

Guide de sécurité des systèmes Oracle® ZFS Storage Appliance

Présentation de la sécurité Oracle ZFS Storage Appliance

Ce guide explore, passe en revue et souligne les considérations nécessaires à la création d'un système de stockage sécurisé et d'une compréhension à l'échelle de l'équipe de vos objectifs spécifiques concernant la sécurité. Nous vous recommandons de lire ce guide avant de configurer votre appareil afin de pouvoir profiter des fonctions de sécurité disponibles et créer les niveaux de sécurité dont vous avez besoin.

Vous pouvez également utiliser ce guide comme référence pour trouver plus d'informations détaillées à propos des considérations de sécurité des différentes fonctions et capacités des systèmes Oracle ZFS Storage Appliance (ZFSSA). Pour les procédures de configuration, consultez le guide d'administration des systèmes Oracle ZFS Storage System.

Les sections suivantes constituent une brève description des fonctions de sécurité de ZFSSA :

- **Installation initiale** - Décrit comment configurer l'accès administratif, comment le compte root est établi ainsi que les effets d'une réinitialisation des paramètres d'usine de ZFSSA.
- **Sécurité physique** - Décrit l'environnement de sécurité physique pour ZFSSA.
- **Modèle administratif** - Décrit la restriction de l'accès à CLI et BUI, le modèle de patches système, les mises à jour différées, les lots d'informations pour le support et la sauvegarde de configuration.
- **Utilisateurs ZFSSA** - Décrit les rôles d'administration, qui peut administrer ZFSSA et gérer les autorisations utilisateur.
- **Listes de contrôle d'accès (ACL)** - Décrit le mécanisme qui autorise ou interdit l'accès aux fichiers et aux répertoires.
- **Réseau de stockage (SAN)** - Décrit les numéros d'unité logique (LUN) et les groupes d'initiateurs associés, ainsi que les options et les configurations par défaut d'authentification d'initiateurs.
- **Services de données** - Décrit les services de données pris en charge par ZFSSA et la sécurité proposée par les différents services de données.
- **Services d'annuaire** - Décrit les services d'annuaire qui peuvent être configurés sur ZFSSA et leurs implications de sécurité.
- **Paramètres système** - Décrit les paramètres système : Phone Home, les indicateurs de maintenance, SMTP, SNMP, Syslog, System Identity, le nettoyage de disque et la prévention de destruction.
- **Accès administratif distant** - Décrit l'accès distant via la BUI et la CLI.
- **Journaux** - Décrit les types de journaux adaptés à la sécurité.

Installation initiale

ZFSSA est fourni aux clients avec le logiciel ZFSSA préinstallé. Aucune installation de logiciel n'est nécessaire et aucun média n'est fourni.

L'installation initiale est réalisée avec le nom et le mot de passe du compte par défaut, le mot de passe root par défaut doit être modifié après l'installation. Si le logiciel ZFSSA est réinitialisé sur les paramètres par défaut d'usine, le mot de passe root est également réinitialisé sur les paramètres par défaut pour ZFSSA et le processeur de service.

Lors de l'installation initiale d'un logiciel ZFSSA, un nom et un mot de passe du compte par défaut sont associés au processeur de service du système. Le compte par défaut permet à un administrateur système d'obtenir un accès initial au ZFSSA, l'administrateur doit ensuite exécuter les étapes d'installation initiale du système. Une des étapes nécessaires consiste à configurer un nouveau mot de passe ZFSSA administratif, ce qui réinitialise ensuite le mot de passe par défaut du processeur de service sur la même valeur.

Sécurité physique

Pour contrôler l'accès à votre système, vous devez maintenir la sécurité physique de votre environnement informatique. Par exemple, un système qui est connecté et laissé sans surveillance est vulnérable aux accès non autorisés. La zone alentour de l'ordinateur et le matériel de l'ordinateur doivent être en permanence physiquement protégés contre tout accès non autorisé.

ZFSSA est destiné à être utilisé dans des zones à accès limité, dans lesquelles les accès sont contrôlés au moyen de systèmes de sécurité (par exemple, à clé, verrou, dispositif ou badge). Le personnel autorisé à accéder à ces zones doit avoir été préalablement informé des raisons justifiant la limitation des accès et de toutes les précautions à prendre.

Modèle administratif

Cette section décrit la sécurité pour les modèles administratifs de ZFSSA.

Accès restreint (CLI et BUI)

L'accès administratif à l'interface utilisateur de navigateur (BUI) et à l'interface de ligne de commande (CLI) est limité à l'utilisateur root, aux administrateurs locaux définis avec les privilèges appropriés et ceux possédant une autorisation grâce à des serveurs d'identité tels que Lightweight Directory Access Protocol (LDAP) et le service d'informations réseau (NIS).

L'administration est effectuée grâce à une connexion Secure Sockets Layer (SSL) par ligne de commande ou une session de navigateur HTTP secure (HTTPS). Les sessions HTTPS sont chiffrées avec un certificat autosigné possédant une génération unique pour chaque ZFSSA au moment de l'installation initiale. Les sessions HTTPS ont un délai d'expiration de 15 minutes de session par défaut défini par l'utilisateur.

Mises à jour du système

Les mises à jour du système sont appliquées comme des remplacements binaires entiers du logiciel système. Avant la mise à jour, un instantané du pool du système actif est pris. Cela permet à l'administrateur de revenir à la version précédente si nécessaire.

Mises à jour différées

Une mise à jour différée est une fonction ou un élément de fonctionnalité qui fait partie d'une mise à jour système et qui n'est pas activée lorsque la mise à jour système est exécutée. L'administrateur décide quand ou s'il faut appliquer les mises à jour différées. Les mises à jour qui n'ont pas été appliquées lors d'une mise à jour système sont toujours disponibles lors de mises à jour système successives. Vous ne pouvez pas sélectionner de mises à jour individuelles à appliquer, lorsque vous choisissez d'appliquer des mises à jour différées, vous pouvez appliquer toutes les mises à jour ou aucune. Après avoir appliqué une mise à jour, vous ne pouvez pas revenir à une version logicielle système antérieure.

Lots de support

Lorsque votre système est inscrit pour le support Phone Home s'il souffre d'une panne majeure, l'état du système est envoyé à My Oracle Support où il pourra être examiné par le personnel du service de support

d'ingénierie et un lot d'informations pour le support peut être créé. Les informations de l'état du système envoyées à My Oracle Support ne contiennent aucune données utilisateur ; seules des informations de configuration sont envoyées.

