Nouveautés d'Oracle® Solaris 11.4

Août 2018

Référence: E74962-01

Ce document présente toutes les fonctions introduites ou améliorées dans Oracle Solaris 11.4.

Fonctions clés d'Oracle Solaris 11.4

Oracle Solaris est une plate-forme rapide et sécurisée, conçue pour les déploiements d'entreprise d'envergure. Oracle Solaris offre des fonctions de mise à jour simple, desurveillance de la conformité, de surveillance des performances et de virtualisation sans temps système pour l'isolement des charges de travail stratégiques.

Sécurité et conformité éprouvées et automatisées :

- Protocole KMIP (Key Management Interoperability Protocol) – Les clients de cryptographie KMIP d'Oracle Solaris peuvent communiquer avec des serveurs KMIP, où les clés sont créées et gérées dans des systèmes sécurisés de données au repos.
- Mémoire sécurisée de silicium (SSM) – Protège automatiquement votre application et votre système d'exploitation avec SSM.
- Modernisez les audits de sécurité avec la génération de rapports de conformité automatisés et intégrés.
- Sécurisez le déploiement de plate-forme applicative avec un nouvel outil de gestion de modèle d'environnement restreint d'application.

Optimisation :

- Plate-forme plus rapide et plus sécurisée pour l'exécution d'Oracle Database et de Java.
- Renforcez la sécurité multilocataire et l'isolement d'Oracle Database.

Simplicité :

- Migrez, en toute transparence, des charges de données traditionnelles vers des machines virtuelles.
- Utilisez `cloudbase-init` pour configurer les déploiements de système d'exploitation invité.
- Utilisez le tableau de bord de l'interface Web du système Oracle Solaris pour visualiser les données, les performances et la conformité du système.

Mises à jour logicielles fournies en standard. Pour plus d'informations, reportez-vous à la section "Mises à jours des logiciels fournis avec Oracle Solaris 11.4" du manuel *Freewares disponibles dans Oracle Solaris 11.4*.

- Nouvelles versions de nombreux packages logiciels fournis en standard, notamment GNOME 3.24, ISC BIND 9.10, MySQL 5.7, Open Fabric Enterprise Distribution 3.18, Oracle Instant Client 12.2, Perl 5.26, Puppet 5.5, Python 3.5 et Xorg 1.19.
- Nouveaux logiciels fournis en standard, y compris Augeas, Cython, le module Python `cx_Oracle`, le compilateur Google Go, LLVM/Clang, MCollective, Oracle Database Programming Interface-C (ODPI-C) et le filtre d'impression `paps`.

Oracle Solaris 11.4 prend en charge les mises à jour d'application suivantes :

- Oracle VM Server for SPARC 3.6. Reportez-vous à la page Oracle VM Server for SPARC et à la bibliothèque de documentation Oracle VM Server for SPARC 3.6.
- Oracle Solaris Cluster 4.4. Reportez-vous à la page Oracle Solaris Cluster et à la bibliothèque d'informations Oracle Solaris Cluster 4.4.

Fonctionnalités de sécurité et de conformité

Cette section décrit les nouvelles fonctionnalités de sécurité et de conformité disponibles dans cette version. Ces nouvelles fonctionnalités permettent d'empêcher de nouvelles menaces via une protection antimalware et permettent de répondre aux obligations les plus strictes en matière de conformité.

Modèles d'environnement restreint sécurisés

Les modèles d'environnement restreint sont des ensembles d'attributs de processus à nom unique pouvant être utilisés pour spécifier des exigences de sécurité et d'isolement des ressources. Dans Oracle Solaris 11.4, vous pouvez exécuter des processus non sécurisés dans des modèles d'environnement restreint temporaires. Vous pouvez créer des modèles d'environnement restreint persistants et hiérarchiques à l'aide de la commande `sandboxadm`. Vous pouvez accéder aux modèles d'environnement restreint temporaires et persistants à l'aide de la commande `sandbox`.

Les modèles d'environnement restreint conviennent aussi bien aux applications avec privilèges que sans. Des contrôles renforcés contre les attaques malveillantes, qui tirent parti de la fonctionnalité Silicon Secured Memory (SSM) de SPARC, protègent automatiquement les applications clés et le noyau système.

Pour plus d'informations, reportez-vous à la section "Configuring Sandboxes for Project Isolation" du manuel *Securing Users and Processes in Oracle Solaris 11.4* et aux pages de manuel `sandboxing`(7), `sandbox`(1) et `sandboxadm`(8).

Evaluation de la conformité à la sécurité

Cette version d'Oracle Solaris permet d'exécuter et de stocker des rapports de conformité à distance et de les filtrer en fonction des métadonnées.

- Vous pouvez exécuter et administrer des rapports de conformité à partir d'un système central et les stocker sur un serveur commun. Reportez-vous au Chapitre 2, "Centrally Managing Compliance Assessments" du manuel *Oracle Solaris 11.4 Compliance Guide* et à la page de manuel `compliance-roster`(8).
- Vous pouvez baliser les évaluations de conformité pour identification et filtrage. Reportez-vous à la section "Using Metadata to Manage Assessments" du manuel *Oracle Solaris 11.4 Compliance Guide* et à la section *Match Parameters* de la page de manuel `compliance`(8).

Contrôles de conformité Oracle Solaris Cluster

Le test d'évaluation standard pour la commande `compliance` d'Oracle Solaris inclut des contrôles pour Oracle Solaris Cluster. Les contrôles Oracle Solaris Cluster s'exécutent uniquement si Oracle Solaris Cluster est installé et configuré sur le système.

Pour plus d'informations sur les tests d'évaluation, les profils, la commande `compliance` et les contrôles de conformité Oracle Solaris Cluster, consultez la documentation suivante :

- Page de manuel `compliance`(8)
- Section "What's New in Compliance in Oracle Solaris 11.4" du manuel *Oracle Solaris 11.4 Compliance Guide*
- Directives de sécurité d'*Oracle Solaris Cluster 4.4*

Audit par fichier

L'audit par fichier dans Oracle Solaris 11.4 fournit un audit détaillé des accès à des fichiers et répertoires spécifiques. Grâce à cette fonction, les administrateurs du système et de la sécurité peuvent cibler les fichiers à auditer. Les fichiers spécifiés sont accessibles par certains moyens, ce qui facilite grandement la collecte et l'analyse des données d'audit.

Par exemple :

```
# chmod A+everyone@:write_data/read_data:successful_access/failed_access:audit /data/db1
```

Cette entrée de contrôle d'accès d'audit garantit qu'un enregistrement d'audit est généré pour toutes les lectures ou écritures, à la fois pour les accès autorisés et refusés, sur le fichier `/data/db1` par tout utilisateur du système. Il est également possible d'ajouter des entrées de contrôle d'accès d'audit pour les modifications de métadonnées.

Pour plus d'informations, reportez-vous à la section "What's New in the Audit Service in Oracle Solaris 11.4" du manuel *Managing Auditing in Oracle Solaris 11.4*.

Audit Verified Boot

Dans Oracle Solaris 11.4, cette nouvelle fonction vous aide à générer des enregistrements d'audit pour indiquer les résultats de la vérification de signature des modules de noyau. Cette fonction contrôle la valeur `boot_policy` de Verified Boot à l'initialisation d'Oracle Solaris 11.4 et génère la valeur de sortie dans un enregistrement d'audit pour l'événement `AUE_SYSTEMBOOT`. Lorsque la fonction Verified Boot est activée avec la propriété `boot_policy` définie avec la valeur `warning` ou `enforce`, l'audit Oracle Solaris produit des événements d'audit `AUE_MODLOAD` en cas d'échec d'une vérification de signature elfsign quand un module doit être chargé. Avec Verified Boot, vous pouvez suivre les événements des modules de noyau qui ont des signatures non valides ou des signatures qui n'ont pas été chargées dans le système.

Pour plus d'informations, reportez-vous à la section "New Feature – Auditing Verified Boot" du manuel *Managing Auditing in Oracle Solaris 11.4*.

Génération de rapports d'historique d'exécution de commande avec privilège

Oracle Solaris 11.4 introduit l'utilitaire `admhist`, qui fournit un résumé des événements liés à l'administration système qui ont été exécutés sur le système, dans un format utile et facile à comprendre. L'utilitaire `admhist` exploite pleinement les données d'audit pour permettre aux utilitaires `praudit` et `auditreduce` de fournir une analyse des journaux plus détaillée.

Diverses options permettent d'affiner les résultats par utilisateur, date, heure, ou type d'événement comme suit. Par exemple, vous pouvez identifier les exécutions de commande avec privilège en fonction d'un ID utilisateur au cours des dernières 24 heures :

```
# admhist -v -a "last 24 hours"
2017-05-09 10:58:55 user1@example.com cwd=/export/home/user1 /usr/sbin/zfs get quota rpool/export/home/
user1
2017-05-09 10:59:16 user1@example.com cwd=/export/home/user1 /usr/sbin/zfs set quota 40g
2017-05-09 10:59:27 user1@example.com cwd=/export/home/user1 /usr/sbin/zfs get quota rpool/export/home/
user1
2017-05-09 10:59:31 user1@example.com cwd=/export/home/user1 /usr/bin/bash
2017-05-09 10:59:31 user1@example.com cwd=/ /usr/bin/su
```

La sortie montre que l'utilisateur `user1` a pris le rôle d'utilisateur `root` et a augmenté son quota. Les privilèges utilisés tout au long de la vie du processus sont examinés à la sortie de l'exécution de la commande, raison pour laquelle l'opération `su` est affichée à la fin de la sortie.

Pour plus d'informations, reportez-vous à la page de manuel `admhist`(8), à la section "New Feature – Per-Privilege Logging of Audit Events" du manuel *Managing Auditing in Oracle Solaris 11.4* et à *Utilisation des fonctions d'analyse Oracle Solaris 12*.

Support client KMIP

Oracle Solaris 11.4 fournit le support client pour l'utilisation du protocole KMIP (Key Management Interoperability Protocol) version 1.1. Le nouveau fournisseur PKCS#11, `pkcs11_kmip`, est compris dans la structure cryptographique d'Oracle Solaris qui permet aux applications PKCS#11 de fonctionner en tant que clients KMIP et de communiquer avec des serveurs KMIP.

Oracle Solaris 11.4 inclut également une nouvelle commande, `kmipcfg`, qui permet d'initialiser et de gérer les états du fournisseur `pkcs11_kmip`.

Pour plus d'informations, reportez-vous au Chapitre 5, "KMIP and PKCS #11 Client Applications" du manuel *Managing Encryption and Certificates in Oracle Solaris 11.4* et aux pages de manuel `pkcs11_kmip`(7) et `kmipcfg`(8).

Etiquetage des fichiers et processus

L'étiquetage des fichiers et processus dans Oracle Solaris 11.4 fournit une structure permettant de restreindre l'accès aux informations sensibles. Il est désormais possible d'étiqueter les fichiers et répertoires pour fournir l'accès aux utilisateurs ou rôles disposant d'une `autorisation` suffisante. La stratégie d'autorisation (`clearance`) s'applique également aux processus ayant tous les privilèges. Oracle Solaris 11.4 peut générer des journaux pour chaque accès aux fichiers étiquetés, qui peuvent être utilisés pour le suivi des normes de conformité telles que `PCI-DSS` et `HIPAA`.

Pour plus d'informations, reportez-vous à la section "Etiquettes et autorisations" du manuel *Sécurisation des fichiers et vérification de l'intégrité des fichiers dans Oracle Solaris 12* et à la page de manuel `clearance`(7).

Protection renforcée contre les attaques malveillantes avec la mémoire sécurisée de silicium

La fonctionnalité Silicon Secured Memory (SSM) ajoute un contrôle en temps réel de l'accès aux données en mémoire pour renforcer la protection contre les intrusions malveillantes et les failles de programme en production, et offrir ainsi une sécurité et une fiabilité accrues.

SSM est disponible via le programme d'allocation de mémoire système par défaut et dans une zone de noyau. Reportez-vous à "Prise en charge de la mémoire sécurisée de silicium dans les zones de noyau Oracle Solaris" à la page 19.

Le programme d'allocation de mémoire système par défaut (`libc malloc`) est maintenant compatible avec l'intégrité des données d'application (ADI, Application Data Integrity). Les fichiers binaires balisés avec la commande `sxadm` bénéficient automatiquement de la protection. Reportez-vous aux informations sur les protections `ADIHEAP` et `ADISTACK` dans la section Extensions de sécurité de la page de manuel `sxadm`(8).

Les interfaces de programmation d'application SSM sont disponibles pour la personnalisation avancée. Reportez-vous à la section "Protecting Against Malware With Security Extensions" du manuel *Securing Systems and Attached Devices in Oracle Solaris 11.4* et à la page de manuel `adi`(2).

