Per l'utente acsss, possono essere:
  - .bash_history
  - .psql_history

- .sh_history

In Solaris /var/adm/sulog registra i tentativi riusciti e non riusciti di eseguire *su* e diventare utente privilegiato o un altro utente.

Configurazione e uso dei log di controllo di Linux

Per informazioni dettagliate sulla raccolta e l'analisi dei log di controllo e di sistema, consultare le sezioni Configuring and Using Auditing e Configuring and Using System Logging in *Oracle Linux: Security Guide for Release 6*.

Configurazione e uso dei log di controllo di WebLogic

Per informazioni sulle opzioni di protezione di un server WebLogic e sulle possibilità di audit trail con WebLogic, consultare *Oracle Fusion Middleware; Understanding Security for Oracle WebLogic Server 11g Release 1 (10.3.6)*.

WebLogic registra l'accesso alla GUI di ACSLS nella directory indicata di seguito.

/export/home/SSLM/AcslsDomain/servers/AdminServer/logs

Questa directory include i seguenti file:

- access.log
  - Sono disponibili versioni archiviate denominate access.log*nnnnn* (ad esempio, access .log00001)
  - In questo modo si ottiene un audit trail dettagliato dell'attività di un utente della GUI.
  - Per i login, cercare "AcslsLoginForm".

    Nota:

    È disponibile un collegamento al log di accesso in: $ACS_HOME/logs/sslm/guiAccess.log.
- AcslsDomain.log
  - Sono riportate le operazioni di WebLogic e della GUI di ACSLS.

    Nota:

    È disponibile un collegamento al log di accesso in: $ACS_HOME/logs/sslm/AcslsDomain.log.
- AdminServer.log
  - Sono riportate le operazioni di WebLogic e della GUI di ACSLS.

    Nota:

    È disponibile un collegamento al log di accesso in: $ACS_HOME/logs/sslm/AdminServer.log.

4

Considerazioni sulla sicurezza per gli sviluppatori

Questa sezione contiene informazioni utili per gli sviluppatori che sviluppano o supportano applicazioni che utilizzano ACSLS per la gestione delle librerie a nastro StorageTek di Oracle.

Abilitazione della sicurezza del firewall sul server dell'applicazione client

Limitare le porte utilizzate per la comunicazione e disabilitare portmapper sul server dell'applicazione client abilitando la sicurezza del firewall. Consultare *CSC Developer's Toolkit User's Guide*, "Appendix B: Firewall-Secure Operation."

Appendice A

Elenco di controllo per la distribuzione sicura

1. Applicare la gestione delle password.
2. Limitare l'accesso alla rete.
   a. ACSLS e le librerie a nastro che gestisce devono essere protetti dal firewall aziendale.
   b. Abilitare l'opzione di sicurezza del firewall ACSLS.
   c. Considerare la possibilità di abilitare la sicurezza del firewall per le applicazioni client ACSLS.
3. Potenziare il sistema operativo Solaris o Linux.
4. Applicare tutte le patch e le soluzioni di sicurezza.
5. Se vengono rilevati punti di vulnerabilità in StorageTek ACSLS, contattare Oracle Services, Oracle Tape Library Engineering o il rappresentante dell'account.

Appendice B

Riferimenti

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

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

Negli URL delle singole librerie di documentazione su ACSLS è incluso il numero di versione. Per questo motivo, il collegamento a una libreria specifica diventa obsoleto non appena la libreria viene aggiornata. La documentazione su ACSLS include:

- *ACSLS Installation Guide*
- *ACSLS Administrator's Guide*
- *ACSLS Product Information*

  Sono inclusi requisiti software e hardware, una panoramica su ACSLS, nonché i supporti, le librerie a nastro e le unità nastro supportati.
- Messaggi ACSLS (e codici di stato)
- *ACSLS Release Notes*
- *ACSLS-HA Cluster: Installation, Configuration, and Operations*
- *ACSLS Interface Reference Manual*

Oracle Solaris
La libreria di informazioni su Oracle Solaris 11.2 include il documento *Securing the Oracle Solaris 11 Operating System*. Consultarlo per informazioni dettagliate.

Oracle Linux
La libreria di informazioni su Oracle Linux 6 include il documento *Oracle Linux 6 Security Guide*. Consultarlo per informazioni dettagliate.

Oracle WebLogic
La libreria della documentazione sul server Oracle WebLogic per WebLogic 10.3.6 (utilizzato da ACSLS 8.2) include una sezione sulla sicurezza.

Oracle Fusion Middleware; Understanding Security for Oracle WebLogic Server 11g Release 1 (10.3.6) illustra i dettagli sulla protezione di un server WebLogic.