Sauvegarde de configuration

Les configurations système peuvent être sauvegardées localement pour être restaurées ultérieurement. Ces sauvegardes ne contiennent aucune données utilisateur ; seuls les paramètres de configuration sont sauvegardés.

Utilisateurs ZFSSA

Il existe deux types d'utilisateurs ZFSSA :

- **Utilisateurs de services de données** - Clients qui accèdent à des ressources de fichier et de bloc à l'aide de protocoles pris en charge, tels que NFS, SMB, Fibre Channel, iSCSI, http et FTP.
- **Utilisateurs administratifs** - Utilisateurs qui gèrent la configuration et les services pour le logiciel ZFSSA. Cette section s'applique uniquement aux utilisateurs administratifs.

Rôles d'utilisateurs administratifs

Il est possible d'accorder des privilèges aux administrateurs en leur assignant des rôles personnalisés. Un rôle est un ensemble de privilèges que vous pouvez assigner à un administrateur. Il peut être souhaitable de créer des rôles administrateur et opérateur avec des niveaux d'autorisation différents. Les membres du personnel peuvent recevoir n'importe quel rôle adapté à leurs besoins, sans qu'il soit nécessaire d'assigner des privilèges supplémentaires.

L'utilisation de ces rôles est plus sécurisée que celle des mots de passe administrateur partagés à accès complet (par exemple, l'affectation du mot de passe root à tout le monde). Les rôles restreignent les utilisateurs à des ensembles d'autorisations définies. De plus, les rôles utilisateur sont traçables vers des noms d'utilisateur individuels dans les journaux d'audit. Le rôle "Basic administration" existe par défaut. Il contient un minimum d'autorisations.

Les utilisateurs administratifs peuvent être :

- Les utilisateurs locaux - toutes les informations de compte sont enregistrées sur le logiciel ZFSSA.
- Les utilisateurs de l'annuaire - des comptes NIS ou LDAP existants sont utilisés et des paramètres d'autorisation supplémentaires sont enregistrés sur le logiciel ZFSSA. Cela permet aux utilisateurs NIS/LDAP existants de se connecter et d'administrer le ZFSSA mais les utilisateurs NIS/LDAP existants ne peuvent pas se connecter au ZFSSA par défaut. L'accès au ZFSSA doit être explicitement octroyé.

Portées administratives

Les autorisations permettent aux utilisateurs d'effectuer des tâches spécifiques telles que la création de partages, la réinitialisation de ZFSSA et la mise à jour du logiciel système. Des groupes d'autorisations sont appelés des portées. Chaque portée est susceptible d'être limitée par un ensemble de filtres facultatif. Par exemple, au lieu de posséder une autorisation de redémarrage de tous les services, vous pouvez définir un filtre afin de permettre à cette autorisation de ne redémarrer que le service HTTP.

Listes de contrôle d'accès (ACL)

ZFSSA fournit un accès aux fichiers via des listes de contrôle d'accès (ACL). Une liste de contrôle d'accès est un mécanisme qui autorise ou interdit l'accès à un fichier ou un répertoire en particulier.

Le modèle ACL fourni par ZFSSA se base sur le modèle ACL NFSv4 qui est dérivé d'une sémantique ACL Windows. Il s'agit d'un modèle ACL riche qui permet un accès fin aux fichiers et aux répertoires. Chaque fichier et répertoire à l'intérieur du stockage ZFSSA possède une ACL et toutes les décisions de contrôle d'accès pour SMB et NFS passent par les mêmes algorithmes afin de déterminer qui a autorisé ou interdit l'accès à des fichiers ou des répertoires.

Une ACL est composée d'une ou plusieurs entrées de contrôle d'accès (ACE). Chaque ACE contient une entrée pour les autorisations qu'elle octroie ou refuse, à qui l'ACE s'applique et les indicateurs de niveau d'héritage utilisés.

Héritage d'ACL

Les ACL NFSv4 permettent aux ACE individuelles d'être héritées par des fichiers et des répertoires récemment créés. L'héritage des ACE est contrôlé par plusieurs indicateurs de niveau d'héritage qu'un administrateur configure sur l'ACL lorsqu'elle est initialement configurée.

Déterminer l'accès ACL

Les ACL NFSv4 dépendent d'un ordre et sont traitées de haut en bas. Une fois qu'une autorisation est octroyée, une ACE ultérieure ne peut pas la supprimer. Une fois qu'une autorisation est refusée, une ACE ultérieure ne peut pas l'octroyer.

ACL SMB de niveau de partage

Une ACL SMB de niveau de partage est une ACL combinée avec l'ACL d'un fichier ou d'un répertoire dans le partage afin de déterminer les autorisations en vigueur pour ce fichier. L'ACL de niveau de partage offre une couche supplémentaire de contrôle d'accès par rapport aux ACL de fichiers et permet de configurer plus précisément le contrôle d'accès. Les ACL de niveau de partage sont définies lorsque le système de fichiers est exporté à l'aide du protocole SMB. Si le système de fichiers n'est pas exporté à l'aide du protocole SMB, le paramétrage de l'ACL de niveau de partage n'a aucune conséquence. Par défaut, les ACL de niveau de partage octroient un contrôle total à tout le monde.

Propriétés ACL ZFS

Les propriétés de comportement et d'héritage des ACL sont uniquement applicables aux clients NFS. Les clients SMB utilisent une sémantique Windows stricte et prévalent sur les propriétés ZFS. NFS utilise une sémantique POSIX, à la différence des clients SMB. Les propriétés sont principalement compatibles avec POSIX.

Réseau de stockage (SAN)

Dans un réseau de stockage, les groupes de cibles et d'initiateurs définissent des ensembles de cibles et d'initiateurs pouvant être associés à des unités logiques de stockage (LUN). Une LUN associée à un groupe de cibles est uniquement accessible par le biais des cibles de ce groupe. Une LUN associée à un groupe d'initiateurs est uniquement accessible par le biais des initiateurs de ce groupe. Lors de la création d'une

LUN, vous appliquez les groupes d'initiateurs et les groupes de cibles à la LUN. La création d'une LUN ne peut pas être terminée avec succès sans définir au moins un groupe de cibles et un groupe d'initiateurs.

