Guide de sécurité des systèmes Oracle® ZFS Storage Appliance, version OS8.7.0

Référence: E81238-01
Mars 2017

Référence: E81238-01

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

Guide de sécurité des systèmes 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. Pour les procédures de configuration, consultez le *Guide d'administration des systèmes Oracle ZFS Storage Appliance*.

Les sections suivantes fournissent une description des fonctions de sécurité et des recommandations spécifiques à Oracle ZFS Storage Appliance :

- **Premières étapes** - Décrit la sécurité de la connexion pendant l'installation initiale de l'appareil et fournit des recommandations pour la sécurité physique du système.
- **Modèle administratif** - Décrit l'accès distant via la BUI et la CLI, la restriction de l'accès à la BUI et la CLI, le modèle de patches système, les mises à jour différées, les lots de support et la sauvegarde de configuration.
- **Utilisateurs d'appareil** - Décrit les rôles d'administration, qui peut administrer l'appareil 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.
- **Services de données** - Décrit les services de données pris en charge par l'appareil et la sécurité proposée par les différents services de données.
- **Services d'annuaire** - Décrit les services d'annuaire qui peuvent être configurés sur l'appareil et leurs implications de sécurité.
- **Paramètres système** - Décrit les paramètres système : Phone Home, indicateurs de maintenance, Kerberos, SMTP, SNMP, syslog, identité du système, nettoyage de disque et prévention de destruction.
- **Journaux de sécurisation** - Décrit les types de journaux adaptés à la sécurité.

Premières étapes

Cette section décrit la sécurité de la connexion pendant l'installation initiale de l'appareil et fournit des recommandations pour la sécurité physique du système.

Installation initiale

Oracle ZFS Storage Appliance est fourni avec le logiciel d'appareil pré-installé. 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 Oracle ZFS Storage Appliance est réinitialisé sur les paramètres d'usine par défaut, le mot de passe root l'est également pour l'appareil et le processeur de service.

Lors de l'installation initiale d'un appareil Oracle ZFS Storage Appliance, un nom et un mot de passe du compte par défaut sont associés au processeur de service du système. Ce compte par défaut permet à un administrateur système d'obtenir un accès initial à l'appareil, l'administrateur devant ensuite exécuter les étapes d'installation initiale. Une des étapes nécessaires consiste à configurer un nouveau mot de passe administratif d'appareil, 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.

Oracle ZFS Storage Appliance 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 le modèle administratif Oracle ZFS Storage Appliance.

Accès administratif distant

Cette section décrit la sécurité d'accès distant à Oracle ZFS Storage Appliance.

Interface utilisateur de navigateur

La BUI (Browser User Interface) est utilisée pour l'administration générale de l'appareil. Les écrans BUI Services permettent d'afficher et de modifier les services et les paramètres d'accès distant.

L'administration s'effectue via une session de navigateur (HTTPS) sécurisée. Les sessions HTTPS sont chiffrées avec un certificat autosigné possédant une génération unique pour chaque Oracle ZFS Storage Appliance 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.

Interface de ligne de commande

La CLI (Command Line Interface) permet d'effectuer la plupart des opérations d'administration pouvant être réalisées dans l'interface utilisateur du navigateur.

SSH (Secure Shell) permet aux utilisateurs de se connecter à Oracle ZFS Storage Appliance via une connexion SSL (Secure Sockets Layer) à la CLI. 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.

Autorisation d'utilisateur restreinte

L'accès administratif 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 LDAP (Lightweight Directory Access Protocol) et le service d'informations réseau (NIS).

Par ailleurs, l'appareil peut utiliser Kerberos pour authentifier les utilisateurs qui se connectent en tant qu'administrateur depuis la BUI, la CLI ou l'API RESTful et leur permettre d'accéder à des services tels que NFS, HTTP, FTP, SFTP et SSH. Il est également possible de recourir à Kerberos pour définir la sécurité des partages individuels qui utilisent le protocole NFS, comme indiqué dans la section "Options d'authentification et de chiffrement NFS" à la page 15.

API RESTful Oracle ZFS Storage Appliance

L'API RESTful Oracle ZFS Storage Appliance permet de gérer Oracle ZFS Storage Appliance. L'architecture RESTful repose sur un modèle client-serveur en couches qui permet aux services

d'être redirigés de manière transparente à l'aide de hubs, routeurs et autres systèmes réseau standard sans nécessiter la configuration du client.

L'API Oracle ZFS Storage Appliance RESTful utilise les mêmes informations d'identification que la BUI et la CLI. Toutes les demandes des clients externes sont authentifiées individuellement à l'aide des informations d'identification de l'appareil et sont conduites via une connexion HTTPS au port 215. L'API RESTful prend en charge des sessions HTTPS ayant un délai d'expiration par défaut de 15 minutes défini par l'utilisateur.

Pour obtenir des informations sur la gestion d'Oracle ZFS Storage Appliance avec l'API RESTful, reportez-vous au *Guide de l'API (Application Programming Interface) Oracle ZFS Storage Appliance RESTful*.

Mises à jour du système

Pour que vous puissiez profiter des dernières améliorations apportées à la sécurité, Oracle vous recommande de maintenir le logiciel système à jour.

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 mais 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

Si votre système est inscrit pour le support Phone Home et qu'il souffre d'une panne majeure, l'état du système est envoyé à My Oracle Support où il est 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 d'appareil

Il existe deux types d'utilisateurs d'Oracle ZFS Storage Appliance :

- **Utilisateurs de services de données** – Les clients qui accèdent aux ressources de fichiers et de blocs via les protocoles pris en charge (par exemple, NFS (Network File System), SMB (Server Message Block), Fibre Channel, iSCSI (Internet Small Computer System Interface), (HTTP) Hypertext Transfer Protocol) et FTP (File Transfer Protocol).
- **Utilisateurs administratifs** - Utilisateurs qui gèrent la configuration et les services sur l'appareil.

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 :

- **Utilisateurs locaux** – toutes les informations de compte sont enregistrées dans Oracle ZFS Storage Appliance.
- **Utilisateurs de l'annuaire** - des comptes NIS ou LDAP existants sont utilisés et des paramètres d'autorisation supplémentaires sont enregistrés sur l'appareil. L'accès à l'appareil doit être accordé de manière explicite aux utilisateurs NIS/LDAP, qui peuvent alors se connecter et administrer l'appareil. L'accès ne peut pas être accordé par défaut.

Portées administratives

Les autorisations permettent aux utilisateurs d'effectuer des tâches spécifiques telles que la création de partages, la réinitialisation de l'appareil et la mise à jour du logiciel système. Groups of authorizations are called scopes. 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

Oracle ZFS Storage Appliance assure le contrôle d'accès aux fichiers au moyen de listes de contrôle d'accès (ACL, Access Control Lists). Il s'agit d'un mécanisme qui autorise ou refuse l'accès à un fichier ou un répertoire particulier.

Le modèle ACL fourni par Oracle ZFS Storage Appliance 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 d'appareil 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 de plusieurs entrées de contrôle d'accès (ACE). Chaque ACE contient une entrée pour les autorisations qu'elle octroie ou refuse, les personnes 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.

Détermination de 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 au niveau du partage SMB

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 tous les utilisateurs.

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.

Services de données

Le tableau suivant fournit une description et indique les ports utilisés pour chaque service 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

SERVICE	DESCRIPTION	PORTS UTILISES
		Datagramme NetBIOS 138 Service de noms NetBIOS 137
Analyse antivirus	Analyse antivirus du système de fichiers	
FTP	Accès au système de fichiers via le protocole FTP	21
HTTP	Accès au système de fichiers via le protocole HTTP	80
HTTPS	Ports HTTPS (pour les connexions entrantes sécurisées)	443
NDMP	Service hôte NDMP	10000
Réplication distante	Réplication distante	216 et 217
Chiffrement	Chiffrement transparent des systèmes de fichiers et des LUN	
Migration shadow	Migration des données shadow	
SFTP	Accès au système de fichiers via le protocole SFTP	218
TFTP	Accès au système de fichiers via le protocole TFTP	
Réseau de stockage	Groupes de cibles et d'initiateurs SAN (Storage Area Network)	

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 c'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, les ports 216 et 217 doivent également être ouverts.

Options d'authentification et de chiffrement NFS

Kerberos peut être utilisé pour authentifier les utilisateurs qui se connectent en tant qu'administrateur et donner accès aux services. Il peut aussi servir à définir la sécurité pour des partages individuels qui utilisent le protocole 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'ID utilisateur (UID) et l'ID de groupe (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.

Service de données iSCSI

Lorsque vous configurez un LUN sur Oracle ZFS Storage Appliance, vous pouvez exporter ce volume via une cible iSCSI. 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 (Challenge-Handshake Authentication Protocol). De plus, le service prend en charge la gestion des données d'authentification CHAP dans une base de données RADIUS (Remote Authentication Dial-In User Service).

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

RADIUS (Remote Authentication Dial-In User Service) 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 Oracle ZFS Storage Appliance d'effectuer l'authentification CHAP à l'aide de RADIUS, les conditions suivantes doivent être remplies :

- L'appareil doit spécifier l'adresse du serveur RADIUS et le secret à utiliser lors de la communication avec le serveur RADIUS concerné
- Le serveur RADIUS doit comporter une entrée (par exemple, dans son fichier clients) indiquant l'adresse de l'appareil et spécifiant le même secret que ci-dessus.
- Le serveur RADIUS doit comporter une entrée (par exemple, dans son fichier utilisateurs) 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), l'appareil 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, l'appareil doit comporter une entrée Initiator distincte pour l'initiateur concerné indiquant le mappage d'un nom IQN vers un nom CHAP. Cette entrée Initiateur n'a pas besoin d'indiquer le secret CHAP de l'initiateur.

Service de données SMB

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 Requise** - 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

En mode domaine, les utilisateurs sont définis dans Microsoft Active Directory (AD). Les clients SMB peuvent se connecter à Oracle ZFS Storage Appliance à l'aide de l'authentification Kerberos ou NTLM.

Lorsqu'un utilisateur se connecte par le biais d'un nom d'hôte Oracle ZFS Storage Appliance 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 à l'appareil, 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 à l'appareil par le biais d'un nom d'hôte complet. Pour plus d'informations, reportez-vous à l'article du réseau des développeurs Microsoft :

`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 Oracle ZFS Storage Appliance. Lorsqu'un client SMB se connecte à un appareil dans le mode groupe de travail, le mot de passe de cet utilisateur et les hachages de mot de passe sont utilisés pour authentifier l'utilisateur localement.

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

La liste suivante montre le comportement d'Oracle ZFS Storage Appliance 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 l'appareil 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 (Microsoft Management Console) 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 des événements Les membres du groupe Administrators peuvent également définir et modifier les ACL de niveau de partage.

Analyse antivirus

Le service Analyse antivirus vérifie la présence de 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 qu'Oracle ZFS Storage Appliance contacte. Le moteur externe n'est pas inclus dans le logiciel d'appareil.

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 Oracle 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.

Service de données FTP

FTP autorise l'accès au système de fichiers via des 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. Le serveur FTP utilise un certificat de sécurité auto-signé ou un certificat fourni par le client.
- **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 utilise du texte simple, ce qui 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

Service de données HTTP

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). Les clients peuvent ainsi accéder aux systèmes de fichiers partagés via un navigateur Web ou en tant que système de fichiers local si cette option est prise en charge par leur logiciel client.

Le serveur HTTPS utilise un certificat de sécurité auto-signé ou un certificat fourni par le client. Pour obtenir un certificat fourni par le client, vous devez générer une demande de signature de certificat (CSR, Certificate Signing Request) et l'envoyer à l'autorité de certification (CA) pour la signature. Une fois le certificat renvoyé par la CA, il peut être installé sur l'appareil. Si un certificat est signé par une CA non root, vous devez également obtenir des certificats auprès de CA de niveau secondaire et de haut niveau. Pour plus d'informations sur la gestion des certificats, veuillez vous reportez au *Guide d'administration des systèmes Oracle ZFS Storage Appliance*.

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, Oracle ZFS Storage Appliance 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, l'appareil ne tente pas d'authentifier les informations d'identification.

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.

Service de données NDMP

Le protocole NDMP (Network Data Management Protocol) permet à Oracle ZFS Storage Appliance 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 de l'appareil (par exemple, les données stockées dans les partages créés par l'administrateur sur l'appareil) 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.

Service de données de réplication distante

La réplication distante Oracle ZFS Storage Appliance facilite la réplication des projets et des partages. Ce service permet d'afficher les appareils qui ont répliqué des données vers un appareil spécifique et de déterminer les appareils vers lesquels un appareil spécifique peut répliquer.

Lorsque ce service est activé, l'appareil reçoit des mises à jour de réplication à partir des autres appareils 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 l'appareil distant est nécessaire pour configurer les cibles de réplication distantes pour l'appareil. Ces cibles sont utilisées pour établir une connexion de pair de réplication qui permet aux appareils 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 appareils lors de communications ultérieures.

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

La fonction de réplication hors ligne d'Oracle ZFS Storage Appliance permet de gagner du temps, de réduire les ressources et les erreurs de données potentielles lors de la réplication d'un ensemble de données de grande taille sur un réseau avec une bande passante limitée. La réplication hors ligne exporte le flux de réplication vers un fichier sur le serveur NFS, qui peut être déplacé physiquement sur un site cible distant, ou copié sur un média externe pour être expédié (facultatif). Sur le site cible, l'administrateur importe le fichier contenant le flux de réplication sur l'appareil cible.

Pour limiter l'accès au flux de réplication exporté, présentez le partage NFS uniquement à l'adresse IP des appareils source et cible. Pour chiffrer les données, activez le chiffrement sur disque pour le partage NFS sur le serveur NFS. Pour plus d'informations, reportez-vous à la documentation de votre serveur NFS. Remarquez qu'un flux de réplication exporté n'est jamais chiffré par l'appareil.

Utilisation du chiffrement de données

NOTICE RELATIVE A LA LICENCE : *le chiffrement peut faire l'objet d'une évaluation à titre gratuit, mais cette fonction requiert l'achat d'une licence distincte pour un usage en production. Les licences pour la fonction de chiffrement sont uniquement disponibles pour les modèles Oracle ZFS Storage ZS5-4, Oracle ZFS Storage ZS5-2, Oracle ZFS Storage ZS4-4 et Oracle ZFS Storage ZS3-4. Au terme de la période d'évaluation, il est nécessaire d'acquérir une licence ou de désactiver la fonction. Oracle se réserve le droit de vérifier la conformité de la licence à tout moment. Pour plus d'informations, reportez-vous au document "Oracle Software License Agreement ("SLA") and Entitlement for Hardware Systems with Integrated Software Options (contrat de licence du logiciel Oracle et droits concédés pour les systèmes matériels comprenant des options logicielles intégrées)."*

Oracle ZFS Storage Appliance offre un chiffrement transparent des données pour les partages individuels (systèmes de fichiers et LUN) et les partages créés au sein des projets.

Gestion des clés de chiffrement

L'appareil inclut un keystore LOCAL intégré et présente la possibilité de se connecter au système OKM (Oracle Key Manager). Chaque projet ou partage chiffré nécessite une clé d'encapsulation provenant soit du keystore LOCAL, soit du keystore OKM. Les clés de chiffrement des données sont gérées par l'appareil de stockage, stockées de manière permanente et chiffrées par la clé d'encapsulation provenant du keystore LOCAL ou du keystore OKM.

Oracle Key Manager (OKM) est un système de gestion de clés (KMS) complet, conçu pour répondre aux besoins sans cesse croissants des entreprises en matière de chiffrement des données basé sur le stockage. Développé en conformité avec les normes de sécurité ouvertes, OKM fournit la capacité, l'évolutivité et l'interopérabilité nécessaires pour gérer de manière centrale les clés de chiffrement à travers des infrastructures de stockage largement distribuées et hétérogènes.

OKM répond aux défis uniques de la gestion des clés de stockage, notamment :

- **Conservation de clés à long terme** : OKM assure la disponibilité ininterrompue des données et conserve de manière sécurisée les clés de chiffrement pendant la totalité du cycle de vie des données.
- **Interopérabilité** : OKM fournit l'interopérabilité nécessaire à la prise en charge d'une gamme étendue de périphériques de stockage, qui peuvent être connectés à des mainframes

ou des plates-formes de systèmes ouverts sous un service unique de gestion des clés de stockage.

- **Haute disponibilité** : fournit une haute disponibilité grâce au clustering actif à N noeuds, l'équilibrage dynamique de la charge et le basculement automatisé, que les appareils soient dans la même pièce ou répartis dans le monde entier.
- **Haute capacité** : OKM peut gérer un grand nombre de périphériques de stockage et plus encore de clés de stockage. Un appareil en cluster unique peut fournir des services de gestion des clés pour des milliers de périphériques de stockage et des millions de clés de stockage.
- **Configuration de clé flexible** : pour un cluster OKM, les clés peuvent être générées automatiquement ou individuellement pour un keystore LOCAL ou OKM. Les administrateurs de la sécurité sont chargés de fournir les noms de clés qui, combinés avec la banque de clés, associent une clé d'encapsulation données à un projet ou un partage.

Maintien des clés

Les partages et les projets qui utilisent des clés OKM à l'état désactivé demeurent accessibles. Pour empêcher l'utilisation d'une clé OKM, l'administrateur OKM doit explicitement supprimer la clé.

Pour vous assurer que les partages et les projets chiffrés sont accessibles, sauvegardez vos configurations d'appareil et vos valeurs de clés de keystore LOCAL. Si une ou plusieurs clés ne sont plus disponibles, les partages ou les projets utilisant ces clés ne sont plus accessibles. Si la clé d'un projet n'est pas disponible, de nouveaux partages ne peuvent pas être créés dans ce projet.

Les clés peuvent devenir indisponibles comme suit :

- Les clés sont supprimées
- Restauration d'une version ne prenant pas en charge le chiffrement
- Restauration d'une version où les clés ne sont pas configurées
- Réinitialisation des paramètres d'usine
- Le serveur OKM n'est pas disponible

Cycle de vie d'une clé de chiffrement

Le cycle de vie d'une clé de chiffrement est flexible car vous pouvez changer de clé à tout moment sans déconnecter les services de données.

Lorsqu'une clé est supprimée de la banque de clés, tous les partages qui l'utilisent sont démontés et les données qu'ils contiennent deviennent inaccessibles. La sauvegarde des clés dans la

banque de clés d'OKM doit être effectuée à l'aide des services de sauvegarde d'OKM. La sauvegarde des clés dans le keystore LOCAL est incluse dans la sauvegarde de la configuration système. Pour la banque de clés LOCAL, il est également possible de fournir la valeur de la clé au moment de la création afin de permettre son stockage dans un système externe, offrant ainsi une solution de sauvegarde/restauration de clé alternative.

Service de données de 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 sous le contrôle de l'utilisateur d'Oracle ZFS Storage Appliance. 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.

Service de données SFTP

Le protocole SFTP (SSH File Transfer Protocol) 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.

Service de données TFTP

TFTP (Trivial File Transfer Protocol) est un protocole simplifié de 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.

Réseau de stockage

Dans un réseau de stockage (SAN), 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 - Utiliser le groupe d'initiateurs par défaut pourrait résulter dans des initiateurs LUN indésirables ou conflictuels.

Services d'annuaire

Cette section décrit les services d'annuaire qui peuvent être configurés sur l'appareil et leurs implications de sécurité.

NIS (Network Information Service)

NIS (Network Information Service) est un service de noms pour la gestion centralisée des répertoires. Oracle ZFS Storage Appliance peut se comporter comme un client NIS pour les utilisateurs et les groupes de telle manière que les utilisateurs NIS puissent se connecter à FTP et HTTP/WebDAV. Les utilisateurs NIS peuvent aussi recevoir des privilèges pour l'administration de l'appareil. L'appareil complète les informations NIS à l'aide de ses propres privilèges.

LDAP (Lightweight Directory Access Protocol)

Oracle ZFS Storage Appliance utilise le protocole LDAP (Lightweight Directory Access Protocol) pour authentifier les utilisateurs administratifs et certains utilisateurs de services de données (FTP, HTTP). La sécurité LDAP via SSL est prise en charge par l'appareil. 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.
- Met les noms en correspondance vers et depuis les utilisateurs et les groupes, pour les protocoles de données tels que NFSv4 qui utilisent les noms.
- Définit l'appartenance aux groupes à utiliser dans le contrôle d'accès.
- De manière facultative, authentifie 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 à Oracle ZFS Storage Appliance, l'appareil 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) :
  - Non sécurisé
  - Le serveur est authentifié à l'aide de Kerberos
  - 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 d'Oracle ZFS Storage Appliance via le protocole SMB ou NFS et chacun d'entre eux dispose d'un identifiant 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 l'appareil.

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.

Identity Management for UNIX

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 RFC 2307 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 plate-forme 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 d'Oracle ZFS Storage Appliance 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 Oracle ZFS Storage Appliance 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 Oracle ZFS Storage Appliance 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.

Service Kerberos

Le service Kerberos permet à l'appareil d'authentifier les utilisateurs qui se connectent en tant qu'administrateur et de leur accorder l'accès à des services tels que NFS, HTTP, FTP, SFTP et SSH dans le cadre d'un environnement Kerberos. L'utilisateur de l'appareil doit posséder un principal Kerberos du même nom pour accéder à ces services via l'authentification Kerberos. Il est également possible de recourir à Kerberos pour définir la sécurité des partages individuels qui utilisent le protocole NFS, comme indiqué dans la section "Options d'authentification et de chiffrement NFS" à la page 15.

Kerberos et Active Directory peuvent être actifs en même temps, car ils utilisent des domaines et des clés distincts. Lorsque les deux services sont actifs, le domaine Kerberos est la valeur par défaut. Lorsque seul Active Directory est actif, son domaine est la valeur par défaut.

Protocole de transport des messages simple

Le protocole SMTP (Simple Mail Transport Protocol) envoie tous les courriers générés par le système Oracle ZFS Storage Appliance, généralement en réponse aux alertes configurées. Le service SMTP n'accepte pas le courrier externe. Il envoie uniquement les messages générés automatiquement par l'appareil.

Par défaut, le service SMTP utilise DNS (enregistrements MX) pour déterminer la destination du courrier. Si DNS n'est pas configuré pour le domaine de l'appareil ou si les enregistrements

MX DNS ne sont pas définis correctement pour le domaine de destination du courrier sortant, l'appareil peut être configuré de façon à faire suivre tous les messages via un serveur de courrier sortant.

Protocole de gestion de réseau simple

Le protocole SNMP (Simple Network Management Protocol) fournit deux fonctions sur Oracle ZFS Storage Appliance : les informations de statut de l'appareil peuvent être gérées par SNMP et les alertes peuvent être configurées pour envoyer des déroutements SNMP. Les versions v1, v2c et v3 de SNMP sont disponibles lorsque le service est activé. L'appareil prend en charge un maximum de 128 interfaces réseau physiques et logiques.

Message Syslog

Un message Syslog est un petit message d'événement transmis depuis Oracle ZFS Storage Appliance sur un ou plusieurs systèmes distants. Syslog fournit deux fonctions d'appareil :

- La fonction Alertes peut être configurée de façon à envoyer des messages syslog à un ou plusieurs systèmes distants.
- Les messages syslog des services de l'appareil compatibles peuvent être 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 de l'appareil
- 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 le nom et l'emplacement du système si vous déplacez Oracle ZFS Storage Appliance 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 à Oracle ZFS Storage Appliance 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 appareil Oracle ZFS Storage Appliance 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.

Journaux de sécurisation

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

Journal d'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

Date/heure	Utilisateur	Hôte	Récapitulatif	Annotation de session
2013-10-12 05:20:24	root	galaxie	Service ftp désactivé	
2013-10-12 03:17:05	root	galaxie	Utilisateur connecté	
2013-10-11 22:38:56	root	galaxie	Session de navigateur expirée	
2013-10-11 21:13:35	root	<console>	Service ftp activé	

Journal du 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

Date/heure	Description	Résultat
2013-10-12 05:24:09	Fichier chargé 'cores/ak.45e5ddd1-ce92-c16e-b5eb-9cb2a8091f1c.tar.gz' sur le support Oracle	OK

En savoir plus

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

https://docs.oracle.com

Lorsque vous utilisez la BUI pour configurer un appareil Oracle ZFS Storage Appliance, vous pouvez cliquer sur le lien Aide en haut à droite d'un écran pour afficher l'aide de cet écran.