Filtrage de paquets

Oracle Solaris 11.4 inclut le pare-feu OpenBSD Packet Filter (PF) pour filtrer le trafic TCP/IP. Le pare-feu PF offre une alternative au filtre IP (IPF) existant dans Oracle Solaris 11.4, ce qui permet à la fois la gestion de la bande passante et la priorisation de paquets. Pour utiliser le pare-feu PF, installez le package `pkg:/network/firewall` et activez l'instance de service `svc:/network/firewall:default`.

Remarque - Veillez à configurer le pare-feu avant d'activer le service. Avec la configuration par défaut, le service a un état dégradé. Le pare-feu dégradé bloque toutes les sessions entrantes à l'exception de `ssh`. Les sessions sortantes sont autorisées.

PF inclut la fonction `pflogd`, un démon de journalisation de paquets qui sauvegarde les paquets journalisés par le pare-feu PF. Ces paquets sont disponibles à partir d'une liaison de données de capture. Le démon lit les paquets à partir de cette liaison de données et les stocke dans un fichier. Pour plus d'informations, reportez-vous à la page de manuel `pflogd`(8).

PF prend en charge `ftp-proxy`, un proxy semi-transparent pour FTP, prenant en charge la traduction d'adresses réseau (NAT) IPv4. Les systèmes exécutant le pare-feu PF pour la traduction NAT peuvent utiliser `ftp-proxy` pour autoriser les connexions FTP à traverser le pare-feu. Pour plus d'informations, reportez-vous à la page de manuel `ftp-proxy`(8).

Pour plus d'informations, reportez-vous au Chapitre 4, "Oracle Solaris Firewall" du manuel *Securing the Network in Oracle Solaris 11.4* et aux pages de manuel `pfctl`(8), `pf.conf`(7) et `pf.os`(7).

Kerberos

Oracle Solaris 11.4 fournit une version mise à jour de Kerberos, qui inclut les améliorations apportées à la dernière version de MIT Kerberos, ainsi que celles apportées à Oracle Solaris. Kerberos fournit l'authentification réseau et assure éventuellement l'intégrité et la confidentialité des messages, selon la façon dont une application l'utilise.

Pour plus d'informations, reportez-vous au Chapitre 1, "Kerberos on Oracle Solaris" du manuel *Managing Kerberos in Oracle Solaris 11.4* et à la page de manuel `kerberos.7`.

`libsasl2`

La couche SASL (Simple Authentication and Security Layer) est une structure fournissant des services d'authentification et de sécurité facultatifs aux protocoles réseau. Oracle Solaris 11.4 base son implémentation SASL sur la version open source Cyrus SASL 2.1.26, avec quelques modifications.

Les plug-ins SASL se trouvent dans le répertoire `/usr/lib/sasl2` et l'emplacement par défaut des fichiers de configuration SASL est le répertoire `/etc/sasl2`. En basant la version SASL sur open source, Oracle Solaris 11.4 est à même d'offrir les dernières fonctions SASL, y compris les mises à jour de sécurité.

Pour plus d'informations, reportez-vous au Chapitre 2, "Using Simple Authentication and Security Layer" du manuel *Managing Authentication in Oracle Solaris 11.4*.

Service `account-policy`

Cette version d'Oracle Solaris offre une alternative à la modification des fichiers individuels dans le répertoire `/etc` pour établir la stratégie du système. Le service `account-policy` de l'utilitaire de gestion des services (SMF), stocke le `login`, le `su`, les variables shell, la journalisation, la stratégie de sécurité (`policy`.

conf) et les paramètres de contrôle d'accès basé sur les rôles (RBAC) en tant que propriétés dans SMF. Lorsque le service est activé, vous définissez et vous obtenez la stratégie du système via celui-ci. Notez que les fichiers /etc peuvent ne pas indiquer les stratégies actives. Pour plus d'informations, reportez-vous à la page de manuel account-policy(8S) et à la section "Modifying Rights System-Wide As SMF Properties" du manuel *Securing Users and Processes in Oracle Solaris 11.4*.

Prise en charge de PKCS #11 v2.40 pour la structure cryptographique d'Oracle Solaris

La structure cryptographique d'Oracle Solaris a été mise à jour de PKCS #11 v2.20 vers PKCS #11 v2.40. Les mises à jour incluent certains des mécanismes les plus récents de PKCS #1 v2.40, y compris ceux de PKCS #11 v2.30. Un nouveau code d'erreur et une nouvelle valeur ont également été introduits dans PKCS #11 v2.40. Les nouveaux mécanismes suivants ont été ajoutés :

- Signature et vérification AES

  CKM_AES_XCBC_MAC
  CKM_AES_XCBC_MAC_96
  CKM_AES_CMAC
  CKM_AES_GMAC

- Chiffrement et déchiffrement AES

  CKM_AES_GCM
  CKM_AES_CCM
  CKM_AES_CFB128

- Condensé de messages SHA-512/t

  CKM_SHA512_224
  CKM_SHA512_256
  CKM_SHA512_T

- Longueur générale SHA-512/t avec HMAC

  CKM_SHA512_224_HMAC_GENERAL
  CKM_SHA512_256_HMAC_GENERAL
  CKM_SHA512_T_HMAC_GENERAL
  CKM_SHA512_224_HMAC
  CKM_SHA512_256_HMAC
  CKM_SHA512_T_HMAC

- Dérivation de clé SHA-512/t

  CKM_SHA512_224_KEY_DERIVATION
  CKM_SHA512_256_KEY_DERIVATION
  CKM_SHA512_T_KEY_DERIVATION

- TLS 1.2

  CKM_TLS12_MASTER_KEY_DERIVE
  CKM_TLS12_MASTER_KEY_DERIVE_DH
  CKM_TLS12_KEY_AND_MAC_DERIVE
  CKM_TLS12_KEY_SAFE_DERIVE
  CKM_TLS_KDF - replacing CKM_TLS_PRF
  CKM_TLS_MAC - replacing CKM_TLS_PRF

- Code d'erreur CKR_CURVE_NOT_SUPPORTED pour courbe elliptique

  Si une courbe elliptique spécifique ne peut pas être prise en charge, le code d'erreur CKR_CURVE_NOT_SUPPORTED est renvoyé. Dans la version précédente, le code d'erreur CKR_TEMPLATE_INCONSISTENT était renvoyé dans ce cas.

- `CK_UNAVAILABLE_INFORMATION`

  Lorsque la fonction `C_GetAttributeValue()` est appelée, et si un attribut ne peut pas être renvoyé parce qu'il n'est pas valide ou n'est pas disponible, `ulValueLen` est défini sur `CK_UNAVAILABLE_INFORMATION`. L'appelant doit vérifier si la valeur d'attribut renvoyée n'est pas valide ou n'est pas disponible en comparant la valeur `ulValueLen` à `CK_UNAVAILABLE_INFORMATION`. En outre, l'appelant doit traiter `ulValueLen = 0` en tant que valeur valide.
- Attributs `CKA_DESTROYABLE` et `CKR_ACTION_PROHIBITED`

  Si un objet a `CKA_DESTROYABLE = CK_FALSE`, une demande `C_DestroyObject` pour cet objet donné doit générer le renvoi de `CKR_ACTION_PROHIBITED` en tant que code d'erreur.
- Suppression des restrictions avec `CKU_SO`

  Cette modification supprime les restrictions sur l'ouverture en lecture seule tandis que `CKU_SO` est connecté. Alors que des sessions en lecture seule peuvent maintenant coexister avec `CKU_SO`, ces sessions se comportent comme `CKS_RO_PUBLIC_SESSION`. Une session en lecture seule ne peut pas être utilisée pour `C_Login` avec `CKU_SO`.

  `CKR_SESSION_READ_ONLY_EXISTS` et `CKR_SESSION_READ_WRITE_SO_EXISTS` sont en phase d'abandon.

Pour plus d'informations, reportez-vous aux pages de manuel `SUNW_C_GetMechSession`(3EXT), `SUNW_C_KeyToObject`(3EXT), `libpkcs11`(3LIB), `pkcs11_softtoken`(7), `pkcs11_kms`(7) et `pkcs11_tpm`(7).

Fonctions de gestion des données

Cette section décrit les nouvelles fonctions de gestion des données de cette version. Ces fonctionnalités permettent de développer la conception en offrant une capacité illimitée en vue de la croissance future et une amélioration de l'intégrité des données.

Voir aussi "Configurer des zones immuables via l'exécution dans le chemin de confiance" à la page 19.

Retrait de périphérique de niveau supérieur ZFS

La commande `zpool remove` permet de retirer des périphériques de données de niveau supérieur. Le retrait d'un périphérique de données de niveau supérieur migre les données du périphérique à retirer vers les périphériques de données restants dans le pool. La commande `zpool status` signale la progression de l'opération de retrait jusqu'à la fin de la réargenture.

Pour plus d'informations sur le retrait des périphériques de données de niveau supérieur, reportez-vous à Oracle Solaris ZFS Device Removal, "Removing Devices From a Storage Pool" du manuel *Managing ZFS File Systems in Oracle Solaris 11.4* et à la page de manuel `zpool`(8).

Nettoyage programmé du ZFS

Par défaut, le nettoyage du pool ZFS s'exécute en arrière-plan tous les 30 jours avec une priorité réglée automatiquement. La priorité du nettoyage est faible par défaut, mais est automatiquement augmentée si le système est inactif. La priorité du nettoyage est ajustée en fonction de l'intervalle de nettoyage spécifié, de la progression et de la charge système. L'heure de début du dernier nettoyage réussi est signalée par la commande `zpool status`.

Vous pouvez personnaliser la programmation du nettoyage du pool, voire le désactiver, en définissant la propriété `scrubinterval`. Pour plus d'informations sur les propriétés `scrubinterval` et `lastscrub`, reportez-vous à la section "Scheduled Data Scrubbing" du manuel *Managing ZFS File Systems in Oracle Solaris 11.4* et à la page de manuel `zpool`(8).

Copie rapide de fichiers basée sur ZFS

Les fonctions `reflink()` et `reflinkat()` permettent de copier des fichiers très rapidement à l'aide de la technologie ZFS sous-jacente. La fonction `reflink()` crée un nouveau fichier avec le contenu d'un fichier existant sans lire ou écrire les blocs de données sous-jacents. Le fichier existant et le fichier à créer doivent se trouver dans le même pool ZFS.

Pour plus d'informations, reportez-vous à la page de manuel `reflink`(3C).

L'option `-z` (copie rapide) de la commande `cp` utilise `reflink`. Pour plus d'informations, reportez-vous à la page de manuel `cp`(1).

Flux d'envoi bruts ZFS

Dans Oracle Solaris 11.4, vous pouvez optimiser les transmissions de flux d'envoi (`send`) ZFS des systèmes de fichiers compressés et réduire le trafic de transmission réseau à l'aide des flux d'envoi (`send`) ZFS bruts.

Dans les versions précédentes, un flux d'envoi (`send`) d'un système de fichiers ZFS compressé était d'abord décompressé lors de la transmission, puis les blocs étaient recompressés si la compression était activée à l'extrémité de la réception. Dans la version Oracle Solaris 11.4, ces deux étapes sont évitées car les blocs du système de fichiers compressés dans le flux restent compressés. Cette optimisation permet également de réduire le trafic de transmission réseau. Vous pouvez optimiser un flux `send` ZFS en l'envoyant en mode brut avec la nouvelle option `-w` de la commande `zfs send`. L'activation de cette nouvelle option permet au flux `send` d'encoder la présence de blocs bruts afin qu'un système de réception puisse les traiter sans les compresser.

Par exemple, pour créer un système de fichiers ZFS avec compression activée et envoyer le flux d'instantané avec et sans l'option `-w` et vérifier les tailles de flux en résultant :

```
# zfs create compression=on pond/cdata
# cp -r somefiles /pond/data
# zfs snapshot pond/cdata@snap1
# zfs get compressratio pond/cdata@snap1
NAME              PROPERTY       VALUE  SOURCE
pond/cdata@snap1  compressratio  1.79x  -

# zfs send pond/cdata@snap1 > /tmp/stream
# zfs send -w compress pond/cdata@snap1 > /tmp/cstream
# ls -lh /tmp/*stream*
-rw-r--r--   1 root     root        126M Feb 15 14:35 /tmp/cstream
-rw-r--r--   1 root     root        219M Feb 15 14:35 /tmp/stream
```

Les systèmes exécutant les versions précédentes d'Oracle Solaris ne peuvent pas recevoir ce type de flux ; un message d'erreur sera généré.

Pour plus d'informations, reportez-vous au manuel *Gestion des systèmes de fichiers ZFS dans Oracle Solaris 12*.

Flux d'envoi ZFS avec possibilité de reprise

Dans Oracle Solaris 11.4, si une transmission réseau est interrompue ou qu'une erreur se produit, les flux d'envoi (`send`) ZFS peuvent être relancés là où ils se sont arrêtés.