A part l'authentification CHAP (Challenge-Handshake Authentication Protocol), qui peut être sélectionnée uniquement pour l'accès initiateur iSCSI/iSER, aucune authentification n'est réalisée.

REMARQUE : l'utilisation du groupe d'initiateurs par défaut peut exposer la LUN à des initiateurs non souhaités ou incompatibles.

Services de données

TABLEAU 1 Services de données

SERVICE	DESCRIPTION	PORTS UTILISES
NFS	Accès au système de fichiers via les protocoles NFSv3 et NFSv4	111 et 2049
iSCSI	Accès aux LUN via le protocole iSCSI	3260 et 3205
SMB	Accès au système de fichiers via le protocole SMB	SMB via NetBIOS 139
		SMB via TCP 445
		Datagramme NetBIOS 138
		Service de noms NetBIOS 137
FTP	Accès au système de fichiers via le protocole FTP	21
HTTP	Accès au système de fichiers via le protocole HTTP	80
NDMP	Service hôte NDMP	10000
Réplication distante	Réplication distante	216
Migration shadow	Migration des données shadow	
SFTP	Accès au système de fichiers via le protocole SFTP	218
SRP	Blocage de l'accès via le protocole SRP	
TFTP	Accès au système de fichiers via le protocole TFTP	
Virus scan	Analyse antivirus du système de fichiers	

Ports minimum requis :

Pour assurer la sécurité d'un réseau, vous pouvez créer des pare-feux. Les numéros de port sont utilisés pour la création de pare-feux et identifient de manière unique une transaction sur un réseau en indiquant l'hôte et le service.

La liste suivante indique les ports minimum requis pour la création de pare-feux :

Ports entrants

- icmp/0-65535 (PING)
- tcp/1920 (EM)
- tcp/215 (BUI)
- tcp/22 (SSH)
- udp/161 (SNMP)

Ports entrants supplémentaires si le partage de fichiers http est utilisé (ce qui n'est généralement pas le cas)

- tcp/443 (SSL WEB)
- tcp/80 (WEB)

Ports sortants

- tcp/80 (WEB)

Remarque : pour la réplication, utilisez les tunnels Generic Routing Encapsulation (GRE) lorsque cela est possible. Cela permet au trafic de s'exécuter sur les interfaces arrière et permet d'éviter le pare-feu où le trafic pourrait être ralenti. Si les tunnels GRE ne sont pas disponibles sur le noyau NFS, vous devez exécuter la réplication sur l'interface avant. Dans ce cas, le port 216 doit également être ouvert.

Options d'authentification et de chiffrement NFS

Les partages NFS sont alloués avec une authentification AUTH_SYS RPC par défaut. Vous pouvez également les configurer pour les partager avec la sécurité Kerberos. A l'aide de l'authentification AUTH_SYS, l'UID et le GID UNIX du client sont transmis de manière non authentifiée sur le réseau par le serveur NFS. Ce mécanisme d'authentification est facilement anéanti par toute personne possédant un accès root sur un client. Il est donc préférable d'utiliser un autre mode de sécurité disponible.

Les contrôles d'accès supplémentaires peuvent être spécifiés par partage afin d'autoriser ou de refuser l'accès aux partages pour des hôtes spécifiques, des domaines DNS ou des réseaux.

Modes de sécurité

Les modes de sécurité sont définis par partage. La liste suivante décrit les paramètres de sécurité Kerberos disponibles.

- krb5 - Authentification d'utilisateur final via Kerberos V5
- krb5i - krb5 plus préservation de l'intégrité (les paquets de données résistent aux dégradations)
- krb5p - krb5i plus préservation de la confidentialité (les paquets de données résistent aux dégradations et sont chiffrés)

Les combinaisons de types de Kerberos peuvent également être spécifiées dans le paramètre du mode de sécurité. La combinaison de modes de sécurité permet aux clients de monter n'importe quel type de Kerberos répertorié.

Types de Kerberos

- sys - Authentification système
- krb5 - Kerberos v5 uniquement, les clients doivent monter à l'aide de ce type.
- krb5:krb5i - Kerberos v5, avec intégrité, les clients peuvent monter avec n'importe quel type.
- krb5i - Kerberos v5 intégrité uniquement, les clients doivent monter à l'aide de ce type.
- krb5:krb5i:krb5p - Kerberos v5, avec intégrité ou confidentialité, les clients peuvent monter avec n'importe quel type.
- krb5p - Kerberos v5 confidentialité uniquement, les clients doivent monter à l'aide de ce type.

iSCSI

Lorsque vous configurez une LUN sur ZFSSA, vous pouvez exporter ce volume via une cible iSCSI (Internet Small Computer System Interface). Le service iSCSI permet aux initiateurs iSCSI d'accéder aux cibles par le biais du protocole iSCSI.

Ce service prend en charge la détection, la gestion et la configuration à l'aide du protocole iSNS. Le service iSCSI prend en charge l'authentification unidirectionnelle (la cible authentifie l'initiateur) et bidirectionnelle (la cible et l'initiateur s'authentifient mutuellement) par le biais du protocole CHAP. De plus, le service prend en charge la gestion des données d'authentification CHAP dans une base de données RADIUS.

Le système commence par effectuer l'authentification puis l'autorisation au cours de deux étapes indépendantes. Si l'initiateur local possède un nom et une clé secrète CHAP, le système procède à l'authentification. Si l'initiateur local ne possède pas de propriétés CHAP, le système n'effectue pas d'authentification et tous les initiateurs sont éligibles à l'autorisation.

Le service iSCSI vous permet de spécifier une liste globale d'initiateurs que vous pouvez utiliser au sein de groupes d'initiateurs. Lors de l'utilisation d'une authentification iSCSI et CHAP, RADIUS peut être utilisé comme protocole iSCSI qui diffère toutes les authentifications CHAP sur le serveur RADIUS sélectionné.

Support RADIUS

Remote Authentication Dial-In User Service (RADIUS) est un système permettant d'utiliser un serveur centralisé pour effectuer l'authentification CHAP au nom des noeuds de stockage. Lorsque vous utilisez une authentification iSCSI et CHAP, vous pouvez sélectionner RADIUS pour le protocole iSCSI, qui s'applique à iSCSI et à iSER (iSCSI Extensions for RDMA) et envoie toutes les authentification CHAP au serveur RADIUS sélectionné.

