StorageTek Automated Cartridge System Library Software

Guide de sécurité

Version 8.4

E68247-01

Septembre 2015

ORACLE

StorageTek Automated Cartridge System Library Software
Guide de sécurité

E68247-01

Table des matières

Préface

Ce document décrit les fonctions de sécurité du logiciel StorageTek Automated Cartridge System Library Software (ACSLS) d'Oracle et la solution haute disponibilité ACSLS (ACSLS HA).ACSLS HA et l'agent SNMP ACSLS s'exécutant également sur le serveur ACSLS, la protection du serveur ACSLS garantit la protection d'ACSLS, d'ACSLS HA et de l'agent SNMP ACSLS.

Public

Ce guide s'adresse à toute personne pouvant être amenée à utiliser les fonctions de sécurité et à effectuer des opérations d'installation et de configuration d'ACSLS.

Accessibilité de la documentation

Pour plus d’informations sur l’engagement d’Oracle pour l’accessibilité à la documentation, visitez le site Web Oracle Accessibility Program, à l'adresse `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Accès aux services de support Oracle
Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si vous êtes malentendant.

1

Présentation

Cette section contient une présentation d'ACSLS et explique les principes généraux de sécurité des applications.

Remarque:

Dans ce document, le produit Automated Cartridge System Library Software est également désigné par le sigle ACSLS et la solution haute disponibilité ACSLS est désignée par ACSLS HA.

Présentation du produit

ACSLS est le logiciel serveur de bibliothèque de bandes d'Oracle qui contrôle une ou plusieurs bibliothèques de bandes StorageTek pour les clients de systèmes ouverts. Un système automatisé de cartouches (ACS, Automated Cartridge System) est une bibliothèque de bandes ou un groupe de bibliothèques de bandes connectées via des ports PTP (Pass-Thru-Port). ACSLS gère un ou plusieurs ACS via des commandes de "chemin de contrôle" transmises sur un réseau. Le logiciel inclut un composant d'administration système, des interfaces vers les applications système client et des équipements de gestion de bibliothèques.

Principes généraux de sécurité

Les principes suivants sont essentiels pour une utilisation sécurisée des produits.

Mise à jour du logiciel

L'un des principes fondamentaux d'une utilisation sécurisée est l'installation régulière des dernières versions et patches du logiciel. Ce document suppose que vous exécutez ACSLS 8 .4 ou une version ultérieure et que vous avez installé toutes les versions de maintenance correspondantes. En exécutant la dernière version d'ACSLS, vous êtes certain de disposer des dernières améliorations et corrections.

Appliquez tous les correctifs de sécurité importants au système d'exploitation et aux services installés avec ce dernier. Appliquez ces correctifs de façon sélective, car l'application de toutes les mises à jour disponibles risque d'installer de nouvelles fonctionnalités et même de nouvelles versions du SE avec lesquelles ACSLS et ACSLS HA n'ont pas été testés.

Limitation de l'accès via le réseau aux services critiques

Le logiciel ACSLS et les bibliothèques qu'il gère doivent être protégés par un pare-feu. Il est recommandé d'utiliser un réseau privé pour les communications TCP/IP entre ACSLS et les bibliothèques de bandes.

Application du principe du moindre privilège

Le principe du moindre privilège stipule qu'il ne faut octroyer aux utilisateurs que les privilèges strictement nécessaires à la réalisation de leur travail. Passez régulièrement en revue les privilèges des utilisateurs pour déterminer s'ils sont en accord avec les responsabilités professionnelles de ces derniers.

Appliqué à ACSLS, ce principe signifie que les utilisateurs qui n'exécutent que des commandes de routine à l'aide de cmd_proc doivent se connecter en tant qu'utilisateur acssa. Les administrateurs système qui se connectent en tant qu'utilisateur acsss ont accès à un plus grand nombre d'utilitaires et de commandes de configuration. Le recours à l'ID utilisateur acsdb n'est pas nécessaire pour les opérations normales.

Surveillance de l'activité du système

La sécurité du système repose sur trois fondements : des protocoles de sécurité efficaces, la configuration correcte du système et la surveillance du système. Cette troisième exigence est satisfaite par la réalisation d'audits et le passage en revue des enregistrements d'audit. Chacun des composants d'un système dispose de dispositifs de surveillance plus ou moins étendus. Suivez les conseils relatifs à l'audit figurant dans ce document et surveillez régulièrement les enregistrements d'audit

Consultation des dernières informations de sécurité

Oracle s'efforce d'améliorer continuellement les logiciels et la documentation. Consultez ce document à chaque nouvelle version logicielle.

2

Installation sécurisée

Cette section détaille les processus de planification et d'implémentation à mettre en oeuvre pour garantir une installation et une configuration sécurisées. Elle décrit également plusieurs topologies de déploiement recommandées pour ACSLS.

Présentation de votre environnement

Les réponses aux questions suivantes peuvent vous aider à comprendre les exigences de sécurité :

Quelles sont les ressources à protéger ?

Les ressources principales gérées par ACSLS sont des bibliothèques de bandes, des lecteurs et des cartouches. Ces ressources doivent être protégées de tout accès malveillant ou par inadvertance. Empêchez par exemple les utilisateurs de se connecter à un autre serveur ACSLS par mégarde en associant des mots de passe différents aux ID utilisateur ACSLS sur les différents serveurs.

De quels utilisateurs les ressources doivent-elles être protégées ?

Il faut protéger les ressources de stockage sur bande des accès non autorisés internes aussi bien qu'externes.

Que peut-il se passer en cas de défaillance de la protection des ressources stratégiques ?

ACSLS peut monter des cartouches sur des lecteurs de bande. Si un utilisateur peut se connecter au lecteur de bande en passant par le chemin d'accès des données, il peut également lire les données sur la bande si celles-ci ne sont pas chiffrées.

Des utilisateurs ayant accès à la fois à ACSLS et à une bibliothèque de bandes peuvent insérer et éjecter des cartouches d'une bibliothèque de bandes.