L'utilisation des opérations `send` et `receive` de ZFS pour transférer des instantanés ZFS entre les systèmes est un moyen pratique pour répliquer les données de système de fichiers ZFS qui présentaient auparavant les problèmes suivants :

- Une opération d'envoi ZFS pouvait prendre des heures, voire des jours. Pendant ce temps, l'opération `send` pouvait être interrompue en raison d'une indisponibilité du réseau ou d'une défaillance du système.
- En cas d'échec, l'opération `send`, même si elle était presque terminée, devait être relancée du début.
- L'opération `send` de ZFS pouvait ne pas pouvoir transférer de larges flux dans la période disponible entre les interruptions.
- Une opération `recv` de ZFS pouvait ne pas pouvoir détecter et signaler des erreurs de transmission avant la fin du traitement du flux dans sa totalité.

Cette version Oracle Solaris 11.4 permet à ZFS d'envoyer des flux avec possibilité de reprise au point de leur interruption à l'aide des nouvelles options suivantes :

- `zfs receive -C` – Ecrit un point de reprise de réception vers `stdout`.
- `zfs send -C` – Lit un point de reprise de réception depuis `stdin`.
- `zfs send -s` (nocheck) – Désactive le nouveau format de compression simultanée.
- `zfs list -I` (state) – Affiche de manière récursive les jeux de données incomplets car ils ne sont pas affichés par défaut.

Pour plus d'informations, reportez-vous au manuel *Gestion des systèmes de fichiers ZFS dans Oracle Solaris 12*.

Limites de débit de lecture et d'écriture ZFS configurables

La version Oracle Solaris 11.4 permet de limiter les lectures et les écritures sur disque du système de fichiers ZFS. Vous pouvez activer une limite de lecture (`read`) ou d'écriture (`write`) sur un système de fichiers ZFS en définissant les propriétés `readlimit` et `writelimit`, en unités d'octets par seconde. Ces fonctions vous permettent d'optimiser les ressources d'E/S ZFS dans un environnement multilocataire.

Les propriétés `defaultwritelimit` et `defaultreadlimit` sont ajoutées pour faciliter la gestion d'un grand nombre de systèmes de fichiers ZFS. Si les propriétés `defaultwritelimit` et `defaultreadlimit` sont définies, tous les descendants du système de fichiers héritent de la valeur affectée. Si vous appliquez la limite `read` ou `write` par défaut au système de fichiers ZFS, celle-ci ne s'applique qu'aux systèmes de fichiers descendants et pas au système de fichiers lui-même. Les propriétés `effectivereadlimit` et `effectivewritelimit` en lecture seule sont ajoutées pour fournir une vue de ce qu'est la limite effective sur un système de fichiers. La limite effective signalée est la limite de données la plus basse à n'importe quel point entre le parent et le système de fichiers indiqué.

Par exemple, vous définiriez les limites `read` et `write` comme suit :

```
# zfs set writelimit=500mb pond/apps/web
# zfs set readlimit=200mb pond/apps/logdata
```

L'exemple suivant montre comment afficher les limites `read` et `write` :

```
# zfs get -r writelimit,readlimit pond/apps
NAME                 PROPERTY    VALUE    SOURCE
pond/apps            writelimit  default  default
pond/apps            readlimit   default  default
pond/apps/logdata    writelimit  default  default
pond/apps/logdata    readlimit   200M     local
pond/apps/web        writelimit  500M     local
pond/apps/web        readlimit   default  default
pond/apps/web/tier1  writelimit  default  default
pond/apps/web/tier1  readlimit   default  default
```

Vous pouvez afficher la limite d'écriture effective comme suit :

```
# zfs get effectivewritelimit pond/apps/web
NAME           PROPERTY             VALUE  SOURCE
pond/apps/web  effectivewritelimit  500M   local
```

Pour plus d'informations, reportez-vous au manuel *Gestion des systèmes de fichiers ZFS dans Oracle Solaris 12*.

Surveiller et gérer la migration shadow ZFS

La version Oracle Solaris 11.4 offre une opération de migration shadow ZFS dotée d'améliorations pour une meilleure visibilité en matière de surveillance des erreurs de migration et de contrôle des migrations en cours. Les nouvelles options suivantes ont été ajoutées :

- `shadowstat -E` et `-e` – Permet la surveillance des erreurs pour toutes les migrations ou une migration unique.
- `shadowadm` – Permet de contrôler les migrations en cours.

Par exemple, vous pouvez identifier les erreurs de migration shadow de plusieurs opérations de migration :

```
# shadowstat
                                  EST
                          BYTES   BYTES           ELAPSED
DATASET                   XFRD    LEFT    ERRORS  TIME
tank/logarchive           16.4M   195M    1       00:01:20
pond/dbarchive            4.49M   248M    -       00:00:51
tank/logarchive           16.6M   194M    1       00:01:21
pond/dbarchive            4.66M   248M    -       00:00:52
tank/logarchive           16.7M   194M    1       00:01:22
pond/dbarchive            4.80M   248M    -       00:00:53
tank/logarchive           17.1M   194M    1       00:01:23
pond/dbarchive            5.00M   248M    -       00:00:54
tank/logarchive           17.3M   194M    1       00:01:24
pond/dbarchive            5.16M   247M    -       00:00:55
```

Vous pouvez identifier une erreur de migration spécifique comme suit :

```
# shadowstat -E
tank/logarchive:
PATH                                            ERROR
e-dir/socket                                    Operation not supported
pond/dbarchive:
No errors encountered.
```

Par exemple, pour annuler la migration car le socket d'ouverture ne peut pas être migré :

```
# shadowadm cancel tank/logarchive
```

Pour plus d'informations, reportez-vous au manuel *Gestion des systèmes de fichiers ZFS dans Oracle Solaris 12*.

Conservation d'héritage d'ACL dans ZFS

Dans Oracle Solaris 11.4, une nouvelle fonction ACL de ZFS permet d'offrir une meilleure expérience lors du partage d'un système de fichiers ZFS sur les protocoles NFS et SMB (Server Message Block). Une nouvelle valeur d'héritage pour la propriété `aclinherit` a été ajoutée, qui permet la sémantique passthrough mais remplace les autorisations définies dans les entrées de contrôle d'accès `owner@`, `group@` et `everyone@` par les valeurs demandées dans l'appel système `open`, `create` ou `mkdir`. Lorsque les entrées de contrôle d'accès (ACE) pouvant être héritées sont définies, l'héritage des bits est préservé. Ce comportement s'avère important pour permettre au partage SMB et NFS d'hériter des listes de contrôle d'accès (ACL) de façon naturelle. La nouvelle valeur est appelée `passthrough-mode-preserve`. Aucune modification n'est apportée à la propriété `aclmode`, mais une opération `chmod` tient compte du comportement d'héritage par rapport à la propriété `aclinherit`. En particulier, elle préserve les bits d'héritage lors d'une opération `chmod`.

Pour plus d'informations, reportez-vous au manuel *Gestion des systèmes de fichiers ZFS dans Oracle Solaris 12*.

Prise en charge du serveur pour NFS version 4.1

Oracle Solaris 11.4 inclut la prise en charge du serveur pour NFS version 4.1. Le protocole fournit les nouvelles fonctions et considérations suivantes :

- Exactly Once Semantics (EOS) – Fournit un cache fiable de demandes en double pour le protocole NFS version 4.1. Ce cache de demandes en double garantit que les demandes non idempotentes, telles que la demande de retrait, s'exécutent une seule fois, même dans les cas de défaillances réseau et de retransmissions temporaires. Cette fonction élimine les problèmes de longue date des versions 3 et 4 de NFS.
- `reclaim_complete` – Nouvelle fonction du protocole qui permet au serveur de reprendre le service NFS rapidement après un redémarrage du serveur. Contrairement à NFS version 4, l'utilisateur n'a pas à attendre un délai spécifique, appelé délai de grâce, avant d'effectuer une reprise du service. Avec `reclaim_complete`, le serveur peut mettre fin au délai de grâce une fois tous les clients récupérés. Cette fonction s'avère particulièrement importante pour les environnements à haute disponibilité.
- Récupération planifiée sans période de grâce (PGR, Planned GRACE-less Recovery) - Permet à un serveur Oracle Solaris NFS version 4 ou NFS version 4.1 de conserver l'état NFS version 4 lors des redémarrages de service NFS ou de la réinitialisation progressive du système afin que le serveur NFS version 4 n'entre pas dans la période de grâce pour récupérer l'état NFS version 4. Les applications client NFS peuvent ainsi éviter une indisponibilité des données de 90 secondes environ lors des redémarrages de service NFS ou des réinitialisations progressives du système.
- Tenez compte des problèmes d'interopérabilité suivants :
  - Le serveur Oracle Solaris NFS version 4.1 prend à la fois en charge les clients Linux et VMware. Toutefois, la délégation doit être désactivée sur le serveur pour les clients Linux.
  - Il existe des problèmes connus de verrouillage et de récupération en l'état lors de l'utilisation de la délégation avec le client Linux client.

    ```
    # sharectl set -p server_delegation=off nfs
    ```

    Vous pouvez désactiver la prise en charge de NFS version 4.1 sur le serveur comme suit :

    ```
    # sharectl set -p server_versmax=4.0 nfs
    ```

Pour plus d'informations sur NFS, reportez-vous à *Gestion des systèmes de fichiers réseau dans Oracle Solaris 12*.

Montage NFSv3 avec TCP

Lorsqu'un système de fichiers est monté à l'aide de NFS Version 3 et que TCP est le transport sélectionné, la configuration de montage initiale utilisera également TCP en tant que transport. Dans les versions précédentes d'Oracle Solaris, UDP était utilisé pour la configuration de montage et TCP n'était utilisé qu'une fois le montage établi.

Si vous autorisez les montages NFS à travers un pare-feu, cette fonction peut vous permettre de simplifier la configuration du pare-feu.

Elle vous permet également d'utiliser NFS Version 3 sur des sites où le trafic UDP est bloqué.

Pour plus d'informations, reportez-vous à *Gestion des systèmes de fichiers réseau dans Oracle Solaris 12* et à la page de manuel `mount_nfs`(8).

Attributs étendus de système de fichiers dans `tmpfs`

Les systèmes de fichiers `tmpfs` prennent en charge les attributs système étendus. Pour plus d'informations, reportez-vous aux pages de manuel `tmpfs`(4FS) et `fgetattr`(3C).

Prise en charge de SMB 3.1.1

Oracle Solaris 11.4 prend en charge le protocole SMB 3.1.1 dans le serveur Oracle Solaris SMB, qui inclut les fonctions SMB suivantes :

- Partages disponibles en continu – Cette fonction permet à un serveur Oracle Solaris SMB d'assurer la disponibilité continue des partages en cas de panne ou de réinitialisation d'un serveur.
- Multicanal – Cette fonction permet à un serveur de fichiers Oracle Solaris SMB d'utiliser plusieurs connexions réseau par session SMB afin d'offrir un débit accru et une meilleure tolérance aux pannes.
- Chiffrement – Cette fonction permet à un serveur Oracle Solaris SMB de chiffrer le trafic du réseau SMB entre les clients et le serveur. Le chiffrement SMB sécurise les sessions SMB et les protège contre l'altération et les attaques de type écoute électronique.

Pour plus d'informations, reportez-vous à *Managing SMB File Sharing and Windows Interoperability in Oracle Solaris 11.4* et à la page de manuel `smbstat`(8).

Fonctions de mise en réseau

Cette section décrit les nouvelles fonctions de mise en réseau de cette version. Ces fonctionnalités améliorent la technologie de mise en réseau et la mise en réseau définie par logiciel existantes pour créer des services répondant aux exigences de performance de l'organisation et pour fournir une plus grande souplesse d'application et la flexibilité que vous exigez.

Migration d'une configuration réseau persistante vers SMF

Dans Oracle Solaris 11.4, la configuration réseau persistante a été migrée vers le référentiel de l'utilitaire de gestion des services (SMF). Cette migration vous permet de personnaliser les paramètres réseau et de créer des configurations réseau plus complexes lors d'une installation automatisée. Cette modification aligne également la configuration réseau avec d'autres composants réseau qui utilisent SMF en tant que référentiel de stockage principal. Pour prendre en charge la migration des paramètres de configuration réseau vers SMF, certains noms de propriété `dladm` ont également été modifiés.

Pour plus d'informations sur les modifications de nom de propriété `dladm`, reportez-vous au Chapitre 2, "Administering Datalink Configuration in Oracle Solaris" du manuel *Configuration et gestion des composants réseau dans Oracle Solaris 12* et à la page de manuel `dladm`(8). Pour plus d'informations, reportez-vous à *Installation automatique de systC(mes Oracle Solaris 11.4*.