Pour permettre à ZFSSA d'effectuer l'authentification CHAP à l'aide de RADIUS, les conditions suivantes doivent être remplies :

- ZFSSA doit spécifier l'adresse du serveur RADIUS et le secret à utiliser lors de la communication avec le serveur RADIUS concerné.
- Le serveur RADIUS (par exemple dans son fichier clients) doit comporter une entrée indiquant l'adresse du ZFSSA et spécifiant le même secret que ci-dessus.
- Le serveur RADIUS (par exemple dans son fichier utilisateurs) doit comporter une entrée indiquant le nom et le secret CHAP pour chaque initiateur.
- Si l'initiateur utilise son nom IQN en tant que nom CHAP (ce qui correspond à la configuration recommandée), ZFSSA n'a pas besoin d'une entrée Initiator distincte pour chaque case Initiator, le serveur RADIUS peut effectuer toutes les étapes d'authentification.
- Si l'initiateur utilise un nom CHAP distinct, ZFSSA doit comporter une entrée Initiator distincte pour l'initiateur concerné indiquant le mappage d'un nom IQN vers un nom CHAP. Cette entrée Initiator n'a PAS besoin d'indiquer le secret CHAP de l'initiateur.

Protocole SMB (Server Message Block)

Le protocole SMB (aussi appelé CIFS (Common Internet File System)) fournit principalement un accès partagé aux fichiers sur un réseau Microsoft Windows. Il fournit aussi une authentification.

Les options SMB suivantes ont des implications de sécurité :

- **Restreindre l'accès anonyme à la liste de partages** - Cette option nécessite que les clients s'authentifient à l'aide de SMB avant de recevoir une liste de partages. Si cette option est désactivée, les clients anonymes peuvent accéder à la liste de partages. Cette option est désactivée par défaut.
- **Signature SMB activée** - Cette option active l'interopérabilité avec les clients SMB à l'aide de la fonction de signature SMB. Si cette option est activée, un paquet signé aura la signature vérifiée. Si l'option est désactivée, un paquet non signé sera accepté sans vérification de signature. Cette option est désactivée par défaut.
- **Signature SMB Requisite** - Cette option peut être utilisée lorsque la signature SMB est requise. Lorsque l'option est activée, tous les paquets SMB doivent être signés ou ils seront rejetés. Les clients

ne prenant pas en charge la signature SMB ne peuvent pas se connecter au serveur. Cette option est désactivée par défaut.

- **Activer l'énumération basée sur les accès** - Définir cette option filtre les entrées de répertoire en fonction des informations d'identification du client. Lorsqu'un client n'a pas accès à un fichier ou à un répertoire, ce fichier ne figure pas dans la liste d'entrées envoyée au client. Cette option est désactivée par défaut.

Authentification du mode domaine de l'Active Directory (AD)

En mode domaine, les utilisateurs sont définis dans l'Active Directory. Les clients SMB peuvent se connecter au ZFSSA à l'aide de l'authentification Kerberos ou NTLM.

Lorsqu'un utilisateur se connecte par le biais d'un nom d'hôte ZFSSA complet, les clients Windows dans le même domaine ou dans un domaine autorisé utilisent l'authentification Kerberos ou l'authentification NTLM.

Lorsqu'un client SMB utilise une authentification NTLM pour se connecter au ZFSSA, les informations d'identification de l'utilisateur sont transmises au contrôleur de domaine AD pour authentification. Ce processus s'appelle l'authentification d'intercommunication.

Si les stratégies de sécurité Windows qui restreignent l'authentification NTLM sont définies, les clients Windows doivent se connecter au ZFSSA par le biais d'un nom d'hôte complet. Pour plus d'informations, consultez cet article MSDN : <http://technet.microsoft.com/en-us/library/jj865668%28v=ws.10%29.aspx>.

Après l'authentification, un "contexte de sécurité" est établi pour la session SMB de l'utilisateur. L'utilisateur représenté par le contexte de sécurité a un SID (Security Descriptor) unique. Le SID remplace l'appartenance des fichiers et est utilisé pour déterminer les privilèges d'accès aux fichiers.

Authentification du mode groupe de travail

En mode groupe de travail, les utilisateurs sont définis localement sur le ZFSSA. Lorsqu'un client SMB se connecte à un ZFSSA en mode groupe de travail, les hachages du nom d'utilisateur et du mot de passe de cet utilisateur sont utilisés pour authentifier localement l'utilisateur.

Le niveau de compatibilité LAN Manager (LM) est utilisé pour spécifier le protocole utilisé pour l'authentification lorsque le ZFSSA est en mode groupe de travail.

La liste suivante montre le comportement du ZFSSA pour chaque niveau de compatibilité LM :

- Niveau 2 : Accepte l'authentification LM, NTLM et NTLMv2
- Niveau 3 : Accepte l'authentification LM, NTLM et NTLMv2
- Niveau 4 : Accepte l'authentification NTLM et NTLMv2
- Niveau 5 : Accepte uniquement l'authentification NTLMv2.

Une fois que l'utilisateur du groupe de travail est authentifié avec succès, un contexte de sécurité est établi. Un SID unique est créé pour les utilisateurs définis sur le ZFSSA à l'aide d'une combinaison du SID de la machine et de l'UID de l'utilisateur. Tous les utilisateurs locaux sont définis comme utilisateurs UNIX.

Groupes locaux et privilèges

Les groupes locaux désignent des groupes d'utilisateurs de domaine qui confèrent des privilèges supplémentaires à ces utilisateurs. Les administrateurs peuvent contourner les autorisations d'accès aux

fichiers pour modifier la propriété des fichiers. Les opérateurs de sauvegarde peuvent contourner les contrôles d'accès aux fichiers pour sauvegarder et restaurer des fichiers.

Opérations d'administration via la console MMC (Microsoft Management Console)

Pour garantir que seuls les utilisateurs appropriés ont accès aux opérations d'administration, les opérations exécutées à distance via la console MMC sont sujettes à un certain nombre de restrictions d'accès.

