StorageTek Automated Cartridge System Library Software

Guia de Segurança

Release 8.4

E68251-01

Setembro de 2015

ORACLE

StorageTek Automated Cartridge System Library Software
Guia de Segurança

E68251-01

Índice

Prefácio 5

Público-alvo 5
Acessibilidade da Documentação 5

1. Visão Geral 7

Visão Geral do Produto 7
Princípios Gerais de Segurança 7
Manter o Software Atualizado 7
Restringir o Acesso à Rede aos Serviços Críticos 7
Seguir o Princípio de Menos Privilégios 8
Monitorar a Atividade do Sistema 8
Manter-se Atualizado com as Informações Mais Recentes de Segurança 8

2. Instalação Segura 9

Compreender seu Ambiente 9
Quais recursos precisam ser protegidos? 9
Contra quem os recursos estão sendo protegidos? 9
O que acontecerá se as proteções dos recursos estratégicos falharem? 9
Procedimento Recomendado para Proteger o ACSLS 9
Protegendo a Comunicação com a Internet do ACSLS 10
Proteger o ACSLS e as Bibliotecas de Fitas com o Firewall Corporativo 10
Opção de Segurança de Firewall do ACSLS 10
Portas Ethernet Usadas para a Comunicação do ACSLS 11
Configurando Firewalls executados no Servidor ACSLS 13
Instalando e Configurando o Solaris 14
Instalando e Configurando o Linux 15
Auditando a Segurança no Linux 16
Segurança do SELinux 16
Instalando e Configurando o ACSLS 17
Executar uma Instalação Padrão do ACSLS 17
Usar Senhas Fortes para IDs de Usuário do ACSLS 17
Restringir o Acesso aos Arquivos do ACSLS 17
Definir ’root’ como o ID de Usuário Efetivo para Três Arquivos do ACSLS 17

Revisar Configurações de Variáveis Estáticas e Dinâmicas do ACSLS 18
Configurando o WebLogic 18
Use o utilitário userAdmin.sh do ACSLS para criar e manter usuários do ACSLS GUI 18
Usando o ACSLS GUI 18
Instalar a Versão Mais Recente do JRE nos Sistemas Cliente GUI 19
Acessando o ACSLS GUI 19
Usando o ACSLS GUI 19
Certificado de demonstração do ACSLS 19
Configurando um certificado digital autoassinado 19
Certificados digitais assinados por outra autoridade de assinatura 20
Instalando o ACSLS HA 20

3. Recursos de Segurança 21

O Modelo de Segurança 21
Configurando e Usando Autenticação 21
Autenticação de Usuário do ACSLS pelos Sistemas Operacionais Solaris ou Linux 21
Autenticação de Usuário do ACSLS GUI pelo WebLogic 22
Considerações de Auditoria 22
Mantendo Gerenciáveis as Informações Auditadas 22
Avalie a finalidade da auditoria 22
Auditoria competente 22
Configurando e Usando os Logs de Auditoria do ACSLS 22
Diretório de Logs do ACSLS 23
Diretório de Logs/sslm do ACSLS 24
Exibindo Trilhas de Auditoria do ACSLS no Log Viewer da GUI 25
Exibir Eventos de Sistema na GUI 25
Configurando e Usando os Logs de Auditoria do Solaris 25
Configurando e Usando os Logs de Auditoria do Linux 25
Configurando e Usando os Logs de Auditoria do WebLogic 26

4. Considerações de Segurança para Desenvolvedores 27

Ativar a Segurança de Firewall no Servidor do Aplicativo Cliente 27

A. Lista de Verificação para uma Implantação Segura 29

B. Referências 31

Prefácio

Este documento descreve os recursos de segurança do StorageTek Automated Cartridge System Library Software (ACSLS) e da solução ACSLS High Availability (ACSLS HA) da Oracle. Como o ACSLS HA e o Agente ACSLS SNMP também são executados no servidor ACSLS, a proteção desse servidor protegerá o ACSLS, o ACSLS HA e o Agente ACSLS SNMP.

Público-alvo

Este guia destina-se a todos os envolvidos com o uso dos recursos de segurança e da instalação e configuração seguras do ACSLS.

Acessibilidade da Documentação

Para obter informações sobre o comprometimento da Oracle com a acessibilidade, visite o site do Oracle Accessibility Program em http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Acesso ao Oracle Support
Os clientes da Oracle que adquiriram serviços de suporte têm acesso a suporte eletrônico por meio do My Oracle Support. Para obter informações, visite http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info ou http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs se você for portador de deficiência auditiva.

1

Visão Geral

Esta seção apresenta uma visão geral do ACSLS e explica os princípios gerais de segurança de aplicativo.

Observação:

Em todo este documento, o produto Automated Cartridge System Library Software é designado como ACSLS e a solução ACSLS High Availability é designada como ACSLS HA.

Visão Geral do Produto

O ACSLS é um software de servidor de biblioteca de fitas da Oracle que controla uma ou mais bibliotecas de fitas StorageTek em clientes de sistemas abertos. O ACS (Automated Cartridge System) é uma biblioteca de fitas ou um grupo de bibliotecas de fitas conectadas por PTPs (pass-thru-ports). O ACSLS gerencia um ou mais ACSs por meio dos comandos ”control path” enviados por uma rede. O software inclui um componente de administração de sistema, interfaces para aplicativos de sistema cliente e recursos de gerenciamento de biblioteca.

Princípios Gerais de Segurança

Os princípios a seguir são essenciais para o uso seguro de qualquer produto.

Manter o Software Atualizado

Um dos princípios da boa prática de segurança é manter todas as versões e patches do software atualizados. Este documento pressupõe que você esteja executando o ACSLS 8.4 ou uma release posterior, com toda a manutenção relevante aplicada. Executar a última release do ACSLS garante que você tenha os aprimoramentos e correções mais recentes.

Aplique todos os patches de segurança relevantes ao SO e aos serviços instalados com ele. Instale esses patches seletivamente porque a aplicação de todas as atualizações disponíveis poderá instalar novos recursos, inclusive novas releases do SO com as quais o ACSLS e o ACSLS HA não foram testados.