Prise en charge côté client d'Oracle Solaris pour IEEE 802.1X

Dans Oracle Solaris 11.4, vous pouvez authentifier les clients Oracle Solaris à l'aide de la norme IEEE802. 1X. Auparavant, si un LAN sécurisé qui était déployé nécessitait des systèmes client pour être authentifié avant de fournir des services, l'authentification n'était pas prise en charge sur un système Oracle Solaris.

Cette nouvelle fonction permet aux administrateurs réseau de configurer un système client Oracle Solaris et de l'activer pour être authentifié par un serveur derrière un LAN sécurisé. Le démon `nacd` s'exécute sur le système Oracle Solaris. Le système client est connecté à un LAN sécurisé via un port sur un commutateur sur le LAN. Le démon communique avec un serveur sur le LAN sécurisé pour être authentifié, avant d'obtenir un service, tel que DHCP, du LAN. Un administrateur réseau peut également utiliser la commande `nacadm` pour configurer les informations d'identification de sécurité et utiliser la commande `dladm` pour activer ou désactiver l'authentification sur une liaison donnée.

Pour plus d'informations, reportez-vous aux pages de manuel `nacd`(8), `nacadm`(8) et `dladm`(8). Voir aussi

Datacenter TCP

Oracle Solaris 11.4 inclut Datacenter TCP (DCTCP), une amélioration apportée au contrôle de congestion TCP pour le trafic de centre de données. DCTCP utilise le traitement ECN (Explicit Congestion Notification ou signalisation explicite des congestions) pour estimer la fraction d'octets qui rencontre la congestion, au lieu de détecter simplement que la congestion est survenue. DCTCP adapte ensuite la fenêtre de congestion en fonction de cette estimation. Cette méthode assure une tolérance aux rafales élevées, une faible latence et un haut débit avec des commutateurs mis en mémoire tampon superficielle.

Pour plus d'informations, reportez-vous à la section "Implementing Traffic Congestion Control" du manuel *Administration des réseaux TCP/IP, d'IPMP et des tunnels IP dans Oracle Solaris 12*.

Migration en direct et basculement HA pour les ressources `anets` activées par SR-IOV

Oracle Solaris 11.4 fournit la nouvelle fonctionnalité DLMP suivante et une prise en charge appropriée pour les zones de noyau Oracle Solaris :

- Nouvelle architecture DLMP permettant la création de cartes VNIC SR-IOV et de partitions IPoIB dans la zone globale
- Prise en charge de la migration en direct pour les ressources `anets` activées par SR-IOV dans les zones de noyau Oracle Solaris
- Basculement haute disponibilité pour les ressources `anets` activées par SR-IOV dans les zones de noyau Oracle Solaris

Pour plus d'informations, reportez-vous au Chapitre 2, "Configuring High Availability by Using Link Aggregations" du manuel *Gestion des liaisons de données réseau dans Oracle Solaris 12*.

Indication d'un nom pour une route statique permanente

Dans Oracle Solaris 11.4, la commande `route` ajoute une option `-name` pour permettre la dénomination des routes statiques permanentes. Ce nom de route peut être utilisé pour modifier, obtenir ou supprimer la route statique. Il permet également de distinguer les différentes routes statiques permanentes.

Pour plus d'informations, reportez-vous à la page de manuel `route`(8). Vous pouvez également vous reporter à la section "How to Specify a Name for a Persistent Route" dans *Configuring and Managing Network Components in Oracle Solaris 11.4*.

Open Fabric Enterprise Distribution 3.18

Les composants suivants de la structure de contournement de système d'exploitation InfiniBand (IB) provenant d'Open Fabrics Enterprise Distribution (OFED) ont été mis à jour vers la version 3.18 :

- Bibliothèque de verbes (transport) InfiniBand
- Pilote d'espace utilisateur pour les HCA InfiniBand Mellanox ConnectX
- Bibliothèque du gestionnaire de communication RDMA de l'espace utilisateur
- Bibliothèque de datagramme de gestion (MAD) InfiniBand
- Bibliothèque de datagramme de gestion d'espace utilisateur (uMAD) InfiniBand
- Utilitaires de gestion InfiniBand niveau utilisateur
- Outils de diagnostic InfiniBand

- Commande `qperf`

Pour plus d'informations, reportez-vous aux pages de manuel fournies avec les packages `network/open-fabrics`.

ISC BIND 9.10.3

Oracle Solaris 11.4 inclut une version mise à jour d'ISC BIND offrant beaucoup de nouvelles fonctions, telles que la resignature automatique des zones DNSSEC, de nouveaux rapports sur les statistiques et la limitation des retards de réponse. Les utilisateurs peuvent maintenant déployer DNSSEC facilement. La surveillance est simplifiée et le service est mieux protégé contre les attaques de type déni de service.

Performances et observabilité

Cette section décrit les améliorations apportées à la plate-forme et aux performances dans cette version. Ces fonctions permettent d'optimiser les systèmes Oracle Solaris for SPARC et x86 en améliorant les performances, mais fournissent également un meilleur diagnostic pour vos systèmes.

Fournisseur SCSI DTrace

La version Oracle Solaris 11.4 présente un nouveau fournisseur SCSI DTrace destiné à assurer le suivi des commandes SCSI et des fonctions de gestion de tâches émises par un système Oracle Solaris. Le fournisseur SCSI offre les avantages suivants :

- Il permet d'assurer le suivi des commandes SCSI sur un système Oracle Solaris sans connaître la structure interne.
- Il inclut des sondes et des structures respectant autant que possible les normes SCSI T10.
- Il offre une contrepartie au fournisseur d'E/S DTrace qui suit le trafic d'E/S sur une autre couche.
- Il fournit un script `scsitrace` qui consomme les nouvelles sondes.

L'exemple suivant illustre un suivi sur une ligne identifiant les réinitialisations de cible SCSI :

```
# dtrace -n 'scsi:::tmf-request
                     /(args[1] == SCSI_TMF_TARGET_RESET) &&
                      (args[0]->addr_path != "NULL")/ {
       printf("Target Reset sent to %s", args[0]->addr_path);}'
```

Pour plus d'informations, reportez-vous à la section "iscsi Provider" du manuel *Guide d'utilisation d'Oracle Solaris 12 DTrace (Dynamic Tracing)*.

Fournisseur `fileops` DTrace

Le fournisseur `fileops` présente un jeu complet de sondes d'opération de fichier UNIX standard qui sont plus destinées à un administrateur Oracle Solaris qu'à un développeur. Par exemple, le fournisseur peut afficher les informations de latence de lecture (`read`) ou d'écriture (`write`) pour tous les systèmes de fichiers, y compris les pseudo-systèmes de fichiers.

Les sondes `fileops` s'appliquent aux opérations de fichiers suivantes : `open`, `close`, `read`, `write`, etc. Ces sondes ne sont spécifiques d'aucun type de système de fichiers et ne sont pas dépendantes des E/S vers les périphériques de stockage externes. Par exemple, la sonde `fileops:::read` se déclenche sur n'importe quelle lecture d'un fichier, que les données proviennent du disque ou soient mises en mémoire cache.

Vous pouvez utiliser la sonde `read` pour observer les latences de lecture sur différents types de système de fichiers. Par exemple :

```
fileops:::read
{
    @[args[0]->fi_fs] =
    quantize(args[1]);
}
```

La sortie en résultant fournit un graphique du nombre de lectures et des latences sur tous les types de système de fichiers du système.

Pour plus d'informations, reportez-vous à la section "fileops Provider" du manuel *Guide d'utilisation d' Oracle Solaris 12 DTrace (Dynamic Tracing)*.

Fournisseur MIB DTrace pour TCP, UDP et IP

La version Oracle Solaris 11.4 étend le fournisseur MIB DTrace pour l'observation des événements de la pile réseau avec des informations de protocole afin que les connexions TCP, UDP et IP puissent être identifiées.

Pour plus d'informations, reportez-vous à la section "mib Provider" du manuel *Guide d'utilisation d'Oracle Solaris 12 DTrace (Dynamic Tracing)*.

Action `pcap()` DTrace

Une nouvelle action, `pcap()`, a été ajoutée à DTrace. L'action `pcap()` effectuera l'une des opérations suivantes :

- Affiche les données de paquet comme le fait `tracemem()`, mais fusionnées dans un tampon contigu.
- Si `freopen()` a spécifié un fichier de capture, l'action `pcap()` capturera les données de paquet dans un fichier de capture de paquet via la fonction `libpcap pcap_dump()`. DTrace effectue les opérations suivantes sur les données de paquet :

  1. Collecte les données de paquet dans un contexte de sonde.
  2. Fusionne les données de paquet dans un tampon contigu si elles ne s'y trouvent pas déjà.
  3. Vide les données dans le fichier spécifié via la fonction `pcap_dump()`, qui a été appelée lors de la collecte des données.

L'action `pcap()` suivante vide la mémoire dans `stdout` comme le fait `tracemem()` :

```
pcap(mblk, protocol);
```

Les appels suivants vident les données de paquet dans le fichier de capture avec un suffixe spécifiant le `pid` actuel :

```
freopen("/tmp/cap.%d", pid);
pcap(mblk, protocol);
```

Cela vous permet d'assembler les suivis de paquet par processus ou service, par exemple. Comme `freopen()` est classée en tant qu'action destructive, le script ci-dessus doit spécifier l'option `-w` (”destructive”) `dtrace`. L'action `pcap()` n'est pas destructive.

Action `print()` DTrace

DTrace présente une nouvelle action `print()` pour afficher les types arbitraires, comme l'illustre l'exemple suivant :

```
# dtrace -q -n 'fop_close:entry {print(*args[0]);exit(0)}'

vnode_t {
 v_lock = {
   _opaque = [ NULL ]
 }
 v_flag = 0x0
 v_count = 0x1
 v_data = 0xffffc10054425378
 v_vfsp = specfs`spec_vfs
 v_stream = 0xffffc100623354e8
 v_type = VCHR
 v_rdev = 0xee00000026
 v_vfsmountedhere = NULL
 v_op = 0xffffc10029d98040
 v_pages = NULL
 v_filocks = NULL
 v_shrlocks = NULL
 v_nbllock = {
   _opaque = [ NULL ]
 }
 v_cv = {
   _opaque = 0x0
 }
 v_pad = 0xbadd
 v_count_dnlc = 0x0
 v_locality = NULL
 v_femhead = NULL
 v_path = "/devices/pseudo/udp@0:udp"
 v_rdcnt = 0x0
 v_wrcnt = 0x0
 v_mmap_read = 0x0
 v_mmap_write = 0x0
 v_mpssdata = NULL
 v_fopdata = NULL
 v_vsd_lock = {
   _opaque = [ NULL ]
 }
 v_vsd = NULL
 v_xattrdir = NULL
 v_fw = 0xbaddcafebaddcafe
}

#
```

Pour plus d'informations, reportez-vous à la section "print Action" du manuel *Guide d'utilisation d'Oracle Solaris 12 DTrace (Dynamic Tracing)*.

Structure kstat v2

La structure v2 des statistiques relatives au noyau (kstats) offre de meilleures performances et un certain nombre d'optimisations par rapport à la structure kstat précédente. Les nouveaux composants notables incluent notamment :

- Une API de noyau permettant de créer et de manipuler des kstats v2. Les kstats sont identifiées à l'aide d'un URI unique et incluent des métadonnées pour la kstat et les paires nom-valeur qu'elle contient. Cette API permet à la kstat de décrire les valeurs qu'elle signale.
- Une bibliothèque `libkstat2` qui fournit l'accès aux kstats v2 créées dans le noyau. Les kstats sont consultées en fonction de leur URI unique et sont présentées en tant que tables de hachage. Les développeurs peuvent s'abonner aux événements à un niveau d'URI de kstat donné et être informés lorsque des kstats sont ajoutées sous les événements dans l'arborescence d'URI ou qu'elles en sont retirées.
- L'utilitaire `/usr/bin/kstat2` qui fournit l'accès via la CLI à la kstat. Ce nouvel utilitaire examine les kstats disponibles sur le système et signale les statistiques qui correspondent aux critères spécifiés sur la ligne de commande. Chaque statistique correspondante est alors imprimée avec son URI et sa valeur réelle. Différents formats de sortie sont pris en charge, notamment les formats lisibles par l'utilisateur, les formats analysables et les formats JSON (JavaScript Object Notation).

Pour plus d'informations sur l'API de noyau, reportez-vous aux pages de manuel `kstat2_create`(9F), `kstat2_create_with_template`(9F) et `kstat2_create_histogram`(9F). Pour plus d'informations sur la bibliothèque `libkstat2`, reportez-vous aux pages de manuel `libkstat2`(3LIB) et `kstat2`(3KSTAT2). Pour plus d'informations sur l'utilitaire `kstat2`, reportez-vous à la page de manuel `kstat2`(8).