La liste suivante montre les utilisateurs et leurs opérations autorisées :

- Utilisateurs standard - Etablissement de listes de partages
- Membres du groupe Administrators - Etablissement de la liste des fichiers ouverts et des fichiers fermés, fermeture des connexions utilisateur, consultation du journal des services et du journal d'événements
- Les membres du groupe Administrators peuvent également définir/modifier les ACL de niveau de partage
- Membres du groupe Administrators - Etablissement de la liste des fichiers ouverts et des fichiers fermés, fermeture des connexions utilisateur, consultation du journal des services et du journal d'événements

Virus scan

Le service Virus Scan recherche des virus au niveau du système de fichiers. Lorsque vous accédez à un fichier par le biais de n'importe quel protocole, le service Virus scan commence par analyser le fichier. Si un virus est trouvé, l'accès au fichier est bloqué et il est mis en quarantaine. L'analyse est effectuée par un moteur externe que le ZFSSA contacte. Le moteur externe n'est pas inclus dans le logiciel ZFSSA.

Lorsqu'un fichier est analysé à l'aide des dernières définitions de virus, il n'est pas réanalysé jusqu'à sa nouvelle modification. L'analyse antivirus est fournie principalement pour les clients SMB qui sont susceptibles d'introduire des virus. Les clients NFS peuvent également utiliser l'analyse antivirus, mais en raison du fonctionnement du protocole NFS, un virus peut ne pas être détecté aussi rapidement qu'avec le client SMB.

Moteur temporisé pour les attaques temporelles

SMB n'implémente aucun moteur temporisé pour empêcher les attaques temporelles. Il repose sur une structure de chiffrement Solaris.

Chiffrement des données en simultané

Le service SMB utilise la version 1 du protocole SMB, qui ne prend pas en charge le chiffrement des données en simultané.

FTP (File Transfer Protocol)

FTP autorise l'accès au système de fichiers de clients FTP. Le service FTP n'autorise pas les connexions anonymes et les utilisateurs doivent s'authentifier avec le service de noms configuré.

Le FTP prend en charge les paramètres de sécurité suivants : Ces paramètres sont partagés pour tous les systèmes de fichiers pour lesquels l'accès par protocole FTP est activé :

- Activer SSL/TLS - Autorise les connexions FTP SSL/TLS chiffrées et s'assure que la transaction FTP est chiffrée. Cette option est désactivée par défaut.
- Autoriser la connexion de root - Permet à l'utilisateur root de se connecter au FTP. Cette option est désactivée par défaut, car l'authentification FTP en texte brute présente un risque de sécurité lors des attaques survenant durant la détection du réseau
- Nombre maximum de tentatives de connexion autorisées - Nombre de tentatives de connexion ayant échoué avant qu'une connexion FTP soit interrompue et que l'utilisateur doive se reconnecter pour essayer à nouveau. Le nombre par défaut est 3.
- Niveau de journalisation - Verbosité du journal.

Le FTP prend en charge les journaux suivants :

- proftpd - Consigne les événements FTP, y compris les connexions réussies et les tentatives de connexions ayant échoué
- proftpd_xfer - Journal de transfert de fichiers
- proftpd_tls - Consigne les événements FTP liés au chiffrement SSL/TLS

HTTP (Hypertext Transfer Protocol)

Le service HTTP permet d'accéder aux systèmes de fichiers à l'aide des protocoles HTTP et HTTPS et de l'extension HTTP WebDAV (Web based Distributed Authoring and Versioning). Cela permet aux clients d'accéder aux systèmes de fichiers partagés par le biais d'un navigateur Web ou d'un système de fichiers local si leur logiciel client le prend en charge. Le serveur HTTPS utilise un certificat de sécurité auto-signé.

Les propriétés disponibles sont les suivantes :

- Exiger la connexion des clients - Les clients doivent s'authentifier pour bénéficier de l'accès au partage et pour que les fichiers qu'ils créent leur appartiennent. Si cette propriété n'est pas définie, les fichiers créés appartiendront au service HTTP et l'utilisateur sera "nobody".
- Protocoles - Sélectionnez les méthodes d'accès à prendre en charge : HTTP, HTTPS ou les deux.
- Port HTTP (pour les connexions entrantes) - Port HTTP, le port par défaut est 80.
- Port HTTPS (pour les connexions entrantes sécurisées) - Port HTTP, le port par défaut est 443.

Si l'option Exiger la connexion des clients est activée, ZFSSA refuse l'accès aux clients qui ne fournissent pas d'informations d'identification valides pour un utilisateur local, NIS ou LDAP. L'authentification Active Directory n'est pas prise en charge. Seule l'authentification HTTP basique est prise en charge. Si HTTPS n'est pas utilisé, le nom d'utilisateur et le mot de passe non chiffrés sont transmis, ce qui n'est pas nécessairement approprié dans tous les environnements. Si l'option Exiger la connexion des clients est désactivée, ZFSSA n'essaie pas de procéder à l'authentification.

Quel que soit le type d'authentification, aucune autorisation n'est masquée dans les fichiers et les répertoires créés. Les fichiers nouvellement créés peuvent être lus et écrits par tous. Les répertoires nouvellement créés peuvent être lus, écrits et exécutés par tous.

Network Data Management Protocol (NDMP)

Le service NDMP permet au ZFSSA de participer aux opérations de sauvegarde et restauration NDMP contrôlées par un client NDMP distant appelé application de gestion des données (DMA, Data Management Application). A l'aide de NDMP, les données utilisateur du ZFSSA (par exemple, les données stockées dans les partages créés par l'administrateur sur le ZFSSA) peuvent être sauvegardées et restaurées à la fois sur les lecteurs de bande connectés en local et sur les systèmes distants. Les périphériques connectés en local peuvent également être sauvegardés et restaurés via DMA.

Réplication distante

La réplication ZFSSA distante facilite la réplication de projets et de partages. Ce service vous permet de voir les ZFSSA qui ont répliqué des données sur ce ZFSSA et configure les ZFSSA sur lesquels ce ZFSSA peut répliquer.

Lorsque ce service est activé, le ZFSSA reçoit des mises à jour de réplication à partir des autres ZFSSA et envoie des mises à jour de réplication pour les projets et les partages locaux en fonction des actions configurées. Lorsque le service est désactivé, les mises à jour de réplication entrantes échouent et aucun projet ni partage local n'est répliqué.

Le mot de passe root pour le ZFSSA distant est nécessaire pour configurer les cibles de réplication distantes pour le ZFSSA. Ces cibles sont utilisées pour établir une connexion de pair de réplication qui permet aux ZFSSA de communiquer.