Procédure recommandée pour la sécurisation d'ACSLS

Suivez cette procédure lors de la sécurisation d'ACSLS et des composants d'infrastructure requis afin d'assurer le bon fonctionnement d'ACSLS une fois les modifications effectuées :

- Installez ACSLS.
- Vérifiez qu'ACSLS fonctionne correctement. Pour cela, vérifiez la configuration et l'audit de bibliothèques, le montage et le démontage de bandes, l'insertion et l'éjection de bandes, ainsi que la sauvegarde et la restauration de la base de données.
- Implémentez les modifications pour renforcer la sécurité.
- Vérifiez qu'ACSLS fonctionne toujours correctement.

Sécurisation de la communication Internet d'ACSLS

Cette section décrit les recommandations de déploiement d'ACSLS pour sécuriser l'accès à Internet.

Sécurisation d'ACSLS et des bibliothèques de bandes derrière le pare-feu de l'entreprise

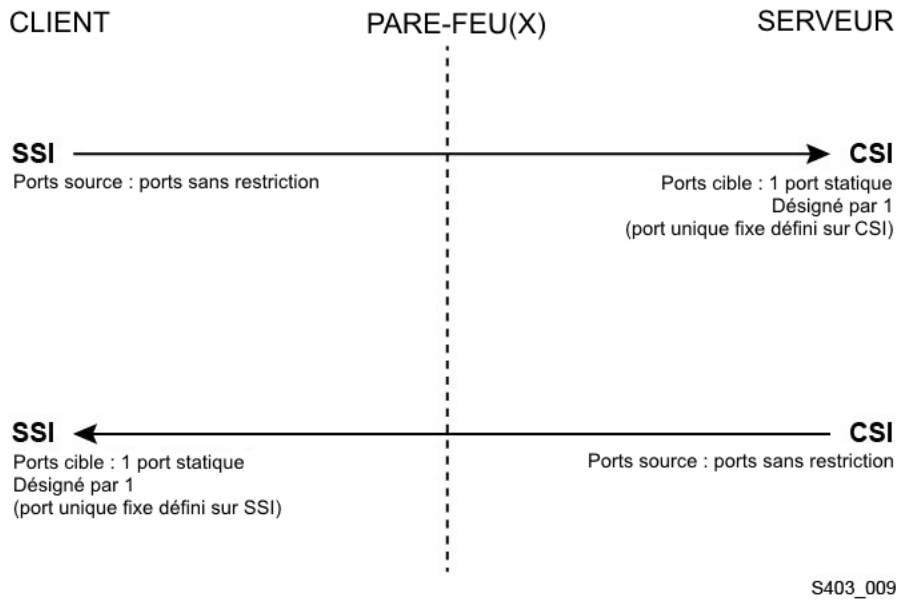
Le logiciel ACSLS et les bibliothèques de bandes qu'il prend en charge doivent être déployés derrière le pare-feu de l'entreprise. Si un utilisateur travaillant à distance a besoin de se connecter au serveur ACSLS, il peut y accéder en passant par un VPN.

Remarque:

Si vous disposez d'un pare-feu de périmètre IPv4, il doit être configuré pour rejeter tous les paquets sortants 41 du protocole IPv4 et les paquets 3544 du port UDP, afin d'empêcher que des hôtes Internet utilisent du trafic transitant par des tunnels IPv6 sur IPv4 pour atteindre des hôtes internes.

Option Firewall Security Option d'ACSLS

Si des applications clientes qui utilisent ACSLS pour le montage de bandes et la gestion de bibliothèques de bandes sont séparées d'ACSLS par un pare-feu, nous vous recommandons d'activer l'option Firewall Security Option. Même si les applications clientes ne sont pas séparées d'ACSLS par un pare-feu, l'implémentation de l'option Firewall Security Option sécurise davantage ACSLS en limitant les ports utilisés pour la communication entre ACSLS et ses applications clientes, comme illustré ci-dessous. C'est pour ces raisons que la variable statique CSI_FIREWALL_SECURE est, par défaut, définie sur TRUE dans ACSLS à partir de la version 8.1.



Pour plus d'informations, reportez-vous à l'annexe relative à l'option Firewall Security Option du *guide de l'administrateur d'ACSLS*.

Ports Ethernet utilisés pour la communication d'ACSLS

- Les ports suivants sont utilisés sur le serveur ACSLS. Assurez-vous que les éventuels pare-feux sont configurés pour permettre au trafic d'accéder à ces ports. Cela concerne notamment les pare-feux implémentés par ipfilter sous Solaris ou par iptables sous Linux.
  - 22 dans les deux directions – utilisé pour l'accès ssh.
  - 111 Portmapper, sauf si Portmapper a été désactivé.
  - 115 utilisé pour SFTP (Secure File Transfer Protocol).
  - 161 port par défaut pour l'agent SNMP d'ACSLS - get/set/walk.
  - 162 port par défaut pour l'agent SNMP d'ACSLS - déroutements.

    Remarque:

    Les ports utilisés par l'agent SNMP d'ACSLS peuvent être configurés à l'aide de la commande : *`AcslsAgtdSnmpConf [ -p port ] [-t trap port] [-d]`*. L'option *`-d`* affiche le paramétrage actuel. Après avoir modifié les paramètres du port, vous devez redémarrer l'agent à l'aide de la commande *`agentRegister`*.

  - 5432 port par défaut pour la communication interne entre ACSLS et la base de données PostgreSQL (la variable d'environnement PGPORT pour l'ID utilisateur acsss).

    Si le port 5432 est déjà utilisé, le premier numéro de port supérieur disponible est utilisé.

    Remarque:

    Il suffit que le port 5432 soit accessible à partir de localhost (127.0.0.1).

  - 7001 et 7002 - utilisé par WebLogic et l'interface graphique d'ACSLS.

  - 30031 ou port d'écoute CSI d'ACSLS, défini par CSI_INET_PORT.
  - 50003 port utilisé pour la communication interne depuis l'interface graphique et les composants Java d'ACSLS vers le traitement ACSLS hérité. Il ne peut pas être configuré.

- Pour permettre aux applications clientes de communiquer avec ACSLS par le biais de l'ACSAPI, les ports suivants doivent être ouverts :
  - L'application cliente doit pouvoir communiquer avec le port d'écoute CSI d'ACSLS. Par défaut, il s'agit du port 30031, qui est défini par la variable statique CSI_INET_PORT.