Diagnostics de dump noyau FMA

Oracle Solaris 11.4 inclut la fonction de diagnostic de dump noyau, qui offre un résumé des télémétriques des dumps noyau d'utilisateur, génère des alertes FMA pour informer l'utilisateur, et fournit une stratégie de conservation de diagnostic ainsi qu'une association de cas SMF.

Les fichiers noyau de diagnostic ne contiennent que le nécessaire, ce qui fait que leur contenu est de petite taille. Les fichiers noyau seront supprimés une fois les fichiers récapitulatifs de texte générés, réduisant ainsi l'espace disque. Avec d'autres nouvelles fonctions telles que le diagnostic de pile, FMA peut rechercher les problèmes connus dans les piles du fichier récapitulatif de la base de données Oracle. La stratégie de conservation permet à l'utilisateur de définir la stratégie principale de diagnostic via la commande `coreadm`. La commande `coreadm` fournit également des fonctionnalités telles que la suppression immédiate des noyaux ou la conservation d'un nombre de noyaux donné pendant un certain temps. La fonction d'association de cas concerne le moteur de diagnostic `sw-diag-response`. Toutes les alertes de diagnostic de noyau menant à une défaillance du service logiciel peuvent être consultées avec le jeu des données de pile et d'environnement de chaque événement.

L'utilisateur peut maintenant mieux contrôler les noyaux de diagnostic. Lorsqu'un service logiciel ne s'exécute pas correctement et est mis hors service, l'administrateur peut facilement et rapidement voir tous les événements qui ont conduit à la défaillance du service et être mieux informé sur les processus qui ont échoué ainsi que sur l'emplacement de l'échec de chaque processus dans son code d'exécution.

Pour plus d'informations, reportez-vous à la page de manuel `coreadm`(8).

Améliorations apportées à la commande `pfiles`

Dans Oracle Solaris 11.4, la commande `pfiles` accepte un nom de dump noyau en tant qu'argument et peut afficher des informations sur les descripteurs de fichier ouvert par un processus qui effectue un dump noyau. Cette fonctionnalité fournit une aide supplémentaire pour déboguer le dump noyau de processus et connaître la cause à l'origine du dump.

Contrairement aux versions précédentes, dans Oracle Solaris 11.4, la commande `pfiles` n'arrête plus un processus cible en cours d'exécution lors de l'extraction des données sur des fichiers ouverts dans ce processus.

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

Surveiller la latence d'E/S via `fsstat`

La commande `fsstat` comporte une nouvelle option `-l` qui signale les informations de latence pour les opérations `read`, `write` et `readdir`. Les informations de latence étant indépendantes des opérations d'E/S physiques, elles sont représentatives des performances du système de fichiers, telles qu'elles sont constatées par les applications. Cette fonction permet aux utilisateurs d'observer la latence du système de fichiers pour les types de système de fichiers ou les systèmes de fichiers individuels. Elle s'avère utile pour résoudre les problèmes de performances de système de fichiers.

Pour plus d'informations, reportez-vous à la page de manuel `fsstat`(8).

Statistiques de répartition du temps de réponse d'E/S SCSI

Oracle Solaris 11.4 fournit désormais des informations sur le temps de réponse d'E/S SCSI ou sur la répartition de la latence d'E/S pour une meilleure observabilité. La répartition du temps de réponse d'E/S permet d'identifier les valeurs aberrantes de temps de réponse. La répartition est stockée dans un histogramme avec trois options d'échelle `x` : `linear`, `log2-based` et `log10-based`. La répartition peut être affichée à l'aide de la commande `iostat`. L'option `-L` est ajoutée en conjonction avec les options `-x` et `-Y` pour afficher l'histogramme. Ces informations de répartition permettent d'examiner les problèmes de performances.

Pour plus d'informations, reportez-vous aux pages de manuel `sd`(4D) et `iostat`(8).

Fonctions de virtualisation

Cette section décrit les nouvelles fonctions de virtualisation de cette version. Ces fonctions offrent une virtualisation efficace de cloud, sans perte de performances, et permettent l'exécution d'applications à grande échelle dans le cloud grâce à l'utilisation optimisée des ressources.

Configurer des zones immuables via l'exécution dans le chemin de confiance

La fonction de système de fichiers immuable qui a d'abord été introduite dans Oracle Solaris 11 11/11 (root en lecture seule pour les zones non globales) a été considérablement étendue, de sorte que les zones immuables sont maintenant nettement plus faciles à adopter et à utiliser.

Auparavant, pour apporter certaines modifications de configuration aux zones immuables, vous deviez rendre la zone temporairement muable. Dans Oracle Solaris 11.4, vous pouvez lancer l'exécution dans le domaine de chemin de confiance (TPD ou Trusted Path Domain) alors que la zone est encore immuable pour d'autres utilisateurs.

Pour une exécution dans le TPD, effectuez l'une des opérations suivantes :

- Ajoutez l'utilisateur au fichier `/etc/security/tpdusers` et définissez `start/trusted_path` sur `true` dans le service `console-login`.
- Pour l'accès RAD distant au chemin de confiance, définissez `method_context/trusted_path` sur `true` dans le service `rad:remote` et ajoutez `tpd=yes` à l'entrée `user_attr` pour chaque utilisateur disposant d'une autorisation d'accès distant au TPD.

Ces procédures sont décrites en détail dans la section "Administering an Immutable Zone by Using the Trusted Path Domain" du manuel *Creating and Using Oracle Solaris Zones*.

Outre l'exécution dans le TPD par les administrateurs, vous pouvez configurer certains services pour qu'ils s'exécutent dans le TPD, comme décrit dans la section "SMF Services in Immutable Zones" du manuel *Creating and Using Oracle Solaris Zones*.

Prise en charge de la mémoire sécurisée de silicium dans les zones de noyau Oracle Solaris

La prise en charge de Software in Silicon dans les zones de noyau Oracle Solaris a été étendue pour inclure la mémoire sécurisée de silicium (SSM). La fonctionnalité Silicon Secured Memory (SSM) ajoute un

contrôle en temps réel de l'accès aux données en mémoire pour renforcer la protection contre les intrusions malveillantes et code programme incorrect en production et offrir ainsi une sécurité et une fiabilité accrues.

La protection SSM est utilisée par Oracle Database 12c par défaut et est facile à activer pour d'autres applications. Reportez-vous à la section "Software in Silicon Features on Kernel Zones" du manuel *Creating and Using Oracle Solaris Kernel Zones*.

Voir aussi "Protection renforcée contre les attaques malveillantes avec la mémoire sécurisée de silicium" à la page 5.

Prise en charge de zone de noyau Oracle Solaris pour les coprocesseurs SPARC M7 et M8 DAX

Cette fonction permet au logiciel Oracle Solaris d'utiliser la fonctionnalité de requête DAX (Data Analytics Accelerator) des SPARC M7 et M8 en exploitant la bibliothèque HPK (High Performance Kernels) du produit de base de données en mémoire d'Oracle, lors de l'exécution sur une zone de noyau Oracle Solaris.

La bibliothèque HPK du produit SGBDR fournit des opérations optimisées pour le matériel sur des données vectorielles ou en colonne pour les bases de données IMC (In-Memory Columnar). La bibliothèque tire parti des fonctionnalités propres au matériel pour optimiser l'exécution des opérations et peut utiliser des fonctions de requête DAX, lorsqu'elles sont disponibles, dans une zone de noyau Oracle Solaris.

Pour plus d'informations, reportez-vous *Ressources de configuration pour les zones Oracle Solaris*, "Software in Silicon Features on Kernel Zones" du manuel *Création et utilisation des zones de noyau Oracle Solaris* et à la page de manuel `zonecfg`(8).

Zones de noyau Oracle Solaris pour VLAN

Les VLAN fractionnent un réseau de couche 2 (L2) en plusieurs réseaux logiques, afin que chacun ait son propre domaine de diffusion. Avec cette fonction, tous les périphériques connectés à un VLAN peuvent voir le cadre de diffusion de tous les autres périphériques, quel que soit leur emplacement physique.

Auparavant, les zones de noyau Oracle Solaris ne pouvaient déclarer qu'un seul ID VLAN. Dans la version Oracle Solaris 11.4, vous pouvez déclarer d'autres ID VLAN par `anet`, en spécifiant le nouveau type de ressource `vlan` dans une configuration de zone.

Pour plus d'informations, reportez-vous à la section "Configuring Virtual LANs in Kernel Zones" du manuel *Creating and Using Oracle Solaris Kernel Zones*.

Agent de redémarrage délégué de zones Oracle Solaris

L'agent de redémarrage délégué de zones (`system/zones:default`) permet de contrôler l'ordre d'initialisation à l'aide de dépendances et de priorités. Dans les versions précédentes d'Oracle Solaris, ce service ne permettait pas de définir la priorité ni de gérer l'ordre d'initialisation des zones. Si des applications dans différentes zones d'un même système dépendent les unes des autres, par exemple, vous pourriez souhaiter initialiser toutes ces zones en parallèle.

En plus de fournir des jalons pour l'initialisation des zones, l'agent de redémarrage délégué permet également d'ajouter des dépendances pour d'autres zones ou services. Par exemple, la `Zone-C` peut être configurée pour démarrer après la fin de l'initialisation de la `Zone-A` et de la `Zone-B` ou après le démarrage d'un service de pare-feu.

Reportez-vous aux pages de manuel `svc.zones`(8) et `zonecfg`(8) pour plus d'informations sur les nouvelles propriétés `boot-priority` et `smf-dependency`.

Reconfiguration de zone en direct pour les jeux de données sur des zones natives Oracle Solaris

La possibilité de modifier la configuration d'une zone Oracle Solaris sans provoquer d'interruption pour l'utilisateur final ou le service est essentielle pour satisfaire les contrats de niveau de service actuels. Avec la reconfiguration de zone en direct, les utilisateurs peuvent apporter des modifications à la configuration de zone Oracle Solaris, puis les propager vers une zone en cours d'exécution en tant que modification permanente ou temporaire, sans avoir à réinitialiser la zone.

Dans la version Oracle Solaris 11.4, vous pouvez ajouter des jeux de données ZFS à une zone native Oracle Solaris ou en retirer à l'aide de la méthodologie de reconfiguration de zone en direct.

Pour plus d'informations, reportez-vous au Chapitre 4, "Live Zone Reconfiguration of Kernel Zones" du manuel *Création et utilisation des zones de noyau Oracle Solaris*.

Déplacement de zones Oracle Solaris

Oracle Solaris 11.4 vous permet d'utiliser la commande `zoneadm` avec la sous-commande `move` pour déplacer une zone Oracle Solaris installée sur différents URI de stockage. Vous pouvez effectuer les actions suivantes :

- Déplacer une zone Oracle Solaris d'un système de fichiers local (par défaut) vers un stockage partagé
- Déplacer une zone Oracle Solaris d'un stockage partagé vers un système de fichiers local
- Déplacer une zone Oracle Solaris d'un emplacement de stockage partagé vers un autre, tout en changeant également de `zonepath`
- Changer de `zonepath` sans déplacer l'installation de zone Oracle Solaris

Pour plus d'informations, reportez-vous aux pages de manuel `solaris`(7), `zones`(7) et `zoneadm`(8). Vous pouvez également vous reporter à *Création et utilisation des zones Oracle Solaris* .

Migration à froid de zone

Dans Oracle Solaris 11.4, les zones Oracle Solaris ayant un état installé utilisant le stockage partagé peuvent être migrées vers un autre système à l'aide de la commande `zoneadm`. Les zones de noyau Oracle Solaris ayant un état installé ou suspendu utilisant le stockage partagé peuvent également être migrées. Les zones Oracle Solaris et les zones de noyau Oracle Solaris qui ne sont pas en cours d'exécution peuvent être évacuées à l'aide de la commande `sysadm` qui offre une disponibilité de zone accrue lors des temps d'arrêt programmés de zone globale.

Pour plus d'informations, reportez-vous aux pages de manuel `zoneadm`(8), `solaris`(7), `solaris-kz`(7) et `sysadm`(8).

Fonctionnalité multipathing pour les HBA SCSI virtuels Oracle VM Server for SPARC

Dans Oracle Solaris 11.4, le sous-système HBA virtuel prend en charge les pilotes HBA physiques pour lesquels la fonctionnalité multipathing est activée dans leurs fichiers `driver.conf` respectifs. Cette fonction

permet à la fonctionnalité multipathing d'E/S d'Oracle Solaris d'être prise en charge sur un domaine de service `sun4v` sur une base par port HBA, comme décrite dans *Gestion des périphériques SAN et du multipathing dans Oracle Solaris 12*.

Le module `vhba` prend en charge la fonctionnalité multipathing dans le domaine invité depuis la version initiale d'Oracle Solaris 11.3. La prise en charge de la fonctionnalité multipathing dans les deux domaines d'un système `sun4v` améliore la tolérance aux pannes et le débit d'E/S vers les périphériques SCSI.

Masquage de périphérique pour les HBA SCSI virtuels Oracle VM Server for SPARC

Oracle Solaris 11.4 permet à un utilisateur de configurer un périphérique de réseau de stockage (SAN) virtuel afin qu'il représente un jeu explicite de périphériques SCSI physiques. Le comportement original et par défaut d'un périphérique SAN virtuel (vSAN) vise à représenter *tous* les périphériques SCSI physiques accessibles à partir du port initiateur du HBA SCSI spécifié par l'utilisateur.

Dans Oracle Solaris 11.4, un utilisateur peut saisir des commandes pour ajouter et retirer dynamiquement des périphériques SCSI physiques explicites d'un périphérique vSAN spécifié. En associant un périphérique vSAN spécifique à un domaine invité donné, l'utilisateur exerce un contrôle complet sur les périphériques SCSI physiques auxquels un domaine invité donné peut accéder.

Fonctions de gestion du système

Cette section décrit les nouvelles fonctions de gestion système de cette version. Ces nouvelles fonctionnalités permettent de configurer des services grâce à une gestion transparente de la configuration, d'automatiser la mise en application des configurations sur les systèmes, mais également de fournir un accès administratif distant sécurisé.

Voir aussi "Configurer des zones immuables via l'exécution dans le chemin de confiance" à la page 19.

Visualisation des données système et analyse des performances avec le tableau de bord de l'interface Web du système Oracle Solaris

Oracle Solaris offre un grand nombre d'outils d'observabilité système, parmi lesquels des outils de statistiques (tels que `mpstat`), DTrace et des enregistrements d'audit. Le tableau de bord de l'interface Web du système Oracle Solaris vous permet d'afficher facilement différents types de données de performances d'application ou système, sous forme graphique, pour une observabilité et une analyse plus efficaces. Identifiez l'état actuel du système et visualisez des statistiques, des pannes et des modifications administratives au fil du temps et en comparaison avec d'autre périodes. Ouvrez une fiche de données pour voir plus de détails et des données connexes supplémentaires. Comparez les graphiques de données actuels et historiques pour visualiser les anomalies et les tendances, consulter des données connexes dans d'autres diagrammes sur la même page et voir des événements, tels que des événements d'audit sur le même graphique avec d'autres données.

Le tableau de bord de l'interface Web du système Oracle Solaris permet de visualiser les performances actuelles et récentes, les éventuelles pannes système récentes ainsi que d'autres événements. Cette combinaison d'informations vous aide à déterminer les ressources système à examiner pour diagnostiquer les problèmes.

Vous pouvez afficher l'utilisation moyenne de toutes les ressources d'un type sélectionné ou l'utilisation d'une seule ressource. Par exemple, vous pouvez déterminer quelles applications sont responsables de la plupart du trafic du réseau sur un système. De la même façon, outre les données sur l'utilisation globale de CPU, vous pouvez sélectionner la partition de zone des données d'utilisation de CPU pour déterminer quelles zones utilisent le plus de CPU. Vous pouvez déterminer si une ressource est allouée à une zone ou une charge de travail en particulier.

Pour plus d'informations, reportez-vous à *Utilisation des fonctions d'analyse Oracle Solaris 12*. Pour plus d'informations sur le mode de stockage de vos données dans le magasin de statistiques sous-jacent, reportez-vous à *Ajout de données personnalisées à des analyses Oracle Solaris 12*.

Affichage de l'utilisation et des performances DAX

Sur les systèmes SPARC M7, M8, T7 et T8, vous pouvez utiliser la commande `daxstat` pour afficher les statistiques DAX (par dax, par cpu ou par file d'attente) sous forme de tableau.

La commande `daxinfo` permet aux utilisateurs de déterminer la configuration statique du matériel DAX disponible sur un système. Ces informations permettent de générer des rapports de performances et de diagnostic.

Pour plus d'informations, reportez-vous à la section "Displaying DAX Information" du manuel *Managing System Information, Processes, and Performance in Oracle Solaris 11.4* et aux pages de manuel `daxstat`(8) et `daxinfo`(8).

Groupes de propriétés imbriqués SMF

L'utilitaire de gestion des services (SMF) d'Oracle Solaris fournit une infrastructure pour stocker les données de configuration système dans un emplacement central, plutôt que dans des fichiers de configuration spécifiques d'une application. La fonction de modélisation SMF était limitée dans sa capacité à modéliser les affiliations parmi les données de configuration.

La version Oracle Solaris 11.4 modifie la relation de groupe de propriétés SMF afin qu'un groupe de propriétés ne puisse pas être uniquement apparenté par un service ou une instance, mais puisse également l'être par un autre groupe de propriétés. Avec l'introduction de cette relation, il est désormais possible de modéliser une grande diversité de données de configuration système. Conséquence de l'ajout de cette relation, lors de l'identification d'un groupe de propriétés, vous devez tenir compte du nom mais aussi du lignage.

Les groupes de propriétés imbriqués sont soumis au même modèle de privilège ainsi qu'à la même vérification de modèle que les groupes de propriétés. Pour plus d'informations, reportez-vous à la page de manuel `smf_template`(7).

Nouvelles couches de profil SMF

Oracle Solaris 11.4 présente trois nouvelles couches de profil SMF : `enterprise-profile`, `node-profile` et `sysconfig-profile`. Dans les versions précédentes, la configuration SMF pouvait uniquement être appliquée aux couches `site-profile` et `admin`. Dans cette version, en utilisant plusieurs couches, vous pouvez appliquer une configuration générale à la couche `enterprise-profile`, une configuration propre à l'emplacement à la couche `site-profile` et une configuration spécifique de l'hôte à la couche `node-profile`. Cette fonction favorise l'utilisation optimale des profils SMF dans des environnements où des sous-ensembles de systèmes ou des systèmes individuels doivent remplacer une configuration plus générale.

Pour plus d'informations, reportez-vous à la section "Repository Layers" du manuel *Managing System Services in Oracle Solaris 11.4* et au Chapitre 5, "Configuring Multiple Systems" du manuel *Managing System Services in Oracle Solaris 11.4*. Voir aussi les pages de manuel `smf`(7), `svccfg`(8) et `svcprop`(1) et les pages de manuel `sysconfig`(8), `solaris`(7), `solaris-kz`(7) et `smf_bootstrap`(7).

Services d'objectif

Oracle Solaris 11.4 inclut un nouveau type de services, les services d'objectif, qui fournissent un seul point de surveillance pour un ensemble de services configurables, dont dépendent les services d'objectif. Si une dépendance d'un service d'objectif ne peut pas être satisfaite, le service prend l'état de maintenance et génère une alerte FMA de logiciel.

Pour plus d'informations, reportez-vous au Chapitre 7, "Creating a Service that Notifies if Conditions are not Satisfied" du manuel *Développement de services système dans Oracle Solaris 12* et aux pages de manuel `smf`(7) et `svcadm`(8).

Diagnostic des défaillances de connexion à chaud de périphérique

Dans Oracle Solaris 11.4, la nouvelle fonction Informations sur l'utilisation de périphérique facilite le diagnostic des défaillances de la commande `hotplug`. Dans les versions précédentes, en cas d'échec de retrait d'un périphérique occupé par la commande `hotplug`, le message d'erreur indiquant que "les périphériques ou les ressources étaient occupés" s'affichait sans autre explication, ce qui rendait difficile le diagnostic du problème. Grâce à cette nouvelle fonction, des informations supplémentaires s'affichent pour expliquer ce qui a ouvert ou retenu le périphérique, ce qui facilite le diagnostic du problème.

Par exemple, pour vérifier si le périphérique est occupé, utilisez la commande suivante :

```
# hotplug offline /pci@0,0 pci.1,0
ERROR: devices or resources are busy.
/pci@0,0/pci8086,3408@1/pci1000,1000@0/sd@0,0:
   { Hold: module devfs (modid=6). }
   { Hold: module specfs (modid=3): spec_open() }
   { Open: process format[123501]. }
   { Open: module zfs (modid=49). }
```

Pour plus d'informations, reportez-vous à *Gestion des périphériques dans Oracle Solaris 12*.

Utilitaire `sysadm`

Oracle Solaris 11.4 ajoute le nouvel utilitaire `sysadm` qui peut être utilisé pour contrôler le mode de maintenance d'un système et exécuter l'évacuation des zones hébergées sur le système. Le démarrage d'un mode de maintenance journalise un enregistrement d'audit et empêche le rattachement, l'initialisation ou la migration entrante suivants de toutes les zones dans le système. L'hôte peut être évacué en migrant toutes les zones de marque `solaris-kz` du système vers des cibles spécifiées dans l'instance de service SMF des zones.

Le mode de maintenance et l'évacuation peuvent être utilisés pour effectuer l'administration sur un hôte de zones ou pour le retirer du service. Vous pouvez empêcher les nouvelles zones de se rattacher ou de s'initialiser, de migrer vers des zones de noyau en cours d'exécution et effectuer certaines tâches de maintenance nécessitant une réinitialisation, telles que la mise à jour d'Oracle Solaris, et enfin migrer en retour ces zones de noyau, avec seulement quelques commandes et sans interruption pour les zones de noyau en cours d'exécution.

Pour plus d'informations, reportez-vous à la page de manuel `sysadm`(8).

Automatisation de la configuration des serveurs OpenLDAP et OUD

L'utilitaire `ldapservercfg` automatise la configuration des serveurs OpenLDAP et OUD (Oracle Unified Directory) pour prendre en charge les services de dénomination LDAP et la gestion des comptes Oracle Solaris. L'utilitaire est intégré au service SMF `svc:/network/ldap/server:openldap` et configure automatiquement le serveur lors de sa première activation. Il peut également être exécuté en mode interactif pour personnaliser la configuration du serveur OpenLDAP ou pour configurer le serveur OUD. L'utilitaire `ldapservercfg` aide les utilisateurs à déployer facilement les serveurs OpenLDAP et OUD sur des systèmes Oracle Solaris. Il active également la fonctionnalité pour la gestion des comptes distante à l'aide de RAD.

Pour plus d'informations, reportez-vous à la page de manuel `ldapservercfg(8)`.

Logiciel de gestion de la configuration Puppet

Puppet est un logiciel que vous pouvez utiliser sur plusieurs plates-formes pour automatiser la gestion de la configuration, notamment les serveurs Oracle Solaris et leurs sous-systèmes.

Puppet vous permet de standardiser et d'appliquer des configurations de ressources à l'ensemble de votre infrastructure informatique. Oracle Solaris 11.4 inclut les types de ressources Puppet de base : fichiers, packages, utilisateurs et services. En outre, de nombreux modules sont inclus pour la gestion d'autres logiciels tiers sur Oracle Solaris. Enfin, plusieurs types de ressources propres à Oracle Solaris sont fournis pour être utilisés dans la version Oracle Solaris, notamment les zones Oracle Solaris.

La nouvelle option de configuration Puppet d'Oracle Solaris `config/degrade_smf_on_error` `Degrade_smf_on_error` fait passer le service `puppet:agent` à l'état dégradé lorsqu'une erreur de ressource se produit lors de l'application du manifeste Puppet. Puppet continue de s'exécuter une fois marqué comme étant dégradé. Grâce à cette option, les erreurs de ressource dans les applications du manifeste Puppet sont plus faciles à voir pour les utilisateurs.

Notez qu'Oracle Solaris 11.4 prend en charge Puppet 5.5. Ce package logiciel n'est pas installé par défaut sur votre système.

Si une précédente version Puppet est installée sur un système, elle sera automatiquement mise à niveau vers Puppet 5.5. Pour les informations importantes sur cette mise à niveau, reportez-vous à la section "What's New in Puppet in Oracle Solaris 11.4" du manuel *Utilisation de Puppet pour la gestion de la configuration dans Oracle Solaris 12*.

Pour des informations générales sur Puppet, reportez-vous à la documentation Puppet.

MCollective

The Marionette Collective, également appelé MCollective, est une structure qui vous permet de créer et de gérer facilement un grand nombre de serveurs. Lorsque l'on travaille avec un grand nombre de serveurs, il est difficile de s'appuyer sur une liste statique d'outils pour la gestion système. MCollective utilise une méthode de découverte basée sur les métadonnées, ainsi que le filtrage pour rechercher des hôtes.

MCollective utilise également un modèle de publication-abonnement pour diffuser une demande à tous les serveurs connectés au composant middleware. Ces demandes comportent des filtres joints, de sorte que seuls les serveurs correspondant à un filtre répondront aux demandes.

Pour plus d'informations, reportez-vous à *Utilisation de Puppet pour la gestion de la configuration dans Oracle Solaris 12* et à Using MCollective Command Line Applications.