Lors de la création de cibles, le mot de passe root est utilisé pour confirmer l'authenticité de la demande et pour produire et échanger des clés de sécurité qui seront utilisées pour identifier les ZFSSA lors de communications ultérieures.

Les clés générées sont stockées de manière permanente dans le cadre de la configuration ZFSSA. Le mot de passe root n'est jamais stocké de manière permanente. Le mot de passe root n'est jamais transmis en clair. Toutes les communications ZFSSA sont protégées par la technologie SSL, y compris cet échange initial d'identité.

Migration shadow

La migration shadow autorise la migration automatique des données de sources externes ou internes et contrôle la migration automatique en arrière-plan. Les données sont migrées de façon synchrone pour les demandes in-band, que le service soit activé ou non. Le but principal de ce service est de permettre aux utilisateurs d'ajuster le nombre des threads dédiés à la migration en arrière-plan.

Les montages NFS sur une source NFS ne sont pas contrôlés par l'utilisateur ZFSSA. Les montages de migration shadow ne peuvent pas être sécurisés ; donc si le serveur attend une demande Kerberos ou une demande similaire, le montage source est rejeté.

SSH File Transfer Protocol, protocole de transfert de fichier SSH (SFTP)

SFTP autorise l'accès au système de fichiers de clients SFTP. Les connexions anonymes ne sont pas autorisées, les utilisateurs doivent donc s'authentifier avec le service de noms configuré.

Lorsque vous créez une clé SFTP, vous devez inclure la propriété "user" à une affectation d'utilisateur valide. Les clés SFTP sont regroupées par utilisateur et authentifiées via SFTP à l'aide du nom d'utilisateur.

REMARQUE : pour des raisons de sécurité, vous devriez recréer toutes les clés SFTP existantes qui n'incluent pas la propriété user, même si l'authentification reste possible.

TFTP (Trivial File Transfer Protocol)

TFTP est un protocole simple pour le transfert de fichiers. Il est conçu pour être petit et facile à implémenter, mais il ne possède pas la plupart des fonctionnalités de sécurité d'un FTP. Le protocole

TFTP lit et écrit des fichiers uniquement en amont ou en aval d'un serveur distant. Il ne peut pas lister les répertoires et ne propose pas de mécanismes d'authentification utilisateur à ce jour.

Services d'annuaire

NIS (Network Information Service)

NIS est un service de noms pour la gestion centralisée des répertoires. Le ZFSSA peut se comporter tel un client NIS pour les utilisateurs et les groupes, de sorte que les utilisateurs NIS puissent se connecter au FTP et au HTTP/WebDav : Les utilisateurs NIS peuvent également recevoir des privilèges pour l'administration du ZFSSA. Le ZFSSA complète les informations NIS à l'aide de ses propres privilèges.

Lightweight Directory Access Protocol (LDAP)

Le ZFSSA utilise le LDAP pour authentifier les utilisateurs administratifs et certains utilisateurs de services de données (ftp, http). La sécurité LDAP sur SSL est prise en charge par le ZFSSA. Le LDAP est utilisé pour récupérer des informations concernant les utilisateurs et les groupes, des manières suivantes :

- Fournit des interfaces utilisateur qui acceptent et affichent des noms pour les utilisateurs et les groupes.
- Mappe des noms depuis et vers les utilisateurs et les groupes, pour des protocoles de données qui utilisent des noms (NFSv4, par exemple).
- Définit l'appartenance à un groupe pour leur utilisation dans le contrôle d'accès.
- De manière facultative, afin d'authentifier les données utilisées pour l'authentification d'accès administrative et aux données.

Les connexions LDAP peuvent être utilisées comme mécanisme d'authentification. Par exemple, lorsqu'un utilisateur tente de s'authentifier au ZFSSA, le ZFSSA peut essayer de s'authentifier au serveur LDAP en tant qu'utilisateur, comme mécanisme de vérification de l'authentification.

Il existe un ensemble de contrôles pour la sécurité de connexion au LDAP :

- Authentification appareil-serveur :
 - L'appareil est anonyme
 - L'appareil s'authentifie à l'aide d'informations d'identification d'un utilisateur Kerberos
 - L'appareil s'authentifie à l'aide d'un utilisateur et d'un mode de passe "proxy" spécifique
- Authentification serveur-appareil (s'assurer que le bon serveur a été contacté) :
 1. Non sécurisé
 2. Le serveur est authentifié à l'aide de Kerberos
 3. Le serveur est authentifié à l'aide d'un certificat TLS

Les données transmises sur une connexion LDAP sont chiffrées si Kerberos ou TLS sont utilisés mais pas chiffrés. Lorsque TLS est utilisé, la première connexion lors de la configuration n'est pas sécurisée. Le certificat du serveur collecté à ce moment-là est utilisé pour authentifier les connexions de production ultérieures.

Il n'est pas possible d'importer le certificat d'une autorité de certification afin d'authentifier plusieurs serveurs LDAP ; il n'est pas non plus possible d'importer manuellement un certificat de serveur LDAP spécifique.

Seul un TLS brut (LDAPS) est pris en charge. Les connexions STARTTLS, qui commencent sur une connexion LDAP non sécurisée puis passent sur une connexion sécurisée, ne sont pas prises en charge. Les serveurs LDAP qui nécessitent un certificat client ne sont pas pris en charge.

Mappage des identités

Les clients peuvent accéder aux ressources de fichiers sur le ZFSSA à l'aide de SMB ou de NFS et chacun d'entre eux a un identificateur utilisateur unique. Les utilisateurs SMB/Windows ont des SID (Security Descriptors) et les utilisateurs UNIX/Linux ont des ID utilisateur (UIDs). Les utilisateurs peuvent également faire partie de groupes qui sont identifiés par SID de groupe (pour les utilisateurs Windows) ou ID de groupe (GID) pour les utilisateurs UNIX/Linux.

Dans des environnements où les ressources de fichiers sont accessibles à l'aide des deux protocoles, il est souvent recommandé d'établir des équivalences d'identité où un utilisateur UNIX est équivalent à un utilisateur Active Directory, par exemple. Cette pratique est utile pour déterminer les droits d'accès aux ressources de fichiers sur le ZFSSA.

Il existe différents types de mappage des identités qui concernent les services d'annuaire tels que Active Directory, LDAP et NIS. Assurez-vous de suivre les meilleures pratiques de sécurité pour le service d'annuaire utilisé.

