Guide de sécurité d'Oracle® Solaris Cluster 4.3

Référence: E62322
Octobre 2015

Référence: E62322

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.

Table des matières

Utilisation de la documentation 7

1 Présentation de la sécurité d'Oracle Solaris Cluster 9
Présentation d'Oracle Solaris Cluster et de la sécurité 10
Présentation de Geographic Edition et de la sécurité 10
Principes de sécurité généraux 11
Installation et configuration sécurisées d'Oracle Solaris Cluster 11
Installation et configuration sécurisées de Geographic Edition 12
Fonctions de sécurité de Oracle Solaris Cluster 13
Fonctions de sécurité de Geographic Edition 14
Considérations relatives à la sécurité pour les développeurs 15

Index 17

Utilisation de la documentation

- **Présentation** – Fournit un aperçu de la sécurité dans Oracle Solaris Cluster, ainsi que des informations destinées aux développeurs sur la sécurité des installations et de la configuration, les fonctions de sécurité et la sécurité en général.
- **Public visé** : techniciens, administrateurs système et fournisseurs de services agréés
- **Connaissances nécessaires** : expérience avancée dans le dépannage et le remplacement de matériel

Bibliothèque de documentation produit

La documentation et les ressources de ce produit et des produits associés sont disponibles sur le site Web `http://www.oracle.com/pls/topic/lookup?ctx=E62277`.

Commentaires

Faites part de vos commentaires sur cette documentation à l'adresse : `http://www.oracle.com/goto/docfeedback`.

♦ ♦ ♦ CHAPITRE 1

Présentation de la sécurité d'Oracle Solaris Cluster

Oracle Solaris Cluster est une solution matérielle et logicielle intégrée permettant de créer des services hautement disponibles et évolutifs. Ce guide fournit un aperçu de la sécurité dans Oracle Solaris Cluster, ainsi que des informations destinées aux développeurs sur la sécurité des installations et de la configuration, les fonctions de sécurité et la sécurité en général. Utilisez ce guide avec l'ensemble de la documentation relative à Oracle Solaris Cluster pour obtenir une vue d'ensemble du logiciel Oracle Solaris Cluster.

Le logiciel Geographic Edition est une extension en couches du logiciel Oracle Solaris Cluster. La structure Geographic Edition protège les applications contre les interruptions inopinées grâce à plusieurs clusters géographiquement séparés par de grandes distances. Ces clusters contiennent des copies de l'infrastructure Geographic Edition, qui gèrent les données répliquées entre les clusters.

Ce chapitre contient les sections suivantes :

- "Présentation d'Oracle Solaris Cluster et de la sécurité" à la page 10
- "Présentation de Geographic Edition et de la sécurité" à la page 10
- "Principes de sécurité généraux" à la page 11
- "Installation et configuration sécurisées d'Oracle Solaris Cluster" à la page 11
- "Installation et configuration sécurisées de Geographic Edition" à la page 12
- "Fonctions de sécurité de Oracle Solaris Cluster" à la page 13
- "Fonctions de sécurité de Geographic Edition" à la page 14
- "Considérations relatives à la sécurité pour les développeurs" à la page 15

Pour plus d'informations sur la sécurité du système d'exploitation Oracle Solaris, reportez-vous aux manuels *Oracle Solaris 11 - Fonctions de sécurité et directives de sécurisation* et *Sécurisation des systèmes et des périphériques connectés dans Oracle Solaris 11.3* .

Présentation d'Oracle Solaris Cluster et de la sécurité

Dans l'environnement Oracle Solaris Cluster, Oracle Solaris devient un système d'exploitation en cluster. Un cluster est un ensemble d'un ou plusieurs noeuds appartenant exclusivement à cet ensemble.

Les avantages du logiciel Oracle Solaris Cluster sont les suivants :

- Il réduit ou élimine les temps d'arrêt du système dus à des défaillances logicielles ou matérielles.
- Il garantit que les données et les applications restent disponibles pour les utilisateurs, même en cas de défaillance qui entraînerait l'arrêt d'un système à un seul serveur.
- Il optimise le rendement des applications en permettant aux services de s'adapter aux processeurs supplémentaires via l'ajout de noeuds au cluster et l'équilibrage de la charge.
- Il améliore la disponibilité du système en vous permettant de procéder à la maintenance sans arrêter l'ensemble du cluster.

Un cluster présente de nombreux avantages par rapport aux systèmes à un seul serveur. Parmi ces avantages figurent la prise en charge du basculement en cas d'incident, des services évolutifs et de la croissance modulaire, la possibilité de définir des limites de charge pour les noeuds, ainsi qu'un prix d'entrée peu élevé par rapport à celui des systèmes tolérants aux pannes matérielles traditionnels.

Dans un cluster s'exécutant sous le SE Oracle Solaris, les *clusters globaux* et les *clusters de zones* sont des types de cluster. Les clusters peuvent être globaux et/ou de zones. Pour en savoir plus sur les avantages liés à la configuration d'un cluster de zones, consultez *Oracle Solaris Cluster 4.3 Concepts Guide* .

Présentation de Geographic Edition et de la sécurité

Le logiciel Geographic Edition est une extension en couche du logiciel Oracle Solaris Cluster. Un logiciel de réplication de données permet aux applications exécutées sur un cluster Geographic Edition de supporter les sinistres grâce à la migration des services vers un cluster secondaire géographiquement séparé. Un sinistre tel qu'un tremblement de terre, un incendie ou un orage peut désactiver le cluster sur le site principal.

En cas de sinistre, le cluster Geographic Edition peut continuer à fournir des services en utilisant les niveaux de redondance suivants :

- Un cluster secondaire
- Une configuration d'application dupliquée sur le cluster secondaire
- Des données dupliquées sur le cluster secondaire

Le logiciel Geographic Edition fournit une suite d'outils permettant de gérer et de configurer des clusters géographiquement séparés par la migration de services entre sites. Les clusters peuvent être globaux ou de zones. Le logiciel Geographic Edition peut gérer la disponibilité entre plusieurs emplacements physiques grâce à une sécurité renforcée, à la migration des services d'application et à la réplication de données, afin de supporter des sinistres sur un système d'entreprise.

Principes de sécurité généraux

Les principes suivants sont essentiels pour utiliser l'application Oracle Solaris Cluster en toute sécurité :

- garantir la mise à jour des logiciels ;
- limiter l'accès réseau aux services critiques ;
- respecter le principe du moindre privilège ;
- surveiller l'activité du système ;
- s'informer sur les consignes de sécurité Oracle.

Installation et configuration sécurisées d'Oracle Solaris Cluster

Cette section contient des liens permettant d'accéder à des informations sur la planification et l'exécution d'une installation et d'une configuration sécurisées d'Oracle Solaris Cluster.

- **Installation** – Pour installer le logiciel Oracle Solaris Cluster, vous pouvez utiliser le programme d'installation automatisée d'Oracle Solaris 11. Pour plus d'informations, reportez-vous à la section "Installation du logiciel" du manuel *Guide d’installation du logiciel Oracle Solaris Cluster 4.3* .
- **Packages de cluster** – Les packages Oracle Solaris Cluster utilisent des noms de package Oracle Solaris Image Packaging System (IPS).

  Pour afficher une liste des packages du noyau Oracle Solaris Cluster, du service de données et Geographic Edition, reportez-vous au manuel *Oracle Solaris Cluster 4.3 Package Group Lists* .
- **Configuration** – Vous pouvez configurer et administrer un cluster global et un cluster de zones. Pour en savoir plus, consultez le Chapitre 3, "Etablissement d’un cluster global" du manuel *Guide d’installation du logiciel Oracle Solaris Cluster 4.3* , le Chapitre 6, "Création de clusters de zones" du manuel *Guide d’installation du logiciel Oracle Solaris Cluster 4.3* , et Chapitre 1, "Présentation de l’administration d’Oracle Solaris Cluster" du manuel *Guide d’administration système d’Oracle Solaris Cluster 4.3* .