Augeas

Augeas est une bibliothèque et un outil de ligne de commande permettant de modifier des fichiers de configuration UNIX ayant des formats distincts. Lorsqu'il est appelé, Augeas fournit une interface de ligne de commande où les fichiers de configuration peuvent être lus et présentés sous une forme arborescente. Ces données peuvent alors être manipulées dans l'interface Augeas. Les données sont ensuite reconverties dans le format des fichiers de configuration d'origine pour sauvegarde.

Augeas fournit une API publique unique pour la manipulation de divers fichiers de configuration UNIX. D'autres applications peuvent tirer parti de cette API, au lieu que chaque application fournisse sa propre solution pour la modification des fichiers de configuration.

Attributs utilisateur par défaut pour les comptes LDAP

Dans Oracle Solaris 11.4, la fonctionnalité des attributs utilisateur qualifiés est étendue pour fournir des paramètres par défaut pour des hôtes ou des groupes réseau spécifiques. Les comptes utilisateur basés sur LDAP sans attributs explicitement affectés peuvent hériter des attributs par défaut de l'hôte sur lequel ils sont exécutés. Si aucun attribut par défaut basé sur l'hôte n'est spécifié et que l'utilisateur est membre d'un groupe réseau, les attributs associés au groupe réseau sont hérités. Cette fonctionnalité simplifie l'administration des comptes basés sur LDAP en leur permettant de partager des attributs utilisateur communs fondés sur l'appartenance à un groupe réseau.

Pour plus d'informations, reportez-vous aux pages de manuel `user_attr`(5), `useradd`(8), `userdel`(8) et `usermod`(8).

Outil `useradm`

L'outil `useradm` est un outil basé sur un menu interactif pour l'administration des comptes d'utilisateur et de rôle. Cet outil remplace le Gestionnaire d'utilisateurs Visual Panels. L'outil est implémenté en tant que client RAD à l'aide des liaisons Python décrites dans `usermgr(3rad)`, et peut être exécuté dans n'importe quelle fenêtre de terminal. L'interface utilisateur comprend des menus hiérarchiques contenant des listes de sélections disponibles.

L'interface basée sur menu de l'outil `useradm` simplifie la gestion des utilisateurs et des rôles, et prend en charge tous les aspects de la gestion des comptes, tels que les droits d'accès, l'audit et la gestion des mots de passe. Tous les choix valides sont présentés dans des listes déroulantes que vous pouvez sélectionner à l'aide des combinaisons de touches appropriées.

Pour plus d'informations, reportez-vous à la page de manuel `useradm`(8).

Bogues identifiés par la sortie affichant les pannes

Une nouvelle fonction `stackdiag` permet à `fmadm faulty` d'afficher la liste des bogues susceptibles d'avoir provoqué la panne. Grâce à cette liste de bogues connus, vous pouvez rechercher des solutions sur My Oracle Support.

Pour plus d'informations, reportez-vous à *Gestion des pannes, des défauts et des alertes dans Oracle Solaris 12* et à la page de manuel `stackdiag`(1).

Utilitaire `fcinfo`

Dans Oracle Solaris 11.4, l'utilitaire `fcinfo` a été amélioré pour fournir la fonctionnalité suivante :

- Etablir si un port HBA a accès à un port distant ou non. La commande `fcinfo remote-port` permet d'afficher le nombre et les détails de tous les ports distants pour chaque port HBA, en l'absence d'option.
- Etablir la classe du chemin et l'état du chemin de tous les LUN présentés par une baie de stockage donnée. La commande `fcinfo lu -v` peut spécifier le port distant et le nom universel (WWN) du noeud avec les options `-P` et `-N`, respectivement.

Pour plus d'informations, reportez-vous à la page de manuel `fcinfo`(8).

Nouvelles options de gestion de référentiel IPS

L'Image Packaging System (IPS) d'Oracle Solaris présente de nouvelles options pour faciliter la gestion de l'accès au référentiel de package et la résolution de certains problèmes d'installation et de mise à jour :

- Ignorer le cache réseau. Une nouvelle option globale nommée `--no-network-cache` est ajoutée pour permettre d'ignorer les données réseau mises en cache.

  Les problèmes d'accès aux données de package peuvent être provoqués par la mise en cache de proxies entre le client du package et les référentiels de packages basés sur le réseau. Pour résoudre ces problèmes, utilisez l'option `--no-network-cache` afin de pouvoir toujours obtenir les données de package à partir d'un référentiel et pas à partir des caches que pourrait avoir un proxy HTTP.

  Pour plus d'informations, reportez-vous à la section "Initial Troubleshooting Steps" du manuel *Ajout et mise à jour de logiciels sur des systèmes Oracle Solaris 12* et à la page de manuel `pkg`(1).
- Activer ou désactiver une origine spécifique. La combinaison des options `-d`, `-e` et `-g` de la sous-commande `pkg set-publisher` permet d'activer ou de désactiver l'origine spécifique d'un serveur de publication.

  Pour plus d'informations, reportez-vous à la section "Enabling and Disabling Publisher Origins" du manuel *Ajout et mise à jour de logiciels sur des systèmes Oracle Solaris 12* et à la page de manuel `pkg`(1).

IPS présente aussi de meilleurs messages d'erreur. Par exemple, un message d'erreur qui signale une entrée de fichier manquante inclut également le package qui fournit le fichier.

Fonctions d'installation et de gestion des logiciels

Cette section décrit les nouvelles fonctions d'installation et de gestion des logiciels de cette version. Ces fonctions permettent des déploiements et des mises à jour rapides via des outils de gestion et d'installation de logiciels.

Démarrage des services système à la première initialisation

L'outil `svc-create-first-boot` fournit une interface unique pour créer, personnaliser et publier un package de service de première initialisation. Indiquez le chemin d'accès au référentiel du package et le script de première initialisation en tant qu'arguments de ligne de commande ; l'outil publiera le package de services de première initialisation vers le référentiel spécifié. L'utilisation de cet outil simplifie automatiquement l'exécution des scripts lors de la première initialisation.

Pour plus d'informations, reportez-vous à la page de manuel `svc-create-first-boot`(1).

API RAD pour programme d'installation automatisée

Oracle Solaris 11.4 présente l'API RAD pour le programme d'installation automatisée. Cette API fournit une fonctionnalité pour l'administration distante d'un serveur d'installation automatisée (AI). Vous pouvez écrire des programmes pour gérer le serveur AI à l'aide de tout langage client pris en charge par RAD.

Pour plus d'informations, reportez-vous à la page de manuel `autoinstall(3rad)`.

Prise en charge du programme d’installation automatisée pour HMAC-SHA256

Les installations automatisées d'Oracle Solaris peuvent maintenant être sécurisées par HMAC-SHA256. Les administrateurs peuvent choisir HMAC-SHA256 en tant que stratégie pour l'algorithme HMAC pour la sécurisation des nouveaux services et clients AI. Ils peuvent également mettre à niveau le type HMAC pour que les services et les clients soient appliqués immédiatement, ou générer des clés HMAC-SHA256 devant être installées par l'utilisateur, après quoi HMAC-SHA256 peut être appliqué par l'administrateur. Les systèmes existants sécurisés avec HMAC-SHA1 continueront de l'être jusqu'à la mise à niveau de HMAC-SHA1.

HMAC-SHA256 fournit l'authentification et l'intégrité pour les premières phases d'initialisation d'une installation automatisée d'Oracle Solaris utilisant le protocole d'initialisation de réseau WAN. Cette prise en charge dans AI, couplée à la prise en charge du microprogramme OBP de SPARC, garantit des normes de sécurité modernes pour les installations de réseau étendu (WAN).

Pour plus d'informations, reportez-vous à la page de manuel `installadm`(8).

Déshydratation et réhydratation des archives Oracle Solaris Unified Archives

La déshydratation et la réhydratation des archives Oracle Solaris Unified Archives (UAR) améliore la technologie d'archivage actuelle pour utiliser la technologie de déshydratation et de réhydratation d'IPS et réduire ainsi l'encombrement d'une archive UAR créée.

Dans ce contexte, déshydrater une archive consiste à retirer tous les fichiers packagés non modifiables et les liens physiques packagés du root de remplacement d'une image d'archive. Un fichier packagé non modifiable est un fichier fourni par la version actuellement installée d'un package ne comportant aucun attribut de conservation ou de recouvrement ou qui n'a aucune valeur balisée de `dehydrate=False`. Par ailleurs, la réhydratation réinstalle tous les fichiers et liens physiques retirés par la déshydratation pour restaurer l'image d'archive à son état d'origine.

Cette fonction permet aux éditeurs de logiciels indépendants de fournir des piles applicatives dans une archive UAR où le système d'exploitation de base serait déshydraté, sans se préoccuper du copyright et des droits de distribution associés au système d'exploitation. De fait, l'éditeur de logiciels pourrait créer une pile applicative entièrement déployable et une image du système d'exploitation, puis au moyen d'une opération de déshydratation l'image du système d'exploitation serait retirée d'une archive en laissant seulement l'application de l'éditeur. Un client pourrait ensuite déployer cette archive déshydratée et réhydrater le système d'exploitation à partir d'une copie légale du référentiel du système d'exploitation.

Comme les archives sont parfois très volumineuses, la déshydrations offre une solution pratique pour qu'elles prennent moins de place sur un système, ce qui permet une meilleure gestion du stockage pour les archives multiples.

Dans le cas où les clients disposent d'archives déshydratées qu'ils souhaitent déployer sur plusieurs systèmes, la sous-commande `rehydrate` leur serait utile. En réhydratant une archive pour qu'elle retrouve son

état d'hydratation normal, vous pouvez réduire le temps nécessaire au déploiement car une archive hydratée est plus rapide à déployer qu'une archive déshydratée.

Pour plus d'informations, reportez-vous à la page de manuel `archiveadm`(8).

Prise en charge de `cloudbase-init`

Le service `cloudbase-init` effectue la configuration initiale des systèmes d'exploitation invités dans le cloud. Ces tâches incluent la création d'utilisateurs, la génération de mots de passe, la configuration de réseaux statiques, le nom d'hôte, les clés publiques SSH et les scripts de données utilisateur.

La version Oracle Solaris 11.4 de `cloudbase-init` est un service SMF (`application/cloudbase-init`) fourni par le package IPS `cloudbase-init`.

- Le package `cloudbase-init` n'est pas installé par défaut. Installez le package uniquement dans des images qui seront déployées dans des environnements cloud.
- Le service est activé par défaut.
- Le fichier de configuration, `/etc/cloudbase-init.conf`, active uniquement le module d'extension `UserData`.

Les scripts qui sont exportés par le biais des données utilisateur exécutent généralement des tâches de configuration d'application et de système nécessitant un accès privilégié. En conséquence, le service `cloudbase-init` s'exécute en tant qu'utilisateur `root`, et les scripts de données utilisateur doivent également s'exécuter en tant que `root`.

Initialisation d'Oracle Solaris via des pools d'initialisation sur iSCSI-iSER

Avec cette fonction, les pools d'initialisation peuvent utiliser iSCSI-iSER en tant que protocole de transport par défaut à la place du protocole iSCSI-IPoIB pour initialiser Oracle Solaris. Le serveur peut utiliser des pools d'initialisation pour initialiser des périphériques de stockage inaccessibles par microprogramme sur des cibles iSCSI. L'utilisation du protocole iSCSI-iSER offre les avantages suivants :

- Initialisation d'Oracle Solaris plus rapide que sur iSCSI-IPoIB
- Accès à `rpool` via iSCSI-iSER avec :
  - Débit supérieur
  - Latence de transport faible
  - Utilisation de CPU faible
- Aucune configuration requise

Initialisation UEFI sécurisée

L'initialisation UEFI sécurisée sur Oracle Solaris x86 vous permet d'installer et d'initialiser Oracle Solaris sur des plates-formes où l'initialisation UEFI sécurisée est activée. Cette fonction fournit une sécurité supérieure en maintenant une chaîne de confiance lors de l'initialisation : les signatures numériques des microprogrammes et logiciels sont vérifiées avant l'exécution de la phase suivante. La chaîne n'est jamais rompue à cause de microprogrammes ou logiciels non signés, endommagés ou non fiables pendant le processus d'initialisation. Cette fonction contribue à assurer que les microprogrammes et logiciels utilisés pour initialiser Oracle Solaris sur une plate-forme matérielle sont corrects et non pas été modifiés ou altérés.

Pour plus d'informations, reportez-vous à *Sécurisation des systèmes et des périphériques connectés dans Oracle Solaris 12*.

Améliorations pour les développeurs

Cette section décrit les améliorations à l'attention des développeurs comprises dans cette version qui facilitent le développement d'applications sur la plate-forme Oracle Solaris grâce aux bibliothèques de pointe et à la fiabilité des structures.