IDMU

Microsoft offre une fonctionnalité appelée Identity Management for Unix (IDMU). Ce logiciel est disponible pour Windows Server 2003 et intégré à Windows Server 2003 R2 et aux versions ultérieures. Cette fonction fait partie de l'ancien logiciel Services pour Unix non fourni en standard.

L'utilisation principale d'IDMU est la prise en charge de Windows en tant que serveur NIS/NFS. IDMU permet à l'administrateur de spécifier un nombre de paramètres UNIX : UID, GID, shell de connexion, annuaire personnel et de même type pour les groupes. Ces paramètres sont accessibles dans AD via un schéma similaire (mais pas identique) à celui du document RFC2307 et via le service NIS.

Lorsque le mode IDMU est utilisé, le service de mappage des identités utilise ces attributs Unix pour établir des correspondances entre les identités Windows et Unix. Cette approche est très similaire au mappage basé sur un annuaire. La seule différence tient au fait que le service de mappage des identités interroge le schéma de propriété établi par le logiciel IDMU au lieu d'autoriser un schéma personnalisé. Lorsque cette approche est utilisée, aucun autre mappage basé sur un annuaire ne peut être utilisé.

Mappage basé sur un annuaire

Ce type de mappage comprend l'annotation d'un objet LDAP ou Active Directory à l'aide d'informations relatives à la manière dont l'identité est mise en correspondance avec une identité équivalente sur la plateforme opposée. Ces attributs supplémentaires associés à l'objet doivent être configurés.

Mappage basé sur un nom

L'approche du mappage basé sur un nom consiste en la création de différentes règles de mise en correspondance des identités par nom. Ces règles établissent des équivalences entre les identités Windows et UNIX.

Mappage éphémère

Si aucune règle de mappage basé sur un nom ne s'applique à un utilisateur spécifique, celui-ci reçoit des informations d'identification temporaires via un mappage éphémère (à moins qu'un mappage de refus ne l'interdise). Lorsqu'un utilisateur Windows portant un nom UNIX éphémère crée un fichier sur le système,

les clients Windows qui accèdent au fichier par le biais de SMB voient que le fichier appartient à cette identité Windows. En revanche, pour les clients NFS, le fichier appartient à "nobody".

Paramètres système

Les sections suivantes décrivent les paramètres de sécurité système disponibles.

Phone Home

Le service Phone Home permet de gérer l'enregistrement du ZFSSA de la même manière que le service de support à distance de Phone Home. Aucune donnée ou métadonnée utilisateur n'est transmise dans ce message.

- L'enregistrement connecte votre ZFSSA au portail d'inventaire Oracle qui vous permet de gérer l'équipement Oracle. L'enregistrement est un prérequis à l'utilisation du service Phone Home.
- Le service Phone Home communique avec le support Oracle pour fournir les éléments suivants :
 - Compte-rendu des pannes - le système signale les problèmes actifs à Oracle afin d'assurer une intervention automatisée. En fonction de la nature de la panne, un cas de prise en charge peut être ouvert.
 - Signal d'activité - des pulsations quotidiennes sont envoyées à Oracle pour indiquer que le système est actif et en cours d'exécution. Le support Oracle peut informer le contact technique chargé d'un compte lorsque l'un des systèmes activés ne parvient pas à envoyer un signal d'activité pendant une période prolongée.
 - Configuration système - des messages sont régulièrement envoyés à Oracle pour décrire les versions et la configuration logicielle et matérielle actuelles, ainsi que la configuration du stockage.

Indicateurs de maintenance

Les indicateurs de maintenance sont utilisés pour faciliter la prise en charge et l'inventaire des produits, en permettant d'interroger le ZFSSA sur des données telles que :

- Numéro de série du système
- Type de système
- Numéros de version logicielle

Vous pouvez enregistrer ces indicateurs de maintenance auprès du support Oracle, ce qui vous permet de garder facilement la trace de votre équipement Oracle et de raccourcir la durée des appels liés à la maintenance. Les indicateurs de maintenance sont activés par défaut.

SMTP

SMTP envoie tous les courriers générés par le ZFSSA, généralement en réponse aux alertes configurées. Le service SMTP n'accepte pas le courrier externe. Il envoie uniquement les messages générés automatiquement par le ZFSSA.

Par défaut, le service SMTP utilise DNS (enregistrements MX) pour déterminer la destination du courrier. Si DNS n'est pas configuré pour le domaine du ZFSSA ou si les enregistrements MX DNS ne sont pas définis correctement pour le domaine de destination du courrier sortant, ZFSSA peut être configuré de façon à faire suivre tous les messages via un serveur de courrier sortant, couramment appelé hôte intelligent.

SNMP (Simple Network Management Protocol)

SNMP fournit deux fonctions sur le ZFSSA ; les informations sur l'état du ZFSSA peuvent être gérées par SNMP et les alertes peuvent être configurées pour envoyer des dérivements SNMP. Les versions 1 et 2c de SNMP sont disponibles.

Syslog

Un message Syslog est un petit message d'événement transmis depuis le ZFSSA sur un ou plusieurs systèmes distants. Syslog fournit deux fonctions ZFSSA :

- La fonction Alerts peut être configurée de façon à envoyer des messages Syslog à un ou plusieurs systèmes distants.
- Les messages Syslog des services du ZFSSA compatibles sont envoyés aux systèmes distants.

Le service Syslog peut être configuré de façon à utiliser le format de sortie classique décrit dans le document RFC 3164 ou le format de sortie le plus récent avec version décrit dans le RFC 5424. Les messages Syslog sont transmis en tant que datagrammes UDP. Par conséquent, ils sont susceptibles d'être ignorés par le réseau ou de ne pas être envoyés du tout si le système d'envoi dispose de peu de mémoire ou si le réseau est encombré. Les administrateurs doivent donc partir du principe que, dans certains scénarios de panne complexe de réseau, certains messages peuvent manquer et avoir été ignorés.

Ce message contient les éléments suivants :

- Facility : indique le type de composant système qui a envoyé le message
- Severity : indique le niveau de gravité de la condition associée au message
- Timestamp : indique la date et l'heure associées à l'événement au format UTC (temps universel)
- Hostname : indique le nom canonique du ZFSSA
- Tag : indique le nom du composant système qui a envoyé le message.
- Message : décrit l'événement.