    La commande suivante exécutée depuis le shell Unix permet d'identifier les ports utilisés par ACSLS pour écouter les demandes des clients ACSAPI :

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

    Les ID des ports sont listés dans le dernier champ de l'affichage.
  - Le client ACSAPI (un serveur NetBackup ou SAM-QFS par exemple) définit son port entrant fixe à l'aide de la variable d'environnement SSI_INET_PORT. Spécifiez un port compris entre 1024 et 65535, à l'exception des ports 50001 et 50004. Le serveur ACSLS doit pouvoir communiquer avec ce port.

    Remarque:

    Sur un serveur client ACSAPI, les ports 50001 and 50004 sont utilisés pour la communication inter-processus entre le domaine AF_INET et le mini journal des événements ainsi que pour la communication entre les applications clientes et SSI.

  Pour plus d'informations sur la communication entre les applications clientes et ACSLS, reportez-vous à l'annexe relative à l'option Firewall Security Option du *guide de l'administrateur d'ACSLS*.

- Si le composant XAPI est installé, le serveur XAPI utilise un port d'écoute fixe pour recevoir les demandes TCP entrantes des clients ELS. Le port d'écoute XAPI est défini par la variable statique XAPI_PORT. XAPI_PORT est renseigné par défaut par 50020. Il doit être compris entre 1024 et 65535, et ne peut pas entrer en conflit avec un autre port utilisé par ACSLS ou d'autres applications.

  Pour plus d'informations sur XAPI_PORT, reportez-vous à l'annexe relative à l'interface client XAPI du *guide de l'administrateur ACSLS*. Cette annexe fournit également des détails sur l'affichage et la définition de la variable statique XAPI_PORT.

- Les ports suivants doivent être ouverts dans une bibliothèque SL8500 ou SL3000 :

  ACSLS communique avec ces ports grâce aux connexions Ethernet 2A et 2B d'une bibliothèque SL8500 ou SL3000. Si la communication est bloquée entre ACSLS et ces ports, ACSLS ne peut pas gérer la bibliothèque.
  - 50001 – Utilisé pour toutes les communications normales entre ACSLS et la bibliothèque

- 50002 – Utilisé par ACSLS HA pour déterminer si le noeud HA de rechange peut communiquer avec la bibliothèque avant le basculement sur le noeud de rechange.

Configuration des pare-feux qui s'exécutent sur le serveur ACSLS

Parallèlement aux pare-feux externes, il est possible d'implémenter une protection par pare-feu sur votre serveur ACSLS au moyen d'ipfilter sous Solaris ou d'iptables sous Linux. Cette section indique comment gérer ces pare-feux qui s'exécutent sur votre serveur ACSLS.

- Gestion d'ipfilter sous Solaris :

  Pour plus d'informations, consultez les pages de manuel relatives à ipf et à ipfilter.

  - Le pare-feu ipfilter est activé (ou désactivé) par 'root' à l'aide de la commande :

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

  - Pour connaître le statut actuel d'ipfilter :

    ```
    svcs ipfilter
    ```

  - Les stratégies de pare-feu sont définies dans le fichier : /etc/ipf/ipf.conf

    Pour permettre à des composants hébergés sur l'hôte local de communiquer librement (ACSLS et WebLogic par exemple, ou l'interface graphique et la base de données ACSLS), insérez une instruction semblable aux suivantes :

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

    ou

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

    Vous devez définir des stratégies qui autorisent l'accès à tous les ports requis pour ACSLS. Par exemple, pour inclure une stratégie qui permet à des navigateurs Web distants d'accéder à l'interface graphique d'ACSLS, vous devez ouvrir les ports 7001 et 7002.

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

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

    Une fois que vous avez identifié les ports utilisés par ACSLS pour écouter les demandes émanant de clients ACSAPI, insérez des instructions 'pass in quick' pour chacun de ces ports.

    Il peut être nécessaire d'inclure une instruction 'pass in quick' pour le port Portmapper RPC : 111.

La dernière instruction de l'ensemble de règles proposé, "block in from any", indique qu'aucun trafic ne doit atteindre l'hôte, sauf si cela a été expressément autorisé dans une instruction précédente.

- Gestion d'iptables sous Linux :
  - Le pare-feu iptables est activé (ou désactivé) par 'root' à l'aide de la commande :

    ```
    service iptables start (service iptables stop)
    ```
  - Pour vérifier le statut d'iptables :

    ```
    service iptables status
    ```
  - Le fichier de stratégie pour iptables est /etc/sysconfig/iptables :

    Vous devez définir des stratégies qui autorisent l'accès à tous les ports requis pour ACSLS. Par exemple, pour inclure une stratégie qui autorise l'accès http/https distant à l'interface graphique d'ACSLS, vous devez mettre à jour ce fichier afin d'insérer des exceptions pour les ports 7001 et 7002 à l'aide d'instructions telles que les suivantes :

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

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

    Une fois que vous avez identifié les ports utilisés par ACSLS pour écouter les demandes émanant de clients ACSAPI, vous devez ajouter des exceptions pour chacun de ces ports au fichier de stratégie iptables. Il peut être nécessaire d'inclure une instruction d'exception pour le port Portmapper RPC : 111.

Installation et configuration de Solaris

Cette section indique comment installer et configurer Solaris de façon sécurisée.

Voici quelques recommandations :

- Appliquez tous les correctifs de sécurité importants au système d'exploitation et aux services installés avec ce dernier. Appliquez ces correctifs de façon sélective, car l'application de toutes les mises à jour disponibles risque d'installer de nouvelles fonctionnalités et même de nouvelles versions du SE avec lesquelles ACSLS et ACSLS HA n'ont pas été testés.
- Désactivez telnet et rlogin. A leur place, utilisez ssh. Désactivez également ftp et utilisez à sa place sftp.

  Désactivez les services telnet, rlogin et ftp en émettant les commandes suivantes en tant qu'utilisateur root.

  Pour voir tous les services :

  ```
  svcs
  ```

Pour désactiver telnet, rlogin et ftp :

```
svcadm disable telnet

svcadm disable rlogin

svcadm disable ftp
```

- Ne désactivez pas ssh. Il est préférable que les utilisateurs se connectent à distance à ACSLS à l'aide de ssh et non à l'aide de telnet ou rlogin. Ne désactivez pas non plus sftp.
- ACSLS nécessite rpc-bind. Ne le désactivez pas.

  Si Solaris est installé avec l'option Secure by Default (sécurisé par défaut), vous devez modifier une propriété de configuration réseau pour rpc-bind pour permettre aux clients ACSAPI d'envoyer des demandes à ACSLS.

  Pour plus d'informations, reportez-vous à la section décrivant l'installation de Solaris dans le chapitre traitant de l'installation d'ACSLS sur Solaris dans le *manuel d'installation d'ACSLS*.
- Certains ports Ethernet sur le serveur ACSLS doivent être ouverts pour permettre la communication avec ACSLS. Les applications clientes utilisent des ports Ethernet spécifiques pour communiquer avec ACSLS, et ACSLS communique avec des ports spécifiques sur les bibliothèques de bandes. Reportez-vous à la section Ports Ethernet utilisés pour la communication d'ACSLS pour connaître les ports qui doivent être disponibles pour la communication d'ACSLS. Sur le serveur ACSLS, assurez-vous qu'ipfilter est configuré de manière à permettre au trafic d'accéder aux ports utilisés par ACSLS.

Déterminez votre stratégie d'audit Solaris. Reportez-vous à la section "Audit dans Oracle Solaris" du manuel "Administration d'Oracle Solaris : Services de sécurité" pour savoir quels événements soumettre à un audit, où enregistrer les journaux d'audit et comme passer en revue les journaux d'audit.

Installation et configuration de Linux

Suggestions pour l'installation et la configuration sécurisées de Linux :

- Appliquez tous les correctifs de sécurité importants au système d'exploitation et aux services installés avec ce dernier. Appliquez ces correctifs de façon sélective, car l'application de toutes les mises à jour disponibles risque d'installer de nouvelles fonctionnalités et même de nouvelles versions du SE avec lesquelles ACSLS et ACSLS HA n'ont pas été testés.
- Assurez-vous que telnet et rlogin ne sont pas installés ou qu'ils sont désactivés. A leur place, utilisez ssh.

  Assurez-vous également que ftp n'est pas installé ou qu'il est désactivé. A sa place, utilisez sftp.

Pour voir tous les services, connectez-vous en tant qu'utilisateur root et :

```
service –-status-all
```

- Pour supprimer des services de manière permanente, utilisez :

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

- Ne désactivez pas ssh. Il est préférable que les utilisateurs se connectent à distance à ACSLS à l'aide de ssh et non à l'aide de telnet ou rlogin. Ne désactivez pas non plus sftp.
- Les services réseau, plus précisément rpcbind, doivent être activés pour permettre la communication client ACSLS.

  Sous Linux, lancez rpc avec l'indicateur –i.
- Certains ports Ethernet sur le serveur ACSLS doivent être ouverts pour permettre la communication avec ACSLS. Les applications clientes utilisent des ports Ethernet spécifiques pour communiquer avec ACSLS, et ACSLS communique avec des ports spécifiques sur les bibliothèques de bandes. Reportez-vous à la section Ports Ethernet utilisés pour la communication d'ACSLS pour connaître les ports qui doivent être disponibles pour la communication d'ACSLS. Sur le serveur ACSLS, assurez-vous que iptables est configuré de manière à permettre au trafic d'accéder aux ports utilisés par ACSLS.

Audit de la sécurité de Linux

Déterminez vos stratégies d'audit pour Linux. Reportez-vous à la section relative à la configuration et à l'utilisation de l'audit du *guide de sécurité de la version 6 d'Oracle Linux* pour savoir quels événements soumettre à un audit, où enregistrer les journaux d'audit et comme passer en revue les journaux d'audit.

Les journaux système et commandes suivants peuvent être utiles pour examiner la sécurité de Linux :

- Affichez var/log/secure en tant que root pour voir l'historique des tentatives de connexion et les messages d'accès.
- La commande 'last | more' fournit un historique des utilisateurs connectés.
- Le journal /var/log/audit/audit.log.[0-9] consigne les tentatives d'accès qui ont été rejetées par SE Linux. Vous devez être un utilisateur root pour les voir.

Sécurité SELinux

ACSLS 8.4 est conçu pour fonctionner dans des environnements équipés du module optionnel Security Enhanced Linux. SELinux fournit un contrôle d'accès aux fichiers, aux répertoires et aux autres ressources système qui dépasse le niveau de protection standard des environnements Unix. Outre l'accès par autorisation propriétaire-groupe-public, SELinux inclut un contrôle d'accès basé sur les rôles des utilisateurs, les domaines et les contextes. L'agent qui applique le contrôle d'accès à toutes les ressources système est le noyau Linux.

L'utilisateur root sur un système Linux peut activer ou désactiver l'application à l'aide de la commande *setenforce*.

setenforce [Enforcing | Permissive | 1 | 0]

Utilisez *Enforcing* ou 1 pour placer SELinux en mode "Appliqué" (Enforcing). Utilisez *Permissive* ou 0 pour placer SELinux en mode "Permissif" (Permissive).

Servez-vous de la commande *getenforce* pour voir le statut d'application actuel du système.

Trois modules de stratégie SELinux sont chargés dans le noyau lorsque vous installez ACSLS : allowPostgr, acsdb et acsdb1. Ces modules fournissent les définitions et les exceptions à l'application nécessaires pour permettre à ACSLS d'accéder à sa propre base de données et aux autres ressources système lorsque l'application de SELinux est active. Une fois ces modules installés, vous pouvez effectuer toutes les opérations ACSLS normales, y compris des opérations sur la base de données telles que bdb.acsss, rdb.acsss, db_export.sh et db_import.sh, sans avoir à désactiver l'application de SELinux.

Pour plus d'informations, reportez-vous à la section relative à SELinux dans l'annexe traitant du Dépannage dans le *guide de l'administrateur de StorageTek ACSLS 8.4*.

Installation et configuration d'ACSLS

Cette section explique comment installer ACSLS de manière sécurisée.

Installation standard d'ACSLS

En effectuant une installation standard d'ACSLS, vous êtes certain de disposer de tous les composants nécessaires.

Si vous migrez d'une version d'ACSLS vers une version supérieure du logiciel, passez en revue le paramétrage des variables dynamiques et statiques afin de décider si vous souhaitez opter pour des options plus sécurisées, en particulier en ce qui concerne l'option Firewall Secure Option.

Utilisation de mots de passe fiables pour les ID utilisateur ACSLS

ACSLS nécessite les ID utilisateurs ACSLS : acsss, acssa et acsdb. Choisissez des mots de passe fiables et modifiez-les régulièrement.

Limitation de l'accès aux fichiers d'ACSLS

En règle générale, ACSLS limite l'accès à ses fichiers au groupe acsls, qui inclut les ID utilisateur acsss, acssa, acsdb et root. Certains fichiers de la base de données et de diagnostic

sont seulement accessibles par un ID utilisateur acsls unique. ACSLS fonctionne avec un paramètre umask de 027.

Il n'est pas recommandé de rendre les fichiers ACSLS lisibles ou inscriptibles par tous. Cependant, la définition de paramètres d'accès plus restrictifs que les paramètres par défaut peut entraîner l'échec de fonctions d'ACSLS.

Définition de "root" en tant qu'ID utilisateur effectif pour trois fichiers ACSLS

Le script d'installation recommande aux clients de définir l'id utilisateur effectif 'root' (setuid) dans trois fichiers exécutables dans le système de fichiers /export/home/ACSSS :

- *`acsss`* (Ce fichier binaire doit être exécuté avec des privilèges 'root' parce qu'il sert à démarrer et arrêter les services système requis par l'application ACSLS.)
- *`db_command`* (Ce fichier binaire démarre et arrête le moteur de base de données PostgreSQL qui contrôle et gère la base de données ACSLS.)
- *`get_diags`* (Ce fichier binaire est appelé par un client pour rassembler des informations de diagnostic système complètes qui peuvent être demandées lors d'une conversation téléphonique avec le service d'assistance.)

Lors de l'installation d'ACSLS avec pkgadd, la question suivante s'affiche : *`Do you want to install these as setuid/setgid files?`* En répondant *`y`*, vous permettez aux utilisateurs du groupe acsls d'exécuter ces trois commandes, même si les utilitaires effectuent certaines opérations système nécessitant des privilèges root.

Vérification des paramètres des variables statiques et dynamiques d'ACSLS

Les variables statiques et dynamiques d'ACSLS contrôlent le comportement de nombreuses fonctions d'ACSLS. Définissez ces variables à l'aide de l'utilitaire *`acsss_config`*. Ce document décrit le paramétrage sécurisé d'un grand nombre de ces variables. Si vous répondez par un point d'interrogation (?) après avoir affiché les options d'une variable à l'aide de *`acsss_config`*, des explications détaillées relatives à la variable s'affichent. Ces informations sont également disponibles dans le chapitre relatif à la configuration des variables contrôlant le comportement d'ACSLS du *guide de l'administrateur d'ACSLS*.

Configuration de WebLogic

A partir de la version 8.1, ACSLS utilise WebLogic en tant que serveur Web. WebLogic est installé en même temps qu'ACSLS.

Reportez-vous à *Oracle Fusion Middleware; Understanding Security for Oracle WebLogic Server 11g Release 1 (10.3.6)* pour connaître les options permettant de sécuriser un serveur WebLogic ainsi que les possibilités de pistes d'audit avec WebLogic.

Recours à l'utilitaire userAdmin.sh d'ACSLS pour créer et gérer les utilisateurs de l'interface graphique d'ACSLS

L'utilitaire *`userAdmin.sh`* piloté par menus permet d'administrer les mots de passe des utilisateurs de l'interface graphique d'ACSLS. Vous pouvez ajouter, supprimer et lister les utilisateurs ainsi que modifier les mots de passe des utilisateurs. WebLogic doit être en cours d'exécution pour permettre l'accès à l'utilitaire. Si WebLogic n'est pas en cours d'exécution, l'utilitaire démarre l'application et attend son arrivée en ligne avant d'afficher le menu.

L'utilitaire *`userAdmin.sh`* doit être exécuté par l'utilisateur root et nécessite une authentification acsls_admin. Le compte utilisateur acsls_admin est configuré pendant l'installation d'ACSLS.

Utilisation de l'interface graphique d'ACSLS

Pour utiliser l'interface graphique d'ACSLS, vous devez installer la dernière version de JRE et accéder à l'interface graphique via un navigateur.

Installation de la dernière version de JRE sur les systèmes client de l'interface graphique

Assurez-vous que la dernière version de l'environnement d'exécution Java (JRE) est installée sur les systèmes qui utiliseront l'interface graphique d'ACSLS pour accéder à ACSLS.

Accès à l'interface graphique d'ACSLS

Ouvrez votre navigateur et saisissez une URL contenant l'adresse du nom d'hôte du serveur ou l'adresse IP au format suivant :

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

Il est recommandé d'utiliser un nom d'hôte complet ou l'adresse IP de la machine hôte. Certaines pages, notamment les pages d'aide d'ACSLS, ne s'affichent pas correctement si l'URL ne peut pas être complètement résolue par WebLogic.

Si vous utilisez http sur le port 7001, WebLogic vous redirige automatiquement sur https sur le port 7002.

Etant donné que WebLogic utilise le protocole sécurisé https, il est possible que votre navigateur vous informe que le certificat de sécurité du site n'a pas été enregistré et qu'il n'est donc pas sécurisé. Si vous êtes certain que l'URL correspond à votre machine ACSLS locale, vous pouvez continuer sans risque. L'écran de connexion doit ensuite s'afficher.

Utilisation de l'interface graphique d'ACSLS

Pour accéder à AcslsDomain dans WebLogic, utilisez le protocole sécurisé https. Ce protocole utilise une communication chiffrée entre le navigateur et le serveur à l'aide de

clés privées et de certificats numériques. Voici les options permettant d'obtenir un certificat numérique :

Certificat de démonstration ACSLS

ACSLS est livré avec un certificat appelé "certificat de démonstration". Il fournit un niveau minimal de sécurité par cryptage, qui permet aux utilisateurs de commencer à utiliser l'interface graphique d'ACSLS sans avoir recours à des étapes de configuration supplémentaires. Lorsque l'interaction client avec la bibliothèque ACSLS a entièrement lieu au sein d'un intranet sécurisé, cette méthode de certification de démonstration est généralement suffisante. Toutefois, cette méthode utilise une clé de cryptage 512 bits qui n'est pas prise en charge sur certains navigateurs, notamment Internet Explorer et FireFox version 39 et suivantes.

Configuration d'un certificat numérique autosigné

Le guide d'installation d'ACSLS fournit aux administrateurs d'ACSLS une méthode détaillée permettant de configurer un certificat numérique autosigné d'une longueur de 2 048 bits. Dans la section intitulée "Configuration d'une clé de cryptage SSL", cette méthode fournit un certificat pris en charge sur tous les navigateurs. Il est conseillé aux utilisateurs qui accèdent à un site https avec un certificat autosigné de ne pas poursuivre sur le site s'ils ne sont pas sûrs que la ressource Web est un site sécurisé. En ce qui concerne les utilisateurs d'ACSLS et le serveur de contrôle de bibliothèque, ce niveau de sécurisation est généralement bien compris et dans la plupart des cas, il n'est pas nécessaire que le site prouve son intégrité à l'aide d'une vérification de signature tierce.

Certificats numériques signés par une autorité de signature tierce

Il appartient à chaque site client de déterminer s'il doit fournir une authentification de certificat émise par une autorité de signature tierce telle que Verisign ou Entrust.net. La procédure de génération d'un certificat numérique signé de ce type est décrite dans le document en ligne d'Oracle, Configuring Identity and Trust on :

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

Installation d'ACSLS HA

Si vous utilisez la solution haute disponibilité d'ACSLS, suivez les instructions de la documentation détaillant l'installation, la configuration et les opérations du cluster ACSLS-HA.

3

Fonctions de sécurité

Cette section décrit les mécanismes de sécurité spécifiques qu'offre ACSLS.

Modèle de sécurité

L'objectif principal des fonctions de sécurité d'ACSLS est d'assurer la protection des données : il s'agit d'une part de se prémunir contre les pertes et l'altération accidentelles de données, et d'autre part de lutter contre les tentatives délibérées et non autorisées d'accéder ou de modifier ces données. Dans un second temps, elles servent également à lutter contre les délais excessifs lors de l'accès ou de l'utilisation des données ou à protéger les données contre les interférences pouvant mener à des dénis de service.

Les principales fonctions de sécurité qui assurent ces protections sont les suivantes :

- Authentification – garantit que seules les personnes autorisées ont accès au système et aux données.
- Autorisation – fournit un contrôle d'accès aux privilèges du système et aux données. Cette protection s'appuie sur l'authentification pour garantir que les utilisateurs ne disposent que d'un accès correspondant à leurs besoins.
- Audit – permet aux administrateurs de détecter les tentatives de violation du mécanisme d'authentification et les tentatives réussies ou non de violation du contrôle d'accès.

Configuration et utilisation de l'authentification

Par défaut sous Linux ou Solaris, les utilisateurs ACSLS sont authentifiés par des modules PAM (Pluggable Authentication Modules). Reportez-vous aux pages de manuel Solaris ou au manuel *Linux-PAM System Administrators Guide*.

Les utilisateurs de l'interface graphique ACSLS sont authentifiés par le serveur LDAP intégré dans WebLogic. Consultez le document, Managing the Embedded LDAP Server:

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

Authentification des utilisateurs d'ACSLS par les systèmes d'exploitation Solaris ou Linux

Les utilisateurs d'ACSLS acsss et acssa doivent se connecter à Solaris ou Linux et être authentifiés par le système d'exploitation avant de pouvoir utiliser cmd_proc ou, pour

l'utilisateur acsss, avant de pouvoir exécuter les utilitaires et les commandes de configuration d'ACSLS. L'ID utilisateur acsdb est également utilisé pour les opérations de la base de données. Dans le cadre du processus d'installation d'ACSLS, les clients doivent définir des mots de passe pour ces ID la première fois qu'ils se connectent. Pour plus d'informations, reportez-vous au *Guide d'installation d'ACSLS*.

Authentification des utilisateurs de l'interface graphique d'ACSLS par WebLogic

Les utilisateurs de l'interface graphique d'ACSLS doivent se connecter et être authentifiés par WebLogic. L'ID acsls_admin est créé pendant l'installation d'ACSLS et les clients doivent définir son mot de passe. Les clients peuvent, s'ils le souhaitent, ajouter d'autres utilisateurs de l'interface graphique à l'aide de l'utilitaire `userAdmin.sh`. Pour plus d'informations, reportez-vous au *guide d'installation d'ACSLS* et à la section `userAdmin.sh` du chapitre relatif aux utilitaires du *guide de l'administrateur d'ACSLS*.

Considérations relatives à l'audit

Cette section énumère des considérations générales relatives à l'audit qui s'appliquent à ACSLS.

Gestion des informations auditées

Même si l'exécution d'un audit est relativement peu onéreuse, essayez de limiter autant que possible les événements audités. Vous minimisez ainsi l'impact sur les performances de l'exécution des instructions d'audit et la taille de la piste d'audit, ce qui facilite l'analyse, la compréhension et la gestion.

Suivez les recommandations générales suivantes lorsque vous élaborez une stratégie d'audit :

Evaluez les raisons d'effectuer un audit

Une fois que vous avez bien cerné les raisons d'effectuer un audit, vous pouvez élaborer une stratégie d'audit appropriée et éviter les audits inutiles.

Effectuez un audit ciblé

Ne soumettez à l'audit que le nombre d'instructions, d'utilisateurs et d'objets strictement nécessaires pour obtenir les informations ciblées.

Configuration et utilisation des journaux d'audit d'ACSLS

ACSLS propose plusieurs journaux d'informations dans lesquels vous pouvez enregistrer et examiner les activités d'ACSLS.

- Vous pouvez utiliser vi ou d'autres éditeurs pour les afficher. Les événements système ne peuvent être affichés qu'à l'aide de l'interface graphique d'ACSLS.

- La plupart de ces journaux peuvent être automatiquement archivés lorsqu'ils atteignent une taille définie par le client, et le système conserve le nombre de journaux spécifiés par le client. Pour éviter de remplir le système de fichiers d'ACSLS, le nombre de journaux conservés est soumis à une limite configurable. Si vous souhaitez conserver un plus grand nombre de fichiers journaux ou si vous souhaitez les conserver sur un autre système, vous devez développer votre propre procédure pour les archiver dans un emplacement qui dispose d'un espace suffisant.
- La taille, le nombre de journaux archivés à conserver et d'autres caractéristiques de ces fichiers sont définis par les variables dynamiques ou statiques d'ACSLS.

Répertoire des journaux d'ACSLS

Le répertoire des journaux d'ACSLS est contrôlé par la variable statique LOG_PATH. La valeur par défaut est le répertoire $ACS_HOME/log. Ce répertoire comprend les journaux suivants :

acsss_event.log
Il enregistre les messages d'erreurs, d'événements système et d'événements de bibliothèques ACSLS importants.

Lorsque le journal acsss_event.log atteint une taille limite définie par la variable dynamique LOG_SIZE, il est copié dans event0.log puis effacé. Pendant le processus de copie, les journaux d'événements conservés sont copiés dans des journaux conservés portant un numéro supérieur. Le journal conservé portant le numéro le plus élevé est remplacé. Par exemple : le journal event8.log est copié sur le journal event9.log, le journal event7.log est copié sur le journal event8.log, …, le journal event0.log est copié sur le journal event1.log, le journal acsss_event.log est copié sur le journal event0 .log, et le journal acsss_event.log est effacé. Ce processus est contrôlé par les variables suivantes :

- *EVENT_FILE_NUMBER* spécifie le nombre de journaux d'événements à conserver.
- *LOG_SIZE* spécifie la taille limite à laquelle le journal d'événements est copié sur un journal d'événements conservé, puis tronqué.

Servez-vous de l'utilitaire *`greplog`* pour filtrer le journal acsss_event en incluant ou en excluant les messages contenant des mots-clés donnés. Pour plus d'informations, reportez-vous au chapitre relatif aux utilitaires du *guide de l'administrateur d'ACSLS*.

Journaux de configuration
Deux journaux enregistrent des informations lorsqu'ACSLS met à jour la configuration de bibliothèque stockée dans la base de données d'ACSLS. Ils consignent les modifications apportées à la configuration provenant de *`acsss_config`* et de *`Dynamic Config`* (l'utilitaire *`config`*).

acsss_config.log
Enregistre les informations relatives à toutes les configurations ou reconfigurations de la bibliothèque ou des bibliothèques prises en charge par ACSLS. La dernière modification de configuration est ajoutée à la liste des configurations antérieures.

acsss_config_event.log
Enregistre les événements lors des processus de configuration ou de reconfiguration.

rpTrail.log
Enregistre les réponses à toutes les demandes adressées à ACSLS émanant de cmd_proc ou de clients ACSAPI, ainsi que toutes les demandes adressées à l'interface graphique ou à l'interface client SCSI aux bibliothèques logiques, à l'exception des requêtes à la base de données. Sont consignées les informations relatives au demandeur, à la demande et à l'horodatage de la demande.

rpTrail.log est géré par les variables suivantes :

- *LM_RP_TRAIL* active cette piste d'audit d'événements ACSLS. La valeur par défaut est TRUE.
- *RP_TRAIL_LOG_SIZE* indique la taille limite à laquelle le journal rpTrail.log est compressé et archivé.
- *RP_TRAIL_FILE_NUM* indique le nombre de journaux rpTrail archivés à conserver.
- *RP_TRAIL_DIAG* indique si les messages rpTrail doivent inclure des informations de diagnostic supplémentaires. La valeur par défaut est FALSE.

Statistiques des volumes de bibliothèques
Enregistre tous les événements qui ont une incidence sur les volumes (cartouches) d'une bibliothèque de bandes, y compris le montage, le démontage, le déplacement, l'insertion et l'éjection des volumes ainsi que la détection des volumes par l'audit ou par Cartridge Recovery. Si l'option Library Volume Statistics est activée, ces informations sont enregistrées dans le journal acsss_stats.log.

Les statistiques des volumes de bibliothèques sont gérées par les variables suivantes :

- *LIB_VOL_STATS* active l'option Library Volume Statistics. La valeur par défaut est OFF.
- *VOL_STATS_FILE_NUM* indique le nombre de fichiers acsss_stats.log archivés à conserver.
- *VOL_STATS_FILE_SIZE* indique la taille limite à laquelle le journal acsss_stats.log est archivé.

Répertoire Log/sslm d'ACSLS

A l'intérieur du répertoire des journaux d'ACSLS, des informations concernant l'interface graphique d'ACSLS et l'interface client SCSI aux bibliothèques logiques sont enregistrées dans le répertoire sslm. Ce répertoire contient des liens vers des journaux d'audit WebLogic. Le répertoire sslm comprend les journaux suivants :

slim_event.g#.log[.pp#]
Ce journal consigne des événements provenant de l'interface graphique d'ACSLS et de l'interface client SCSI. Il inclut les messages relatifs aux modifications apportées à la configuration de bibliothèques logiques et les événements des clients SCSI.

- .g# correspond au numéro de génération de ce journal.
- .pp# correspond au numéro de processus parallèle de ce journal. Si plusieurs processus sont consignés simultanément, un numéro de processus parallèle est attribué aux journaux des processus supplémentaires.

smce_trace.log
Ce journal assure le suivi des activités entre les clients SCSI et les bibliothèques logiques d'ACSLS à l'aide de l'émulation de l'interface de changeur de média SCSI.

guiAccess.log
Il s'agit d'un lien vers le journal access.log de WebLogic. Voir Configuration et utilisation des journaux d'audit de WebLogic.

AcslsDomain.log
Il s'agit d'un lien vers le journal AcslsDomain.log de Weblogic. Voir Configuration et utilisation des journaux d'audit de WebLogic.

AdminServer.log
Il s'agit d'un lien vers le journal AdminServer.log de WebLogic. Voir Configuration et utilisation des journaux d'audit de WebLogic.

Affichage des pistes d'audit d'ACSLS sur le visionneur de journaux de l'interface graphique

Accédez au visionneur de journaux à partir de la section Configuration and Administration de l'arborescence de navigation de l'interface graphique. Le visionneur de journaux affiche les informations combinées des journaux ???TITLE??? et ???TITLE???.

Affichage des événements système sur l'interface graphique

Vous pouvez également afficher les événements système à partir de la section Configuration and Administration de l'arborescence de navigation de l'interface graphique. Toute les activités individuelles de la bibliothèque sont enregistrées dans le journal d'événements système. Chaque enregistrement de ce journal contient un horodatage des événements, le type d'événement et une description de l'événement.

Configuration et utilisation des journaux d'audit de Solaris

Déterminez votre stratégie d'audit Solaris. Reportez-vous à la section "Audit dans Oracle Solaris" du manuel *Administration d'Oracle Solaris : Services de sécurité* pour savoir quels événements soumettre à un audit, où enregistrer les journaux d'audit et comme passer en revue les journaux d'audit.

Si vous n'avez pas activé de piste d'audit Solaris personnalisée, vous disposez des pistes d'audit de connexions et commandes Unix émises par les utilisateurs acsss, acsdb, et acssa suivantes :

- Les utilisateurs actuellement connectés à Unix sont enregistrés dans la base de données utmpx d'Unix et les anciens accès utilisateur sont enregistrés dans la base de données wtmpx.
- Utilisez la commande *`last`* pour afficher tous les accès d'un ID utilisateur (par exemple : *`last acsss`*). Pour plus d'informations, reportez-vous aux pages de manuel de wtmpx, *`last`* et getutxent.
- Les fichiers .*_history (c'est-à-dire [point]*_history) dans le répertoire personnel d'un utilisateur enregistrent les commandes émises par cet utilisateur.

  Pour l'utilisateur acsss, il peut s'agir des fichiers :
  - .bash_history
  - .psql_history
  - .sh_history

  Dans Solaris, /var/adm/sulog enregistre les tentatives réussies ou non d'exécuter *`su`* afin de devenir superutilisateur ou un autre utilisateur.

Configuration et utilisation des journaux d'audit de Linux

Pour plus d'informations sur la collecte et l'analyse des journaux d'audit et des journaux système, reportez-vous à la section relative à la configuration et à l'utilisation de l'audit et à la section relative à la configuration et à l'utilisation de la connexion au système du *guide de sécurité de la version 6 d'Oracle Linux*.

Configuration et utilisation des journaux d'audit de WebLogic

Reportez-vous à *Oracle Fusion Middleware; Understanding Security for Oracle WebLogic Server 11g Release 1 (10.3.6)* pour connaître les options permettant de sécuriser un serveur WebLogic ainsi que les possibilités de pistes d'audit avec WebLogic.

WebLogic enregistre les accès à l'interface graphique d'ACSLS dans le répertoire suivant :

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

Ce répertoire contient les fichiers suivants :

- access.log
  - Il existe des versions archivées appelées access.log##### (par exemple access.log00001)
  - Ce fichier fournit une piste d'audit détaillée de l'activité des utilisateurs de l'interface graphique.
  - Pour les connexions, recherchez "AcslsLoginForm".

    Remarque:

    $ACS_HOME/logs/sslm/guiAccess.log contient un lien vers le journal des accès.
- AcslsDomain.log

- Ce journal consigne les opérations de WebLogic et de l'interface graphique d'ACSLS.

  Remarque:

  $ACS_HOME/logs/sslm/AcslsDomain.log contient un lien vers le journal des accès.

- AdminServer.log
  - Ce journal consigne les opérations de WebLogic et de l'interface graphique d'ACSLS.

    Remarque:

    $ACS_HOME/logs/sslm/AdminServer.log contient un lien vers le journal des accès.

4

Considérations de sécurité pour les développeurs

Cette section fournit des informations utiles pour les développeurs qui développent ou assurent le support d'applications utilisant ACSLS pour gérer des bibliothèques de bandes StorageTek d'Oracle.

Activation de la protection par pare-feu sur le serveur d'applications du client

Limitez les ports utilisés pour la communication et désactivez Portmapper sur le serveur d'applications du client en activant la protection par pare-feu. Reportez-vous à l'annexe B du *guide de l'utilisateur de CSC Developer's Toolkit*, qui traite du fonctionnement protégé par pare-feu.

Annexe A

Liste de contrôle du déploiement sécurisé

1. Appliquez la gestion des mots de passe.
2. Limitez l'accès au réseau.
   a. Le logiciel ACSLS et les bibliothèques de bandes qu'il gère doivent se trouver derrière le pare-feu de l'entreprise.
   b. Activez l'option ACSLS Firewall Secure Option.
   c. Envisagez d'activer la protection par pare-feu pour les applications clientes d'ACSLS.
3. Sécurisez le système d'exploitation Solaris ou Linux.
4. Appliquez tous les patches de sécurité et les solutions de contournement.
5. Contactez le service de support Oracle, le service Oracle en charge des bibliothèques de bandes ou le responsable de votre compte si vous constatez des failles de sécurité dans le logiciel StorageTek ACSLS.

Annexe B

Références

Documentation ACSLS
La documentation ACSLS est enregistrée dans des bibliothèques organisées selon la version d'ACSLS. Vous pouvez y accéder à la partir de la page de documentation des produits de stockage sur bande.

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

(Les différentes bibliothèques de documentation ACSLS incluent le numéro version dans leur URL. C'est pourquoi le lien vers une bibliothèque donnée devient obsolète dès lors que la bibliothèque est mise à jour.) La documentation ACSLS inclut :

- *Guide d'installation d'ACSLS*
- *Guide de l'administrateur d'ACSLS*
- *Informations sur le produit ACSLS*

  Ce document inclut la configuration matérielle et logicielle requise, une présentation d'ACSLS, ainsi que les bibliothèques de bandes, les lecteurs de bandes et les médias pris en charge.
- Messages ACSLS (et codes de statut)
- *Notes de version d'ACSLS*
- *Cluster ACSLS-HA : installation, configuration et opérations*
- *Manuel de référence de l'interface ACSLS*

Oracle Solaris
La bibliothèque d'informations Oracle Solaris 11.2 inclut la partie *Securing the Oracle Solaris 11 Operating System*. Reportez-vous à la bibliothèque pour plus de détails à ce sujet.

Oracle Linux
La bibliothèque d'informations Oracle Linux 6 inclut le *Guide de sécurité de la version 6 d'Oracle Linux*. Reportez-vous à la bibliothèque pour plus de détails à ce sujet.

Oracle WebLogic
La bibliothèque de documentation du serveur Oracle WebLogic 10.3.6 (utilisé par ACSLS 8.2) comprend une section relative à la sécurité.

Oracle Fusion Middleware; Understanding Security for Oracle WebLogic Server 11g Release 1 (10.3.6) détaille la procédure de sécurisation d'un serveur WebLogic.