Restringir o Acesso à Rede aos Serviços Críticos

Mantenha o ACSLS e as bibliotecas que ele gerencia protegidos por um firewall. É recomendável usar uma rede privada para as comunicações TCP/IP entre o ACSLS e as bibliotecas de fitas.

Seguir o Princípio de Menos Privilégios

O princípio de menos privilégios indica que os usuários devem receber o mínimo de privilégios para executar suas tarefas. Os privilégios do usuário devem ser revistos periodicamente a fim de determinar a relevância para as responsabilidades do cargo atual.

No ACSLS, isso significa que os operadores que apenas executam comandos de rotina usando o cmd_proc devem fazer login como o usuário acssa. Os administradores de sistema que efetuam login como o usuário acsss também têm acesso a um conjunto mais abrangente de utilitários e comandos de configuração. O uso do ID de usuário acsdb não é necessário para a execução de operações normais.

Monitorar a Atividade do Sistema

A segurança do sistema baseia-se em três pilares: bons protocolos de segurança, configuração adequada do sistema e monitoramento do sistema. A auditoria e a análise dos registros de auditoria tratam desse terceiro requisito. Todo componente de um sistema possui algum grau de capacidade de monitoramento. Siga o conselho de auditoria fornecido neste documento e monitore regularmente os registros de auditoria

Manter-se Atualizado com as Informações Mais Recentes de Segurança

A Oracle aprimora continuamente seu software e documentações relacionadas. Verifique se há revisões em cada versão deste documento.

2

Instalação Segura

Esta seção destaca o processo de planejamento e implementação de uma instalação e configuração seguras, bem como descreve as topologias de implantação recomendadas para o ACSLS.

Compreender seu Ambiente

Para compreender melhor suas necessidades de segurança, as seguintes perguntas devem ser feitas:

Quais recursos precisam ser protegidos?

Os principais recursos que o ACSLS gerencia são bibliotecas de fitas, unidades e cartuchos. Eles precisam estar protegidos contra o acesso inadvertido e mal-intencionado. Por exemplo, impedir que pessoas façam login por engano em um servidor ACSLS diferente usando senhas distintas para os IDs de usuário do ACSLS em vários servidores.

Contra quem os recursos estão sendo protegidos?

Você deseja proteger os recursos de armazenamento em fita contra acessos internos e externos não autorizados.

O que acontecerá se as proteções dos recursos estratégicos falharem?

O ACSLS pode montar cartuchos em unidades de fita. Se um usuário conseguir se conectar à unidade de fita por meio do caminho de dados, ele poderá ler os dados contidos na fita que não estão criptografados.

Usuários com acesso ao ACSLS e a bibliotecas de fitas poderão inserir e ejetar cartuchos de bibliotecas de fitas.

Procedimento Recomendado para Proteger o ACSLS

Ao proteger o ACSLS e os componentes de infraestrutura necessários, siga este procedimento para garantir que o ACSLS continuará a funcionar depois que as alterações forem feitas:

- Instale o ACSLS.

- Verifique se o ACSLS está funcionando corretamente. Inclua operações de configuração e auditoria de bibliotecas, montagem e desmontagem de fitas, inserção e ejeção de fitas e backup e restauração do banco de dados.
- Implemente a alteração para aumentar a segurança.
- Verifique se o ACSLS ainda funciona corretamente.

Protegendo a Comunicação com a Internet do ACSLS

Esta seção descreve as recomendações para a implantação do ACSLS para um acesso seguro à Internet.

Proteger o ACSLS e as Bibliotecas de Fitas com o Firewall Corporativo

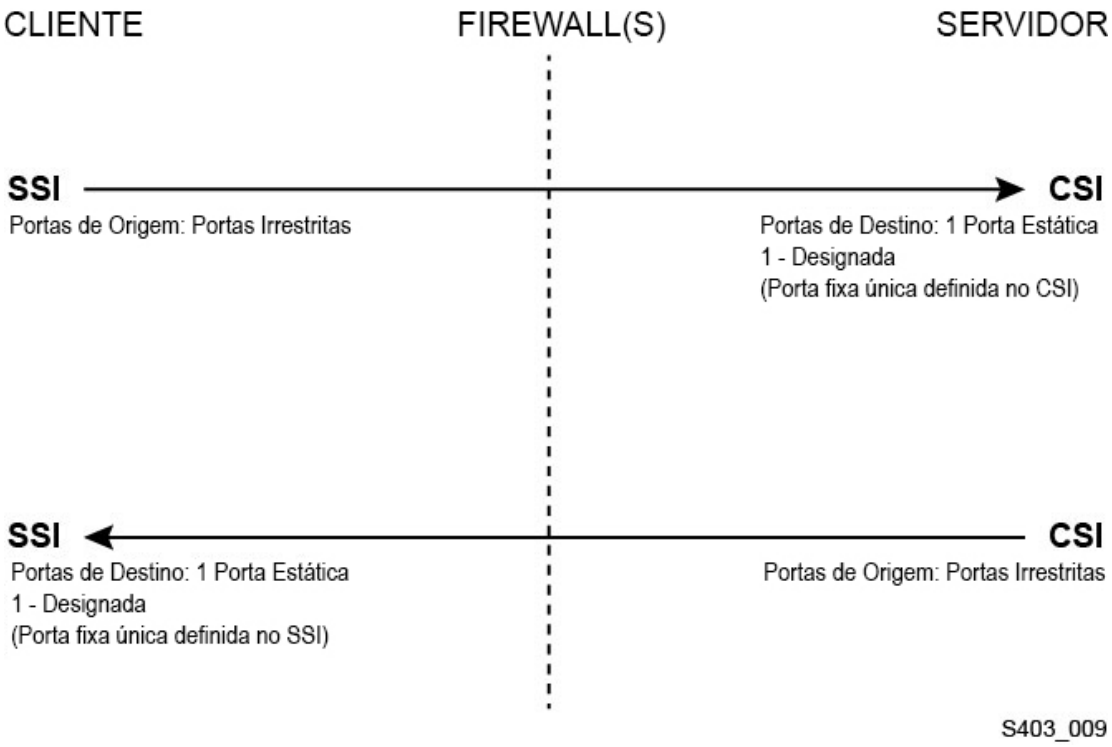
O ACSLS e as bibliotecas de fitas que ele suporta devem ser implantados com a proteção do firewall corporativo. Se as pessoas que trabalham remotamente precisarem fazer login no servidor ACSLS, elas poderão acessá-lo por meio de uma VPN.