Identité du système

Ce service offre une configuration pour le nom et l'emplacement du système. Vous devrez peut-être modifier ces éléments si vous déplacez le ZFSSA vers un nouveau réseau ou si vous modifiez son utilisation.

Nettoyage des disques

Le nettoyage des disques doit être réalisé sur une surface régulière afin de permettre au ZFSSA de détecter et corriger les données endommagées sur le disque. Le nettoyage des disques est un processus en arrière-plan qui lit les disques pendant des périodes d'inactivité pour détecter des erreurs de lecture irrémédiables dans des secteurs rarement consultés. Afin d'éviter la perte de données, il est important de détecter à temps les erreurs de secteur latentes.

Prévention de la destruction

Lorsque la fonctionnalité Prévention de la destruction est activée, le partage ou le projet ne peuvent pas être détruits. Cela comprend la destruction d'un partage par le biais de clones dépendants, la destruction d'un partage contenu dans un projet ou la destruction d'un package de réplication. Cependant, cela ne concerne pas les partages détruits par le biais des mises à jour de réplication. Si un partage est détruit sur un ZFSSA

qui est la source de la réplication, le partage correspondant sur la cible sera détruit, même si cette propriété est activée.

Pour détruire un partage, cette propriété doit d'abord être explicitement désactivée au cours d'une étape distincte. Par défaut, cette propriété est désactivée.

Accès administratif distant

Cette section décrit la sécurité d'accès distant au ZFSSA.

Interface utilisateur de navigateur (BUI, Browser User Interface)

Les écrans BUI Services permettent d'afficher et de modifier les services et les paramètres d'accès distant.

SSH (Secure Shell)

Le service SSH permet aux utilisateurs de se connecter au ZFSSA par le biais de la CLI et d'effectuer la plupart des opérations d'administration pouvant être réalisées dans l'interface utilisateur du navigateur. Le service SSH peut également servir de moyen d'exécution des scripts automatiques à partir d'un hôte distant, comme pour extraire les journaux quotidiens ou les statistiques Analytics.

Journaux

Cette section décrit les fonctionnalités de journalisation relative à la sécurité.

Audit

Le journal d'audit enregistre les événements liés à l'activité des utilisateurs, notamment les connexions et les déconnexions à la BUI et à la CLI et les actions administratives. Le tableau suivant montre des exemples d'entrées du journal d'audit telles qu'elles s'afficheraient dans la BUI :

TABLEAU 2 Enregistrement de journal d'audit

Temps	Utilisateur	Hôte	Résumé	Annotation de session
2009-10-12 05:20:24	root	galaxie	Service ftp désactivé	
2009-10-12 03:17:05	root	galaxie	Utilisateur connecté	
2009-10-11 22:38:56	root	galaxie	Session de navigateur expirée	
2009-10-11 21:13:35	root	<console>	Service ftp activé	

Phone Home

Si le Phone Home est utilisé, ce journal affiche les événements de communication avec le support Oracle. Le tableau suivant est un exemple d'entrée de Phone Home tel qu'il s'afficherait dans la BUI :

TABLEAU 3 Enregistrement de journal du Phone Home

Temps	Description	Résultat
2009-10-12 05:24:09	Fichier chargé 'cores/ak.45e5ddd1-ce92-c16e-b5eb-9cb2a8091f1c.tar.gz' sur le support Oracle	OK

Plus d'informations

Vous pouvez trouver une aide en ligne spécifique au contexte pour chaque page de la BUI de ZFSSA en cliquant sur le bouton aide situé en haut à gauche de chaque page.

Vous pouvez trouver des informations complètes relatives au produit pour Oracle ZFS Storage Appliance à l'adresse suivante :

www.oracle.com/us/products/servers-storage/storage/nas/overview

Mappage de la documentation

Utilisez les tableaux ci-dessous pour localiser la documentation détaillée pour chaque service, configuration ou autre fonctionnalité du ZFSSA. Lorsque vous utilisez la BUI pour configurer un ZFSSA, vous pouvez cliquer sur le lien AIDE en haut à droite d'un écran pour afficher l'aide de cet écran.

TABLEAU 4 Services

Service	Emplacement de la documentation
Active Directory	Services:Active_Directory
Mappage des identités	Services:Mappage_des_identités
DNS	Services:DNS
Routage dynamique	Services:Routage_dynamique
IPMP	Services:IPMP
NTP	Services:NTP
Phone Home	Services:Phone_Home
Indicateurs de maintenance	Services:Indicateurs_de_maintenance
SMTP	Services:SMTP
SNMP	Services:SNMP
Syslog	Services:Syslog
Identité du système	Services:Identité_du_système
SSH	Services:SSH

TABLEAU 5 Configuration

Configuration	Emplacement de la documentation
SAN	Configuration:SAN
SAN:FC	Configuration:SAN:FC

Configuration	Emplacement de la documentation
SAN:iSCSI	Configuration:SAN:iSCSI
SAN:SRP	Configuration:SAN:SRP
Cluster	Configuration:Cluster
Utilisateurs	Configuration:Utilisateurs
Préférences	Configuration:Préférences
Alertes	Configuration:Alertes
Stockage	Configuration:Stockage

TABLEAU 6 Stockage

Stockage	Emplacement de la documentation
Partages	Partages
Concepts	Partages:Concepts
Migration_shadow	Partages:Migration_shadow
Gestion_de_l'espace	Partages:Gestion_de_l'espace
Systèmes de fichiers_Espace de noms	Partages:Systèmes de fichiers_Espace de noms
Partages	Partages:Partages
Général	Partages:Partages:Général
Protocoles	Partages:Partages:Protocoles
Accès	Partages:Partages:Accès
Clichés	Partages:Partages:Clichés
Projets	Partages:Projets
Projets:Général	Partages:Projets:Général
Projets:Protocoles	Partages:Projets:Protocoles
Projets:Réplication	Partages:Projets:Réplication
Schéma	Partages:Schéma

Copyright © 2013, 2014, Oracle et/ou ses affiliés. Tous droits réservés.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf disposition expresse de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, accorder de licence, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est livré sous licence au Gouvernement des Etats-Unis, ou à quiconque qui aurait souscrit la licence de ce logiciel ou l'utilise pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique :

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer un risque de dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour des applications dangereuses.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée de The Open Group.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation.