Présentation d'Oracle® Solaris Zones

Référence: E54009-02
Décembre 2014

ORACLE

Table des matières

Utilisation de la présente documentation

- **Présentation** : décrit la technologie des zones et les ressources disponibles dans la zone.
- **Public visé** : administrateurs système, techniciens et fournisseurs de services agréés.
- **Connaissances requises** : utilisation préalable du système d'exploitation Oracle Solaris, avec pratique de la configuration réseau et de l'allocation de ressources.

Bibliothèque de documentation produit

Les informations de dernière minute et les problèmes connus pour ce produit sont inclus dans la bibliothèque de documentation accessible à l'adresse : http://www.oracle.com/pls/topic/lookup?ctx=E56338.

Accès aux services de support Oracle

Les clients Oracle 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.

Commentaires en retour

Faites part de vos commentaires sur cette documentation à la page suivante : http://www.oracle.com/goto/docfeedback.

♦ ♦ ♦ CHAPITRE 1

Présentation d'Oracle Solaris Zones

L'utilitaire Oracle™ Solaris Zones du système d'exploitation Oracle Solaris permet de disposer d'un environnement isolé pour y exécuter des applications sur le système.

Ce chapitre propose une vue d'ensemble des zones.

Il couvre également les rubriques générales suivantes :

Le chapitre suivant traite des ressources et des propriétés de configuration des zones.

Pour passer directement à la création de zones sur votre système, reportez-vous aux documents “ Création et utilisation des zones de noyau d’Oracle Solaris ” et “ Création et utilisation d’Oracle Solaris Zones ”. Pour passer directement à la migration d'un système exécutant Oracle Solaris 10, ce qui peut inclure des zones `native` non globales, vers des zones d'un système Oracle Solaris 11, reportez-vous au document “ Création et utilisation des zones Oracle Solaris 10 ”.

Remarque - Pour plus d'informations sur l'utilisation des zones dans un système Oracle Solaris Trusted Extensions, reportez-vous au Chapitre 13, “ Gestion des zones dans TrustedÂ Extensions ” du manuel “ Configuration et administration de Trusted Extensions ”.

Présentation des zones

La technologie de partitionnement Oracle Solaris Zones est utilisée pour virtualiser les services du système d'exploitation et fournir un environnement isolé et sécurisé pour l'exécution des applications. La zone non globale, appelée *zone*, est un environnement de système d'exploitation virtualisé, créé au sein d'une instance unique du système d'exploitation Oracle Solaris. L'instance du système d'exploitation est appelée la zone globale. La zone de noyau Oracle Solaris peut exécuter une mise à jour du référentiel support (SRU) ou une version de noyau différente de celle de l'hôte.

L'objectif de la virtualisation est de passer de la gestion de composants de centres de données individuels à la gestion de pools de ressources. Une virtualisation de serveur réussie permet d'améliorer l'utilisation du serveur et de ses ressources. La virtualisation de serveur permet également de garantir le succès des projets de consolidation de serveur gérant chacun des systèmes distants.

La virtualisation est encouragée par la nécessité de consolider plusieurs hôtes et services sur une seule machine. La virtualisation permet de réduire les coûts grâce au partage du matériel, des infrastructures et des tâches d'administration. Principaux avantages :

- Augmentation du taux d'utilisation des ressources matérielles
- Plus grande souplesse dans l'allocation des ressources
- Diminution des besoins en alimentation
- Réduction des coûts de gestion
- Baisse du coût de possession
- Limites de ressources et d'administration d'une application à l'autre sur un système

En créant une zone, vous créez un environnement d'exécution d'applications dans lequel les processus sont isolés du reste du système. Cela empêche les processus exécutés dans une zone de surveiller ou d'affecter les processus exécutés dans d'autres zones. Ainsi, même un processus exécuté avec les informations d'identification root ne peut affecter l'activité des autres zones. Oracle Solaris Zones permet de conserver le modèle de déploiement d'une application par serveur, tout en partageant les ressources matérielles.

Toute zone fournit également une couche abstraite qui sépare les applications des attributs physiques de la machine sur laquelle elles sont déployées, par exemple les chemins d'accès aux périphériques physiques.

L'utilitaire Zones peut être utilisé sur toute machine équipée d'Oracle Solaris 10 ou Oracle Solaris 11. La nombre maximum de zones `solaris` et `solaris10` sur un système est de 8 192. Le nombre de zones pouvant être hébergées sur un même système est déterminé par les besoins en ressources totaux de l'application exécutée sur toutes les zones et par la taille du système. Ces concepts sont traités au Chapitre 1, “ Planification et configuration de zones non globales ” du manuel “ Création et utilisation d’Oracle Solaris Zones ”.

Pour plus d'informations sur ces concepts si vous exécutez Oracle Solaris Kernel Zones, reportez-vous à la section " Configuration matérielle et logicielle pour les zones de noyau Oracle Solaris " du manuel " Création et utilisation des zones de noyau d'Oracle Solaris ".

Zones prises en charge dans cette édition

Les zones de marque `solaris` et `solaris10` non globales exécutées à l'aide d'une seule zone globale hôte sont prises en charges sur toutes les architectures définies par Oracle Solaris 11.2 en tant que plates-formes prises en charge.

Oracle Solaris Kernel Zones peut s'exécuter sur des machines SPARC T4+ et M5+, des machines Intel Nehalem+ et des machines AMD Barcelona+. Pour plus d'informations sur la configuration système requise pour les zones de noyau, reportez-vous à la section " Configuration matérielle et logicielle pour les zones de noyau Oracle Solaris " du manuel " Création et utilisation des zones de noyau d'Oracle Solaris ".

Zones immuables

Les zones immuables sont des zones `solaris` dotées de roots en lecture seule. Les zones globales et les zones non globales peuvent être des zones immuables. Une zone en lecture seule peut être configurée en définissant la propriété `file-mac-profile`. Plusieurs configurations sont possibles. Un root de zone en lecture seule étend la limite d'exécution sécurisée.

Les zones globales immuables Oracle Solaris ont étendu la fonctionnalité des zones immuables à la zone globale. Dans le cas des zones immuables et des zones de noyau immuables, la connexion Trusted Path peut être appelée via la commande `zlogin` `zlogin`(1).

Les zones recevant des jeux de données supplémentaires via `zonecfg add dataset` conservent un contrôle total sur ces jeux. Les zones recevant des systèmes de fichiers supplémentaires via `zonecfg add fs` les contrôlent totalement, excepté si ces systèmes de fichiers sont en lecture seule.

Pour plus d'informations, reportez-vous au Chapitre 12, " Configuration et administration de zones immuables " du manuel " Création et utilisation d'Oracle Solaris Zones ".

A propos de la conversion de zones `ipkg` en zones `solaris`

Dans le cadre de la prise en charge des clients Oracle Solaris 11 Express, toute zone configurée en tant que zone `ipkg` est convertie en tant que zone `solaris` et signalée comme étant `solaris` sur mise à jour `pkg` ou `zoneadm attach` à Oracle Solaris 11.2. Le nom `ipkg` est mappé sur le

nom `solaris`, le cas échéant, lors de la configuration des zones. L'importation d'un fichier `zonecfg` exporté depuis un hôte Oracle Solaris 11 Express est prise en charge.

La sortie de commandes telles que `zonecfg info` ou `zoneadm list -v` affiche une marque de `solaris` pour les zones par défaut, dans un système Oracle Solaris 11.2.

Marques de zone dans cette édition

Oracle Solaris Kernel Zones

La fonctionnalité Oracle Solaris Kernel Zones fournit un environnement complet de noyau et d'utilisateur dans une même zone et augmente la séparation du noyau entre l'hôte et la zone. Le nom de la marque est `solaris-kz`. Les zones de noyau sont gérées depuis la zone globale en utilisant les outils existants `zonecfg`, `zoneadm` et `zlogin`. En tant qu'administrateur d'une zone de noyau, vous disposez d'une plus grande marge de manoeuvre dans la configuration et la gestion de la zone qu'un administrateur de zone `solaris` par défaut. Par exemple, vous pouvez mettre à jour et modifier les packages installés de la zone dans leur intégralité, y compris la version du noyau, sans vous limiter aux packages installés dans la zone globale. Vous pouvez gérer le stockage réservé à la zone, créer et détruire les pools ZFS, et configurer iSCSI et CIFS. Vous pouvez installer les zones `solaris` dans la zone de noyau pour produire des zones hiérarchiques (imbriquées). Les zones de noyau prennent en charge la suspension et la reprise. Vous pouvez migrer une zone de noyau en exécutant une opération de suspension de la zone sur la machine source, puis une opération de reprise de la zone sur la machine cible.

Pour utiliser Oracle Solaris Kernel Zones, vous devez installer le package `brand-solaris-kz` sur votre système. Pour déterminer si votre machine prend en charge les zones de noyau, reportez-vous à la section “A propos d'Oracle Solaris Zones dans cette version” à la page 27. Vous pouvez également exécuter la commande `virtinfo` sur votre machine si Oracle Solaris 11.2 est installé. Pour plus d'informations sur Oracle Solaris Kernel Zones, reportez-vous au document “ Création et utilisation des zones de noyau d’Oracle Solaris ” et à la page de manuel `solaris-kz`(5). Pour plus d'informations sur la commande `virtinfo`, reportez-vous à la section “ Vérification de la prise en charge des zones de noyau sur un hôte ” du manuel “ Création et utilisation des zones de noyau d’Oracle Solaris ” et à la page de manuel `virtinfo`(1M).

Oracle Solaris Zones par défaut

La fonctionnalité Oracle Solaris Zones est un environnement d'exécution complet pour les applications. Une zone offre un mappage virtuel entre l'application et les ressources de la plate-forme. Les zones permettent d'isoler les composants de l'application même si elles partagent

une même instance du système d'exploitation Oracle Solaris. Les zones utilisent des composants de gestion des ressources pour contrôler la façon dont les applications utilisent les ressources système disponibles. Pour plus d'informations sur les fonctionnalités de gestion des ressources, reportez-vous au document " Administration de la gestion des ressources dans Oracle Solaris 11.2 ".

La zone définit les limites de consommation des ressources, comme le temps d'occupation de la CPU, par exemple. Vous pouvez étendre ces limites afin de répondre aux différentes demandes de traitement de l'application s'exécutant dans la zone.

Pour obtenir un niveau d'isolement supplémentaire, il est possible de configurer les zones avec un root en lecture seule (appelées zones immuables).

Oracle Solaris 10 Zones

Les zones Oracle Solaris 10 Zones, également appelées zones non globales marquées `solaris10`, utilisent la technologie BrandZ pour exécuter les applications Oracle Solaris 10 sur le système d'exploitation Oracle Solaris 11. Les applications s'exécutent sans modification dans l'environnement sécurisé fourni par la zone non globale. Cela permet d'utiliser le système Oracle Solaris 10 dans le but de développer, tester et déployer des applications. Les charges de travail en cours d'exécution à l'intérieur de ces zones marquées peuvent tirer parti des améliorations apportées au noyau et utiliser certaines des technologies novatrices disponibles uniquement dans la version Oracle Solaris 11. Ces zones servent à migrer les systèmes Oracle Solaris 10 vers des zones s'exécutant sous Solaris 11. Une zone marquée `solaris10` ne peut pas être un serveur NFS.

Pour plus d'informations, reportez-vous au document " Création et utilisation des zones Oracle Solaris 10 ".

Présentation des marques de zones

Les différences entre les zones `solaris-kz` et les zones marquées `solaris` et `solaris10` sont décrites ci-dessous.

TABLEAU 1-1 Comparaison des fonctionnalités de marque Oracle Solaris Zone

Composant	Marque `solaris-kz`	Marques `solaris`and `solaris10`
Matériel compatible	Prise en charge sur le matériel spécifié. Voir le lien renvoyant au site OTN ou à la liste HCL.	Prise en charge sur tous les systèmes Oracle Solaris 11.2. Voir la liste HCL.
Gestion de la mémoire	Une quantité fixe de RAM physique doit être allouée à la plate-forme virtuelle `solaris-kz`.	Peuvent partager la RAM physique allouée à la zone globale.

Composant	Marque `solaris-kz`	Marques `solaris`and `solaris10`
Version de noyau	Une zone de noyau peut exécuter une version de noyau ou un niveau SRU différent que ceux de l'hôte.	La version de noyau doit être identique à celle de la zone globale.
Gestion du stockage et des périphériques	Réalise tous les accès au stockage. Les zones de noyau ne prennent pas en charge les ressources `zpool` ou `rootzpool`.	Le stockage peut être rendu disponible au niveau du système de fichiers via les ressources `fs`, `zpool` et `dataset` `zonecfg`.
Gestion de réseau	Seules les zones en mode IP exclusif sont prises en charge.	Les zones en mode IP exclusif et en mode IP partagé sont prises en charge.

Utilisation d'Oracle Solaris Zones sur un système Oracle Solaris Trusted Extensions

Pour plus d'informations sur l'utilisation des zones dans un système Oracle Solaris Trusted Extensions, reportez-vous au Chapitre 13, “ Gestion des zones dans TrustedÂ Extensions ” du manuel “ Configuration et administration de Trusted Extensions ”. Notez que seule la marque `labeled` peut être initialisée sur un système Oracle Solaris Trusted Extensions.

Clusters de zones Oracle Solaris Cluster

Les clusters de zones sont une fonction du logiciel Oracle Solaris Cluster. Un cluster de zones est un groupe de zones non globales qui servent de noeuds pour le cluster de zones. Une zone non globale est créée sur chaque noeud du cluster global configuré avec le cluster de zones. Les noeuds d'un cluster de zones peuvent être de la marque `solaris` ou `solaris10`, et utiliser l'attribut de cluster. Aucun autre type de marque n'est autorisé. Vous pouvez exécuter les services pris en charge sur le cluster de zones de la même façon que sur un cluster global, avec l'isolement qui est fourni par zones. Pour plus d'informations, reportez-vous au “ Guide d’administration système d’Oracle Solaris Cluster ”.

A propos des zones marquées

Par défaut, dans un système, une zone non globale exécute le même logiciel de système d'exploitation que la zone globale. La fonction de zones marquées (BrandZ) du système d'exploitation Oracle Solaris est une simple extension d'Oracle Solaris Zones. La structure BrandZ est utilisée pour créer des zones marquées non globales contenant des environnements d'exploitation différents de ceux de la zone globale. Les zones marquées sont utilisées dans le système d'exploitation Solaris pour exécuter des applications. La structure BrandZ étend l'infrastructure Oracle Solaris Zones de différentes façons. Ces extensions peuvent être complexes, par exemple en offrant la possibilité d'exécuter différents environnements de système d'exploitation au sein de la zone, ou simples, par exemple en améliorant

les commandes de zone de base pour offrir de nouvelles fonctionnalités. Par exemple, Oracle Solaris 10 Zones sont des zones marquées non globales capables d'émuler le système d'exploitation Oracle Solaris 10. Les zones par défaut partageant le même système d'exploitation que celui de la zone globale sont également configurées avec une *marque*.

La marque définit l'environnement d'exploitation qu'il est possible d'installer dans la zone et détermine le comportement du système au sein de la zone, afin que le logiciel installé dans cette zone fonctionne correctement. En outre, une marque de zone identifie le type correct d'application au lancement de celle-ci. La gestion de l'ensemble des zones marquées est assurée par le biais d'extensions de la structure de zones standard. La plupart des procédures d'administration sont identiques à toutes les zones.

Les ressources incluses dans la configuration par défaut, telles que les systèmes de fichiers et les privilèges définis, sont présentées dans la documentation de la marque.

La zone marquée étend les outils de zone de la manière suivante :

- La commande `zonecfg` définit le type de marque d'une zone lors de la configuration de cette dernière.
- La commande `zoneadm` signale le type de marque d'une zone et gère cette dernière.

Bien que vous puissiez configurer et installer des zones marquées sur un système Oracle Solaris Trusted Extensions possédant des étiquettes activées, vous ne pouvez pas initialiser de zones marquées dans cette configuration système, *excepté si* la marque initialisée est la marque `avec étiquette` d'une configuration système certifiée.

Vous pouvez modifier la marque d'une zone lors de la *configuration*. Une fois la zone marquée *installée*, la marque ne peut être ni modifiée ni supprimée.

Attention - Si vous prévoyez de migrer votre système Oracle Solaris 10 existant vers une zone marquée `solaris10` située dans un système fonctionnant sous Oracle Solaris 11, vous devez tout d'abord migrer les zones existantes vers le système cible. Les zones `solaris10` ne pouvant pas s'imbriquer, le processus de migration du système rend les zones existantes inutilisables. Pour plus d'informations, reportez-vous au Chapitre 3, “ Migration d’une zone non globale native Oracle Solaris 10 vers une zone Oracle Solaris 10 ” du manuel “ Création et utilisation des zones Oracle Solaris 10 ”.

Exécution de processus dans une zone marquée

Une zone marquée présente un ensemble de points d'interposition au sein du noyau qui s'appliquent uniquement aux processus exécutés dans la zone.

- Ces points résident dans les chemins : chemin `syscall`, chemin de chargement de processus et chemin de création de thread, notamment.

- A chacun de ces points, une marque peut choisir de compléter ou de remplacer le comportement Oracle Solaris Standard.

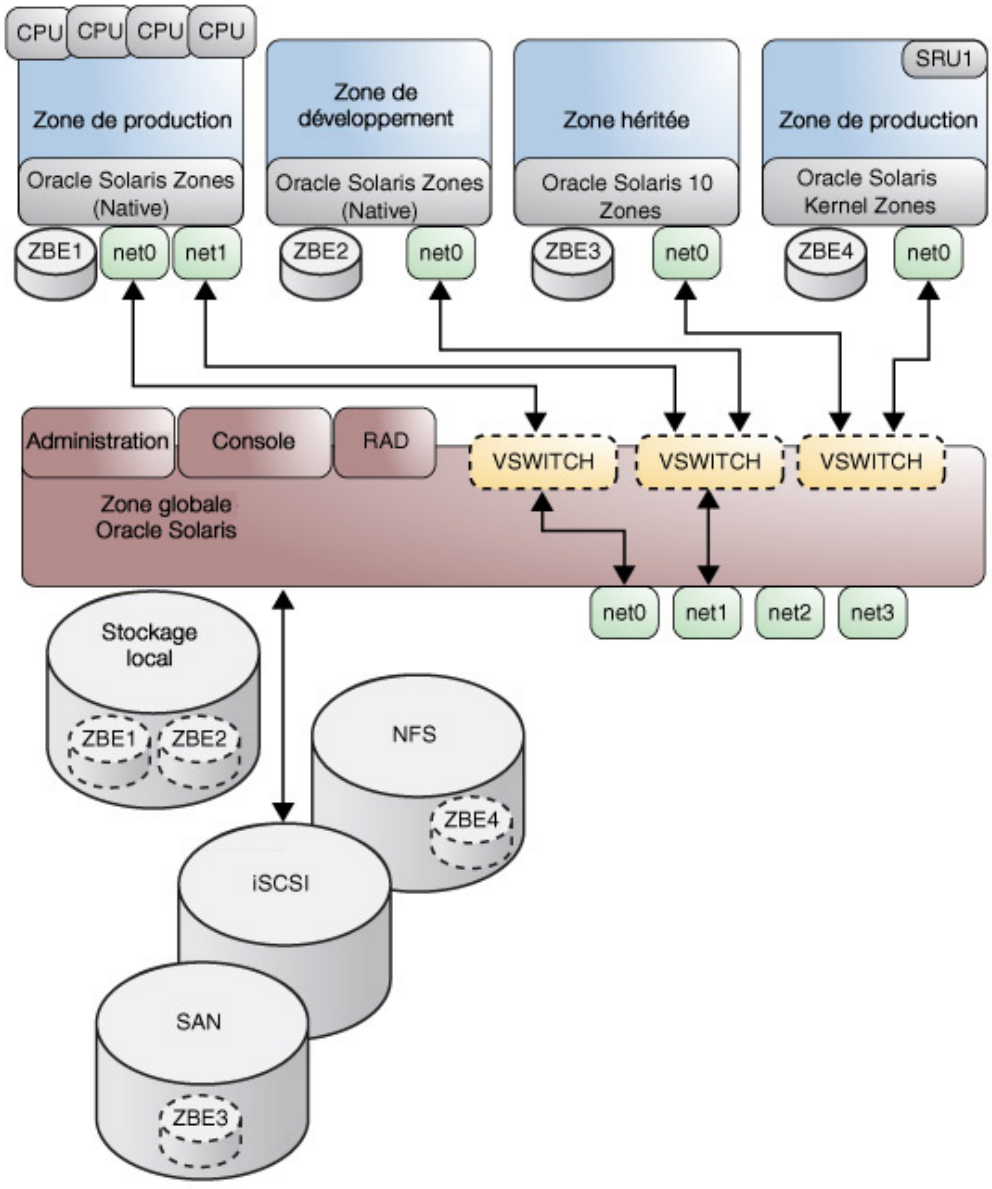
Une marque peut également fournir une bibliothèque de plug-ins pour `librtld_db`. Grâce à celle-ci, les outils Oracle Solaris tels que le débogueur, décrit à la page de manuel `mdb`(1), et DTrace, décrit dans `dtrace`(1M), peuvent accéder aux informations de symbole des processus exécutés dans une zone marquée.

Notez que les zones ne prennent pas en charge les fichiers binaires liés statiquement.

Intérêt des zones

Les zones sont idéales pour les environnements consolidant plusieurs applications sur un serveur unique. La gestion de plusieurs machines pouvant s'avérer coûteuse et complexe, il est intéressant de consolider plusieurs applications sur de gros serveurs, plus évolutifs.

FIGURE 1-1 Exemple de consolidation de serveurs de zones



Les zones permettent d'utiliser plus efficacement les ressources du système. La réallocation dynamique permet de déplacer les ressources non utilisées vers d'autres zones, suivant les

besoins. L'isolement des erreurs et des violations de la sécurité évite par ailleurs d'avoir recours à un système dédié, et donc sous-utilisé, pour les applications à risques. Grâce aux zones, vous pouvez les consolider avec d'autres applications.

Les zones permettent également de déléguer certaines fonctions administratives pendant la maintenance de l'ensemble de la sécurité du système.

Fonctionnement des zones

Une zone non globale peut être considérée comme une boîte dans laquelle vous pouvez exécuter une ou plusieurs applications sans interférer avec le reste du système. Les zones isolent les applications et les services à l'aide de limites flexibles, définies à l'échelle logicielle. Les applications exécutées dans une même instance du système d'exploitation Oracle Solaris peuvent être gérées indépendamment les unes des autres. Vous pouvez donc exécuter différentes versions d'une même application dans différentes zones, en fonction des exigences de la configuration.

Tout processus assigné à une zone peut manipuler, surveiller et communiquer directement avec les autres processus assignés à cette même zone. Cela est toutefois impossible si ces processus sont assignés à d'autres zones du système ou ne sont assignés à aucune zone. Les processus assignés à différentes zones peuvent uniquement communiquer via les API du réseau.

Le réseau IP peut être configuré de deux façons, selon que la zone possède sa propre instance IP ou partage l'état et la configuration de la couche IP avec la zone globale. Le mode IP exclusif est le type par défaut. Pour plus d'informations sur les types d'IP dans les zones, reportez-vous à la section “Interfaces réseau de zones” à la page 43. Pour en savoir plus sur la configuration, reportez-vous à la section “ Configuration d’une zone ” du manuel “ Création et utilisation d’Oracle Solaris Zones ”.

Chaque système Oracle Solaris contient une *zone globale*. La zone globale a deux fonctions principales. La zone globale est à la fois la zone par défaut pour le système et la zone utilisée pour le contrôle administratif au niveau du système. Tous les processus sont exécutés dans la zone globale si aucune zone *non globale* (appelée simplement "zone") n'est créée par l'*administrateur global* ou par un utilisateur à l'aide du profil Sécurité de zone.

C'est la seule zone à partir de laquelle il est possible de configurer, d'installer, de gérer ou de désinstaller une zone non globale. Seule la zone globale peut être initialisée à partir du matériel système. L'administration de l'infrastructure du système, notamment les périphériques physiques, le routage dans une zone en mode IP partagé et la reconfiguration dynamique, n'est réalisable qu'à partir de la zone globale s'exécutant sur un système physique. Les processus auxquels sont affectés les privilèges adéquats et s'exécutant dans la zone globale peuvent accéder à des objets associés à d'autres zones.

Dans certains cas, les processus ne disposant pas de privilèges dans une zone globale peuvent exécuter des opérations non permises aux processus dotés de privilèges dans une zone non globale. Par exemple, les utilisateurs travaillant dans la zone globale peuvent consulter les

informations relatives à tous les processus existant sur le système. Si cette capacité pose un problème pour votre site, vous pouvez limiter l'accès à la zone globale.

Chaque zone, y compris la zone globale, se voit assigner un nom. Celui de la zone globale est toujours `global`. Chaque zone possède également un identificateur numérique unique, qui lui est assigné par le système lors de son initialisation. L'ID de la zone globale est toujours `0`. Si vous établissez une connexion `zlogin` avec une zone de noyau, l'ID reste 0 car il s'agit d'une zone globale virtuelle. Vous trouverez des explications détaillées sur les noms et les ID de zones à la section " Configuration d'une zone " du manuel " Création et utilisation d'Oracle Solaris Zones ".

Chaque zone possède aussi un nom de noeud, indépendant du nom de zone et assigné par l'administrateur de la zone. Pour plus d'informations, reportez-vous à la section " Nom de noeud dans une zone non globale " du manuel " Création et utilisation d'Oracle Solaris Zones ".

Le chemin du répertoire root de chaque zone est lié au répertoire root de la zone globale. Pour plus d'informations, reportez-vous à la section "Utilisation de la commande `zonecfg`" à la page 57.

La classe de programmation des zones non globales est définie sur celle du système par défaut. Pour une explication détaillée des méthodes utilisées pour définir la classe de programmation dans une zone, reportez-vous à la section "Classe de programmation" à la page 39.

Le multipathing de périphérique en mode bloc est géré par `scsi_vhci`(7D). Le format de l'URI `lu: storage` que vous choisissez pour votre configuration détermine les modalités d'utilisation de la configuration. Pour plus d'informations sur l'utilisation des URI `lu:` avec le multipathing, reportez-vous à la page de manuel `suri`(5).

Présentation des zones par fonction

Vous trouverez dans le tableau ci-dessous un résumé des caractéristiques des zones globales et non globales.

Type de zone	Caractéristique
Globale	■ Se voit assigner l'ID `0` par le système ■ Fournit la seule instance du noyau Oracle Solaris pouvant être initialisée et exécutée sur le système ■ Contient une installation complète des packages des logiciels système Oracle Solaris ■ Peut contenir des packages logiciels ou des logiciels supplémentaires, des répertoires, des fichiers et d'autres données non installées par l'intermédiaire de packages ■ Fournit une base de données de produits complète et cohérente contenant les informations relatives à tous les composants logiciels installés dans la zone globale

Type de zone	Caractéristique
Non globale	■ Détient les informations de configuration spécifiques à la zone globale uniquement, par exemple le nom d'hôte de la zone globale et la table du système de fichiers ■ Est la seule zone ayant connaissance de tous les périphériques et systèmes de fichiers ■ Est la seule zone ayant connaissance de l'existence et de la configuration d'une zone non globale ■ Est la seule zone à partir de laquelle il est possible de configurer, d'installer, de gérer ou de désinstaller une zone non globale
	■ Se voit assigner un ID de zone lors de son initialisation (ID assigné par le système) ■ Partage les opérations du noyau Oracle Solaris initialisé à partir de la zone globale ■ Contient un sous-ensemble installé de tous les packages des logiciels système Oracle Solaris ■ Peut contenir les packages logiciels supplémentaires installés ■ Peut contenir d'autres logiciels, répertoires, fichiers et données créés dans la zone non globale et non installés par l'intermédiaire de packages ■ Dispose d'une base de données de produits complète et cohérente, contenant les informations relatives à tous les composants logiciels installés dans la zone ■ N'a pas connaissance de l'existence d'autres zones ■ Ne peut ni installer, ni gérer, ni désinstaller des zones, y compris elle-même ■ Détient des informations de configuration spécifiques à cette zone non globale uniquement, par exemple le nom d'hôte de la zone non globale et la table du système de fichiers ■ Peut posséder son propre paramètre de fuseau horaire

Administration de zones non globales

L'administrateur global possède des privilèges de superutilisateur ou des droits d'administration équivalents. Lorsqu'il est connecté à une zone globale, l'administrateur global peut surveiller le système comme un tout.

Les zones non globales peuvent être administrées par un *administrateur de zone*. L'administrateur global attribue à l'administrateur de zone les autorisations nécessaires, telles que décrites dans la section “Ressource `admin`” à la page 36. Les privilèges d'un administrateur de zone sont limités à une zone non globale donnée.

Création de zones non globales

Vous pouvez définir la configuration et l'installation de zones non globales dans le cadre d'une installation client automatisée (AI). Reportez-vous au manuel “ Installation des systèmes Oracle Solaris 11.2 ” pour plus d'informations. Les zones de noyau Oracle Solaris sont créées principalement selon la méthode d'installation directe. Les méthodes de création de zone de noyau sont documentées à la section “ Installation d’une zone de noyau ” du manuel “ Création et utilisation des zones de noyau d’Oracle Solaris ”.

Pour créer une zone dans un système Oracle Solaris, l'administrateur global utilise la commande `zonecfg` afin de configurer la zone souhaitée en spécifiant divers paramètres pour l'environnement d'application et la plate-forme virtuelle de la zone. Il utilise ensuite la commande d'administration de zone `zoneadm` pour installer les logiciels au niveau du package dans l'arborescence de système de fichiers définie pour la zone. La commande `zoneadm` permet d'initialiser la zone. L'administrateur global ou l'utilisateur autorisé peut se connecter à la zone installée à l'aide de la commande `zlogin`. Dans le cas d'un contrôle d'accès basé sur les rôles (RBAC, Role-Based Access Control), l'administrateur de zone doit avoir l'autorisation `solaris.zone.manage/`*zonename*.

Pour plus d'informations sur la configuration des zones, reportez-vous au Chapitre 2, Présentation de la configuration des zones non globales. Pour plus de détails sur l'installation des zones, reportez-vous au Chapitre 2, “ A propos de l’installation, de la fermeture, de l’arrêt, de la désinstallation et du clonage des zones non globales ” du manuel “ Création et utilisation d’Oracle Solaris Zones ”. Pour plus d'informations sur la connexion aux zones, reportez-vous au Chapitre 4, “ A propos de la connexion à une zone non globale ” du manuel “ Création et utilisation d’Oracle Solaris Zones ”.

Pour configurer et installer Oracle Solaris Kernel Zones, reportez-vous au document “ Création et utilisation des zones de noyau d’Oracle Solaris ”.

Etats des zones non globales

Une zone non globale peut se trouver dans l'un des sept états suivants :

Configuré
: La configuration de la zone est terminée et validée sur unité de stockage stable. Cependant, les éléments devant être spécifiés après l'initialisation initiale de l'environnement applicatif de la zone ne sont pas encore présents.

Incomplet
: Pendant l'installation ou la désinstallation, la commande `zoneadm` définit l'état de la zone cible sur Incomplet. Une fois l'opération correctement effectuée, l'état est défini sur l'état correct.

  Une zone installée endommagée peut être marquée comme étant incomplète à l'aide de la sous-commande `mark` de `zoneadm`. Les zones à l'état incomplet s'affichent dans la sortie de `zoneadm list -iv`.

Indisponible
: Indique que la zone a été installée mais qu'elle ne peut pas être vérifiée, rendue prête, initialisée, rattachée ou déplacée. Une zone saisit l'état indisponible dans les cas suivants :

  - Lorsque le stockage de la zone est indisponible et que `svc:/system/zones:default` démarre, par exemple, pendant l'initialisation du système.

- Lorsque l'espace de stockage de la zone est indisponible
- Lorsque les installations basées sur l'archivage échouent après la réussite de l'extraction de l'archive
- Lorsque le logiciel de la zone est incompatible avec le logiciel de la zone globale, tel qu'après un rattachement forcé incorrect à l'aide de l'option `-F`

Installé	La configuration de la zone est instanciée sur le système. La commande `zoneadm` permet de vérifier que la configuration peut être utilisée sans problème avec le système Oracle Solaris désigné. Les packages sont installés sous le chemin root de la zone. Dans cet état, la zone n'a pas de plate-forme virtuelle associée.
Prêt	La plate-forme virtuelle de la zone est établie. Le noyau crée le processus `zsched` ; les interfaces réseau sont paramétrées et disponibles pour la zone ; les systèmes de fichiers sont montés et les périphériques configurés. Un ID de zone unique est attribué par le système. A ce stade, aucun processus associé à la zone n'a été démarré.
En cours d'exécution	Les processus utilisateur associés à l'environnement d'application de la zone sont en cours d'exécution. La zone passe à l'état En cours d'exécution dès que le premier processus utilisateur associé à l'environnement applicatif (`init`) est créé.
Arrêt en cours et hors service	Ces états sont des états transitoires qui sont visibles pendant l'arrêt de la zone. Cependant, une zone incapable de s'arrêter pour quelque raison que ce soit s'arrêtera dans l'un de ces états.

Le Chapitre 3, “ Installation, initialisation, fermeture, arrêt, désinstallation et clonage des zones non globales ” du manuel “ Création et utilisation d’Oracle Solaris Zones ” et la page de manuel `zoneadm`(1M) indiquent comment utiliser la commande `zoneadm` pour déclencher les transitions entre ces états.

En outre, les zones de noyau Oracle Solaris possèdent trois *états auxiliaires* permettant de transmettre à l'hôte des informations supplémentaires sur l'état actuel de la zone.

Suspendu	L'état principal est "arrêté", avec un état auxiliaire "suspendu".
Débogage	La zone est en cours d'exécution, mais ne peut pas répondre aux événements extérieurs, comme ceux liés au réseau. La commande `zlogin` vérifie si cet état est actif et attend qu'il soit inactif avant de lancer une session `zlogin`.
Erreur grave	La zone a subi une erreur grave et ne pourra plus répondre aux événements extérieurs jusqu'à son redémarrage.

Pour plus d'informations, reportez-vous au document " Création et utilisation des zones de noyau d'Oracle Solaris " et à la page de manuel `solaris-kz`(5).

TABLEAU 1-2 Commandes affectant l'état des zones

Etat actuel de la zone	Commandes pertinentes

Configuré	`zonecfg -z` *zonename* `verify`
	
	`zonecfg -z` *zonename* `commit`
	
	`zonecfg -z` *zonename* `delete`
	
	`zoneadm -z` *zonename* `attach`
	
	`zoneadm -z` *zonename* `verify`
	
	`zoneadm -z` *zonename* `install`
	
	`zoneadm -z` *zonename* `clone`
	
	`zoneadm -z` *zonename* `mark` *incomplete*
	
	`zoneadm -z` *zonename* `mark` *unavailable*
	
	Vous pouvez utiliser la commande `zonecfg` pour renommer une zone en état Configuré. Notez que vous pouvez utiliser la commande `zoneadm` pour renommer une zone Oracle Solaris ou Oracle Solaris 10 en état Configuré ou Installé.

Incomplet	`zoneadm -z` *zonename* `uninstall`
Indisponible	La commande `zoneadm -z` *zonename* `uninstall` désinstalle la zone du système spécifié. `zoneadm -z` *zonename* `attach` La commande `zonecfg -z` *zonename* peut être utilisée pour modifier `zonepath` et toute autre propriété ou ressource pouvant être modifiée lorsque l'état est Installé.

Installé	`zoneadm -z` *zonename* `ready` (facultatif)
	
	`zoneadm -z` *zonename* `boot`
	
	La commande `zoneadm -z` *zonename* `uninstall` désinstalle la configuration de la zone spécifiée du système.
	
	`zoneadm -z` *zonename* `move` *path*
	
	`zoneadm -z` *zonename* `detach`
	
	La commande `zonecfg -z` *zonename* permet d'ajouter ou de supprimer une propriété `attr`, `bootargs`, `capped-memory`, `dataset`, `capped-cpu`, `dedicated-cpu`, `device`, `fs`, `ip-type`, `limitpriv`, `net`, `rctl` ou `scheduling-class`. Vous pouvez également renommer une zone.
	
	Vous pouvez utiliser la commande `zoneadm` pour renommer une zone Oracle Solaris ou Oracle Solaris 10 en état Configuré ou Installé.
	
	`zoneadm -z` *zonename* `mark` *incomplete*

Etat actuel de la zone	Commandes pertinentes
	`zoneadm -z` *zonename* `mark` *unavailable*
Prêt	`zoneadm -z` *zonename* `boot` `zoneadm halt` et la réinitialisation du système passent les zones prêtes à l'état Installé. La commande `zonecfg -z` *zonename* permet d'ajouter ou de supprimer une propriété `attr`, `bootargs`, `capped-memory`, `dataset`, `capped-cpu`, `dedicated-cpu`, `device`, `fs`, `ip-type`, `limitpriv`, `net`, `rctl` ou `scheduling-class`.

En cours d'exécution	`zlogin` *options* `zonename`
	
	`zoneadm -z` *zonename* `reboot`
	
	La commande `zoneadm -z`*zonename* `halt` définit les zones prêtes sur l'état Installé.
	
	`zoneadm halt` et la réinitialisation du système redéfinissent les zones en cours d'exécution sur l'état Installé.
	
	`zoneadm - z shutdown` permet d'arrêter correctement la zone.
	
	La commande `zonecfg -z` *zonename* permet d'ajouter ou de supprimer une propriété `attr`, `bootargs`, `capped-memory`, `dataset`, `capped-cpu`, `dedicated-cpu`, `device`, `fs`, `ip-type`, `limitpriv`, `anet`, `net`, `rctl` ou `scheduling-class`. La ressource `zonepath` ne peut pas être modifiée.

Remarque - Les paramètres modifiés par la commande `zonecfg` n'ont aucune incidence sur les zones en cours d'exécution. La zone doit être réinitialisée pour que les changements soient effectifs.

Caractéristiques des zones non globales

L'isolement assuré par les zones peut porter sur presque tous les niveaux de granularité souhaités. Une zone peut fonctionner sans CPU dédiée, périphérique physique ou toute autre partie de la mémoire physique. Ces ressources peuvent soit être multiplexées sur un certain nombre de zones en cours d'exécution au sein d'un domaine ou d'un système unique, soit être allouées zone par zone grâce aux fonctions de gestion de ressources disponibles sur le système d'exploitation.

Chaque zone fournit un ensemble personnalisé de services. Pour renforcer l'isolement des processus, il est possible de faire en sorte que seuls les processus existants d'une même zone soient détectés ou signalés. La communication entre les zones s'effectue en dotant chaque zone d'une connectivité réseau IP. Une application s'exécutant dans une zone ne peut observer le trafic réseau d'une autre zone. L'isolement est garanti même si les flux de paquets respectifs transitent par la même interface physique.

Une partie de l'arborescence du système de fichiers est attribuée à chacune des zones. Chaque zone étant confinée à sa subdivision de l'arborescence du système de fichiers, la charge s'exécutant dans une zone particulière ne peut accéder aux données sur disque d'une charge s'exécutant dans une autre zone.

Les fichiers utilisés par des services de noms résident dans la vue du système de fichiers root d'une zone. Les services de noms des différentes zones sont ainsi isolés les uns des autres et les services peuvent être configurés différemment.

Utilisation des fonctions de gestion de ressources avec les zones non globales

Si vous utilisez des fonctions de gestion de ressources, vous devez aligner les limites des contrôles de gestion de ressources sur celles des zones. Cet alignement crée un modèle de machine virtuelle plus complet, dans lequel l'accès aux espaces de noms, l'isolement de sécurité et l'utilisation des ressources sont contrôlés.

Les exigences particulières relatives à l'utilisation des fonctions de gestion de ressources avec des zones sont traitées individuellement dans les chapitres consacrés à ces fonctions.

Services SMF liés aux zones

Les services SMF liés aux zones dans la zone globale incluent notamment :

`svc:/system/zones:default`	Démarre chaque zone où `autoboot=true`.
`svc:/system/zones-install:default`	Effectue l'installation de zones à la première initialisation, si nécessaire.
`svc:/application/pkg/zones-proxyd:default`	Utilisé par le système d'empaquetage pour fournir des accès aux zones vers le référentiel du système.
`svc:/application/pkg/system-repository:default`	Serveur de proxy mettant en cache les données `pkg` et les métadonnées utilisées durant l'installation de la zone et les autres opérations `pkg`. Reportez-vous aux pages de manuel `pkg`(1) et `pkg`(5).
`svc:/system/zones-monitoring:default`	Contrôle `zonestatd`.

Le service SMF du client du proxy des zones `svc:/application/pkg/zones-proxy-client:default` s'exécute uniquement dans la zone non globale. Le service est utilisé par le système d'empaquetage afin de fournir aux zones un accès au référentiel système.

Surveillance des zones non globales

Pour générer un rapport sur l'unité centrale (CPU), la mémoire et l'utilisation du contrôle de ressource pour les zones en cours d'exécution, reportez-vous à la section " Utilisation de l'utilitaire zonestat dans une zone non globale " du manuel " Création et utilisation d'Oracle Solaris Zones ". L'utilitaire `zonestat` fournit également des informations sur l'utilisation de la bande passante du réseau, dans les zones en mode IP exclusif. Une zone en mode IP exclusif possède son propre état d'IP, ainsi qu'une ou plusieurs liaisons de données dédiées.

L'utilitaire `fsstat` peut être utilisé pour signaler des statistiques d'opérations de fichier relatives aux zones non globales. Reportez-vous à la page de manuel `fsstat`(1M) et à la section " Surveillance des zones non globales à l'aide de l'utilitaire fsstat " du manuel " Création et utilisation d'Oracle Solaris Zones ".

Caractéristiques des zones non globales

Les zones non globales assurent les fonctions suivantes :

Sécurité	Lorsqu'un processus a été placé dans une zone autre que la zone globale, ni ce processus ni aucun de ses fils ne peuvent être déplacés vers une autre zone. Les services réseau peuvent être exécutés dans une zone. En exécutant les services réseau dans une zone, vous limitez les dommages éventuels en cas de violation de la sécurité. Les actions susceptibles d'être entreprises par un intrus ayant exploité une faille de sécurité dans un logiciel exécuté dans une zone se limitent à cette zone. Les privilèges disponibles dans une zone sont un sous-ensemble de ceux disponibles sur le système.
Isolement	Les zones permettent de déployer de nombreuses applications sur une même machine, même si ces applications s'exécutent sur des domaines de confiance différents, requièrent un accès exclusif à une ressource globale ou posent des problèmes dans le cas de configurations globales. Cela évite que les applications surveillent ou interceptent mutuellement leur trafic réseau, les données de leurs systèmes de fichiers ou l'activité de leurs processus.
Isolement du réseau	Les zones sont configurées en tant que type en mode IP exclusif par défaut. Les zones sont isolées de la zone globale et l'une de l'autre

	au niveau de la couche IP. Cet isolement est utile pour des raisons opérationnelles et de sécurité. Les zones peuvent être utilisées pour consolider les applications qui doivent communiquer sur des sous-réseaux différents à l'aide de leurs propres LAN ou VLAN. Chaque zone peut également définir ses propres règles de sécurité de couche IP.
Virtualisation	Les zones fournissent un environnement virtuel qui peut cacher des détails tels que les périphériques physiques, l'adresse IP principale du système et le nom d'hôte aux applications. Un même environnement applicatif peut être mis à jour sur différentes machines physiques. L'environnement virtuel permet de séparer l'administration de chacune des zones. Les actions entreprises par un administrateur de zone dans une zone non globale n'ont aucune incidence sur le reste du système.
Granularité	L'isolement assuré par les zones peut porter sur presque tous les niveaux de granularité souhaités. Pour plus d'informations, reportez-vous à la section “Caractéristiques des zones non globales” à la page 24.
Environnement	Les zones ne modifient pas l'environnement dans lequel les applications sont exécutées, excepté lorsque cela s'avère nécessaire pour atteindre les objectifs de sécurité et d'isolement voulus. Les zones ne possédant pas d'API ou d'ABI spécifique, il n'est pas nécessaire d'y porter les applications. Celles-ci s'exécutent dans l'environnement applicatif Oracle Solaris standard, doté des interfaces correspondantes, avec certaines limitations. Ces limitations concernent essentiellement les applications qui tentent d'exécuter des opérations requérant des privilèges. Les applications de la zone globale s'exécutent sans changement, que d'autres zones soient configurées ou non.

A propos d'Oracle Solaris Zones dans cette version

Cette section fournit une présentation des nouvelles fonctions Oracle Solaris Zones, y compris Oracle Solaris Kernel Zones.

La zone non globale par défaut de cette version est `solaris`, décrite dans ce guide et dans la page de manuel `solaris`(5).

Pour vérifier la version d'Oracle Solaris et l'architecture machine, tapez :

```
#uname -r -m
```

La commande virtinfo décrite dans la page de manuel `virtinfo`(1M) permet d'obtenir les informations suivantes :

- Déterminer la compatibilité du système avec les technologies de virtualisation Oracle Solaris
- Détecter le type d'environnement virtuel dans lequel Oracle Solaris s'exécute, par exemple Oracle VM Server for SPARC

La zone `solaris` utilise la structure de zones marquées décrite dans la page de manuel `brands`(5) pour exécuter les zones installées avec le même logiciel que celui de la zone globale. Le logiciel système doit toujours être synchronisé sur la zone globale lors de l'utilisation d'une zone non globale `solaris`. Les packages des logiciel système de la zone sont gérés à l'aide d'Image Packaging System (IPS). IPS est le système d'empaquetage d'Oracle Solaris 11, modèle également utilisé par les zones `solaris`.

Les zones `ipkg` par défaut créées par Oracle Solaris 11 Express sont mappées aux zones `solaris`. Reportez-vous à la section “A propos de la conversion de zones `ipkg` en zones `solaris`” à la page 11.

Chaque zone non globale spécifiée dans le manifeste d'installation automatisée (AI) est installée et configurée dans le cadre de l'installation d'un client. Les zones non globales sont installées et configurées lors de la première réinitialisation une fois la zone globale installée. Lors de la première initialisation du système, le service d'auto-assemblage de zones SMF (`svc:/system/zones-install:default`) configure et installe chaque zone non globale définie dans le manifeste AI de la zone globale. Pour plus d'informations, reportez-vous au document “ Ajout et mise à jour de logiciels dans Oracle Solaris 11.2 ”. Il est également possible de configurer et d'installer manuellement des zones sur un système Oracle Solaris déjà installé.

Pour les mises à jour de package, les proxys persistants doivent être définis dans une image à l'aide de l'option `--proxy`. Si aucune configuration de proxy d'image persistant n'est utilisée, les variables d'environnement `http_proxy` et `https_proxy` peuvent être définies.

Les zones peuvent être configurées pour être mises à jour en parallèle plutôt qu'en série. La mise à jour en parallèle améliore considérablement le temps requis pour mettre à jour toutes les zones d'un système.

Par défaut, les zones sont créées avec le type IP exclusif. Par l'intermédiaire de la ressource `anet`, une VNIC est automatiquement incluse dans la configuration de zone, si aucune configuration réseau n'est spécifiée. Pour plus d'informations, reportez-vous à la section “Interfaces réseau de zones” à la page 43.

Pour plus d'informations sur l'adresse `auto-mac-address` utilisée pour obtenir une adresse MAC (`mac-address`) pour une zone, consultez l'entrée `anet` de la section “Propriétés des types de ressources” à la page 67.

Une zone `solaris` sur le stockage partagé possède une ressource `zonecfg rootzpool`. Une zone est encapsulée dans un zpool dédié. Les zones de l'espace partagé accèdent à des ressources de stockage partagé qu'elles gèrent pour les zones. Les zones de noyau ne prennent pas en charge les ressources `zpool` ou `rootzpool`. Une zone de marque `solaris` peut utiliser le stockage

partagé suivant pour les ressources `device` de zone, ainsi que pour les ressources `zpool` et `rootzpool`.

- iSCSI
- LUN FC
- DA

Des propriétés permettant de spécifier les liaisons de données IP over InfiniBand (IPoIB) sont disponibles pour la ressource `zonecfg anet`. IPoIB est pris en charge par les zones de marque `solaris` et `solaris10`.

Le protocole IPC RDS (Reliable Datagram Sockets) est pris en charge à la fois dans les zones non globales en mode IP exclusif et IP partagé.

L'utilitaire `fsstat` a été étendu pour prendre en charge les zones. L'utilitaire `fsstat` fournit des statistiques de groupement et par zone.

Les zones `solaris` peuvent être des serveurs NFS, tel que décrit dans la section " Exécution d'un serveur NFS dans une zone " du manuel " Création et utilisation d'Oracle Solaris Zones ".

Une exécution de test, ou simulation, `zoneadm attach -n`, fournit une validation de `zonecfg`, mais ne valide pas le contenu du package.

Toutes les options `zoneadm` qui prennent des fichiers en tant qu'arguments requièrent des chemins absolus.

Oracle Solaris 10 Zones offre un environnement Oracle Solaris 10 dans Oracle Solaris 11. Vous pouvez migrer un système ou une zone Oracle Solaris 10 vers une zone `solaris10` dans un système Oracle Solaris 11. Reportez-vous au document " Création et utilisation des zones Oracle Solaris 10 ".

L'outil `zonep2vchk` identifie les problèmes, y compris les problèmes de gestion de réseaux susceptibles d'avoir une incidence sur la migration d'un système Oracle Solaris 11 ou Oracle Solaris 10 vers un système exécutant la version Oracle Solaris 11. L'outil `zonep2vchk` est exécuté sur le système source avant de commencer la migration. Il génère également un script `zonecfg` à utiliser sur le système cible. Le script crée une zone qui correspond à la configuration du système source. Pour plus d'informations, reportez-vous au Chapitre 7, " A propos des migrations de zones et de l'outil zonep2vchk " du manuel " Création et utilisation d'Oracle Solaris Zones ".

Il existe des différences entre les zones `solaris` et les zones `native` d'Oracle Solaris 10, comme suit :

- La marque `solaris` est créée sur les systèmes Oracle Solaris 11 à la place de la marque `native`, qui est la valeur par défaut sur les systèmes Oracle Solaris 10.
- Les zones `solaris` sont de type whole root uniquement.

La zone native de type sparse root disponible dans Oracle Solaris 10 utilise le système de gestion du package SVR4, mais IPS n'utilise pas ce système. Une configuration de zone root en lecture seule similaire au type sparse root est disponible.

- Les zones de cette version disposent d'une fonctionnalité de gestion logicielle différente de celle d'Oracle Solaris 10, dans les domaines suivants :
  - Empaquetage IPS contre SVR4.
  - Fonctions d'installation, de séparation, de jonction et de conversion physique/virtuel.
  - La racine de zone non globale est un jeu de données ZFS™.

    Un package installé dans la zone globale n'est plus installé dans toutes les zones actuelles et futures. En général, le contenu de la zone globale en termes de packages ne s'impose plus aux autres zones, que ce soit pour les packages IPS ou pour les packages SVR4.
- Les zones non globales utilisent des environnements d'initialisation. Les zones sont intégrées à `beadm`, la commande d'interface utilisateur destinée à la gestion des environnements d'initialisation ZFS (BE, Boot Environment).

  La commande `beadm` est prise en charge à l'intérieur des zones pour la mise à jour `pkg`, tout comme dans la zone globale. La commande `beadm` commande permet de supprimer tous les BE de zone inactifs associés à la zone. Reportez-vous à la page de manuel `beadm`(1M).
- Tous les référentiels de package IPS activés doivent être accessibles lors de l'installation de la zone. Pour plus d'informations, reportez-vous à la section " Installation d'une zone configurée " du manuel " Création et utilisation d'Oracle Solaris Zones ".
- Le logiciel de zone de départ est réduit au minimum. Tous les packages supplémentaires éventuellement requis par la zone doivent être ajoutés. Pour plus d'informations, reportez-vous au document " Ajout et mise à jour de logiciels dans Oracle Solaris 11.2 ".

Les zones peuvent utiliser les produits et les fonctionnalités Oracle Solaris suivantes :

- Chiffrement Oracle Solaris ZFS
- Virtualisation du réseau et qualité de service (QoS)
- CIFS et NFS

Les fonctionnalités suivantes ne peuvent pas être configurées dans une zone de marque `solaris-kz` :

- Services FC
- Services FCoE

Reconfiguration de zone en direct

La reconfiguration de zone en direct permet de créer des rapports ou de reconfigurer la configuration en direct de zones `solaris` ou `solaris10` sans les réinitialiser. Les modifications peuvent être effectuées de façon temporaire ou permanente.

Servez-vous de la reconfiguration de zone en direct pour générer des informations de configuration en direct sur les zones de marque `solaris-kz`.

Pour plus d'informations, reportez-vous à “ Création et utilisation d’Oracle Solaris Zones ”.

♦ ♦ ♦ CHAPITRE 2

Présentation de la configuration des zones non globales

Ce chapitre constitue une introduction à la configuration des zones non globales.

Les rubriques traitées dans ce chapitre sont les suivantes :

Après avoir étudié la configuration des zones, passez au Chapitre 1, “ Planification et configuration de zones non globales ” du manuel “ Création et utilisation d’Oracle Solaris Zones ” pour configurer les zones non globales en vue de leur installation sur le système.

A propos des ressources dans les zones

Dans une zone, vous pouvez contrôler notamment les ressources suivantes :

- Les pools de ressources ou CPU assignées, qui sont utilisés pour les ressources des machines partitionnées.
- Les contrôles de ressources, qui fournissent un mécanisme de contrainte des ressources système.
- La classe de programmation, qui permet de contrôler l'allocation des ressources CPU disponibles au sein des zones, en fonction de leur importance. Celle-ci se reflète dans le nombre de parts de ressources CPU que vous assignez à chaque zone.

Utilisation des profils de droits et des rôles dans l'administration de zone

Pour plus d'informations sur les profils et les rôles, reportez-vous à la section " Protection et isolation des applications " du manuel " Directives de sécurité d'Oracle Solaris 11 ".

Propriété `zonecfg template`

La propriété `zonecfg template` permet de définir si les propriétés ont été modifiées dans les cas suivants et comment :

- Lorsque de nouvelles instances de ressource sont ajoutées à une configuration.
- Pendant le clonage de la configuration, lorsque certaines propriétés doivent avoir des valeurs uniques. Servez-vous de jetons dans la propriété `template` pour spécifier ces valeurs uniques.

TABLEAU 2-1 Jetons `zonecfg template`

Jeton	Description	Utilisation
`%`*zonename*	Nom de la zone.	Peut être utilisé dans les métadonnées de la marque et dans `zonecfg` en tant qu'entrée saisie par l'utilisateur ou provenant d'une valeur de modèle.
`%`*network-id*	Numéro d'instance unique correspondant aux ressources réseau `net` et `anet`. Ce numéro est unique pour les ressources `net` et `anet` situées dans la zone globale.	Peut être utilisé dans les métadonnées de la marque, en tant qu'attribut par défaut des ressources `net` et `anet` de la propriété `id`.
`%`*resource-id*	Numéro d'instance unique compris dans une étendue globale de ressources donnée, elle-même comprise dans la zone globale, pour toutes les ressources sauf `net` et `anet`.	Peut être utilisé dans les métadonnées de la marque, en tant qu'attribut par défaut de la propriété `id`.
`%`*id*	Numéro d'instance unique correspondant à la valeur de la propriété *id* de la ressource.	Peut être utilisé dans la commande `zonecfg` en tant qu'entrée saisie par l'utilisateur ou provenant d'une valeur de modèle. Doit être compris dans l'étendue des ressources qui

Jeton	Description	Utilisation
		prend en charge la propriété `id`.
`%%`	Donne `%`.	Peut être utilisé dans les métadonnées de la marque et dans la commande `zonecfg` en tant qu'entrée saisie par l'utilisateur.

La configuration du module de démon RAD (Remote Administration Daemon) des zones fournit un moyen global d'exprimer, d'appliquer ou de mettre en oeuvre des modifications à l'aide de modèles de propriété. Reportez-vous à la page de manuel `zonemgr`(3RAD). Si le package `rad-zonemgr` n'était pas déjà installé sur votre système et que vous avez procédé à son installation ultérieurement à l'aide de la commande `pkg install`, vous devez redémarrer le service `rad:local`. Redémarrez également le service `rad:remote`, s'il était en cours d'exécution. Pour redémarrer, exécutez la commande `svcadm`(1M). Vérifiez que le démon RAD a chargé le module.

Configuration avant installation

Avant de pouvoir installer une zone non globale et de l'utiliser sur votre système, vous devez configurer la zone.

La commande `zonecfg` permet de créer la configuration et de déterminer si les ressources et les propriétés spécifiées sont valides sur un système hypothétique. La vérification effectuée par `zonecfg` pour une configuration donnée consiste à :

- S'assurer qu'un chemin d'accès à la zone est spécifié
- Vérifier que toutes les propriétés requises pour chaque ressource sont spécifiées
- s'assurer que la configuration est exempte de conflits. Par exemple, si vous disposez d'une ressource `anet`, la zone est de type IP exclusif et ne peut pas être de type IP partagé. En outre, la commande `zonecfg` émet un avertissement si un jeu de données contenant un alias entre potentiellement en conflit avec des périphériques.

Pour plus d'informations sur la commande `zonecfg`, reportez-vous à la page de manuel `zonecfg`(1M).

Composants des zones

Cette section porte sur les composants de zones, requis et optionnels, susceptibles d'être configurés. Seuls le nom et le chemin de la zone sont requis. Vous trouverez de plus amples informations dans la section “Données de configuration de zones” à la page 61.

Nom de zone et chemin d'accès

Vous devez nommer la zone. Si vous ne spécifiez pas de chemin, la valeur par défaut de `zonepath` est `/system/zones/`*zonename*.

Si vous choisissez un nom et un chemin pour la zone, celle-ci doit faire partie d'un jeu de données ZFS. Le jeu de données ZFS est automatiquement créé lorsque la zone est installée ou jointe. Si un jeu de données ZFS ne peut pas être créé, l'installation ou la jonction de la zone est impossible. Notez que le répertoire parent du chemin de la zone doit également être un jeu de données.

Si le chemin n'est pas spécifié, la valeur par défaut de `zonepath` est `/system/zones/`*zonename*.

Initialisation automatique (autoboot) d'une zone

Le réglage de la propriété `autoboot` détermine si la zone est automatiquement initialisée lorsque la zone globale est initialisée. Le service des zones, `svc:/system/zones:default` doit également être activé.

Propriété `file-mac-profile` pour les zones immuables

Dans les zones `solaris`, la propriété `file-mac-profile` sert à configurer des zones immuables avec des roots en lecture seule.

Pour plus d'informations, reportez-vous au Chapitre 12, “ Configuration et administration de zones immuables ” du manuel “ Création et utilisation d’Oracle Solaris Zones ”.

Ressource `admin`

Le réglage `admin` vous permet de définir l'autorisation d'administration de la zone. La meilleure méthode pour définir les autorisations consiste à utiliser la commande `zonecfg`.

`user` Spécifiez le nom d'utilisateur.

`auths` Spécifiez les autorisations du nom d'utilisateur.

`solaris.zone.login` Si vous utilisez le contrôle RBAC, l'autorisation `solaris.zone.login/`*zonename* est requise pour les connexions interactives. L'authentification par mot de passe s'effectue dans la zone.

`solaris.zone.manage` Si vous utilisez le contrôle RBAC, l'autorisation `solaris.zone.manage/`*zonename* est requise pour les connexions non interactives ou pour contourner l'authentification par mot de passe.

`solaris.zone.clonefrom` Si vous utilisez le contrôle RBAC, les sous-commandes chargées de copier une autre zone exigent une autorisation `solaris.zone.clonefrom/`*source_zone*.

Pour plus d'informations sur les autorisations, reportez-vous aux pages de manuel `auths`(1), `auth_attr`(4) et `user_attr`(4).

Ressource `dedicated-cpu`

La ressource `dedicated-cpu` spécifie qu'un sous-ensemble des processeurs du système doit être dédié à une zone non globale en cours d'exécution. Dès que la zone est initialisée, le système crée de manière dynamique un pool temporaire destiné à être utilisé lorsque la zone est en cours d'exécution.

Vous pouvez propager les paramètres du pool pendant les migrations en les spécifiant dans la commande `zonecfg`.

La ressource `dedicated-cpu` définit les limites de `ncpus` et éventuellement d'`importance`.

`ncpus` Spécifie le nombre de CPU ou une plage de CPU (par exemple 2–4). Si vous optez pour une plage de CPU parce que vous souhaitez que le pool de ressources se comporte de manière dynamique, vous devez également :

- Définir la propriété `importance`
- Activer le service `poold`. Pour obtenir des instructions, reportez-vous à la section " Activation du service de pools de ressources dynamiques à l'aide de svcadm " du manuel " Administration de la gestion des ressources dans Oracle Solaris 11.2 ".

`importance` Si, pour un plus grand dynamisme du pool de ressources, vous avez choisi d'utiliser une plage de CPU, définissez également la propriété `importance`. La propriété `importance` détermine l'importance relative du pool mais est *optionnelle*. Elle n'est nécessaire que si vous spécifiez une plage pour `ncpus` et utilisez des pools de ressources dynamiques gérés par `poold`. Si `poold` n'est pas en cours d'exécution, la propriété `importance` est ignorée. Si `poold` est en cours d'exécution et si la

propriété `importance` n'a pas été définie, `importance` adopte par défaut la valeur `1`. Pour plus d'informations, reportez-vous à la section " Contrainte de propriété pool.importance " du manuel " Administration de la gestion des ressources dans Oracle Solaris 11.2 ".

Les propriétés suivantes servent à définir des ressources `dedicated-cpu` persistantes pour `cpus`, `cores` et `sockets`.

`cpus`	Assignez des CPU spécifiques à une zone de manière permanente.
`cores`	Assignez des coeurs spécifiques à une zone de manière permanente.
`sockets`	Assignez un nombre de sockets spécifique de manière permanente.

Remarque - Les ressources `capped-cpu` et `dedicated-cpu` sont incompatibles. L'instance de contrôle de ressource `cpu-shares` et la ressource `dedicated-cpu` sont incompatibles.

Remarque - Les applications qui dimensionnent et effectuent une mise à l'échelle de manière automatique sur le nombre de CPU disponibles peuvent ne pas reconnaître une limitation capped-cpu. Considérer que toutes les CPU sont disponibles peut avoir un impact négatif sur la mise à l'échelle et les performances dans des applications telles que la base de données Oracle et les machines virtuelles Java (JVM). L'application peut sembler ne pas fonctionner ou être inutilisable. La machine JVM ne doit pas être utilisée avec capped-cpu si les performances sont essentielles. Les applications des catégories affectées peuvent utiliser la ressource dedicated-cpu.

`solaris-kz` uniquement : ressource `virtual-cpu`

Servez-vous de la ressource `virtual-cpu` pour définir le nombre de CPU de zone de noyau. Les CPU hôte dédiés à la zone de noyau sont définis par la valeur `ncpus`. La configuration de zone de noyau par défaut comprend 1 CPU. Vous pouvez ajouter plusieurs CPU à la zone de noyau en ajoutant la propriété `virtual-cpu`.

Notez que si vous avez déjà défini la ressource `dedicated-cpu`, le nombre par défaut de CPU virtuels configurés dans la plate-forme virtuelle correspond à la plus petite valeur de la plage `ncpus` dans la ressource `dedicated-cpu`. Il n'est pas nécessaire de définir les deux ressources `dedicated-cpu` et `virtual-cpu` à la fois.

Ressource `capped-cpu`

La ressource `capped-cpu` définit une limite absolue très précise de la quantité de ressources CPU qu'un projet ou une zone peut consommer. Associée aux jeux de processeurs, la capacité

de CPU limite l'utilisation de ressources CPU au sein d'un jeu. La ressource `capped-cpu` possède une seule propriété `ncpus`, dont la valeur est un nombre décimal positif avec deux chiffres après la virgule. Cette propriété correspond aux unités de CPU. Cette ressource n'accepte pas de plage, mais elle accepte les nombres décimaux. Lorsque vous spécifiez la propriété `ncpus`, notez que la valeur `1` correspond à 100 pourcent d'une CPU. Ainsi, la valeur `1,25` équivaut à 125 pourcent, car 100 pourcent correspond à une CPU complète sur le système.

Remarque - Les ressources `capped-cpu` et `dedicated-cpu` sont incompatibles.

Remarque - Les applications qui dimensionnent et effectuent une mise à l'échelle de manière automatique sur le nombre de CPU disponibles peuvent ne pas reconnaître une limitation `capped-cpu`. Considérer que toutes les CPU sont disponibles peut avoir un impact négatif sur la mise à l'échelle et les performances dans des applications telles que la base de données Oracle et les machines virtuelles Java (JVM). L'application peut sembler ne pas fonctionner ou être inutilisable. La machine JVM ne doit pas être utilisée avec `capped-cpu` si les performances sont essentielles. Les applications des catégories affectées peuvent utiliser la ressource `dedicated-cpu`. Reportez-vous à la section “Ressource `dedicated-cpu`” à la page 37.

Classe de programmation

Vous pouvez utiliser l'*ordonnanceur équitable* (FSS, Fair Share Scheduler) pour contrôler l'allocation des ressources CPU disponibles aux différentes zones en fonction de leur importance. Celle-ci se reflète dans le nombre de *parts* de ressources CPU que vous assignez à chaque zone. Même si vous n'utilisez pas FSS pour gérer l'allocation de ressources CPU aux zones, vous pouvez définir la classe de programmation des zones pour utiliser FSS de manière à pouvoir assigner des parts aux projets au sein des zones.

Lorsque vous définissez explicitement la propriété `cpu-shares`, l'ordonnanceur équitable sert de classe de programmation pour la zone concernée. Dans ce cas, il est cependant préférable de définir FSS comme classe de programmation par défaut du système à l'aide de la commande `dispadmin`. Toutes les zones disposent ainsi d'une part équitable des ressources CPU du système. Toute zone pour laquelle la propriété `cpu-shares` n'est pas définie utilise la classe de programmation par défaut du système. Pour définir la classe de programmation d'une zone, vous pouvez procéder de différentes façons :

- Vous pouvez utiliser la propriété `scheduling-class` de `zonecfg`.
- Vous pouvez avoir recours à l'utilitaire de pools de ressources. Si la zone est associée à un pool dont la propriété `pool.scheduler` est définie sur une classe de programmation valide, les processus exécutés dans cette zone le sont dans cette classe de programmation par défaut. Reportez-vous aux sections “ Introduction aux pools de ressources ” du manuel “ Administration de la gestion des ressources dans Oracle Solaris 11.2 ” et “ Association d’un pool avec une classe de programmation ” du manuel “ Administration de la gestion des ressources dans Oracle Solaris 11.2 ”.

- Si l'instance de contrôle de ressource `cpu-shares` est définie et si vous n'avez pas défini FSS comme la classe de programmation pour la zone, `zoneadmd` s'en charge lors de l'initialisation de celle-ci.
- Si la classe de programmation n'est pas définie par toute autre action, la zone hérite de la classe de programmation par défaut du système.

Notez que vous pouvez utiliser la commande `priocntl` décrite dans la page de manuel `priocntl`(1) pour placer les processus en cours d'exécution dans une autre classe de programmation sans modifier la classe de programmation par défaut et sans réinitialiser.

Contrôle de la mémoire physique et ressource `capped-memory`

La ressource `capped-memory` définit les limites de la mémoire `physical`, `swap` et `locked`. Chaque limite est optionnelle, mais vous devez en définir au moins une. Pour utiliser la ressource `capped-memory`, le package `resource-cap` doit être installé dans la zone globale. Reportez-vous également à la section “Ressource `capped-cpu`” à la page 38.

- Déterminez les valeurs pour cette ressource si vous prévoyez de limiter la mémoire de la zone à l'aide de `rcapd` dans la zone globale. La propriété `physical` de la ressource `capped-memory` est utilisée par `rcapd` comme valeur `max-rss` pour la zone.
- La propriété `swap` de la ressource `capped-memory` permet de définir le contrôle de ressources `zone.max-swap`.
- La propriété `locked` de la ressource `capped-memory` permet de définir le contrôle de ressources `zone.max-locked-memory`.

Remarque - Généralement, les applications ne bloquent pas une quantité importante de mémoire, mais vous pouvez décider de définir un verrouillage de mémoire si les applications de la zone sont susceptibles de bloquer de la mémoire. Si la confiance de la zone est un problème, vous pouvez définir la limite de mémoire verrouillée à 10 % de la mémoire physique du système, ou 10 % de la limite de mémoire physique de la zone.

Pour plus d'informations, reportez-vous aux Chapitre 10, “ A propos du contrôle de la mémoire physique à l’aide du démon de limitation des ressources ” du manuel “ Administration de la gestion des ressources dans Oracle Solaris 11.2 ” et Chapitre 11, “ Administration du démon de limitation des ressources (tâches) ” du manuel “ Administration de la gestion des ressources dans Oracle Solaris 11.2 ” et à la section “ Configuration d’une zone ” du manuel “ Création et utilisation d’Oracle Solaris Zones ”. Pour définir temporairement une limitation de ressources pour une zone, reportez-vous à la section “ Spécification d’une limitation temporaire de ressources pour une zone ” du manuel “ Administration de la gestion des ressources dans Oracle Solaris 11.2 ”.

`solaris` et `solaris10` uniquement : ressource `rootzpool`

La ressource `rootzpool` facultative de l'utilitaire `zonecfg` permet de créer un zpool dédié pour l'installation de zone pour les zones de marque `solaris` et `solaris10`. Le zpool root de la zone peut être hébergé sur les périphériques de stockage partagés définis par un ou plusieurs URI (Universal Resource Identifiers). La propriété `storage` requise identifie l'URI de l'objet de stockage pour qu'il contienne le système de fichiers `zfs` root pour une zone. Un seul `rootzpool` peut être défini pour une zone donnée. Le stockage est automatiquement configuré pour la zone au moment de l'initialisation de la zone.

Les zpools correspondants sont automatiquement créés ou importés durant les opérations d'installation ou de rattachement de la zone. Pour les ressources rootzpool et zpool, vous pouvez créer automatiquement des miroirs zpool dès que la zone a été installée. Pour plus d'informations, reportez-vous au Chapitre 14, “ Prise en main d’Oracle Solaris Zones sur stockage partagé ” du manuel “ Création et utilisation d’Oracle Solaris Zones ”.

Lorsque la zone est désinstallée ou détachée, les actions suivantes ont lieu :

- Les zpools correspondants sont automatiquement exportés ou détruits.
- La configuration des ressources de stockage est automatiquement annulée.

Afin de réutiliser un zpool précréé pour une installation de zone, il convient de l'exporter à partir du système.

La structure des zones prend en charge les types d'URI suivants :

- `dev`

  URI de chemin de périphérique local

  Format:

  `dev:`*local-path-under-*`/dev`
  `dev://`*absolute-path-with-dev*
  `dev:`*absolute-path-with-dev*

  Exemples :

  ```
  dev:dsk/c7t0d0s0
  dev:///dev/dsk/c7t0d0s0
  dev:/dev/dsk/c7t0d0s0
  dev:chassis/SYS/HD1/disk
  ```

- `lu` (unité logique)

  Fibre Channel (FC) et domaines Serial Attached SCSI (SAS)

  Format:

  `lu:luname.naa.`*ID*

```
lu:luname.eui.ID
lu:initiator.naa.ID,target.naa.ID,luname.naa.ID
lu:initiator.naa.ID,target.naa.ID,luname.eui.ID
```

Exemples :

```
lu:luname.naa.5000c5000288fa25
lu:luname.eui.0021280001cf80f6
lu:initiator.naa.2100001d38089fb0,target.naa.2100001d38089fb0,luname.naa.5000c5000288fa25
lu:initiator.naa.2100001d38089fb0,target.naa.2100001d38089fb0,luname.eui.0021280001cf80f6
```

- `iscsi`

  URI iSCSI

  Format:

```
iscsi:///luname.naa.ID
iscsi:///luname.eui.ID
iscsi://host[:port]/luname.naa.ID
iscsi://host[:port]/luname.eui.ID
iscsi:///target.IQN,lun.LUN
iscsi://host[:port]/target.IQN,lun.LUN
```

  Exemples :

```
iscsi:///luname.eui.0021280001cf80f6
iscsi:///luname.naa.600144f03d70c80000004ea57da10001
iscsi://[::1]/luname.naa.600144f03d70c80000004ea57da10001
iscsi://127.0.0.1/luname.naa.600144f03d70c80000004ea57da10001
iscsi://hostname:1234/luname.eui.0021280001cf80f6
iscsi://hostname:3260/luname.naa.600144f03d70c80000004ea57da10001

iscsi://127.0.0.1/target.iqn.com.sun:02:d0f2d311-f703,lun.0
iscsi:///target.iqn.com.sun:02:d0f2d311-f703,lun.6
iscsi://[::1]:1234/target.iqn.com.sun:02:d0f2d311-f703,lun.2
iscsi://hostname:1234/target.iqn.com.sun:4db41b76-e3d7-cd2f-bf2d-9abef784d76c,lun.0
```

L'outil `suriadm` permet d'administrer des objets partagés basés sur les URI de stockage. Pour plus d'informations sur les ID, l'autorité d'adresse de nom NAA (Name Address Authority) et l'obtention d'URI pour les objets de stockage existants, reportez-vous aux pages de manuel `suriadm`(1M) et `suri`(5).

Le système nomme le `rootzpool` nouvellement créé ou importé pour sa zone correspondante. Le nom attribué a la forme suivante : *zonename*_`rpool`.

La propriété `storage` est gérée à l'aide des commandes suivantes depuis l'étendue de la ressource `rootzpool` :

- `add storage` *URI string*

- `remove storage` *URI string*

Ajout d'une ressource `zpool` automatiquement

Un `zpool` peut être délégué à une zone non globale en configurant la ressource `zpool` facultative dans l'utilitaire `zonecfg`. Le `zpool` est automatiquement configuré pour la zone lors de son initialisation.

Les zpools correspondants sont automatiquement créés ou importés durant les opérations d'installation ou de rattachement de la zone.

Lorsque la zone est désinstallée ou détachée, les actions suivantes ont lieu :

- Les zpools correspondants sont automatiquement exportés ou détruits.
- La configuration des ressources de stockage est automatiquement annulée.

La propriété `storage` identifie l'URI de l'objet de stockage associé à cette ressource.

La propriété `storage` est gérée à l'aide des paramètres suivants dans l'étendue de la ressource `rootzpool` :

- `add storage` *URI string*
- `remove storage` *URI string*

La propriété `name` est obligatoire pour la ressource `zpool`. La propriété est utilisée dans le nom d'un zpool délégué à la zone. Le composant `name` du système de fichiers ZFS ne peut pas contenir de barre oblique (`/`).

Le nom assigné au `zpool` nouvellement créé ou importé correspond à la valeur de la propriété `name`. Il s'agit du nom zpool visible à l'intérieur de la zone non globale. Le nom assigné au `zpool` nouvellement créé ou importé se présente sous la forme *zonename_name* lorsqu'il est affiché depuis la zone globale.

Remarque - Une installation de zone risque d'échouer lorsqu'un objet de stockage contient des partitions, des zpools ou des systèmes de fichiers UFS préexistants. Pour plus d'informations, reportez-vous à l'étape 4 de la section “ Installation d’une zone configurée ” du manuel “ Création et utilisation d’Oracle Solaris Zones ”.

Interfaces réseau de zones

Les interfaces réseau configurées à l'aide de l'utilitaire `zonecfg` pour doter les zones d'une connectivité réseau sont automatiquement paramétrées et placées dans la zone concernée lors de son initialisation.

La couche IP accepte et livre les paquets pour le réseau. Cette couche inclut le routage IP, le protocole de résolution d'adresse (ARP, Address Resolution Protocol), l'architecture de sécurité IP (IPsec, IP security architecture) et le filtrage IP.

Deux modes IP sont disponibles pour les zones non globales : le mode IP partagé et le mode IP exclusif. Le type par défaut est le mode IP exclusif. Une zone en mode IP partagé partage une interface réseau avec la zone globale. Vous devez configurer la zone globale à l'aide de l'utilitaire `ipadm` pour utiliser les zones en mode IP partagé. Une zone en mode IP exclusif doit posséder une interface réseau dédiée. Si la zone en mode IP exclusif est configurée à l'aide de la ressource `anet`, une carte d'interface réseau virtuelle dédiée est automatiquement créée et affectée à cette zone. Pour éviter de créer et de configurer les liaisons de données dans la zone globale et d'affecter les liaisons de données aux zones non globales, vous pouvez utiliser la ressource `anet` automatisée. Utilisez la ressource `anet` pour effectuer les opérations suivantes :

- Autoriser l'administrateur de la zone globale à choisir des noms spécifiques pour les liaisons de données affectées aux zones non globales
- Autoriser plusieurs zones à utiliser des liaisons de données du même nom

Pour des raisons de rétrocompatibilité, les liaisons de données préconfigurées peuvent être affectées aux zones non globales.

Pour plus d'informations sur les fonctionnalités IP dans chaque type, reportez-vous aux sections " Mise en réseau dans des zones non globales en mode IP exclusif " du manuel " Création et utilisation d'Oracle Solaris Zones " et " Mise en réseau dans des zones non globales en mode IP partagé " du manuel " Création et utilisation d'Oracle Solaris Zones ".

Remarque - La protection des liaisons décrite dans le document " Sécurisation du réseau dans Oracle Solaris 11.2 " peut être appliquée sur un système exécutant des zones. Cette fonctionnalité est configurée dans la zone globale.

A propos des liaisons de données

Une liaison de données est une interface physique de niveau 2 de la pile de protocoles OSI, représentée dans un système comme une interface STREAMS DLPI (v2). Ce type d'interface peut être monté sous des piles de protocoles telles que TCP/IP. Une liaison de données désigne également une interface physique, par exemple, une carte d'interface réseau (NIC). La liaison de données est la propriété `physical` configurée à l'aide de `zonecfg`(1M). La propriété `physical` peut être une carte d'interface réseau virtuelle (VNIC).

Par défaut dans Oracle Solaris 11, les noms de périphérique réseau physique sont basés sur des noms génériques, par exemple `net0`, au lieu des noms de pilote de périphérique comme `nxge0`.

Pour plus d'informations sur l'utilisation d'IPoIB (IP over Infiniband) pour les zones `solaris`, reportez-vous à la description d'`anet` de la section "Propriétés des types de ressources" à la page 67.

A propos du commutateur virtuel élastique et des zones

Dans le cas d'une ressource `anet` qui se connecte à un commutateur virtuel élastique (EVS) avec les propriétés `evs` et `vport` définies, les propriétés de cette ressource `anet` sont encapsulées dans la paire `evs/vport`. Vous ne pouvez modifier aucune des propriétés suivantes de la ressource `anet` d'un commutateur EVS :

- `mac-address`
- `mtu`
- `maxbw`
- `priority`
- `allowed-address`
- `vlan-id`
- `defrouter`
- `lower-link`

Voici les seules propriétés que vous pouvez définir pour la ressource `anet` d'un commutateur EVS :

- linkname
- `evs`
- `vport`
- `configure-allowed-address`

Vous devez également définir la ressource `tenant`. Les locataires sont utilisés pour la gestion des espaces de noms. Les ressources d'EVS définies dans un locataire (`tenant`) ne sont pas visibles en dehors de l'espace de noms de ce locataire.

Les entrées suivantes pour une zone nommée *evszone* définissent la ressource `tenant` d'un locataire nommé *tenantA*. Les propriétés de la ressource `zonecfg anet` créent une carte VNIC pour une zone dont la ressource `anet` se connecte à un commutateur EVS nommé *evsa* et un VPort nommé *vport0* :

```
zonecfg:evszone> set tenant=tenantA

zonecfg:evszone> add anet

zonecfg:evszone> set evs=EVSA

zonecfg:evszone> set vport=vport0
```

Pour plus d'informations, reportez-vous au Chapitre 5, “ A propos des commutateurs virtuels élastiques ” du manuel “ Gestion de la virtualisation réseau et des ressources réseau dans Oracle Solaris 11.2 ”.

Zones non globales en mode IP partagé

Une zone en mode IP partagé utilise une interface IP à partir de la zone globale. La zone doit contenir une ou plusieurs adresses IP dédiées. Une zone en mode IP partagé partage la configuration et l'état de la couche IP avec la zone globale. Vous devez utiliser l'instance d'IP partagé si les deux conditions suivantes sont vérifiées :

- La zone non globale doit utiliser la même liaison de données que la zone globale, que les zones globales et non globales se trouvent sur le même sous-réseau ou non.
- Vous n'avez pas besoin des autres capacités fournies par les zones en mode IP exclusif.

La ressource `net` de la commande `zonecfg` permet d'assigner une ou plusieurs adresses IP aux zones en mode IP partagé. Il convient également de configurer les noms des liaisons de données dans la zone globale.

Dans la ressource `zonecfg net`, les propriétés `address` et `physical` doivent être définies. La propriété `defrouter` est facultative.

Pour utiliser la configuration réseau en mode IP partagé dans la zone globale, vous devez utiliser `ipadm` , et non la configuration automatique du réseau. Pour déterminer si la configuration réseau s'effectue à l'aide de `ipadm`, exécutez la commande suivante. La réponse affichée doit être `DefaultFixed`.

```
# svcprop -p netcfg/active_ncp svc:/network/physical:default
DefaultFixed
```

Les adresses IP affectées aux zones en mode IP partagé sont associées à des interfaces réseau logiques.

La commande `ipadm` peut être utilisée dans la zone globale pour assigner ou supprimer des interfaces logiques dans une zone en cours d'exécution.

Pour ajouter des interfaces, utilisez la commande suivante :

```
global# ipadm set-addrprop -p zone=my-zone net0/addr1
```

Pour supprimer des interfaces, utilisez l'une des commandes suivantes :

```
global# ipadm set-addrprop -p zone=global net0/addr
```

ou :

```
global# ipadm reset-addrprop -p zone net0/addr1
```

Pour plus d'informations, reportez-vous à la section “ Interfaces réseau en mode IP partagé ” du manuel “ Création et utilisation d’Oracle Solaris Zones ”.

Zones non globales en mode IP exclusif

Le mode IP exclusif est la configuration réseau par défaut des zones non globales.

Une zone en mode IP exclusif possède son propre état d'IP, ainsi qu'une ou plusieurs liaisons de données dédiées.

Les fonctions suivantes peuvent être utilisées dans une zone en mode IP exclusif :

- La configuration automatique d'adresse sans état via DHCPv4 et IPv6
- Le filtrage IP, fonctionnalité NAT comprise
- Le multipathing sur réseau IP (IPMP, IP Network Multipathing)
- Le routage IP
- La commande `ipadm` permettant de définir les paramètres TCP/UDP/SCTP, ainsi que les paramètres réglables IP/ARP
- Les protocoles IPsec (IP security) et IKE (Internet Key Exchange), qui automatisent l'approvisionnement en matériel de chiffrement authentifié pour l'association de sécurité IPsec

Il existe deux façons de configurer les zones en mode IP exclusif :

- Utilisez la ressource `anet` de l'utilitaire `zonecfg` pour créer automatiquement une VNIC temporaire à de l'initialisation de la zone et la supprimer lorsque la zone s'arrête.
- Préconfigurez la liaison de données dans la zone globale et affectez-la à la zone en mode IP exclusif à l'aide de la ressource `net` de l'utilitaire `zonecfg`. La liaison de données est spécifiée à l'aide de la propriété `physical` de la ressource `net`. La propriété `physical` peut être une carte d'interface réseau virtuelle (VNIC). La propriété `address` de la ressource `net` n'est pas définie.

Par défaut, une zone en mode IP exclusif peut configurer et utiliser toute adresse IP de l'interface associée. En option, une liste d'adresses IP séparées par des virgules peut être spécifiée à l'aide de la propriété `allowed-address`. La zone en mode IP exclusif ne peut pas utiliser les adresses IP qui ne figurent pas dans la liste `allowed-address`. En outre, toutes les adresses de la liste `allowed-address` sont automatiquement configurées de façon permanente pour la zone en mode IP exclusif lorsque celle-ci est initialisée. Si cette configuration d'interface n'est pas souhaitée, la propriété `configure-allowed-address` doit être réglée sur `false`. La valeur par défaut est `true`.

Notez que la liaison de données assignée active la commande `snoop`.

La commande `dladm` peut être utilisée avec la sous-commande `show-linkprop` pour afficher l'assignation de liaisons de données aux zones en mode IP exclusif en cours d'exécution. La commande `dladm` peut également être utilisée avec la sous-commande `set-linkprop` pour assigner des liaisons de données supplémentaires aux zones en cours d'exécution. Vous trouverez des exemples d'utilisation à la section “ Gestion des liaisons de données dans les zones non globales en mode IP exclusif ” du manuel “ Création et utilisation d’Oracle Solaris Zones ”.

Dans une zone en mode IP exclusif en cours d'exécution qui possède son propre jeu de liaisons de données, la commande `ipadm` permet de définir la configuration IP, ce qui inclut la possibilité

d'ajouter ou de supprimer des interfaces logiques. Vous pouvez procéder à la configuration IP d'une zone de la même façon que pour une zone globale, à l'aide de l'interface `sysconfig` décrite dans la page de manuel `sysconfig`(1M).

La configuration IP d'une zone en mode IP exclusif ne peut être affichée que depuis la zone globale, à l'aide de la commande `zlogin`.

```
global# zlogin zone1 ipadm show-addr
ADDROBJ           TYPE     STATE        ADDR
lo0/v4            static   ok           127.0.0.1/8
nge0/v4           dhcp     ok           10.134.62.47/24
lo0/v6            static   ok           ::1/128
nge0/_a           addrconf ok           fe80::2e0:81ff:fe5d:c630/10
```

Prise en charge RDS (Reliable Datagram Sockets) dans les zones non globales

Le protocole IPC RDS (Reliable Datagram Sockets) est pris en charge à la fois dans les zones non globales en mode IP exclusif et IP partagé. Le pilote RDSv3 est activé en tant que `rds` de service SMF. Par défaut, le service est désactivé après l'installation. Le service peut être activé dans une zone non globale par un administrateur de zone disposant des autorisations adéquates. Après `zlogin`, `rds` peut être activée dans chacune des zones dans laquelle elle doit être exécutée.

EXEMPLE 2-1 Activation du service `rds` dans une zone non globale

1. Pour activer un service RDSv3 dans une zone en mode IP exclusive ou IP partagé, exécutez zlogin ou la commande `svcadm enable` :

   ```
   # svcadm enable rds
   ```

2. Vérifiez que `rds` est activé :

   ```
   # svcs rds
       STATE          STIME    FMRI
       online         22:50:53 svc:/system/rds:default
   ```

Pour plus d'informations, reportez-vous à la page de manuel `svcadm`(1M).

Différences entre les zones non globales en modes IP partagé et IP exclusif en matière de sécurité

Dans une zone en mode IP partagé, les applications de la zone (superutilisateur compris) ne peuvent pas envoyer de paquets avec des adresses IP source autres que celles assignées à la

zone par le biais de l'utilitaire `zonecfg`. Dans ce type de zone, il est impossible d'envoyer ou de recevoir des paquets de liaisons de données arbitraires (couche 2).

Par contre, dans les zones en mode IP exclusif, `zonecfg` attribue la totalité de la liaison de données spécifiée à la zone. Par conséquent, le superutilisateur ou l'utilisateur disposant du profil de droits requis peut envoyer les paquets falsifiés sur les liaisons de données dans une zone en mode IP exclusif, comme il peut le faire dans la zone globale. Vous pouvez désactiver l'usurpation d'adresse IP en définissant la propriété `allowed-address`. Pour la ressource `anet`, vous pouvez activer d'autres protections telles que `mac-nospoof` et `dhcp-nospoof` en définissant la propriété `link-protection`.

Utilisation simultanée de zones non globales en modes IP partagé et IP exclusif

Les zones en mode IP partagé partagent la couche IP avec la zone globale alors que les zones en mode IP exclusif possèdent leur propre instance de la couche IP. Ces deux types de zones peuvent être utilisées sur une même machine.

Systèmes de fichiers montés dans une zone

Chaque zone possède un jeu de données ZFS délégué par défaut. Ce jeu de données délégué par défaut imite la disposition des jeux de données de la zone globale par défaut. Un jeu de données nommé .../`rpool/ROOT` contient les environnements d'initialisation. Ce jeu de données ne doit pas être manipulé directement. Le jeu de données `rpool`, qui doit exister, est monté par défaut sous .../`rpool`. Les jeux de données .../`rpool/export` et .../`rpool/export/home` sont montés dans `/export` et `/export/home`. Ces jeux de données de zone non globale s'utilisent de la même façon que les jeux de données correspondants de la zone globale et peuvent être gérés à l'identique. L'administrateur de zone peut créer d'autres jeux de données au sein des jeux de données .../`rpool`, .../`rpool/export` et .../`rpool/export/home`.

N'utilisez *pas* la commande `zfs` décrite dans la page de manuel `zfs`(1M) pour créer, supprimer ou renommer des systèmes de fichiers dans la hiérarchie débutant par le système de fichiers de `rpool/ROOT` de la zone. La commande `zfs` peut servir à définir des propriétés autres que `canmount`, `mountpoint`, `sharesmb`, `zoned`, `com.oracle.*:*`, `com.sun:*` et `org.opensolaris.*.*`.

En règle générale, les systèmes de fichiers montés dans une zone comportent :

- Le jeu de systèmes de fichiers montés lors de l'initialisation de la plate-forme virtuelle
- Le jeu de systèmes de fichiers montés dans l'environnement applicatif lui-même

Ces jeux comprennent, par exemple, les systèmes de fichiers suivants :

- Systèmes de fichiers ZFS avec une propriété `mountpoint` définie sur une valeur autre que `none` ou `legacy` et qui comportent la valeur `yes` pour la propriété `canmount`.
- Systèmes de fichiers spécifiés dans le fichier `/etc/vfstab` d'une zone.
- Montages `AutoFS` et amorcés automatiquement par `AutoFS`. Les propriétés `autofs` sont définies à l'aide de la commande `sharectl` décrite dans la page de manuel `sharectl`(1M).
- Montages explicitement exécutés par un administrateur de zone.

  Les autorisations de montage des systèmes de fichiers dans une zone en cours d'exécution sont également définies par la propriété `zonecfg fs-allowed`. Cette propriété ne s'applique pas aux systèmes de fichiers montés dans la zone à l'aide des ressources `zonecfg add fs` ou `add dataset`. Par défaut, seuls les montages de systèmes de fichiers au sein d'un jeu de données délégué par défaut à une zone, `hsfs` les systèmes de fichiers et systèmes de fichiers réseau tels que NFS, sont autorisés au sein d'une zone.

Attention - Les montages autres que ceux par défaut exécutés dans l'environnement applicatif font l'objet de certaines restrictions. qui empêchent l'administrateur de zone de refuser de fournir des services au reste du système ou de réaliser des opérations affectant les autres zones.

Des restrictions de sécurité sont par ailleurs associées au montage de certains systèmes de fichiers à l'intérieur d'une zone et d'autres systèmes de fichiers ont un comportement particulier lorsqu'ils sont montés dans une zone. Vous trouverez des exemples d'utilisation à la section " Systèmes de fichiers et zones non globales " du manuel " Création et utilisation d'Oracle Solaris Zones ".

Pour plus d'informations sur les jeux de données, reportez-vous à la page de manuel `datasets`(5). Pour plus d'informations sur les environnements d'initialisation, reportez-vous à la section " Création et administration d'environnements d'initialisation Oracle Solaris 11.2 ".

Montages et mise à jour du système de fichiers

Il est impossible de monter un système de fichiers de manière à masquer tous les fichiers, liens symboliques ou répertoires faisant partie de l'image système de la zone, comme décrit dans la page de manuel `pkg`(5). Par exemple, si aucun des packages installés ne distribue des contenus dans `/usr/local`, il est possible de monter un système de fichiers sous `/usr/local`. Cependant, si un package quelconque, y compris un package SVR4 hérité, distribue un fichier, un répertoire ou un lien symbolique vers un chemin commençant par `/usr/local`, il n'est pas possible de monter système de fichiers dans `/usr/local`. Vous pouvez néanmoins monter un système de fichiers temporairement dans `/mnt`.

En raison de l'ordre de montage des systèmes de fichiers dans une zone, il est impossible qu'une ressource `fs` monte un système de fichiers dans `/export/filesys` si `/export` provient du jeu de données `rpool/export` de la zone ou d'un autre jeu de données délégué.

ID hôte dans les zones

Vous pouvez définir une propriété `hostid` pour la zone non globale différente de la propriété `hostid` de la zone globale. Cette opération est possible, par exemple, dans le cas d'une machine migrée vers une zone d'un autre système. Les applications désormais à l'intérieur de la zone peuvent dépendre de la propriété `hostid` d'origine. Pour plus d'informations, reportez-vous à la section “Types de ressources et propriétés” à la page 61.

Système de fichiers `/dev` dans les zones non globales

La commande `zonecfg` utilise un système basé sur des règles pour spécifier les périphériques qui doivent figurer dans une zone donnée. Les périphériques répondant à l'une de ces règles sont inclus dans le système de fichiers `/dev` de la zone. Pour plus d'informations, reportez-vous à “ Configuration d’une zone ” du manuel “ Création et utilisation d’Oracle Solaris Zones ”.

Périphérique `lofi` amovible dans les zones non globales

Un périphérique `lofi` de fichier loopback amovible, qui fonctionne comme un périphérique de CD-ROM, peut être configuré dans une zone non globale. Vous pouvez modifier le fichier auquel le périphérique est mappé et créer plusieurs périphériques `lofi` pour qu'ils utilisent le même fichier en mode lecture seule. Ce type de périphérique `lofi` est créé à l'aide de la commande `lofiadm` avec l'option `-r`. Aucun nom de fichier n'est requis au moment de la création. Au cours du cycle de vie d'un périphérique `lofi` amovible, un fichier peut être associé à un périphérique vide ou dissocié d'un périphérique qui n'est pas vide. Un fichier peut être associé simultanément à plusieurs périphériques `lofi` amovibles en toute sécurité. Un périphérique `lofi` amovible est en lecture seule. Vous ne pouvez pas mapper un fichier ayant été mappé à un périphérique `lofi` monté en lecture-écriture ou à un périphérique `lofi` amovible. Le nombre de périphériques `lofi` potentiels est limité par le contrôle de ressources `zone.max-lofi` qui peut être défini à l'aide de `zonecfg`(1M) dans la zone globale.

Une fois créé, un périphérique `lofi` amovible est en lecture seule. Le pilote `lofi` renverra une erreur ou toute opération d'écriture vers un périphérique `lofi` amovible.

La commande `lofiadm` permet également de répertorier les périphériques `lofi` amovibles.

EXEMPLE 2-2 Création d'un périphérique `lofi` amovible avec un fichier associé

```
# lofiadm -r /path/to/file
```

```
/dev/lofi/1
```

EXEMPLE 2-3 Création d'un périphérique `lofi` amovible vide

```
# lofiadm -r
/dev/lofi/2
```

EXEMPLE 2-4 Insertion d'un fichier dans un périphérique `lofi` amovible

```
# lofiadm -r /path/to/file /dev/lofi/1
/dev/lofi/1
```

Pour plus d'informations, reportez-vous aux pages de manuel `lofiadm`(1M), `zonecfg`(1M) et `lofi`(7D). Reportez-vous également au Tableau 2-2, “Contrôles de ressources à l'échelle d'une zone”.

Prise en charge des formats de disque dans les zones non globales

Le partitionnement de disque et l'utilisation de la commande `uscsi` sont permis grâce à l'outil `zonecfg`. Reportez-vous à `device` dans la section “Propriétés des types de ressources” à la page 67 pour obtenir un exemple. Pour plus d'informations sur la commande `uscsi`, reportez-vous à la page de manuel `uscsi`(7I).

- La délégation est prise en charge uniquement pour les zones `solaris`.
- Les disques doivent utiliser la cible `sd` comme indiqué à l'aide de la commande `prtconf` avec l'option `-D`. Reportez-vous à la page de manuel `prtconf`(1M).

Ressources de périphérique de zones de noyau avec des URI de stockage

La prise en charge suivante est disponible :

- `solaris-kz` prend en charge les propriétés `bootpri` et `id` dans les ressources de périphérique.
  - Définissez `bootpri` uniquement sur les disques qui feront partie du pool root de la zone. Si vous définissez bootpri sur des disques qui **ne feront pas** partie du pool root de la zone, vous risquez d'endommager les données enregistrées sur le disque.
  - `id` contrôle l'instance du disque dans la zone de noyau. Par exemple, `id=5` signifie que le disque sera `c1d5` dans la zone.

- Le zpool root qui a été créé sur des disques `solaris-kz` amorçables peut être importé dans la zone globale pendant l'installation. A ce stade, le zpool root est visible sur exécution de la commande `zpool`. Pour plus d'informations, reportez-vous à la page de manuel `zpool`(1M).

Privilèges configurables

Lorsque vous initialisez une zone, un jeu par défaut de privilèges, un jeu par défaut de privilèges *fiables* est inclus dans la configuration. Ces privilèges sont jugés fiables, car ils évitent que tout processus privilégié d'une zone affecte les processus d'autres zones non globales du système ou de la zone globale. La commande `zonecfg` permet :

- D'ajouter des privilèges au jeu par défaut, étant entendu que ces modifications risquent de permettre aux processus d'une zone de contrôler une ressource globale et donc d'affecter les processus d'autres zones.
- De supprimer des privilèges du jeu par défaut, étant entendu que ces modifications risquent d'empêcher certains processus de fonctionner correctement si ces privilèges sont nécessaires à leur exécution.

Remarque - Certains privilèges ne peuvent pas être supprimés du jeu de privilèges par défaut d'une zone et d'autres ne peuvent actuellement pas y être ajoutés.

Pour plus d'informations, reportez-vous à la section " Privilèges dans une zone non globale " du manuel " Création et utilisation d'Oracle Solaris Zones ", " Configuration d'une zone " du manuel " Création et utilisation d'Oracle Solaris Zones " et à la page de manuel `privileges`(5).

Association de pools de ressources

Si vous avez configuré des pools de ressources sur votre système, comme décrit dans le Chapitre 13, " Création et administration des pools de ressources (tâches) " du manuel " Administration de la gestion des ressources dans Oracle Solaris 11.2 ", vous pouvez utiliser la propriété `pool` pour associer la zone à l'un des pools de ressources lorsque vous la configurez.

Vous pouvez spécifier, à l'aide de la ressource `dedicated-cpu`, qu'un sous-ensemble des processeurs du système doit être dédié à une zone non globale tant que celle-ci est en cours d'exécution. Vous pouvez utiliser les propriétés `dedicated-cpu` pour assigner des CPU, des coeurs et des sockets à une zone. Le système crée de manière dynamique un pool temporaire destiné à être utilisé lorsque la zone est en cours d'exécution. Vous pouvez propager les paramètres du pool pendant les migrations en les spécifiant dans la commande `zonecfg`. Si vous configurez des zones de noyau Oracle Solaris, reportez-vous également à la ressource `virtual-cpu`.

La propriété `pool` peut servir à configurer plusieurs zones partageant le même pool.

Remarque - Toute configuration de zone utilisant un pool permanent défini par le biais de la propriété `pool` est incompatible avec un pool temporaire configuré à l'aide de la ressource `dedicated-cpu`. Vous ne pouvez définir que l'une de ces deux propriétés.

Paramétrage des contrôles de ressources à l'échelle de la zone

L'administrateur global ou un utilisateur disposant des autorisations appropriées peut définir des contrôles de ressources privilégiés à l'échelle d'une zone. L'intérêt de ces contrôles est de limiter l'utilisation des ressources totales pour l'ensemble des entités processus à l'intérieur d'une zone.

La commande `zonecfg` permet de spécifier ces limites, pour les zones globales et non globales. Reportez-vous à la section " Configuration d'une zone " du manuel " Création et utilisation d'Oracle Solaris Zones ".

La méthode conseillée, et la plus simple, pour définir un contrôle de ressource à l'échelle de la zone consiste à utiliser le nom de la propriété ou la ressource, par exemple `capped-cpu` au lieu de la ressource `rctl` tel que `cpu-cap`.

Le contrôle de ressources `zone.cpu-cap` définit une limite absolue pour la quantité de ressources CPU consommée par une zone. La valeur `100` représente 100 pourcent d'une CPU selon le paramètre . La valeur `125` équivaut à 125 pourcent, car 100 pourcent correspond à une capacité de CPU complète sur le système.

Remarque - Lors de la définition de la ressource `capped-cpu`, il est possible de définir un nombre décimal pour l'unité. La valeur correspond au contrôle de ressources `zone.cpu-cap`, mais est réduite par 100. La valeur `1` équivaut à la valeur `100` pour le contrôle de ressource.

Le contrôle de ressources `zone.cpu-shares` permet de limiter le nombre de parts de CPU FSS pour une zone. Les parts de CPU sont tout d'abord allouées à la zone, puis subdivisées entre les projets à l'intérieur de celle-ci comme spécifié dans les entrées `project.cpu-shares`. Pour plus d'informations, reportez-vous à la section " Utilisation de l'ordonnanceur FSS sur un système Oracle Solaris doté de zones " du manuel " Création et utilisation d'Oracle Solaris Zones ". Le nom de propriété globale de ce contrôle est `cpu-shares`.

Le contrôle de ressources `zone.max-locked-memory` permet de restreindre la quantité de mémoire physique verrouillée disponible dans une zone. L'allocation de la ressource de mémoire verrouillée sur les projets de la zone peut être gérée à l'aide du contrôle de ressource `project.max-locked-memory`. Pour plus d'informations, reportez-vous à la section " Contrôles de ressources disponibles " du manuel " Administration de la gestion des ressources dans Oracle Solaris 11.2 ".

Le contrôle de ressources `zone.max-lofi` restreint le nombre potentiel de périphériques `lofi` qu'une zone peut créer.

Le contrôle de ressources `zone.max-lwps` renforce l'isolement en empêchant que la présence de trop nombreux LWP dans une zone affecte d'autres zones. Le contrôle de ressource `project.max-lwps` permet de contrôler l'allocation de la ressource LWP aux différents projets à l'intérieur de la zone. Pour plus d'informations, reportez-vous à la section " Contrôles de ressources disponibles " du manuel " Administration de la gestion des ressources dans Oracle Solaris 11.2 ". Le nom de propriété globale de ce contrôle est `max-lwps`.

Le contrôle de ressource `zone.max-processes` renforce l'isolement en empêchant l'utilisation d'un trop grand nombre d'emplacements de table de processus dans une zone, au détriment d'autres zones. L'allocation de la ressource des emplacements de table de processus sur les projets de la zone peut être définie à l'aide du contrôle de ressources `project.max-processes` décrit dans la section " Contrôles de ressources disponibles " du manuel " Administration de la gestion des ressources dans Oracle Solaris 11.2 ". Le nom de propriété globale de ce contrôle est `max-processes`. Le contrôle de ressource `zone.max-processes` peut également englober le contrôle de ressource `zone.max-lwps`. Si `zone.max-processes` est défini, mais pas `zone.max-lwps`, alors `zone.max-lwps` est implicitement défini sur la valeur `zone.max-processes` multipliée par 10 lorsque la zone est initialisée. Notez que, dans la mesure où les processus standard et zombie utilisent tous deux les emplacements de table de processus, le contrôle `max-processes` offre une protection contre les zombies qui épuisent la table de processus. Les processus zombie ne possédant, par définition, aucun LWP, le contrôle `max-lwps` n'offre aucune protection contre cette possibilité.

Les contrôles de ressources `zone.max-msg-ids`, `zone.max-sem-ids`, `zone.max-shm-ids` et `zone.max-shm-memory` permettent de limiter les ressources System V utilisées par tous les processus à l'intérieur d'une zone. Vous pouvez contrôler l'allocation des ressources System V aux différents projets à l'intérieur de la zone à l'aide des versions de projet de ces contrôles de ressources. Les noms de propriétés globales de ces contrôles sont `max-msg-ids`, `max-sem-ids`, `max-shm-ids` et `max-shm-memory`.

Le contrôle de ressources `zone.max-swap` permet de limiter le swap consommé par les mappages d'espace d'adressage des processus utilisateur et les montages `tmpfs` à l'intérieur d'une zone. La commande `prstat -Z` affiche une colonne SWAP indiquant le swap total consommé par les montages `tmpfs` et les processus de la zone. Cette valeur facilite la surveillance du swap réservé par chaque zone, qui peut être utilisé pour choisir un paramètre `zone.max-swap` adéquat.

TABLEAU 2-2 Contrôles de ressources à l'échelle d'une zone

Nom du contrôle	Nom de propriété globale	Description	Unité par défaut	Valeur utilisée par
`zone.cpu-cap`		Limite absolue pour la quantité de ressources CPU correspondant à cette zone.	Quantité (nombre de CPU),	

Nom du contrôle	Nom de propriété globale	Description	Unité par défaut	Valeur utilisée par
			exprimée en pourcentage **Remarque -** Lors de la définition de la ressource `capped-cpu`, il est possible de définir un nombre décimal pour l'unité.	
`zone.cpu-shares`	`cpu-shares`	Nombre de partages CPU de l'ordonnanceur FSS pour cette zone.	Quantité (partages)	
`zone.max-locked-memory`		Quantité totale de mémoire physique verrouillée accessible par une zone. Si `priv_proc_lock_memory` est assigné à une zone, envisagez de paramétrer également ce contrôle de ressource pour empêcher cette zone de verrouiller toute la mémoire.	Taille (octets)	Propriété `locked` de `capped-memory`
`zone.max-lofi`	`max-lofi`	Limitation du nombre potentiel de périphériques `lofi` qu'une zone peut créer.	Quantité (nombre de périphériques `lofi`)	
`zone.max-lwps`	`max-lwps`	Nombre maximum de LWP accessibles simultanément par cette zone.	Quantité (LWP)	
`zone.max-msg-ids`	`max-msg-ids`	Nombre maximum d'ID de file d'attente des messages autorisé pour cette zone.	Quantité (ID de file d'attente des messages)	
`zone.max-processes`	`max-processes`	Nombre maximum d'emplacements de table de processus simultanément disponibles pour cette zone.	Quantité (emplacements de table de processus)	
`zone.max-sem-ids`	`max-sem-ids`	Nombre maximum d'ID de sémaphore autorisé pour cette zone.	Quantité (ID de sémaphore)	

Nom du contrôle	Nom de propriété globale	Description	Unité par défaut	Valeur utilisée par
zone.max-shm-ids	max-shm-ids	Nombre maximum d'ID de mémoire partagée autorisé pour cette zone.	Quantité (ID de mémoire partagée)	
zone.max-shm-memory	max-shm-memory	Quantité totale de mémoire partagée System V autorisée pour cette zone.	Taille (octets)	
zone.max-swap		Quantité totale de swap utilisable par les mappages d'espace d'adressage des processus utilisateur et les montages tmpfs pour cette zone.	Taille (octets)	Propriété swap de capped-memory

Vous pouvez spécifier ces limites en exécutant les processus à l'aide de la commande prctl. Vous trouverez un exemple sous la section " Définition de partages FSS dans la zone globale à l'aide de la commande prctl " du manuel " Création et utilisation d'Oracle Solaris Zones ". Les limites spécifiées à l'aide de la commande prctl ne sont pas persistantes. Elles perdent leur effet dès que vous réinitialisez le système.

Ajout d'un commentaire à une zone

Le type de ressource attr permet d'ajouter un commentaire à une zone. Pour plus d'informations, reportez-vous à " Configuration d'une zone " du manuel " Création et utilisation d'Oracle Solaris Zones ".

Utilisation de la commande zonecfg

La commande zonecfg, décrite dans la page de manuel zonecfg(1M), permet de configurer une zone non globale.

La commande zonecfg permet également de spécifier de manière permanente les paramètres de gestion des ressources pour la zone globale. Par exemple, vous pouvez utiliser la commande pour configurer la zone globale de façon à ce qu'elle utilise une CPU dédiée à l'aide de la ressource dedicated-cpu.

La commande zonecfg peut être utilisée dans différents modes : interactif, ligne de commande ou fichier de commandes. Elle permet d'effectuer les opérations suivantes :

- Créer ou supprimer (détruire) la configuration d'une zone
- Ajouter des ressources à une configuration donnée

- Définir les propriétés des ressources ajoutées à une configuration
- Supprimer les ressources d'une configuration donnée
- Interroger ou vérifier une configuration
- Valider une configuration
- Rétablir une configuration antérieure
- Renommer une zone
- Quitter une session zonecfg

L'invite zonecfg se présente sous la forme suivante :

```
zonecfg:zonename>
```

Lorsque vous configurez un type de ressource donné, par exemple un système de fichiers, celui-ci figure également dans l'invite :

```
zonecfg:zonename:fs>
```

Pour plus d'informations, notamment sur l'utilisation des différents composants zonecfg décrits dans ce chapitre, reportez-vous au Chapitre 1, “ Planification et configuration de zones non globales ” du manuel “ Création et utilisation d’Oracle Solaris Zones ”.

Modes d'exécution de zonecfg

Le concept d'*étendue* s'applique à l'interface utilisateur. L'étendue peut être *globale* ou *propre à une ressource*. Par défaut, elle est globale.

Lorsque l'étendue est globale, les sous-commandes add et select permettent de sélectionner une ressource spécifique. L'étendue devient alors propre à ce type de ressource.

- Dans le cas de add, utilisez la sous-commande end ou cancel pour terminer la spécification de la ressource.
- Dans le cas de select, utilisez la sous-commande end ou cancel pour terminer la modification de la ressource.

L'étendue globale est alors rétablie.

Certaines sous-commandes telles que add, remove et set possèdent une sémantique différente dans chaque type d'étendue.

Mode d'exécution interactif de zonecfg

En mode interactif, les commandes ci-dessous sont prises en charge. Pour plus d'informations sur la sémantique et les options utilisées avec ces sous-commandes, reportez-vous à la page

de manuel zonecfg(1M). Avant d'exécuter une sous-commande susceptible d'entraîner la destruction ou une perte de données, le système demande confirmation à l'utilisateur. L'option -F (force) permet d'ignorer cette confirmation.

help — Imprime l'aide générale ou affiche l'aide concernant une ressource donnée.

```
zonecfg:my-zone:capped-cpu> help
```

create — Commence à créer une configuration en mémoire pour la nouvelle zone spécifiée à l'une des fins suivantes :

- Pour appliquer les paramètres Oracle Solaris par défaut à une nouvelle configuration (méthode par défaut).
- Avec l'option -t *template*, pour créer une configuration identique au modèle spécifié. Le nom de zone (celui du modèle) est remplacé par le nouveau nom de la zone.
- Avec l'option -F, pour écraser la configuration existante.
- Avec l'option -b, pour créer une configuration vide, dans laquelle rien n'est défini.

export — Imprime la configuration sur la sortie standard ou dans le fichier de sortie spécifié, sous une forme pouvant être utilisée dans un fichier de commandes.

add — En étendue globale, ajoute le type de ressource spécifié à la configuration.

En étendue spécifique, ajoute au nom donné une propriété possédant la valeur donnée.

Pour plus d'informations, reportez-vous à la section " Configuration d'une zone " du manuel " Création et utilisation d'Oracle Solaris Zones " et à la page de manuel zonecfg(1M).

set — Assigne un nom de propriété donné à une valeur de propriété donnée. Notez que certaines propriétés telles que zonepath sont globales, alors que d'autres sont spécifiques aux ressources. Cette commande est donc applicable quel que soit le type d'étendue : globale ou propre à une ressource.

select — Uniquement applicable en étendue globale. Sélectionne la ressource de type donné répondant à la paire de critères nom de propriété-valeur de propriété donnés en vue de sa modification. L'étendue devient alors propre à ce type de ressource. Pour que la ressource soit identifiée de manière unique, vous devez spécifier un nombre suffisant de paires nom-valeur de propriété.

`clear` — Efface la valeur des paramètres optionnels. Les paramètres requis ne peuvent pas être effacés. Vous pouvez cependant modifier certains d'entre eux en leur assignant une nouvelle valeur. L'exécution de la commande `clear` sur une propriété rétablit la valeur par défaut de la propriété.

`remove` — En étendue globale, supprime le type de ressource spécifié. Pour que le type de ressource soit identifié de manière unique, vous devez spécifier un nombre suffisant de paires nom-valeur de propriété. Si aucune paire nom-valeur de propriété n'est spécifiée, toutes les instances sont supprimées. S'il en existe plus d'une, le système vous demande confirmation, sauf si vous avez spécifié l'option `-F`.

En étendue spécifique, supprime la paire nom-valeur de propriété spécifiée de la ressource actuelle.

`end` — Uniquement applicable en étendue spécifique. Arrête la spécification de la ressource.

La commande `zonecfg` permet ensuite de vérifier si la ressource actuelle est entièrement spécifiée.

- Le cas échéant, elle est ajoutée à la configuration en mémoire et l'étendue redevient globale.
- Dans le cas contraire, c'est-à-dire si la spécification est incomplète, le système affiche un message d'erreur indiquant la marche à suivre.

`cancel` — Uniquement applicable en étendue spécifique. Arrête la spécification de la ressource et rétablit l'étendue globale. Les ressources partiellement spécifiées ne sont pas conservées.

`delete` — Détruit la configuration spécifiée. Efface la configuration de la mémoire et des unités de stockage stables. Avec `delete`, vous devez utiliser l'option `-F` (force).

Attention - Cette action est instantanée. Elle ne requiert aucune validation et toute zone supprimée ne peut être rétablie.

`info` — Affiche des informations sur la configuration actuelle ou sur les propriétés de ressources globales `zonepath`, `autoboot` et `pool`. Si un type de ressource est spécifié, cette sous-commande affiche uniquement des informations sur les ressources de ce type. En étendue spécifique, elle s'applique uniquement à la ressource en cours d'ajout ou de modification.

`verify` — Vérifie si la configuration actuelle est correcte. S'assure que toutes les propriétés requises des ressources sont spécifiées. Vérifiez la syntaxe de n'importe quel groupe de ressources `rootzpool` et de ses propriétés. L'accessibilité d'un stockage spécifié par un URI n'est pas vérifiée.

`commit` — Valide la configuration actuelle, de la mémoire vers l'unité de stockage stable. Tant que la configuration en mémoire n'est pas validée, les changements peuvent être supprimés à l'aide de la sous-commande `revert`. Pour être utilisée par `zoneadm`, la configuration doit être validée. Cette opération s'effectue automatiquement lorsque vous arrêtez une session `zonecfg`. Seules les configurations correctes peuvent être validées. C'est pourquoi elles sont automatiquement vérifiées.

`revert` — Rétablit le dernier état validé de la configuration.

`exit` — Quitte la session `zonecfg`. Vous pouvez utiliser l'option `-F` (force) avec `exit`.

Au besoin, la commande `commit` s'exécute automatiquement. Notez que vous pouvez également utiliser une marque de fin de fichier (EOF, End Of File) pour quitter la session.

Mode d'exécution fichier de commandes de `zonecfg`

En mode fichier de commandes, l'entrée est extraite d'un fichier. La sous-commande `export` décrite à la section “Mode d'exécution interactif de `zonecfg`” à la page 58 permet de produire ce fichier. La configuration peut être imprimée sur la sortie standard ou dans le fichier de sortie spécifié à l'aide de l'option `-f`.

Données de configuration de zones

Les données de configuration de zone sont constituées de deux types d'entités : les ressources et les propriétés. Les ressources sont classées par type et chacune d'entre elles possède une propriété ou un jeu de propriétés. Ces propriétés ont un nom et possèdent des valeurs. Le jeu de propriétés dépend du type de ressource.

Les seules propriétés requises sont `zonename` et `zonepath`.

Types de ressources et propriétés

Les types de ressources et de propriétés sont décrits comme suit :

`zonename` — Nom de la zone. Les règles suivantes s'appliquent aux noms de zones :

- Chaque zone doit posséder un nom unique.
- Les noms de zones sont sensibles à la casse.
- Ils doivent commencer par un caractère alphanumérique.

  Ils peuvent contenir des caractères alphanumériques, des traits de soulignement (_), des traits d'union (-) et des points (.)
- Les noms de zones ne doivent pas comporter plus de 63 caractères.
- Le nom `global` est réservé à la zone globale.
- Les noms commençant par `SYS` sont réservés et ne peuvent pas être utilisés.

`zonepath`

La propriété `zonepath` spécifie le chemin d'installation de la zone. Le chemin du répertoire root de chaque zone est lié au répertoire root de la zone globale. Lors de l'installation, le répertoire de la zone globale est requis pour bénéficier d'une visibilité limitée. Le répertoire des zones doit appartenir à `root` et être en mode `700`. Si le chemin de la zone n'existe pas, il est automatiquement créé pendant l'installation. Si les autorisations sont incorrectes, elles seront automatiquement corrigées.

Le chemin du répertoire root des zones non globales se trouve un niveau en dessous. Le propriétaire et les droits d'accès du répertoire root de ces zones sont identiques à ceux du répertoire root (`/`) de la zone globale. Le répertoire des zones doit appartenir à `root` et être en mode `755`. Cette hiérarchie permet d'éviter que les utilisateurs ne possédant pas de privilèges dans la zone globale puissent traverser le système de fichiers d'une zone non globale.

La zone doit résider sur un jeu de données ZFS. Le jeu de données ZFS est automatiquement créé lorsque la zone est installée ou jointe. Si un jeu de données ZFS ne peut pas être créé, l'installation ou la jonction de la zone est impossible.

Chemin	Description
`/zones/my-zone`	`zonecfg zonepath`
`/zones/my-zone/root`	Root de la zone

Pour plus d'informations, reportez-vous à la section " Parcours des systèmes de fichiers " du manuel " Création et utilisation d'Oracle Solaris Zones ".

Dans la propriété `zonecfg template`, la valeur par défaut de `zonepath` est `/system/zones/`*zonename*.

Remarque - Vous pouvez déplacer une zone vers un autre emplacement du même système en spécifiant un nouveau chemin complet `zonepath` à l'aide de la sous-commande `move` de `zoneadm`. Vous trouverez des instructions à la section " Déplacement d'une zone non globale " du manuel " Création et utilisation d'Oracle Solaris Zones ".

`autoboot`

Si cette propriété est définie sur `true`, l'initialisation de la zone globale entraîne automatiquement celle de la zone. Elle est définie sur `false` par défaut. Notez cependant que, quelle que soit la valeur de cette propriété, la zone ne s'initialise pas automatiquement si le service `svc:/system/zones:default` des zones est désactivé. Vous pouvez l'activer à l'aide de la commande `svcadm`, décrite dans la page de manuel `svcadm`(1M) :

```
global# svcadm enable zones
```

Pour plus d'informations sur ce réglage au cours de la mise à jour de `pkg`, reportez-vous à la section " Présentation de l'empaquetage des zones " du manuel " Création et utilisation d'Oracle Solaris Zones ".

`bootargs`

Cette propriété permet de définir un argument d'initialisation pour la zone. Cet argument est appliqué, excepté s'il est ignoré par les commandes `reboot`, `zoneadm boot` ou `zoneadm reboot`. Reportez-vous à la section *Zone Boot Arguments*.

`limitpriv`

Cette propriété permet de spécifier un masque de privilège autre que celui par défaut. Reportez-vous à la section " Privilèges dans une zone non globale " du manuel " Création et utilisation d'Oracle Solaris Zones ".

Pour ajouter un privilège, spécifiez son nom en le faisant précéder ou non de `priv_`. Pour exclure un privilège, faites précéder son nom d'un tiret (`-`) ou d'un point d'exclamation (`!`). Les valeurs des privilèges doivent être séparées par des virgules et placées entre guillemets (`"`).

Comme décrit dans la page de manuel `priv_str_to_set`(3C), les jeux spéciaux de privilèges `none`, `all` et `basic` s'étendent à leur définition normale. Le jeu spécial de privilèges `zone` ne peut pas être utilisé, car la configuration des zones a lieu dans la zone globale. Etant donné qu'il est courant de modifier le jeu de privilèges par défaut en ajoutant ou en supprimant certains privilèges, le jeu spécial `default` est mappé avec le jeu de privilèges par défaut. Lorsque `default` figure au début de la propriété `limitpriv`, celle-ci s'applique au jeu par défaut.

L'entrée ci-dessous ajoute la capacité à utiliser des programmes DTrace requérant uniquement les privilèges `dtrace_proc` et `dtrace_user` dans la zone :

```
global# zonecfg -z userzone
zonecfg:userzone> set limitpriv="default,dtrace_proc,dtrace_user"
```

Si le jeu de privilèges de la zone contient un privilège annulé ou inconnu, ou s'il lui manque un privilège, toute tentative de vérification, de préparation ou d'initialisation de la zone échoue et un message d'erreur s'affiche.

`scheduling-class` — Cette propriété définit la classe de programmation de la zone. Pour obtenir informations et conseils, reportez-vous à la section “Classe de programmation” à la page 39.

`ip-type` — Cette propriété doit être obligatoirement définie pour toutes les zones non globales. Reportez-vous aux sections “Zones non globales en mode IP exclusif” à la page 46, “Zones non globales en mode IP partagé” à la page 46 et “ Configuration d’une zone ” du manuel “ Création et utilisation d’Oracle Solaris Zones ”.

`dedicated-cpu` — Cette ressource consacre un sous-ensemble des processeurs du système à la zone tant qu'elle est en cours d'exécution. La ressource `dedicated-cpu` définit les limites de `ncpus` et éventuellement d'`importance`. `ncores`, de `cores` et de `sockets`. Pour plus d'informations, reportez-vous à la section “Ressource `dedicated-cpu`” à la page 37.

solaris-kz uniquement : `virtual-cpu` — Cette ressource `solaris-kz` consacre un sous-ensemble des processeurs du système à la zone tant qu'elle est en cours d'exécution. La ressource `virtual-cpu` définit les limites de `ncpus`. Pour plus d'informations, reportez-vous à la section “`solaris-kz` uniquement : ressource `virtual-cpu`” à la page 38.

`capped-cpu` — Cette ressource définit une limite pour la quantité de ressources CPU que la zone peut consommer lors de son exécution. La ressource `capped-cpu` fournit une limite pour `ncpus`. Pour plus d'informations, reportez-vous à la section “Ressource `capped-cpu`” à la page 38.

`capped-memory` — Cette ressource regroupe les propriétés utilisées lors de la limitation de la mémoire de la zone. La ressource `capped-memory` définit les limites de la mémoire `physical`, `swap`, et `locked`. Vous devez spécifier au moins une de ces propriétés. Pour utiliser la ressource `capped-memory`, le package `service/resource-cap` doit être installé dans la zone globale.

`anet` — La ressource `anet` crée automatiquement une interface VNIC temporaire pour la zone en mode IP exclusif lors de l'initialisation de la zone et la supprime lorsque la zone s'arrête.

`net`

La ressource net affecte une interface réseau de la zone globale à la zone non globale. La ressource de l'interface réseau est le nom de l'interface. Chaque zone peut posséder des interfaces réseau. Elles sont paramétrées lorsque la zone passe de l'état installé à l'état prêt.

`dataset`

Jeu de données est un terme générique désignant un système de fichiers, un volume ou un instantané. L'ajout d'une ressource de jeu de données ZFS™ permet la délégation de l'administration du stockage à une zone non globale. Si le jeu de données délégué est un système de fichiers, l'administrateur de zone peut créer et détruire des systèmes de fichiers au sein de ce jeu de données et modifier les propriétés de l'ensemble de données. L'administrateur de zone peut créer des instantanés, des systèmes de fichiers et volumes enfant, ainsi que des clones de ses descendants. Si le jeu de données délégué est un volume, l'administrateur de zone peut en définir les propriétés et créer des instantanés. Il ne peut cependant ni affecter de jeux de données non ajoutés à la zone, ni dépasser les quotas de niveau maximum définis dans le jeu de données assigné à la zone. Après la délégation d'un jeu de données à une zone non globale, la propriété `zoned` est automatiquement définie. Un système de fichiers `zoned` ne peut pas être monté dans la zone globale car l'administrateur de zone peut être amené à définir le point de montage sur une valeur inacceptable.

Pour ajouter des jeux de données ZFS à une zone, vous pouvez procéder de l'une des manières suivantes :

- Comme pour un système de fichiers `lofs` monté, si le seul but recherché est de partager de l'espace avec la zone globale.
- Comme pour un jeu de données délégué

Lorsque la propriété `zonecfg template` est utilisée, si aucune ressource `rootzpool` n'est spécifiée, le jeu de données zonepath par défaut est *rootpool*`/VARSHARE/zones/`*zonename*. Le jeu de données a été créé par le service `svc-zones` avec un point de montage `/system/zones`. Les propriétés restantes sont héritées de *rootpool*`/VARSHARE/zones/`.

Reportez-vous au Chapitre 9, “ Rubriques avancées Oracle Solaris ZFS ” du manuel “ Gestion des systèmes de fichiers ZFS dans OracleSolaris 11.2 ”, à la section “ Systèmes de fichiers et zones non globales ” du manuel “ Création et utilisation d’Oracle Solaris Zones ” et à la page de manuel `datasets`(5).

Pour plus d'informations sur les questions relatives aux jeux de données, consultez également le Chapitre 13, “ Dépannage des problèmes liés à Oracle Solaris Zones ” du manuel “ Création et utilisation d’Oracle Solaris Zones ”.

`fs`

Toute zone peut posséder plusieurs systèmes de fichiers. Ils sont montés quand la zone passe de l'état installé à l'état prêt. La ressource du système de fichiers spécifie le chemin du point de montage du système de fichiers. Pour plus d'informations sur l'utilisation des systèmes de fichiers dans les zones, reportez-vous à la section " Systèmes de fichiers et zones non globales " du manuel " Création et utilisation d'Oracle Solaris Zones ".

Remarque - Pour utiliser les systèmes de fichiers UFS dans une zone non globale à l'aide de la ressource `fs`, le package `system/file-system/ufs` doit être installé dans la zone après l'installation ou par l'intermédiaire du script manifeste AI.

La commande `quota` documentée dans la page de manuel `quota`(1M) ne permet pas de récupérer les informations sur les quotas des systèmes de fichiers UFS ajoutés à l'aide de la ressource `fs`.

`fs-allowed`

La définition de cette propriété donne à l'administrateur de zone la possibilité de monter un système de fichiers de ce type, soit créé par l'administrateur de zone, soit importé à l'aide de NFS, et d'administrer ce système de fichiers. Les autorisations de montage des systèmes de fichiers dans une zone en cours d'exécution sont également restreintes par la propriété `fs-allowed`. Par défaut, seuls les montages de systèmes de fichiers`hsfs` et de systèmes de fichiers réseau, tels que NFS, sont autorisés au sein d'une zone.

La propriété peut être utilisée avec un périphérique en mode bloc ou un périphérique ZVOL délégué à la zone .

La propriété `fs-allowed` accepte une liste séparée par des virgules des autres systèmes de fichiers qui peuvent être montés au sein d'une zone, par exemple, `ufs,pcfs`.

```
zonecfg:my-zone> set fs-allowed=ufs,pcfs
```

Cette propriété n'a pas d'incidence sur les montages de zone gérés par la zone globale à l'aide des propriétés `add fs` ou `add dataset`.

Pour les questions liées à la sécurité, reportez-vous aux sections " Systèmes de fichiers et zones non globales " du manuel " Création et utilisation d'Oracle Solaris Zones " et " Utilisation de périphériques dans les zones non globales " du manuel " Création et utilisation d'Oracle Solaris Zones ".

`device`

La ressource `zonefigdevice` sert à ajouter des disques virtuels à la plate-forme d'une zone non globale. La ressource périphérique est le spécificateur correspondant au périphérique. Chaque zone peut présenter des périphériques qui doivent être configurés quand la zone passe de l'état installé à l'état prêt.

Remarque - Pour utiliser les systèmes de fichiers UFS dans une zone non globale à l'aide de la ressource `device`, le package `system/file-system/ufs` doit être installé dans la zone après l'installation ou par l'intermédiaire du script manifeste AI.

`pool`
: Cette propriété permet d'associer la zone à un pool de ressources sur le système. Plusieurs zones peuvent partager les ressources d'un pool. Reportez-vous également à la section “Ressource `dedicated-cpu`” à la page 37.

`rctl`
: La ressource `rctl` est dédiée aux contrôles de ressources à l'échelle de la zone. Ces contrôles sont activés lorsque la zone passe de l'état installé à l'état prêt.

  Pour plus d'informations, reportez-vous à la section “Paramétrage des contrôles de ressources à l'échelle de la zone” à la page 54.

Remarque - Pour configurer des contrôles à l'échelle d'une zone à l'aide de la sous-commande `set` *global_property_name* de `zonefig` au lieu de la ressource `rctl`, reportez-vous à la section “ Configuration d’une zone ” du manuel “ Création et utilisation d’Oracle Solaris Zones ”.

`attr`
: Cet attribut générique peut être utilisé pour les commentaires utilisateur ou par d'autres sous-systèmes. La propriété `name` d'un attribut `attr` doit commencer par un caractère alphanumérique. La propriété `name` peut contenir des caractères alphanumériques, des traits d'union (`-`) et des points (`.`). Les noms d'attributs commençant par `zone.` sont réservés au système.

Propriétés des types de ressources

Les ressources ont elles aussi des propriétés qu'il convient de configurer. Vous trouverez ci-dessous la liste des propriétés associées aux différents types de ressources.

`admin`
: Définissez le nom d'utilisateur et les autorisations associées pour une zone donnée.

```
zonecfg:my-zone> add admin
zonecfg:my-zone:admin> set user=zadmin
zonecfg:my-zone:admin> set auths=login,manage
zonecfg:my-zone:admin> end
```

  Les valeurs suivantes peuvent être utilisées pour la propriété `auths` :

  - `login` (`solaris.zone.login`)
  - `manage` (`solaris.zone.manage`)

- `clone` (`solaris.zone.clonefrom`)

Notez que ces valeurs `auths` ne permettent pas de créer une zone. Cette fonctionnalité est incluse dans le profil de sécurité de zone.

`solaris` **et** `solaris10` **uniquement :** `rootzpool`

`storage`

Identifiez l'URI de l'objet de stockage afin de fournir un zpool ZFS dédié pour l'installation de la zone. Pour des informations sur les URI et les valeurs autorisées pour `storage`, reportez-vous à la section “`solaris` et `solaris10` uniquement : ressource `rootzpool`” à la page 41. Durant l'installation de la zone, le zpool est créé automatiquement ou un zpool précréé est importé. Le nom *my-zone*_`rpool` est affecté.

```
zonecfg:my-zone> add rootzpool
zonecfg:my-zone:rootzpool> add storage dev:dsk/c4t1d0
zonecfg:my-zone:rootzpool> end
```

Vous pouvez ajouter une propriété `storage` supplémentaire si vous créez une configuration en miroir :

```
add storage dev:dsk/c4t1d0
add storage dev:dsk/c4t3d0
```

Une seule ressource `rootzpool` peut être configurée par zone.

`solaris` **et** `solaris10` **uniquement :** `zpool`

`storage`, `name`

Définissez un ou plusieurs URI d'objet de stockage pour déléguer un zpool à la zone. Pour des informations sur les URI et les valeurs autorisées pour `storage`, reportez-vous à la section “`solaris` et `solaris10` uniquement : ressource `rootzpool`” à la page 41. Les valeurs autorisées pour la propriété `name` sont définies dans la page de manuel `zpool`(1M).

Dans cet exemple, une ressource de stockage `zpool` est déléguée à la zone. Le zpool est automatiquement créé ou un zpool déjà créé est importé durant l'installation. Le nom du `zpool` est `my-zone_pool1`.

```
zonecfg:my-zone> add zpool
zonecfg:my-zone:zpool> set name=pool1
zonecfg:my-zone:zpool> add storage dev:dsk/c4t2d0
zonecfg:my-zone:zpool> add storage dev:dsk/c4t4d0
zonecfg:my-zone:zpool> end
```

Une configuration de zone peut contenir une ou plusieurs ressources `zpool`.

`dedicated-cpu`

`ncpus`, `importance`, `cores`, `cpus`, `sockets`

Spécifie le nombre de CPU et, éventuellement, l'importance relative du pool. L'exemple ci-dessous spécifie la plage de CPU utilisée par la zone `my-zone`. L'`importance` est également définie.

```
zonecfg:my-zone> add dedicated-cpu
zonecfg:my-zone:dedicated-cpu> set ncpus=1-3
zonecfg:my-zone:dedicated-cpu> set importance=2
zonecfg:my-zone:dedicated-cpu> end
```

Assignez de manière permanente les coeurs `0`, `1`, `2` et `3` à la zone `my-zone`. L'exemple `dedicated-cpu` suivant est basé sur *cores*, mais `cpus=`, `cores=` et `sockets=` permettent également d'effectuer l'assignation.

```
zonecfg:my-zone> add dedicated-cpu
zonecfg:my-zone:dedicated-cpu> set cores=0-3
zonecfg:my-zone:dedicated-cpu> end
```

`virtual-cpu`

`ncpus`

Définit le nombre de CPU. L'exemple ci-dessous spécifie une capacité de 3 CPU pour la zone `my-zone`.

```
zonecfg:my-zone> add virtual-cpu
zonecfg:my-zone:dedicated-cpu> set ncpus=3
zonecfg:my-zone:dedicated-cpu> end
```

`capped-cpu`

`ncpus`

Définit le nombre de CPU. L'exemple ci-dessous spécifie une capacité de 3,5 CPU pour la zone `my-zone`.

```
zonecfg:my-zone> add capped-cpu
zonecfg:my-zone:capped-cpu> set ncpus=3.5
zonecfg:my-zone:capped-cpu> end
```

`capped-memory`

`physical`, `swap`, `locked`

Spécifie les limites de mémoire pour la zone `my-zone`. Chaque limite est optionnelle, mais vous devez en définir au moins une.

```
zonecfg:my-zone> add capped-memory
zonecfg:my-zone:capped-memory> set physical=50m
zonecfg:my-zone:capped-memory> set swap=100m
zonecfg:my-zone:capped-memory> set locked=30m
zonecfg:my-zone:capped-memory> end
```

Pour utiliser la ressource `capped-memory`, le package `resource-cap` doit être installé dans la zone globale.

`fs`

`dir`, `special`, `raw`, `type`, `options`

Les paramètres de la ressource `fs` indiquent les valeurs qui déterminent comment et où monter les systèmes de fichiers. Les paramètres `fs` se définissent comme suit :

`dir`	Spécifie le point de montage du système de fichiers.
`special`	Spécifie le nom du périphérique spécial en mode bloc ou le répertoire de zone globale à monter.
`raw`	Spécifie le périphérique brut sur lequel `fsck` doit être exécuté avant le montage du système de fichiers (ne s'applique pas à ZFS).
`type`	Spécifie le type de système de fichiers.
`options`	Spécifie les options de montage similaires à celles associées à la commande `mount`.

L'exemple ci-dessous spécifie que le jeu de données nommé `pool1/fs1` dans la zone globale doit être monté en tant que `/shared/fs1` dans une zone en cours de configuration. Le type de système de fichiers à utiliser est ZFS.

```
zonecfg:my-zone> add fs
zonecfg:my-zone:fs> set dir=/shared/fs1
zonecfg:my-zone:fs> set special=pool1/fs1
zonecfg:my-zone:fs> set type=zfs
zonecfg:my-zone:fs> end
```

Pour plus d'informations, reportez-vous aux sections “ Option o nosuid ” du manuel “ Création et utilisation d’Oracle Solaris Zones ” et “ Restrictions de sécurité et comportement du système de fichiers ” du manuel “ Création et utilisation d’Oracle Solaris Zones ” et aux pages de manuel `fsck`(1M) et `mount`(1M). Notez aussi que la section 1M des pages de manuel est disponible pour les options de montage spécifiques à un système de fichiers donné. Ces pages de manuel sont nommées de la manière suivante : `mount_`*système de fichiers*.

Remarque - La commande `quota` documentée dans la page de manuel `quota`(1M) ne permet pas de récupérer les informations sur les quotas des systèmes de fichiers UFS ajoutés à l'aide de cette ressource.

`dataset name`, `alias`	`name`

L'exemple ci-dessous spécifie que le jeu de données *sales* doit être visible et monté dans la zone non globale et doit cesser d'être visible dans la zone globale.

```
zonecfg:my-zone> add dataset
zonecfg:my-zone> set name=tank/sales
zonecfg:my-zone> end
```

Un jeu de données délégué peut avoir un alias non par défaut comme indiqué dans l'exemple suivant. Notez que l'alias d'un jeu de données ne peut contenir de barre oblique (/).

```
zonecfg:my-zone> add dataset
zonecfg:my-zone:dataset> set name=tank/sales
zonecfg:my-zone:dataset> set alias=data
zonecfg:my-zone:dataset> end
```

Pour revenir à l'alias par défaut, utilisez `clear alias`.

```
zonecfg:my-zone> clear alias
```

`anet`

`linkname`, `lower-link`, `allowed-address`, `auto-mac-address`, `configure-allowed-address`, `defrouter`, `linkmode` (IPoIB), `mac-address` (non IPoIB), `mac-slot` (non IPoIB),`mac-prefix` (non IPoIB), `mtu`, `maxbw`, `pkey` (IPoIB), `priority`, `vlan-id` (non IPoIB), `rxfanout`, `rxrings`, `txrings`, `link-protection`, `allowed-dhcp-cids`

`solaris` **uniquement :** Ne définissez pas les propriétés `anet` suivantes pour les liaisons de données IPoIB dans `zonecfg`.

- `mac-address`
- `mac-prefix`
- `mac-slot`
- `vlan-id`

Ne définissez pas les propriétés `anet` suivantes pour les liaisons de données non IPoIB dans `zonecfg` .

- `linkmode`
- `pkey`

Définissez uniquement les propriétés suivantes de la ressource `anet` d'un commutateur EVS :

- linkname
- `evs`
- `vport`
- `configure-allowed-address`

La ressource `anet` crée une interface VNIC automatique ou une interface IPoIB lorsque la zone est initialisée et supprime l'interface VNIC ou IPoIB lorsque la zone s'arrête. Notez que la marque `solaris-kz` ne prend pas en charge IPoIB. Les propriétés de la ressource sont gérés par le biais de la commande `zonecfg`. Reportez-vous à la page de manuel `zonecfg`(1M) du texte complet sur les propriétés disponibles.

`lower-link`	Spécifie le lien sous-jacent du lien à créer. Lorsqu'il est défini sur `auto`, le démon `zoneadmd` choisit automatiquement le lien sur lequel la VNIC est créée à chaque initialisation de la zone. Vous pouvez spécifier toute liaison sur laquelle il est possible de créer une carte VNIC en tant que `lower-link` d'une ressource `anet`. Toutes les liaisons IPoIB sont ignorées lorsque vous sélectionnez la liaison de données pour créer automatiquement la VNIC lors de l'initialisation.
`linkname`	Indiquez un nom pour l'interface VNIC ou IPoIB créée automatiquement. Notez que `solaris-kz` ne prend pas en charge IPoIB.
`mac-address` **(pas pour IPoIB)**	Définit l'adresse MAC de la VNIC en fonction de la valeur ou du mot-clé indiqué. Si la valeur n'est pas un mot-clé, elle est interprétée comme une adresse MAC unicast. Pour connaître les mots-clés pris en charge, reportez-vous à la page de manuel `zonecfg`(1M). Si une adresse MAC aléatoire est sélectionnée, l'adresse générée est conservée pour toutes les initialisations de la zone, ainsi que pour les opérations de séparation et de jonction de zone. Si vous utilisez la stratégie par défaut `auto-mac-address`, Oracle Solaris Zones peut obtenir une adresse MAC (`mac-address`) aléatoire.
`pkey` **(IPoIB uniquement)**	Définissez la clé de partition à utiliser pour créer l'interface de liaison de données IPoIB. Cette propriété est obligatoire. La `pkey` spécifiée est toujours traitée au format hexadécimal, qu'elle contienne ou non le préfixe `0x`.

`linkmode` **(IPoIB uniquement)**
: Définit le `linkmode` pour l'interface de liaison de données. La valeur par défaut est `cm`. Les valeurs valides sont :

  `cm` (par défaut)
  : Mode connecté. Ce mode utilise une MTU par défaut de `65520` octets et supporte un total de MTU pouvant aller jusqu'à `65535` octets.

  `ud`
  : Mode datagramme non fiable. Si le mode connecté n'est pas disponible pour un noeud distant, le mode datagramme non fiable est utilisé à la place. Ce mode utilise une MTU par défaut de `2044` octets et supporte un total de MTU pouvant aller jusqu'à `4092` octets.

`allowed-address`
: Configure une adresse IP pour la zone en mode IP exclusif et permet également de limiter le jeu d'adresses IP configurables qu'une zone en mode IP exclusif peut utiliser. Pour spécifier plusieurs adresses, utilisez la liste des adresses IP séparées par des virgules.

`defrouter`
: La propriété `defrouter` peut être utilisée pour définir une route par défaut lorsque la zone non globale et la zone globale résident sur des réseaux distincts.

  Toute zone dont la propriété `defrouter` est définie doit se trouver sur un sous-réseau qui n'est pas configuré dans la zone globale.

Lorsque la commande `zonecfg` crée une zone à l'aide du modèle `SYSdefault`, une ressource `anet` avec les propriétés suivantes est automatiquement incluse dans la configuration de zone si aucune ressource IP n'est définie. `linkname` est automatiquement créé sur la liaison Ethernet physique et défini sur le premier nom disponible au format `net`*N*, `net`*0*. Pour modifier les valeurs par défaut, utilisez la commande `zonecfg`.

Lorsque vous utilisez la stratégie par défaut `auto`, une adresse MAC (`mac-address`) appropriée est assignée :

Zone Oracle Solaris	`mac-address` aléatoire
Zone de noyau Oracle Solaris	`mac-address` aléatoire
Zone Oracle Solaris sous zone de noyau	`mac-address` d'usine
Domaine invité Oracle VM Server for SPARC	`mac-address` d'usine
Zone de noyau Oracle Solaris s'exécutant sur domaine invité Oracle VM Server for SPARC	`mac-address` d'usine

La stratégie par défaut crée une VNIC automatique sur la liaison Ethernet physique, `net0` par exemple, et assigne l'adresse MAC à la VNIC. La propriété `lower-link` facultative est définie sur le lien sous-jacent, `vnic1`, sur lequel la VNIC automatique doit être créée. Vous pouvez spécifier les propriétés VNIC telles que le nom de lien, le lien physique sous-jacent, l'adresse MAC, la limite de bande passante, ainsi que d'autres propriétés à l'aide de la commande `zonecfg`. Notez que `ip-type=exclusive` doit également être spécifié.

```
zonecfg:my-zone> set ip-type=exclusive
zonecfg:my-zone> add anet
zonecfg:my-zone:anet> set linkname=net0
zonecfg:my-zone:anet> set lower-link=auto
zonecfg:my-zone:anet> set mac-address=random
zonecfg:my-zone:anet> set link-protection=mac-nospoof
zonecfg:my-zone:anet> end
```

L'exemple suivant montre une zone de marque `solaris` configurée avec une interface de liaison de données IPoIB sur la liaison physique `net5` avec la clé de partition IB `0xffff` :

```
zonecfg:my-zone> set ip-type=exclusive
zonecfg:my-zone:anet> add anet
zonecfg:my-zone:anet> set linkname=ib0
zonecfg:my-zone:anet> set lower-link=net5
zonecfg:my-zone:anet> set pkey=0xffff
zonecfg:my-zone:anet> end
```

Pour plus d'informations sur les propriétés, reportez-vous à la page de manuel zonecfg(1M). Pour plus d'informations sur les propriétés de lien, reportez-vous à la page de manuel dladm(1M).

net	address, allowed-addressphysical, defrouter

Remarque - Dans une zone en mode IP partagé, l'adresse IP et le périphérique physique doivent être tous deux spécifiés. Le routeur par défaut peut être défini (facultatif).

Dans une zone en mode IP exclusif, seule l'interface physique doit être spécifiée.

- La propriété allowed-address limite le jeu d'adresses IP configurables qu'une zone en mode IP exclusif peut utiliser.
- La propriété defrouter peut être utilisée pour définir une route par défaut lorsque la zone non globale et la zone globale résident sur des réseaux distincts.
- Toute zone dont la propriété defrouter est définie doit se trouver sur un sous-réseau qui n'est pas configuré dans la zone globale.
- Le trafic d'une zone avec un routeur par défaut est envoyé au routeur avant de revenir à la zone de destination.

Lorsque des zones en mode IP partagé existent sur des sous-réseaux différents, ne configurez aucune liaison de données dans la zone globale.

Dans l'exemple suivant d'une zone en mode IP partagé, l'interface physique nge0 est ajoutée à la zone avec l'adresse IP 192.168.0.1. Pour obtenir la liste des interfaces réseau sur le système, tapez :

```
global# ipadm show-if -po ifname,class,active,persistent
lo0:loopback:yes:46--
nge0:ip:yes:----
```

Chaque ligne de la sortie, à l'exception des lignes loopback, contient le nom d'une interface réseau. Les lignes dont les descriptions contiennent LOOPBACK ne concernent pas les cartes. Les indicateurs permanents 46 indiquent que l'interface est configurée de façon permanente dans la zone globale. La valeur active yes indique que l'interface est actuellement configurée et la valeur de classe ip indique que nge0 n'est pas une interface loopback. La route par défaut est définie sur 10.0.0.1 pour la zone. La définition de la propriété defrouter est facultative. Notez que ip-type=shared est obligatoire.

```
zonecfg:my-zone> set ip-type=shared
zonecfg:my-zone> add net
zonecfg:my-zone:net> set physical=vnic1
zonecfg:my-zone:net> set address=192.168.0.1
zonecfg:my-zone:net> set defrouter=10.0.0.1
```

```
zonecfg:my-zone:net> end
```

Dans l'exemple suivant d'une zone en mode IP exclusif, une VNIC est utilisée pour l'interface physique, qui est un VLAN. Pour connaître les liaisons de données disponibles, exécutez la commande `dladm show-link`. La propriété `allowed-address` restreint les adresses IP que la zone peut utiliser. La propriété `defrouter` sert à définir une route par défaut. Notez que `ip-type=exclusive` doit également être spécifié.

```
zonecfg:my-zone> set ip-type=exclusive
zonecfg:my-zone> add net
zonecfg:myzone:net> set allowed-address=10.1.1.32/24
zonecfg:my-zone:net> set physical=vnic1
zonecfg:myzone:net> set defrouter=10.1.1.1
zonecfg:my-zone:net> end
```

Seul le type correspondant aux périphériques physiques doit être spécifié dans l'étape `add net`. La propriété `physical` peut être une carte d'interface réseau virtuelle (VNIC).

Remarque - Le système d'exploitation Oracle™ Solaris prend en charge toutes les interfaces de type Ethernet et leurs liaisons de données peuvent être gérées avec la commande `dladm`.

`device`

`match`, `allow-partition`, `allow-raw-io`

Le nom du périphérique de correspondance peut être un modèle de correspondance ou un chemin absolu. Les propriétés `allow-partition` et `allow-raw-io` peuvent être définies sur `true` ou `false`. La valeur par défaut est `false`. `allow-partition` permet le partitionnement. `allow-raw-io` active `uscsi`. Pour plus d'informations sur ces ressources, reportez-vous à la page de manuel zonecfg(1M).

Les restrictions déterminant les spécifications possibles dans la propriété de ressource `device:match` pour les zones `solaris-kz` comprennent les règles suivantes :

- Une seule ressource est autorisée par LUN.
- Les tranches et les partitions ne sont pas prises en charge.
- Une prise en charge est disponible uniquement pour les périphériques de disque brut.
- Les chemins d'accès de périphérique pris en charge sont `lofi`, `ramdisk`, `dsk` et `zvols`.

Dans l'exemple suivant, les opérations `uscsi` sur un périphérique de disque sont incluses dans la configuration d'une zone `solaris`.

```
zonecfg:my-zone> add device
zonecfg:my-zone:device> set match=/dev/*dsk/cXtYdZ*
```

```
zonecfg:my-zone:device> set allow-raw-io=true
zonecfg:my-zone:device> end
```

Les périphériques du gestionnaire de volume Veritas sont délégués à une zone non globale à l'aide de `add device`.

L'exemple ci-dessous montre l'ajout d'un périphérique de stockage à une zone `solaris-kz` :

```
zonecfg:my-zone> add device
zonecfg:my-zone:device> set storage=iscsi:///
luname.naa.600144f03d70c80000004ea57da10001
zonecfg:my-zone:device> set bootpri=0
zonecfg:my-zone:device> end
```

Attention - Avant d'ajouter les périphériques, reportez-vous aux sections " Utilisation de périphériques dans les zones non globales " du manuel " Création et utilisation d'Oracle Solaris Zones ", " Exécution d'applications dans les zones non globales " du manuel " Création et utilisation d'Oracle Solaris Zones " et " Privilèges dans une zone non globale " du manuel " Création et utilisation d'Oracle Solaris Zones " pour les questions liées aux restrictions et à la sécurité.

`rctl`

`name`, `value`

A l'échelle des zones, les contrôles de ressources suivants sont disponibles :

- `zone.cpu-cap`
- `zone.cpu-shares` (recommandé : `cpu-shares`)
- `zone.max-locked-memory`
- `zone.max-lofi`
- `zone.max-lwps` (recommandé : `max-lwps`)
- `zone.max-msg-ids` (recommandé : `max-msg-ids`)
- `zone.max-processes`(recommandé : `max-processes`
- `zone.max-sem-ids` (recommandé : `max-sem-ids`)
- `zone.max-shm-ids` (recommandé : `max-shm-ids`)
- `zone.max-shm-memory` (recommandé : `max-shm-memory`)
- `zone.max-swap`

Pour définir un contrôle de ressources à l'échelle d'une zone, il est recommandé et plus simple d'utiliser le nom de propriété que la ressource `rctl`, comme indiqué à la section " Configuration d'une zone " du manuel " Création et utilisation d'Oracle Solaris Zones ". Si vous configurez les entrées de contrôle de ressources à l'échelle d'une zone à l'aide de `add rctl`, leur format diffère de celui des entrées de contrôle de ressources de la base de données `project`. Dans une configuration de

zone, le type de ressource `rctl` est composé de trois paires nom/valeur. Les noms sont `priv`, `limit` et `action`. Chacun d'entre eux possède une valeur simple.

```
zonecfg:my-zone> add rctl
zonecfg:my-zone:rctl> set name=zone.cpu-shares
zonecfg:my-zone:rctl> add value
 (priv=privileged,limit=10,action=none)
zonecfg:my-zone:rctl> end

zonecfg:my-zone> add rctl
zonecfg:my-zone:rctl> set name=zone.max-lwps
zonecfg:my-zone:rctl> add value
 (priv=privileged,limit=100,action=deny)
zonecfg:my-zone:rctl> end
```

Pour plus d'informations sur les attributs et les contrôles de ressources, reportez-vous au Chapitre 6, “ A propos des contrôles de ressources ” du manuel “ Administration de la gestion des ressources dans Oracle Solaris 11.2 ” et à la section “ Utilisation de contrôles de ressources dans les zones non globales ” du manuel “ Création et utilisation d’Oracle Solaris Zones ”.

`attr` — `name`, `type`, `value`

L'exemple ci-dessous montre l'ajout d'un commentaire à propos d'une zone.

```
zonecfg:my-zone> add attr
zonecfg:my-zone:attr> set name=comment
zonecfg:my-zone:attr> set type=string
zonecfg:my-zone:attr> set value="Production zone"
zonecfg:my-zone:attr> end
```

Vous pouvez utiliser la sous-commande `export` pour imprimer une configuration de zone sur une sortie standard. La configuration est enregistrée sous une forme pouvant être utilisée dans un fichier de commandes.

Bibliothèque d'édition de ligne de commande Tecla

La bibliothèque d'édition de ligne de commande Tecla est intégrée à la commande `zonecfg`. Elle fournit un support d'édition et d'accès à l'historique des lignes de commande.

Pour plus d'informations, reportez-vous à la page de manuel `tecla`(5).

Glossaire

administrateur de zone Les privilèges d'un administrateur de zone sont limités à une zone non globale.

Voir aussi administrateur global.

administrateur de zone non globale Voir administrateur de zone.

administrateur global Utilisateur root ou administrateur prenant le rôle root. Lorsqu'il est connecté à une zone globale, l'administrateur global ou un utilisateur possédant les autorisations appropriées peut surveiller et contrôler le système dans son ensemble.

Voir aussi administrateur de zone.

analyseur Thread de noyau qui identifie les pages rarement utilisées. En cas de mémoire insuffisante, l'analyseur récupère les pages qui n'ont pas été récemment utilisées.

base de données de service de noms Dans le chapitre Projets et tâches (présentation) du présent document, ce terme fait référence à la fois aux conteneurs LDAP et aux cartes NIS.

cap Seuil d'utilisation des ressources système.

charge de travail Somme de tous les processus d'une application ou d'un groupe d'applications.

comptabilisation étendue Moyen souple d'enregistrer la consommation des ressources sur la base d'une tâche ou d'un processus dans le système d'exploitation Solaris.

configuration dynamique Informations relatives à la disposition des ressources au sein de la structure des pools de ressources pour un système particulier et à un moment donné dans le temps.

configuration statique des pools Représentation de la manière dont un administrateur aimerait configurer un système en fonction des pools de ressources.

consommateur de ressource Il s'agit essentiellement d'un processus Solaris. Les modèles de processus tels que le projet et la tâche représentent des moyens de négocier l'utilisation des ressources en termes de consommation globale.

contrôle de ressource Limite prévue pour la consommation d'une ressource par processus, par tâche ou par projet.

CPU Dans le contexte des zones, se rapporte à un thread matériel.

démon de limitation des ressources Démon ayant pour fonction de réguler la consommation de la mémoire physique par les processus exécutés dans le cadre des projets concernés par la limitation des ressources.

démon des pools Démon système `poold` activé lorsque l'allocation dynamique des ressources est nécessaire.

état de zone Etat d'une zone non globale. L'état d'une zone peut être : configuré, incomplet, installé, prêt, indisponible, en cours d'exécution ou en cours de fermeture.

état de zone auxiliaire Utilisé pour communiquer des informations d'état supplémentaires à la zone globale. Voir aussi état de zone.

étendue globale Actions s'appliquant aux valeurs de chaque contrôle de ressource sur le système.

étendue locale Actions locales exercées dans le cadre d'un processus qui tente de dépasser la valeur de contrôle.

FSS Voir ordonnanceur FSS.

gestion des ressources Fonctionnalité permettant de contrôler l'utilisation des ressources système disponibles par les applications.

jeu de processeurs Regroupement disjoint de CPU. Chaque ensemble de processeurs peut contenir zéro, un ou plusieurs processeurs. Un jeu de processeurs est représenté dans la configuration des pools de ressources comme un élément de ressource. On parle aussi de "pset".

Voir aussi jeu disjoint.

jeu de processeurs par défaut Jeu de processeurs créé par le système lorsque les pools sont activés.

Voir aussi jeu de processeurs.

jeu disjoint Type de jeu dont les membres ne se chevauchent pas et ne sont pas dupliqués.

liaison de données Interface de niveau 2 de la pile de protocoles OSI, qui est représentée dans un système comme une interface STREAMS DLPI (v2). Cette interface peut être montée sous des piles de protocoles tels que TCP/IP. Dans le contexte des zones Oracle Solaris 10, des liaisons de

	données sont des interfaces physiques, des agrégations ou des interfaces à balises VLAN. Une liaison de données peut également désigner une interface physique, par exemple, lorsque l'on se réfère à une carte d'interface réseau ou à une carte d'interface réseau virtuelle.
limitation des ressources	Processus consistant à limiter l'utilisation des ressources système.
lot de ressources	Ressource pouvant être liée à un processus. Dans la plupart des cas, ce terme désigne les objets créés par un sous-système de noyau offrant une possibilité de partitionnement. Les classes de programmation et les jeux de processeurs sont des exemples de lots de ressources.
marque	Instance de la fonctionnalité BrandZ, qui fournit les zones non globales contenant des environnements d'exploitation non natifs servant à exécuter des applications.
mémoire verrouillée	Mémoire pour laquelle il est impossible de charger ou de décharger des pages.
Oracle Solaris 10 Zones	Technologie de partitionnement logiciel qui fournit un environnement d'exécution complet destiné aux applications Solaris 10 s'exécutant dans une zone marquée `solaris10` sur un système fonctionnant sous Oracle Solaris 11.
Oracle Solaris Kernel Zones	Technologie de partitionnement logiciel qui fournit un environnement complet de noyau et d'utilisateur dans une même zone et qui augmente également la séparation du noyau entre l'hôte et la zone.
Oracle Solaris Zones	Technologie de partitionnement logicielle utilisée pour virtualiser les services de système d'exploitation et fournir un environnement sécurisé, isolé, dans lequel exécuter des applications.
ordonnanceur FSS	Catégorie de programmation, aussi connue sous le nom FSS (Fair Share Scheduler), qui permet d'allouer du temps CPU en fonction des parts attribuées. Les parts définissent la portion des ressources CPU d'un système allouées à un projet.
partition d'une ressource	Sous-ensemble exclusif d'une ressource. La somme de toutes les partitions d'une ressource représente la quantité totale de la ressource disponible dans une seule instance Solaris en cours d'exécution.
pool	Voir pool de ressources.
pool de ressources	Mécanisme de configuration utilisé pour partitionner les ressources de la machine. Un pool de ressources représente une association entre des groupes de ressources susceptibles d'être partitionnées.
pool par défaut	Pool créé par le système lorsque les pools sont activés. Voir aussi pool de ressources.
projet	Identificateur administratif valide dans le réseau pour un travail.

reconfiguration dynamique Sur les systèmes SPARC, aptitude à reconfigurer le matériel en cours d'exécution du système. Cette fonctionnalité est également désignée par son acronyme anglais DR (Dynamic Reconfiguration).

ressource Aspect du système informatique pouvant être manipulé afin de modifier le comportement d'une application.

ressources CMT CPU, coeurs et sockets.

RSS Voir taille résidente définie.

seuil d'allocation restrictive Pourcentage d'utilisation de la mémoire physique sur le système au-delà duquel le démon de limitation des ressources applique l'allocation restrictive de mémoire.

tâche Dans le domaine de la gestion des ressources, ensemble des processus représentant un travail donné dans le temps. Chaque tâche est associée à un projet.

taille de travail Capacité du jeu de pages utilisé de façon active par la charge de travail d'un projet pendant son cycle de traitement.

taille résidente définie Capacité du jeu de pages résidant en mémoire physique.

tas Quantité de mémoire de travail allouée par processus.

WSS Voir aussi taille de travail.

zone en lecture seule Zone immuable configurée avec un root en lecture seule.

zone globale Zone contenue dans chaque système Oracle Solaris. En cas d'utilisation de zones non globales, la zone globale correspond à la fois à la zone par défaut du système et à la zone utilisée pour le contrôle administratif à l'échelle du système.

Voir aussi zone non globale.

zone marquée Environnement isolé dans lequel les applications non natives sont exécutées dans des zones non globales.

zone non globale Environnement de système d'exploitation virtualisé créé dans une instance unique du système d'exploitation Oracle Solaris. La technologie de partitionnement logicielle Oracle Solaris Zones est utilisée pour virtualiser les services de système d'exploitation.

zone root entière Type de zone non globale dans laquelle tous les logiciels système requis et tous les packages supplémentaires sont installés sur les systèmes de fichiers privés de la zone.

Index