Pour toutes les méthodes destinées à établir un noeud de cluster global, l'autorisation préalable de l'un des noeuds parrains désignés est requise, afin de permettre uniquement au système désigné d'accéder au noeud qui fera l'objet de la configuration. Si vous le souhaitez, un chiffrement DES peut être utilisé pour sécuriser davantage la configuration. Pour en savoir plus, consultez la page de manuel `clauth`(1CL).

- **Vulnérabilité du conteneur d'agent commun** – la combinaison de conteneur d'agent commun et de certaines anciennes versions de Java est à l'origine d'une vulnérabilité de sécurité dans le logiciel Oracle Solaris Cluster. Pour en savoir plus sur la manière de déterminer si votre système est soumis à cette vulnérabilité et sur la façon de corriger cette dernière, consultez le document de référence My Oracle Support *CVE-2014-3566 Instructions to Mitigate the SSL v3.0 Vulnerability (aka "Poodle Attack") in Oracle Solaris Cluster (Doc ID 1999997.1)* (`https://support.oracle.com/epmos/faces/DocumentDisplay?id=1999997.1&displayIndex=1`). Connectez-vous pour consulter ce document My Oracle Support.
- **HA pour NFS sécurisé avec Kerberos V5** –Si vous devez sécuriser l'accès aux services NFS gérés par HA pour service de données NFS, vous pouvez configurer un client Kerberos V5 afin de sécuriser HA pour service de données NFS. Cela inclut l'ajout d'un principal Kerberos pour NFS sur les noms d'hôte logiques sur tous les noeuds du cluster. Pour plus d'informations, reportez-vous à la section "Securing HA for NFS With Kerberos V5" du manuel *Oracle Solaris Cluster Data Service for NFS Guide* .

Installation et configuration sécurisées de Geographic Edition

Cette section fournit des liens permettant de planifier et d'exécuter l'installation et la configuration sécurisées du logiciel Geographic Edition.

- **Installation** – Le logiciel Geographic Edition doit être installé sur un cluster exécutant le système d'exploitation Oracle Solaris et le logiciel Oracle Solaris Cluster. Utilisez le programme d'installation automatisée Oracle Solaris pour installer le logiciel Geographic Edition en même temps que le logiciel Oracle Solaris Cluster ou ultérieurement. La configuration de la structure Geographic Edition est identique à celle du logiciel Oracle Solaris Cluster. Reportez-vous au Chapitre 2, "Installing and Configuring the Geographic Edition Software" du manuel *Oracle Solaris Cluster 4.3 Geographic Edition Installation and Configuration Guide* .
- **Packages Geographic Edition** – Les packages Geographic Edition utilisent des noms de package Oracle Solaris Image Packaging System (IPS). Pour afficher une liste des packages, reportez-vous au manuel *Oracle Solaris Cluster 4.3 Package Group Lists* .
- **Configuration** – Vous pouvez effectuer toutes les tâches d'administration sur un cluster exécutant la structure Geographic Edition sans provoquer l'échec de noeuds ni du cluster. Vous pouvez installer, configurer, démarrer, utiliser, arrêter et désinstaller le logiciel Geographic Edition sur un cluster opérationnel. Reportez-vous au Chapitre 4,

"Administering RBAC" du manuel *Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide* .

Fonctions de sécurité de Oracle Solaris Cluster

Cette section contient des informations sur les mécanismes de sécurité mis en oeuvre dans Oracle Solaris Cluster.

Une installation sécurisée utilise les fonctions de sécurité critiques suivantes :

- **Contrôle d'accès basé sur les rôles (RBAC)** – Utilisez les autorisations RBAC `solaris.cluster.modify`, `solaris.cluster.admin` et `solaris.cluster.read` pour accéder au cluster. Vous devez vous connecter en tant qu'administrateur disposant du profil de droits User Security (sécurité des utilisateurs) pour modifier la plupart des attributs de sécurité d'un rôle. Pour plus d'informations, reportez-vous à la section "Gestion de l’utilisation des droits" du manuel *Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.3* et à la section "Profils de droits RBAC Oracle Solaris Cluster" du manuel *Guide d’administration système d’Oracle Solaris Cluster 4.3* .
- **Nouveaux noeuds** – Utilisez la commande `claccess` ou l'utilitaire `clsetup` avec les privilèges appropriés pour ajouter un noeud à un cluster. Pour plus d'informations, reportez-vous au Chapitre 8, "Administration des noeuds du cluster" du manuel *Guide d’administration système d’Oracle Solaris Cluster 4.3* .

  Le paramétrage par défaut du statut d'accès est `claccess deny-all`. Ne modifiez ce paramétrage que pour effectuer une opération nécessitant des privilèges, telle que l'ajout d'un noeud. Une fois l'opération effectuée, rétablissez le statut `deny-all`. Si vous envisagez de modifier fréquemment les configurations de cluster, assurez-vous que les nouveaux systèmes sont dignes de confiance. Pour ce faire, sélectionnez un protocole d'authentification plus sécurisé à l'aide de la commande `/usr/cluster/bin/claccess -p protocol=authentication-protocol`. Pour plus d'informations, reportez-vous à la page de manuel `claccess`(1CL) et au Chapitre 10, "Configuration des services réseau d’authentification" du manuel *Gestion de Kerberos et d’autres services d’authentification dans Oracle Solaris 11.3* .
- **Trusted Extensions** – La fonctionnalité Oracle Solaris Trusted Extensions peut être activée dans un cluster de zones. Pour plus d'informations, reportez-vous à la section "Directives pour Trusted Extensions dans un cluster de zones" du manuel *Guide d’installation du logiciel Oracle Solaris Cluster 4.3* et à la section "Installation et configuration de Trusted Extensions" du manuel *Guide d’installation du logiciel Oracle Solaris Cluster 4.3* .
- **Clusters de zones** – Un cluster de zones est constitué d'une ou plusieurs zones non globales de marque `solaris`, `solaris10` ou `labeled`, définies avec l'attribut `cluster`. Un cluster de zones de marque `labeled` peut uniquement être utilisé avec la fonction Trusted Extensions du logiciel Oracle Solaris.

Créez un cluster de zones à l'aide de la commande `clzonecluster` ou de l'utilitaire `clsetup`. Vous pouvez exécuter les services pris en charge sur le cluster de zones similaire à un cluster global, avec l'isolement fourni par les zones Oracle Solaris. Pour plus d'informations, consultez "Création et configuration d’un cluster de zones" du manuel *Guide d’installation du logiciel Oracle Solaris Cluster 4.3* et à la section "Fonctionnement d’un cluster de zones" du manuel *Guide d’administration système d’Oracle Solaris Cluster 4.3* .

- **Connexions sécurisées aux consoles de cluster** – Vous devez établir des connexions de shell sécurisé aux consoles des noeuds de cluster. Pour plus d'informations sur l'utilitaire `pconsole`, consultez "Etablissement d’une connexion sécurisée aux consoles du cluster" du manuel *Guide d’administration système d’Oracle Solaris Cluster 4.3* .
- **Conteneur d'agents communs** – L'interface graphique d'Oracle Solaris Cluster Manager met en oeuvre des techniques de cryptage renforcées pour garantir la communication sécurisée entre les piles de gestion Oracle Solaris Cluster sur chaque noeud d'un cluster. Pour plus d'informations, consultez "Dépannage d’Oracle Solaris Cluster Manager" du manuel *Guide d’administration système d’Oracle Solaris Cluster 4.3* .
- **Journalisation** – Le logiciel Oracle Solaris Cluster fait appel à la commande `syslogd` pour consigner les messages d'erreur et de statut. Pour contrôler l'emplacement de stockage des messages, configurez le fichier `/etc/syslog.conf`. Il est également conseillé de protéger les fichiers journaux, par exemple `/var/adm/messages`. Pour plus d'informations, consultez "Administration du cluster" du manuel *Guide d’administration système d’Oracle Solaris Cluster 4.3* .
- **Audit** – Il est activé par défaut dans Oracle Solaris Cluster, comme dans le système d'exploitation Oracle Solaris. La fonction d'audit enregistre toutes les commandes exécutées dans le fichier `/var/cluster/logs/commandlog`, qui doit être protégé comme il se doit. Pour plus d'informations, consultez "Affichage du contenu des journaux de commande d’Oracle Solaris Cluster" du manuel *Guide d’administration système d’Oracle Solaris Cluster 4.3* .
- **Sécurisation du système d'exploitation Oracle Solaris** – Oracle Solaris Cluster met en oeuvre les techniques de sécurisation pour reconfigurer le système d'exploitation Oracle Solaris à l'état sécurisé. Il peut également activer l'audit du système Oracle Solaris.

Fonctions de sécurité de Geographic Edition

Cette section contient des informations sur les mécanismes de sécurité mis en oeuvre dans Geographic Edition.

Une installation sécurisée utilise les fonctions de sécurité critiques suivantes :

- **Contrôle d'accès basé sur les rôles (RBAC)** – Les profils RBAC du logiciel Geographic Edition reposent sur les profils de droits RBAC utilisés dans le logiciel Oracle Solaris Cluster. Vous devez vous connecter en tant qu'administrateur disposant du profil de droits User Security (sécurité des utilisateurs) pour modifier la plupart des attributs de sécurité

d'un rôle. Prenez le rôle root et utilisez les rôles RBAC `solaris.cluster.geo.modify`, `solaris.cluster.geo.admin` et `solaris.cluster.geo.read` pour accéder au cluster. Pour plus d'informations, consultez *Sécurisation des utilisateurs et des processus dans Oracle Solaris 11.3* et "Modifying a User's RBAC Properties" du manuel *Oracle Solaris Cluster 4.3 Geographic Edition System Administration Guide* .

- **Certificats de sécurité** – Au cours de l'installation, le cluster est configuré pour une communication sécurisée à l'aide de certificats de sécurité (les noeuds d'un même cluster doivent partager les mêmes certificats de sécurité). La communication entre clusters d'un partenariat Geographic Edition est sécurisée par l'intermédiaire du port Java Management Extensions (JMX) avec Secure Sockets Layer (SSL) en utilisant les certificats de sécurité. Pour plus d'informations, consultez "Configuring Trust Between Partner Clusters" du manuel *Oracle Solaris Cluster 4.3 Geographic Edition Installation and Configuration Guide* .
- **Conteneur d'agents communs** – Pour permettre à un cluster de zones de fonctionner comme membre d'un partenariat Oracle Solaris Cluster, le conteneur d'agents communs doit être configuré manuellement dans le cluster de zones. Pour plus d'informations, consultez "Preparing a Zone Cluster for Partner Membership" du manuel *Oracle Solaris Cluster 4.3 Geographic Edition Installation and Configuration Guide* .
- **IP Security Architecture (IPsec)** – Utilisez l'architecture IPsec pour configurer des communications sécurisées au moyen de signaux d'activité TCP/UDP entre des clusters partenaires. Pour plus d'informations, consultez "Securing Inter-Cluster Communication" du manuel *Oracle Solaris Cluster 4.3 Geographic Edition Installation and Configuration Guide* .

Considérations relatives à la sécurité pour les développeurs

Cette section présente des informations destinées aux développeurs d'applications qui utilisent Oracle Solaris Cluster. Les développeurs utilisent l'API Oracle Solaris Cluster. Pour plus d'informations, consultez le Chapitre 3, "Key Concepts for System Administrators and Application Developers" du manuel *Oracle Solaris Cluster 4.3 Concepts Guide* .

Les applications agent créées par les développeurs doivent fonctionner au sein de la structure de sécurité du produit et prendre en charge les fonctions de sécurité suivantes :

- **Méthodes callback d'agent** – Oracle Solaris Cluster prend en charge une large gamme d'agents applicatifs, mis en oeuvre sous forme d'ensemble de méthodes callback pour contrôler le démarrage, l'arrêt, le test et la validation de l'application. Les méthodes callback telles que `Start`, `Stop` ou `Validate` s'exécutent toujours en tant que root. Si un utilisateur non root a accès en écriture à l'un de ces fichiers exécutables de méthode, cela compromet la sécurité car cet utilisateur peut alors renforcer ses privilèges de manière non autorisée en insérant du code dans la méthode callback. Oracle Solaris Cluster vérifie la propriété et les

permissions des fichiers exécutables des méthodes callback. Cette vérification est régie par la propriété de cluster `resource_security`. Si `resource_security` a la valeur `SECURE` et que le code de la méthode est accessible en écriture à un utilisateur non root, l'exécution de la méthode échoue.

Les méthodes d'agent exécutent fréquemment des programmes externes, telles que des commandes d'administration propres à l'application. De tels programmes externes doivent être exécutés avec les privilèges les plus faibles possibles, au moyen d'un wrapper. Oracle Solaris Cluster fournit les propriétés `application_user` et `resource_security`, ainsi que l'API `scha_check_app_user`, pour activer les services de données et garantir une exécution sécurisée de l'application. La commande `scha_check_app_user` peut être appelée au sein de scripts pour vérifier le nom d'utilisateur en le comparant aux propriétés `Application_user` et `Resource_security` configurées. Pour plus d'informations, reportez-vous aux pages de manuel `scha_check_app_user`(1HA), `r_properties`(5) et `cluster`(1CL).

- **Accès sécurisé à une application** – Dans certains cas, l'accès sécurisé à une application est requis lorsque vous exécutez des commandes de gestion ou de configuration. Cet accès sécurisé doit être garanti par une méthode basée sur des informations d'identification, telle qu'Oracle Wallet Manager. Si un mot de passe est requis, il doit être utilisé en toute sécurité et stocké sous forme brouillée. Par exemple, il ne doit pas être saisi sur la ligne de commande, où un utilisateur peut l'afficher au moyen de la commande `ps`. Oracle Solaris Cluster fournit la commande `clpstring`, qui permet de créer des chaînes privées pouvant être utilisées pour stocker des mots de passe codés dans le cluster, et extraites pour les tâches de gestion exigeant un mot de passe. Pour plus d'informations sur cette commande, reportez-vous à la page de manuel `clpstring`(1CL).

Pour plus d'informations sur l'utilisation des fonctions de sécurité lors du développement de services de données, consultez le document *Oracle Solaris Cluster Data Services Developer's Guide* .

Index

A
accès sécurisé à une application, 16
ajout de noeuds, 13
audit, 14

C
`claccess` commande, 13
`clsetup` utilitaire, 13
cluster
  configuration, 11
  fonctions de sécurité, 13
  installation, 11
cluster de zones
  marque étiquetée, 13
cluster global, 10, 11
clusters de zones, 10
Clusters de zones
  Trusted Extensions, 13
clusters de zones de marque étiquetée, 13
clustersde zones
  Geographic Edition, 11
commande `clauth`, 12
configuration, 11, 12
connexions sécurisées aux consoles de cluster, 14
conteneur d'agents communs, 15

D
développeurs
  considérations relatives à la sécurité, 15

F
fonctions de sécurité, 14

I
installation, 11
IPsec, 15

J
journalisation, 14

O
Oracle Solaris Cluster
  présentation, 10
  sécurité, 10
Oracle Solaris Cluster Geographic Edition
  avantages, 10
  configuration, 12
  installation, 12
  présentation, 10

P
packages
  Oracle Solaris Cluster, 11
  Oracle Solaris Cluster Geographic Edition, 12
`pconsole`utilitaire, 14
présentation
  Oracle Solaris Cluster, 10
  Oracle Solaris Cluster Geographic Edition, 10
programme d'installation automatisée, 11, 12

R
RBAC, 13, 14
réplication de données, 10

reprise après sinistre, 10

S

sécurisation du système d'exploitation, 14
sécurité
    certificats, 15
    considérations à l'attention des développeurs, 15
    principes généraux, 10
Sécurité
    Installation de Geographic Edition, 12

T

Trusted Extensions, 13