Observação:

Se você tiver um firewall de borda baseado em IPv4, ele deverá ser configurado para remover todos os pacotes de saída IPv4 do protocolo 41 e pacotes da porta UDP 3544 para impedir que os hosts da Internet usem qualquer tráfego tunelizado IPv6-over-IPv4 para alcançar hosts internos.

Opção de Segurança de Firewall do ACSLS

Se os aplicativos cliente, que usam o ACSLS para montar fitas e gerenciar bibliotecas de fitas, estiverem separados do ACSLS por um firewall, recomendamos ativar a Opção de Segurança de Firewall. Mesmo se os aplicativos cliente não estiverem separados do ACSLS por um firewall, a implementação da Opção de Segurança de Firewall fornece segurança adicional ao ACSLS, pois restringe as portas usadas para comunicação entre o ACSLS e seus aplicativos cliente, conforme mostrado abaixo. Por esses motivos, a variável estática CSI _FIREWALL_SECURE utiliza o padrão TRUE no ACSLS 8.1 e releases posteriores.



Para obter detalhes, consulte o apêndice ”Firewall Security Option” no *ACSLS Administrator’s Guide*.

Portas Ethernet Usadas para a Comunicação do ACSLS

- As portas a seguir são usadas no servidor ACSLS. Certifique-se de que os firewalls estejam configurados para permitir o tráfego nessas portas. Isso incluía os firewalls implementados pelo ipfilter no Solaris ou pelo iptables no Linux.
  - 22 ambas as direções – usada para acesso ssh.
  - 111 portmapper, a menos que o portmapper tenha sido desativado.
  - 115 usada para SFTP (Secure File Transfer Protocol).
  - 161 porta padrão para o agente ACSLS SNMP - get/set/walk.
  - 162 porta padrão para o agente ACSLS SNMP - traps.

    Observação:

    As portas usadas pelo agente ACSLS SNMP são configuráveis pelo comando: `AcslsAgtdSnmpConf [ -p port ] [-t trap port] [-d]`. A opção `-d` exibe a configuração atual. Depois de alterar a configuração da porta, você deverá reiniciar o agente com o comando, `agentRegister`.

  - 5432 porta padrão para comunicação interna do ACSLS com o banco de dados PostgreSQL (a variável de ambiente PGPORT para o ID de usuário acsss).

Se a porta 5432 estiver sendo usada, o próximo número de porta mais alto disponível será usado.

Observação:

A porta 5432 só precisa estar acessível no localhost (127.0.0.1).

- 7001 e 7002 - usadas pelo WebLogic e pelo ACSLS GUI.
- 30031 ou a porta de escuta do ACSLS CSI, definida por CSI_INET_PORT.
- 50003 porta usada para comunicação interna do ACSLS GUI e dos componentes Java com o processamento de ACSLS legado. Não é configurável.

- Para que os aplicativos cliente se comuniquem com o ACSLS por meio do ACSAPI, as seguintes portas deverão estar abertas:
  - O aplicativo cliente deve ser capaz de se comunicar com a porta de escuta do ACSLS CSI. Por padrão, essa porta é a 30031 e é definida pela variável estática CSI _INET_PORT.

    Você pode descobrir quais portas estão sendo usadas pelo ACSLS para escutar solicitações dos clientes ACSAPI com o seguinte comando do shell Unix:

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

    Os IDs de porta serão listados no último campo da tela.
  - O cliente ACSAPI (por exemplo, um servidor NetBackup ou SAM-QFS) define sua porta de entrada fixa usando a variável de ambiente SSI_INET_PORT. Especifique uma porta no intervalo de 1024-65535, excluindo as portas 50001 e 50004. O servidor ACSLS deve ser capaz de se comunicar com essa porta.

    Observação:

    Em um servidor cliente ACSAPI, as portas 50001 e 50004 são usadas para a comunicação IPC entre o domínio AF_INET e o mini Agente de Log de Eventos e entre aplicativos cliente e o SSI.

  Consulte o apêndice Firewall Security Option no *ACSLS Administrator's Guide* para obter mais detalhes sobre a comunicação entre os aplicativos cliente e o ACSLS.

- Se o componente XAPI estiver instalado, o servidor XAPI usará uma porta de escuta fixa para receber as solicitações TCP de entrada dos clientes ELS. A porta de escuta XAPI é definida pela variável estática XAPI_PORT. Por padrão, a porta definida pela variável XAPI_PORT é a 50020. Ela deve estar no intervalo de 1024 a 65535, e não pode estar em conflito com qualquer outra porta usada pelo ACSLS ou por outros aplicativos.

  Consulte o apêndice XAPI Client Interface no *ACSLS Administrator's Guide* para obter mais detalhes sobre a variável XAPI_PORT. Esse apêndice também fornece detalhes sobre como exibir e definir a variável estática XAPI_PORT.

- Portas que devem estar abertas em uma biblioteca SL8500 ou SL3000:

O ACSLS se comunica com essas portas nas conexões Ethernet 2A e 2B de uma biblioteca SL8500 ou SL3000. Se a comunicação do ACSLS com essas portas for bloqueada, o ACSLS não poderá gerenciar a biblioteca.

- 50001 – Usada para toda a comunicação normal entre o ACSLS e a biblioteca
- 50002 – Usada pelo ACSLS HA para determinar se o nó HA alternativo pode se comunicar com a biblioteca antes de ocorrer o seu failover para o nó alternativo

Configurando Firewalls executados no Servidor ACSLS

Além dos firewalls externos, a proteção de firewall pode ser implementada no servidor ACSLS por meio do ipfilter no Solaris ou do iptables no Linux. Esta seção descreve como gerenciar esses firewalls executados no servidor ACSLS.

- Gerenciando o ipfilter no Solaris:

  Consulte as páginas man relativas ao ipf e ao ipfilter para obter informações detalhadas.

  - O firewall ipfilter é ativado (desativado) por 'root' com o comando:

    ```
    svcadm enable ipfilter (svcadm disable ipfilter)
    ```

  - Para conhecer o status atual do ipfilter:

    ```
    svcs ipfilter
    ```

  - As políticas de firewall são definidas no arquivo: /etc/ipf/ipf.conf

    Para permitir uma comunicação livre entre os componentes no host local (ex.: entre o ACSLS e o WebLogic ou entre a GUI e o banco de dados do ACSLS), inclua uma instrução como:

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

    ou

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

    Você precisa definir políticas que permitem acesso a todas as portas necessárias para o ACSLS. Por exemplo, para incluir uma política que permite que os navegadores baseados na Web acessem o ACSLS GUI, você precisa abrir as portas 7001 e 7002.

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

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

    Depois de descobrir quais portas são usadas pelo ACSLS para escutar solicitações de clientes ACSAPI, adicione instruções 'pass in quick' para cada uma dessas portas.

    Talvez seja necessário incluir uma instrução 'pass in quick' para a porta RPC do portmapper, 111.

A última instrução no seu conjunto de regras proposto, "block in from any", indica que nenhum tráfego deve alcançar o host, exceto se especificamente autorizado nas instruções anteriores.

- Gerenciando o iptables no Linux:
  - O firewall iptables é ativado (desativado) por 'root' com o comando:

    ```
    service iptables start (service iptables stop)
    ```
  - Para verificar o status do iptables:

    ```
    service iptables status
    ```
  - O arquivo de política para o iptables é /etc/sysconfig/iptables:

    Você precisa definir políticas que permitem acesso a todas as portas necessárias para o ACSLS. Por exemplo, para incluir uma política que permita o acesso remoto http/https ao ACSLS GUI, você deve atualizar esse arquivo para incluir exceções para as portas 7001 e 7002 usando instruções, como:

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

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

    Depois de descobrir quais portas são usadas pelo ACSLS para escutar as solicitações de clientes ACSAPI, você precisará adicionar exceções para cada um desses arquivos de política do iptables. Talvez seja necessário incluir uma instrução de exceção para a porta RPC do portmapper, 111.

Instalando e Configurando o Solaris

Esta seção descreve como instalar e configurar o Solaris com segurança.

As sugestões incluem:

- Aplique todos os patches de segurança relevantes ao SO e aos serviços instalados com ele. Instale esses patches seletivamente porque a aplicação de todas as atualizações disponíveis poderá instalar novos recursos, inclusive novas releases do SO com as quais o ACSLS e o ACSLS HA não foram testados.
- Desative o telnet e o rlogin. Use o ssh no lugar deles. Também desative o ftp e use o sftp.

  Desative os serviços telnet, rlogin e ftp executando os seguintes comandos como root.

  Para ver todos os serviços:

  ```
  svcs
  ```

  Para desativar o telnet, o rlogin e o ftp:

  ```
  svcadm disable telnet
  ```

```
svcadm disable rlogin

svcadm disable ftp
```

- Não desative o ssh. Você deseja que os usuários façam login remotamente no ACSLS usando ssh, e não telnet ou rlogin. Além disso, não desative o sftp.
- O ACSLS requer rpc-bind. Não desative-o.

  Se o Solaris estiver instalado com a opção Secure by Default, será preciso alterar uma propriedade de configuração de rede para que rpc-bind permita aos clientes ACSAPI enviarem solicitações ao ACSLS.

  Consulte o *ACSLS Installation manual*, capítulo "Installing ACSLS on Solaris", seção "Installing Solaris" para obter detalhes.
- Algumas portas Ethernet no servidor ACSLS precisam estar abertas para comunicação com o ACSLS. Os aplicativos cliente usam portas Ethernet específicas para a comunicação com o ACSLS, e o ACSLS se comunica com portas específicas nas bibliotecas de fitas. Consulte o Portas Ethernet Usadas para a Comunicação do ACSLS para saber quais portas precisam estar disponíveis para a comunicação do ACSLS. No servidor ACSLS, certifique-se de que o ipfilter esteja configurado para permitir o tráfego nas portas usadas pelo ACSLS.

Determine a política de auditoria do Solaris. A seção ”Auditing in Oracle Solaris” no "Oracle System Administration: Security Services" pode ajudá-lo a planejar quais eventos serão auditados, onde seus logs de auditoria devem ser salvos e como você deseja revisá-los.

Instalando e Configurando o Linux

Sugestões para instalar e configurar o Linux com segurança:

- Aplique todos os patches de segurança relevantes ao SO e aos serviços instalados com ele. Instale esses patches seletivamente porque a aplicação de todas as atualizações disponíveis poderá instalar novos recursos, inclusive novas releases do SO com as quais o ACSLS e o ACSLS HA não foram testados.
- Certifique-se de que o telnet e o rlogin não estejam instalados nem desativados. Use o ssh no lugar deles.

  Também certifique-se de que o ftp não esteja instalado nem desativado e, em vez dele, use o sftp.

  Para ver todos os serviços, faça login como root e:

  ```
  service –-status-all
  ```
- Para excluir os serviços permanentemente, use:

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

- Não desative o ssh. Você deseja que os usuários façam login remotamente no ACSLS usando ssh, e não telnet ou rlogin. Além disso, não desative o sftp.
- Os serviços de rede, especificamente o rpcbind, devem ser ativados para permitir a comunicação do cliente ACSLS.

  Ao iniciar o rpc no Linux, use o indicador –i.
- Algumas portas Ethernet no servidor ACSLS precisam estar abertas para comunicação com o ACSLS. Os aplicativos cliente usam portas Ethernet específicas para a comunicação com o ACSLS, e o ACSLS se comunica com portas específicas nas bibliotecas de fitas. Consulte o Portas Ethernet Usadas para a Comunicação do ACSLS para saber quais portas precisam estar disponíveis para a comunicação do ACSLS. No servidor ACSLS, certifique-se de que o iptables esteja configurado para permitir o tráfego nas portas usadas pelo ACSLS.

Auditando a Segurança no Linux

Determine as políticas de auditoria do Linux. A seção ”Configuring and Using Auditing” do *Oracle Linux: Security Guide for Release 6* pode ajudá-lo a planejar quais eventos serão auditados, onde seus logs de auditoria devem ser salvos e como você deseja revisá-los.

Alguns logs e comandos úteis para a auditoria da segurança do Linux incluem:

- Exiba o var/log/secure como root para ver o histórico de tentativas de login e outras mensagens de acesso.
- O comando 'last | more' fornece um histórico dos usuários conectados.
- O /var/log/audit/audit.log.[0-9] mantém um log das tentativas de acesso negadas pelo SE Linux. Você precisa ser o usuário root para exibi-los.

Segurança do SELinux

O ACSLS 8.4 foi projetado para execução em ambientes SELinux (Security Enhanced Linux) opcionais. O SELinux fornece controle de acesso a arquivos, diretórios e outros recursos do sistema que vão além da proteção tradicional encontrada em ambientes Unix padrão. Além do acesso de permissão owner-group-public, o SELinux inclui controle de acesso baseado em atribuição de usuário, domínio e contexto. O agente que impõe o controle de acesso sobre todos os recursos do sistema é o kernel Linux.

Em um sistema Linux, o usuário root pode ativar ou desativar a imposição com o comando *`setenforce`*.

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

Use *`Enforcing`* ou 1 para colocar o SELinux no modo de imposição. Use *`Permissive`* ou 0 para colocar o SELinux no modo permissivo.

Para exibir o status atual de imposição do sistema, use o comando *`getenforce`*.

Três módulos de política do SELinux são carregados no kernel quando você instala o ACSLS: allowPostgr, acsdb e acsdb1. Esses módulos fornecem as definições e exceções de imposição necessárias para o ACSLS acessar seu próprio banco de dados e outros recursos do sistema enquanto a imposição do SELinux está ativa. Com esses módulos instalados, você deve ser capaz de executar operações comuns do ACSLS, incluindo operações de banco de dados, como bdb.acsss, rdb.acsss, db_export.sh e db_import.sh, sem a necessidade de desativar a imposição do SELinux.

Para obter mais informações, consulte a seção sobre o SELinux no apêndice ”Troubleshooting” do *StorageTek ACSLS 8.4 Administrator’s Guide*.

Instalando e Configurando o ACSLS

Esta seção explica como instalar com segurança o ACSLS.

Executar uma Instalação Padrão do ACSLS

A execução de uma instalação padrão do ACSLS garante que você terá todos os componentes necessários.

Se você estiver migrando de uma release anterior do ACSLS para outra mais recente, verifique as configurações de variáveis dinâmicas e estáticas para ver se deseja usar opções mais seguras, principalmente no caso da Opção de Segurança de Firewall.

Usar Senhas Fortes para IDs de Usuário do ACSLS

O ACSLS requer os IDs de usuário do ACSLS: acsss, acssa e acsdb. Escolha senhas fortes para esses IDs e altere as senhas frequentemente.

Restringir o Acesso aos Arquivos do ACSLS

Em geral, o ACSLS restringe o acesso aos arquivos do ACSLS somente ao grupo acsls, que inclui os IDs de usuário acsss, acssa, acsdb e root. Alguns arquivos de banco de dados e de diagnóstico só estão acessíveis para um único ID de usuário acsls. O ACSLS é executado com a opção unmask definida como 027.

Os arquivos do ACSLS não devem ser facilmente legíveis ou graváveis. No entanto, restringir o acesso além dos padrões de instalação poderá causar falha nas funções do ACSLS.

Definir ’root’ como o ID de Usuário Efetivo para Três Arquivos do ACSLS

O script de instalação avisa os clientes que o id de usuário efetivo 'root' deve ser definido (setuid) em três arquivos executáveis no sistema de arquivos /export/home/ACSSS:

- `acsss` (Esse binário deve ser executado com privilégios 'root' porque é usado para iniciar e interromper os serviços do sistema necessários ao aplicativo ACSLS.)

- *db_command* (Esse binário inicia e interrompe o mecanismo de banco de dados PostgreSQL que controla e mantém o banco de dados do ACSLS.)
- *get_diags* (Esse binário é acionado por um cliente para coletar informações abrangentes de diagnóstico do sistema que podem ser necessárias no contexto de uma chamada de serviço de suporte.)

Durante a instalação do ACSLS com o pkgadd, os clientes são solicitados a responder à pergunta *Do you want to install these as setuid/setgid files?* Ao responder *y* à pergunta, você permitirá que esses três comandos sejam executados pelos usuários no grupo acsls, embora os utilitários executem determinadas operações do sistema que exigem privilégios root.

Revisar Configurações de Variáveis Estáticas e Dinâmicas do ACSLS

As variáveis estáticas e dinâmicas do ACSLS controlam o comportamento de várias funções do ACSLS. Defina essas variáveis usando o utilitário *acsss_config*. As configurações de segurança de muitas dessas variáveis são abordadas neste documento. Quando as opções referentes a uma variável são apresentadas pelo *acsss_config*, responder com um ponto de interrogação (?) exibirá uma explicação detalhada da variável. Essas informações também estão disponíveis no capítulo ”Setting Variables that Control ACSLS Behavior” do *ACSLS Administrator’s Guide*.

Configurando o WebLogic

O ACSLS 8.1 e releases posteriores utilizam o WebLogic como servidor Web. O WebLogic é instalado com o ACSLS.

Consulte o *Oracle Fusion Middleware; Understanding Security for Oracle WebLogic Server 11g Release 1 (10.3.6)* para ver as opções de proteção de um servidor do WebLogic e as possibilidades de trilha de auditoria com o WebLogic.

Use o utilitário userAdmin.sh do ACSLS para criar e manter usuários do ACSLS GUI

O utilitário *userAdmin.sh* baseado em menus é usado para administrar as senhas de usuário do ACSLS GUI. Você pode adicionar, remover e listar usuários, bem como alterar as senhas de usuários. O WebLogic deve estar em execução para usar esse utilitário. Caso contrário, esse utilitário iniciará o WebLogic e confirmará que ele está on-line antes de exibir o menu.

O utilitário *userAdmin.sh* deve ser executado por root e exige autenticação acsls_admin. A conta de usuário acsls_admin é configurada durante a instalação do ACSLS.

Usando o ACSLS GUI

Para usar o ACSLS GUI, é preciso instalar a versão mais recente do JRE e acessar o ACSLS GUI por meio de um navegador.

Instalar a Versão Mais Recente do JRE nos Sistemas Cliente GUI

Verifique se a última versão do Java Runtime Environment (JRE) está instalada nos sistemas que usarão o ACSLS GUI para acessar o ACSLS.

Acessando o ACSLS GUI

Abra um navegador e insira um URL com o nome de host ou o endereço IP do servidor no seguinte formato:

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

É melhor usar o nome de host totalmente qualificado ou o endereço IP da máquina host. Algumas páginas, incluindo as páginas de ajuda do ACSLS, talvez não sejam exibidas corretamente se o URL não for totalmente resolvido pelo WebLogic.

Se você usar o http com a porta 7001, o WebLogic automaticamente redirecionará você para o https na porta 7002.

Como o WebLogic está usando o protocolo seguro https, seu navegador poderá avisá-lo que o certificado de segurança do site não foi registrado e, portanto, não é confiável. Se tiver certeza de que o URL é sua máquina ACSLS local, você poderá prosseguir com segurança. Nesse momento, você deverá ver a tela de login.

Usando o ACSLS GUI

O AcslsDomain no WebLogic é acessado com o protocolo seguro, https. Esse protocolo utiliza a comunicação criptografada entre o navegador e o servidor usando chaves privadas e certificados digitais. Estas são as opções para obtenção de um certificado digital:

Certificado de demonstração do ACSLS

O ACSLS é fornecido com um certificado chamado 'demo'. Isso garante um nível mínimo de segurança da criptografia, permitindo que os clientes comecem a usar o ACSLS GUI sem quaisquer etapas de configuração adicionais. Em geral, esse método de certificação de demonstração é suficiente quando a interação do cliente com a Biblioteca ACSLS ocorre exclusivamente em uma intranet protegida. No entanto, esse método utiliza uma chave de criptografia de 512 bits que não é suportada em certos navegadores, especialmente no Internet Explorer e no FireFox Versão 39 e acima.

Configurando um certificado digital autoassinado

O ACSLS Installation Guide fornece um método passo a passo para os administradores do ACSLS configurarem um certificado digital autoassinado de 2048 bits. Na seção 'Configuring an SSL Encryption Key', esse método fornece um certificado que é suportado em todos os

navegadores. Os usuários que acessam um site https com um certificado autoassinado são aconselhados a não entrar no site a menos que tenham certeza de que o recurso Web é um site seguro. No contexto dos usuários do ACSLS e do servidor de controle da biblioteca, geralmente esse nível de confiança é bem compreendido e, na maioria dos casos, não é necessário que o site prove sua integridade usando a verificação de assinatura de terceiros.

Certificados digitais assinados por outra autoridade de assinatura

Cabe ao site de cada cliente determinar se é necessário fornecer uma autenticação de certificado de outra autoridade de assinatura, como Verisign ou Entrust.net. O procedimento para gerar esse tipo de certificado digital assinado é descrito no documento on-line da Oracle, Configuring Identity and Trust em:

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

Instalando o ACSLS HA

Se você estiver usando a solução ACSLS High Availability, siga as instruções fornecidas no ACSLS-HA Cluster: Installation, Configuration, and Operations.

3

Recursos de Segurança

Esta seção descreve os mecanismos de segurança específicos oferecidos pelo ACSLS.

O Modelo de Segurança

Os requisitos de segurança do ACSLS surgem da necessidade de proteger os dados: primeiro, contra perda acidental e corrupção; e, segundo, contra tentativas intencionais não autorizadas de acesso ou alteração desses dados. As preocupações secundárias incluem a proteção contra atrasos indevidos no acesso ou no uso dos dados ou até mesmo contra interferência até a negação do serviço.

Os principais recursos de segurança que oferecem essas proteções são:

- Autenticação – garante que somente indivíduos autorizados tenham acesso ao sistema e aos dados.
- Autorização – fornece controle de acesso aos privilégios e dados do sistema. Baseia-se na autenticação para garantir que os indivíduos tenham somente o acesso apropriado.
- Auditoria – permite que os administradores detectem tentativas de violação do mecanismo de autenticação e tentativas ou violações bem-sucedidas do controle de acesso.

Configurando e Usando Autenticação

Por padrão, no Linux ou no Solaris, os usuários do ACSLS são autenticados pelo PAM (Pluggable Authentication Modules). Consulte as páginas man do Solaris ou o *Linux-PAM System Administrators Guide*.

Os usuários do ACSLS GUI são autenticados pelo servidor LDAP incorporado no WebLogic. Consulte o documento Managing the Embedded LDAP Server:

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

Autenticação de Usuário do ACSLS pelos Sistemas Operacionais Solaris ou Linux

Os usuários do ACSLS acsss e acssa devem efetuar login no Solaris ou no Linux e serem autenticados pelo sistema operacional antes de poderem usar o cmd_proc ou, no caso do usuário acsss, antes de executar os comandos de configuração e os utilitários do ACSLS. O ID de usuário acsdb também é usado para operações relacionadas ao banco de dados. Como

parte do processo de instalação do ACSLS, os clientes devem definir as senhas para esses IDs na primeira vez que efetuam login. Consulte o *ACSLS Installation Guide* para obter detalhes.

Autenticação de Usuário do ACSLS GUI pelo WebLogic

Os usuários do ACSLS GUI devem efetuar login e serem autenticados pelo WebLogic. O acsls_admin é criado durante a instalação do ACSLS, e os clientes devem definir sua senha. Os clientes podem adicionar outros usuários da GUI, conforme desejado, com o utilitário `userAdmin.sh`. Para obter detalhes, consulte o *ACSLS Installation Guide* e o *ACSLS Administrator's Guide*, capítulo "Utilities", no `userAdmin.sh`.

Considerações de Auditoria

As considerações gerais de auditoria que se aplicam ao ACSLS são descritas aqui.

Mantendo Gerenciáveis as Informações Auditadas

Embora o processo de auditoria tenha um custo relativamente baixo, limite o número de eventos auditados na medida do possível. Isso minimiza o impacto em termos de desempenho na execução das instruções auditadas e o tamanho da trilha de auditoria, facilitando a análise, a compreensão e o gerenciamento.

Use as seguintes diretrizes ao elaborar uma estratégia de auditoria:

Avalie a finalidade da auditoria

Depois de ter uma clara compreensão das razões da auditoria, você pode traçar uma estratégia de auditoria apropriada e evitar uma auditoria desnecessária.

Auditoria competente

Faça auditoria do número mínimo de instruções, usuários ou objetos necessários para obter as informações desejadas.

Configurando e Usando os Logs de Auditoria do ACSLS

O ACSLS possui vários logs de informações que permitem registrar e inspecionar a atividade do ACSLS.

- Você pode exibir a maioria deles usando vi e outros editores. Os Eventos do Sistema só podem ser exibidos usando o ACSLS GUI.
- A maioria desses logs pode ser automaticamente arquivada quando atinge um tamanho definido pelo usuário, e um número de logs especificado pelo cliente será retido. Para evitar que o sistema de arquivos do ACSLS fique cheio, há um limite configurável de número de logs que será retido. Caso queira reter mais desses arquivos de log ou retê-los em outro sistema, você precisará desenvolver seu próprio procedimento para arquivá-los em um local que tenha espaço suficiente.

- O tamanho, o número de logs arquivados a ser retido e outras características desses arquivos são definidos pelas variáveis dinâmicas e estáticas do ACSLS.

Diretório de Logs do ACSLS

O diretório de logs do ACSLS é controlado pela variável estática LOG_PATH. O padrão é o diretório $ACS_HOME/log. Esse diretório inclui estes logs:

acsss_event.log
Registra as mensagens relativas a eventos de sistema, eventos de biblioteca e erros significativos do ACSLS.

Quando o acsss_event.log atinge o tamanho limite definido pela variável dinâmica LOG _SIZE, ele é copiado para o event0.log e limpo. Durante o processo de cópia, os logs de evento retidos são copiados para os logs retidos de numeração mais alta, e o log retido com a maior numeração é sobreposto. Por exemplo: o event8.log é copiado sobre o event9.log, o evento7.log é copiado sobre o event8.log, …, o event0.log é copiado sobre o event1.log, o acsss_event.log é copiado sobre o event0.log, e o acsss_event.log é limpo. Isso é controlado pelas seguintes variáveis:

- *EVENT_FILE_NUMBER* especifica o número de logs de eventos a serem retidos.
- *LOG_SIZE* especifica o tamanho limite no qual o log de eventos é copiado para um log de eventos retido e truncado.

Use o utilitário *`greplog`* para filtrar o log acsss_event de modo a incluir ou excluir mensagens que contenham palavras-chave específicas. Consulte greplog no capítulo ”Utilities” do *ACSLS Administrator's Guide* para obter mais detalhes.

Logs de configuração
Existem dois logs que registram detalhes quando o ACSLS atualiza a configuração de biblioteca armazenada no banco de dados do ACSLS. As alterações de configuração do *`acsss_config`* e do *`Dynamic Config`* (o utilitário *`config`*) são registradas aqui.

acsss_config.log
Registra os detalhes de todas as configurações ou reconfigurações da(s) biblioteca(s) que o ACSLS suporta. A última alteração de configuração é adicionada ao registro de configurações anteriores.

acsss_config_event.log
Registra os eventos durante o processo de configuração ou reconfiguração.

rpTrail.log
Registra a resposta de todas as solicitações ao ACSLS feitas por clientes ACSAPI ou pelo cmd_proc, bem como as respostas a todas as solicitações feitas à GUI ou à interface entre o SCSI Client e bibliotecas lógicas, exceto no caso de consultas do banco de dados. As informações registradas incluem o solicitante, a solicitação e o carimbo de data e hora da solicitação.

rpTrail.log é gerenciado pelas seguintes variáveis:

- *LM_RP_TRAIL* ativa essa trilha de auditoria de eventos do ACSLS. O padrão é TRUE.

- *RP_TRAIL_LOG_SIZE* especifica o tamanho limite no qual o rpTrail.log é compactado e arquivado.
- *RP_TRAIL_FILE_NUM* especifica o número de logs rpTrail arquivados a serem retidos.
- *RP_TRAIL_DIAG* especifica se as mensagens do rpTrail devem incluir informações de diagnóstico adicionais. O padrão é FALSE.

Estatísticas de Volume da Biblioteca
Registra todos os eventos relacionados a volumes (cartuchos) em uma biblioteca de fitas, incluindo se um volume foi montado, desmontado, movido, informado, ejetado ou localizado pela auditoria ou pelo processo Cartridge Recovery. Se o recurso de Estatísticas de Volume da Biblioteca estiver ativado, essas informações serão registradas no acsss_stats.log.

As Estatísticas de Volume da Biblioteca são gerenciadas pelas seguintes variáveis:

- *LIB_VOL_STATS* ativa o recurso de Estatísticas de Volume da Biblioteca. O padrão é OFF.
- *VOL_STATS_FILE_NUM* especifica o número de arquivos acsss_stats.log arquivados a serem retidos.
- *VOL_STATS_FILE_SIZE* especifica o tamanho limite no qual o acsss_stats.log é arquivado.

Diretório de Logs/sslm do ACSLS

No diretório de logs do ACSLS, as informações sobre o ACSLS GUI e a interface entre o SCSI Client e bibliotecas lógicas são registradas no diretório sslm. Esse diretório inclui links para os logs de auditoria do WebLogic. O diretório sslm inclui estes logs:

slim_event.g#.log[.pp#]
Registra os eventos do ACSLS GUI e da interface do SCSI Client. Inclui mensagens de alterações de configuração de bibliotecas lógicas e eventos do SCSI Client.

- O .g# é o número de geração desse log.
- O .pp# é o número do processo paralelo desse log. Se houver vários processos registrados ao mesmo tempo, os logs dos processos adicionais receberão um número de processo paralelo.

smce_trace.log
Rastreia a atividade de SCSI Clients para as bibliotecas lógicas do ACSLS usando a emulação do SCSI Media Changer Interface.

guiAccess.log
É um link para o access.log do WebLogic. Consulte Configurando e Usando os Logs de Auditoria do WebLogic.

AcslsDomain.log
É um link para o AcslsDomain.log do WebLogic. Consulte Configurando e Usando os Logs de Auditoria do WebLogic.

AdminServer.log
É um link para o AdminServer.log do WebLogic. Consulte Configurando e Usando os Logs de Auditoria do WebLogic.

Exibindo Trilhas de Auditoria do ACSLS no Log Viewer da GUI

Acesse o Log Viewer na seção Configuração e Administração da Árvore de Navegação da GUI. O Log Viewer exibe informações combinadas do ???TITLE??? and the ???TITLE???.

Exibir Eventos de Sistema na GUI

Você também pode exibir Eventos de Sistema na seção Configuração e Administração da árvore de navegação da GUI. Toda operação de biblioteca discreta é registrada no log System Events. Cada registro desse log contém um carimbo de data e hora de evento, um tipo de evento e uma descrição do evento.

Configurando e Usando os Logs de Auditoria do Solaris

Determine a política de auditoria do Solaris. A seção Oracle Solaris Auditing do manual *Oracle System Administration: Security Services* pode ajudá-lo a planejar quais eventos serão auditados, onde os logs de auditoria serão salvos e como você deseja revisá-los.

Se não você tiver ativado trilhas de auditoria personalizadas do Solaris, estas trilhas de auditoria de logins e comandos do Unix executados pelos usuários acsss, acsdb e acssa estarão disponíveis:

- Os usuários que estão atualmente conectados no Unix são registrados no Unix utmpx e o acesso de usuários anteriores é registrado no banco de dados wtmpx.
- Use o comando `last` para ver todos os acessos de um ID de usuário (por exemplo, `last acsss`). Para obter mais informações, consulte as páginas man referentes a: wtmpx, `last` e getutxent.
- Os arquivos .*_history ([dot]*_history) do diretório home de um usuário registram os comando executados por esse usuário.

  Para o usuário acsss, estão incluídos:
  - .bash_history
  - .psql_history
  - .sh_history

  No Solaris, /var/adm/sulog registra as tentativas bem-sucedidas e malsucedidas de executar `su` e se tornar superusuário ou outro usuário.

Configurando e Usando os Logs de Auditoria do Linux

Consulte as seções Configuring and Using Auditing e Configuring and Using System Logging no *Oracle Linux: Security Guide for Release 6* para obter detalhes sobre como coletar e analisar os logs de auditoria e do sistema.

Configurando e Usando os Logs de Auditoria do WebLogic

Consulte o *Oracle Fusion Middleware; Understanding Security for Oracle WebLogic Server 11g Release 1 (10.3.6)* para ver as opções de proteção de um servidor do WebLogic e as possibilidades de trilha de auditoria com o WebLogic.

O WebLogic registra os acessos ao ACSLS GUI no seguinte diretório:

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

Esse diretório inclui os seguintes arquivos:

- access.log
  - Existem versões arquivadas denominadas access.log##### (por exemplo, access .log00001)
  - Fornece uma trilha de auditoria detalhada de uma atividade de usuário da GUI.
  - Para logins, procure por ”AcslsLoginForm”.

    Observação:

    Existe um link para o log de acesso no: $ACS_HOME/logs/sslm/guiAccess.log.
- AcslsDomain.log
  - Informa as operações do WebLogic e do ACSLS GUI.

    Observação:

    Existe um link para o log de acesso no: $ACS_HOME/logs/sslm/AcslsDomain.log.
- AdminServer.log
  - Informa as operações do WebLogic e do ACSLS GUI.

    Observação:

    Existe um link para o log de acesso no: $ACS_HOME/logs/sslm/AdminServer.log.

4

Considerações de Segurança para Desenvolvedores

Esta seção fornece informações úteis para desenvolver ou suportar aplicativos que utilizam o ACSLS para gerenciar StorageTek Tape Libraries da Oracle.

Ativar a Segurança de Firewall no Servidor do Aplicativo Cliente

Restrinja as portas usadas para a comunicação e desative o portmapper no servidor do aplicativo cliente ativando a segurança do firewall. Consulte o *CSC Developer's Toolkit User's Guide*, "Appendix B: Firewall-Secure Operation."

Apêndice A

Lista de Verificação para uma Implantação Segura

1. Imponha o gerenciamento de senhas.
2. Restrinja o acesso à rede.
   a. O ACSLS e as bibliotecas de fitas que ele gerencia devem estar protegidos pelo firewall corporativo.
   b. Ative a Opção de Segurança de Firewall do ACSLS.
   c. Considere ativar a segurança de firewall para aplicativos cliente do ACSLS.
3. Proteja o sistema operacional Solaris ou Linux.
4. Aplique todos os patches e soluções alternativas de segurança.
5. Entre em contato com a equipe do Oracle Services, do Oracle Tape Library Engineering ou com um representante de conta se você encontrar vulnerabilidades no StorageTek ACSLS.

Apêndice B

Referências

Documentação do ACSLS
A documentação do ACSLS é salva em bibliotecas organizadas por release do ACSLS. Você pode acessá-la na página Tape Storage Documentation.

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

(As bibliotecas de documentação individuais do ACSLS incluem o número de versão em seus URLs. Portanto, um link para uma biblioteca específica se torna obsoleto assim que a biblioteca é atualizada.) A documentação do ACSLS inclui:

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

  Isso inclui os requisitos de software e hardware, uma visão geral do ACSLS, além das bibliotecas de fitas, unidades de fita e mídias suportadas.
- Mensagens do ACSLS (e códigos de status)
- *ACSLS Release Notes*
- *ACSLS-HA Cluster: Installation, Configuration, and Operations*
- *ACSLS Interface Reference Manual*

Oracle Solaris
A Biblioteca de Informações do Oracle Solaris 11.2 inclui o *Securing the Oracle Solaris 11 Operating System*. Consulte-a para obter detalhes.

Oracle Linux
A Biblioteca de Informações do Oracle Linux 6 inclui o *Oracle Linux 6 Security Guide*. Consulte-a para obter detalhes.

Oracle WebLogic
A Oracle WebLogic Server Documentation Library for WebLogic 10.3.6 (usada pelo ACSLS 8.2) contém uma seção sobre Segurança.

O *Oracle Fusion Middleware; Understanding Security for Oracle WebLogic Server 11g Release 1 (10.3.6)* explica os detalhes de como proteger um servidor WebLogic.