Prise en charge de la norme de langage de programmation C11

Oracle Solaris 11.4 assure la prise en charge de la norme de langage de programmation C11 : "ISO/IEC 9899:2011 - Technologie de l'information - Langage de programmation - C". La norme C11 est une version compatible de la norme C99. La norme de langage de programmation C fait partie des spécifications SUS (Single UNIX Specification) depuis longtemps. En revanche, la nouvelle norme de langage de programmation, C11, est disponible séparément et avant la spécification UNIX suivante.

Oracle Solaris 11.4 assure la prise en charge de C11 avec C99 pour fournir aux clients un support C11 avant son inclusion dans une spécification UNIX future. La nouvelle norme peut être utilisée avec Oracle Developer Studio 12.5 ou 12.6, GCC 5 ou 7, et les compilateurs C LLVM/Clang 6.0. Les développeurs peuvent également écrire des programmes en C à l'aide de la nouvelle norme de langage de programmation C disponible.

Environnement de compilation standard

Dans Oracle Solaris 11.4, le mode de compilation par défaut (lorsqu'aucune macro de test de fonction n'est utilisée pour demander la conformité à une norme POSIX donnée), rend visible les éléments suivants :

- L'espace de noms correspondant à la dernière spécification POSIX
- Tous les autres fonctions et noms fournis normalement par le système d'exploitation Oracle Solaris

Pour Oracle Solaris 11.4, la dernière spécification POSIX est IEEE Std. 1003.1-2008 Base Specifications, Issue 7 (également appelée XPG7, UNIX V7, SUSv4).

La compatibilité binaire est conservée. En revanche, la compatibilité source pourrait être affectée comme suit :

Threads POSIX	La macro de test de fonction `_POSIX_PTHREAD_SEMANTICS` est obsolète et n'est plus nécessaire. Elle ne sera testée par aucun en-tête de fichier. Les versions des interfaces qui n'étaient auparavant visibles qu'à l'aide de `-D_POSIX_PTHREAD_SEMANTICS` ou de macros de test de fonction standard appropriées sont maintenant visibles par défaut. Celles-ci incluent `asctime_r()`, `ctime_r()`, `getgrgid_r()`, `getgrnam_r()`, `getlogin_r()`, `getpwnam_r()`, `getpwuid_r()`, `readdir_r()`, `sigwait()` et `ttyname_r()`. Les précédentes interfaces par défaut, qui était basées sur une norme de threads POSIX provisoire, sont toujours disponibles au moment de la compilation à l'aide de `-D__USE_DRAFT6_PROTOTYPES__`. Pour plus d'informations, reportez-vous à la page de manuel `intro`(3).
X/Open Sockets (XNS Issue 4)	Auparavant, `-D_XOPEN_SOURCE=500` était nécessaire pour l'utilisation des interfaces de sockets définies par la norme X/Open. Ces interfaces sont maintenant visibles dans l'environnement de compilation par défaut. La compilation des applications

s'appuyant sur des sockets anciens de style SunOS4.x requiert maintenant l'utilisation de `-D__USE_SUNOS_SOCKETS__`. Pour plus d'informations, reportez-vous à la page de manuel `socket.h`(3HEAD).

Bibliothèque de contrôle des processus

Oracle Solaris 11.4 inclut une nouvelle bibliothèque de contrôle des processus, `libproc`, offrant une interface de niveau supérieur pour les fonctions de l'interface `/proc`. La bibliothèque fournit également l'accès à des informations, telles que des tables de symboles, qui sont nécessaires pour l'examen et le contrôle des processus et des threads.

Un processus de contrôle utilisant `libproc` peut généralement :

- Obtenir un processus victime en suspendant son exécution
- Examiner l'état du processus victime
- Examiner et modifier l'espace d'adressage du processus victime
- Faire exécuter au processus victime des appels système pour le compte du processus de contrôle
- Libérer le processus victime pour qu'il s'exécute à nouveau sans problème

La bibliothèque `libproc` fournit tous les mécanismes nécessaires à un débogueur de point d'arrêt pour faire son travail. Elle facilite également la création d'applications de contrôle ponctuelles pour des tâches simples sur des processus victime sans que les processus soient conscients de l'intrusion.

Pour plus d'informations, reportez-vous à la page de manuel `libproc`(3LIB).

Prise en charge améliorée de l'environnement linguistique

Oracle Solaris 11.4 inclut des améliorations apportées à la prise en charge des API d'environnement linguistique existant fournies par `libc` et l'ajout de nouvelles API définies dans la norme UNIX V7. La commande `uselocale` et d'autres API définies dans la norme UNIX V7 ont été ajoutées pour prendre en charge les environnements linguistiques entre les threads ainsi que la modification de l'environnement linguistique du thread. En combinaison avec les nouvelles API, les API prenant en charge l'environnement linguistique existant ont été mises à jour pour être totalement sécurisées pour l'architecture colocative. Le traitement de l'environnement linguistique sous-jacent dans `libc` a été amélioré pour offrir de meilleures performances et une utilisation de ressources inférieure des applications utilisant plusieurs environnements linguistiques.

Pour plus d'informations, reportez-vous aux pages de manuel `uselocale`(3C), `newlocale`(3C), `freelocale`(3C), `wctype`(3C) et `localedef`(1).

Points d'observation en mode utilisateur

Oracle Solaris 11.4 implémente désormais les points d'observation en mode utilisateur avec la mémoire sécurisée de silicium (SSM) à la place des mappages de mémoire virtuelle. Un point d'observation est un événement qui est déclenché lorsqu'un emplacement de mémoire fait l'objet d'écriture ou de lecture et peut être utilisé pour le débogage et l'analyse des performances. Les points d'observation sont actuellement implémentés en rendant la page contenant l'adresse inaccessible. Cette action ralentit considérablement l'exécution si le thread touche fréquemment des emplacements non connexes sur la même page. Par contraste, SSM offre une granularité beaucoup plus fine avec une ligne de cache de 64 octets. En outre, SSM est multithread, tandis que tous les threads partagent les mêmes pages de mémoire virtuelle.

Pour plus d'informations, reportez-vous aux pages de manuel `dbx(1)` et `mdb`(1).

Bibliothèque DTrace

Oracle Solaris 11.4 inclut une nouvelle bibliothèque de contrôle des processus `libdtrace`, qui permet aux développeurs d'écrire des applications `bespoke` DTrace.

Pour plus d'informations, reportez-vous à l'Annexe A, "libdtrace API Reference," du manuel *Guide d'utilisation d'Oracle Solaris 12 DTrace (Dynamic Tracing)*.

Prise en charge de DWARF dans DTrace

Dans Oracle Solaris 11.4, DTrace peut utiliser DWARF pour effectuer la traduction des métadonnées d'adresse en code source pour les processus utilisateur. La nouvelle option `uresolve` permet aux actions `ustack`, `uaddr` et `printf` de DTrace de traduire des adresses utilisateur en numéros de ligne et noms de fichier de code source, grâce à la présence des informations de débogage DWARF. Cette fonction permet une interprétation plus intuitive de la sortie de diagnostic tout en conservant la compatibilité avec les normes communes de compilateur.

Pour plus d'informations, reportez-vous aux actions `ustack`, `uaddr` et `printf` de la section "Data Recording Actions" du manuel *Guide d'utilisation d'Oracle Solaris 12 DTrace (Dynamic Tracing)*.

Prise en charge de la commande `pstack` pour les numéros de ligne encodés DWARF

Dans Oracle Solaris 11.4, la commande `pstack` annotera les cadres avec les métadonnées de code source, grâce à la présence des informations de débogage DWARF. Cette fonction permet une interprétation plus intuitive de la sortie de diagnostic tout en conservant la compatibilité avec les normes communes de compilateur.

Pour plus d'informations, reportez-vous à la commande `pstack` dans la page de manuel `proc`(1).

Déroulement DWARF dans les commandes `pstack` et `mdb`

Dans Oracle Solaris 11.4, les commandes `pstack` et `mdb` prennent en charge DWARF et le déroulement de pile de style DWARF pour les processus utilisateur. En outre, les commandes `pstack` et `mdb` permettent également la récupération des arguments de fonction à partir de processus compilés avec la nouvelle option `-preserve_argvalues=complete` d'Oracle Developer Studio. Cette fonction apporte des améliorations spécifiques à l'observabilité et la possibilité de diagnostic des processus `amd64`, même si la fonctionnalité s'applique à la fois aux processus 32 et 64 bits sur x64 et SPARC.

La commande `mdb ::stackregs dcmd` est maintenant activée pour `amd64`, où les registres de cadre sont récupérés à l'aide de tables de déroulement de style DWARF.

Cython

Cython est un compilateur statique d'optimisation pour le langage de programmation Python et le langage de programmation Cython étendu basé sur Pyrex. Cette fonction permet la génération de code à hautes performances utilisant Python.

Pour plus d'informations, reportez-vous à Cython C-Extensions for Python.

Oracle Database Programming Interface-C

Oracle Database Programming Interface-C (ODPI-C) est un wrapper OCI (Oracle Call Interface), fonctionnant en toute transparence avec les différentes versions des bibliothèques Oracle Instant Client.

ODPI-C élimine la nécessité pour les applications de définir `LD_LIBRARY_PATH` avant l'exécution. Qui plus est, ODPI-C fonctionne en toute transparence avec plusieurs versions des bibliothèques Oracle Instant Client. Les logiciels qui nécessitent l'utilisation des bibliothèques Oracle Instant Client n'auront pas besoin du paramètre `ORACLE_HOME` avant exécution.

Pour utiliser ODPI-C, installez le package `developer/oracle/odpi`.

Pour plus d'informations sur ODPI-C, reportez-vous au projet Oracle Database Programming Interface for Drivers and Applications sur GitHub et à la page de manuel `libodpic`(3LIB). Oracle Instant Client est disponible au format IPS et il n'est pas nécessaire de visiter OTN pour télécharger les fichiers `.zip`.

Module Python `cx_Oracle`

`cx_Oracle` est un module Python qui permet d'accéder à Oracle Database 12c et 11i à partir d'applications Python. Bien que ce module soit généralement disponible dans des packages pré-intégrés pour d'autres systèmes d'exploitation, il ne l'était pas jusqu'à présent pour Oracle Solaris. Le module est disponible en 32 bits et 64 bits. La version standard 5.2 d'Oracle Solaris peut être utilisée avec Python 2.7 et 3.4.

Pour plus d'informations, reportez-vous à la documentation pour cx_Oracle.

Nouvelles fonctions supplémentaires

Cette section décrit d'autres nouvelles fonctions disponibles dans cette version. Ces nouvelles fonctions et améliorations viennent s'ajouter à la collection exhaustive d'utilitaires, de services et d'outils destinés à améliorer la productivité.

Environnement de bureau GNOME

L'environnement de bureau Oracle Solaris a été mis à niveau de GNOME 2.30 vers GNOME 3.24 dans Oracle Solaris 11.4. Les principales applications de bureau ont également été mises à jour. Certaines applications facultatives ne figurent plus dans Oracle Solaris. Les utilisateurs peuvent opter pour l'environnement shell GNOME ou l'environnement classique GNOME sur l'écran de connexion. Pour plus de détails, consultez le document *Oracle Solaris 11.4 Desktop*.

Oracle Solaris 11.4 ne prend plus en charge le bureau multiniveau étiqueté Trusted Extensions et les configurations Sun Ray. Pour plus de détails, reportez-vous à End of Features (EOF) Planned for Future Releases of Oracle Solaris.

Améliorations apportées à la commande `man`

Dans Oracle Solaris 11.4, les pages de manuel utilisant les sections System V ont été renumérotées en sections standard. Les sections `1m`, `4`, `5`, `7`, et leurs sous-sections utilisées dans les versions précédentes correspondent maintenant aux sections `8`, `5`, `7`, `4` et à leurs sous-sections, respectivement. Les utilisateurs qui connaissent bien d'autres plates-formes, telles que BSD, Linux ou MacOS X peuvent utiliser les mêmes numéros de section avec la commande `man`.

La commande `man` prend en charge la recherche de nom de page hiérarchique, avec une ou plusieurs barres obliques. Par exemple, `man system/name-service/switch` peut afficher la page de manuel à partir de `usr/share/man/man8s/system/name-service/switch.8s`.

La commande `man` prend également en charge le style d'abréviation pour les sous-sections. Par exemple, il est possible de rechercher la page de manuel `printf(3c)` en utilisant `man printf.3` ou `man -s 3 printf`.

La commande `man` peut mapper les anciens numéros de section System V aux numéros standard, si nécessaire, ce qui facilite la recherche de références dans la documentation plus ancienne.

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

Documents Oracle Solaris en ligne pour RAD et le tableau de bord Web

Les documents en ligne Oracle Solaris pour RAD et l'application de tableau de bord Web affichent des documents faciles à rechercher dans le tableau de bord de l'interface Web du système Oracle Solaris. Pour accéder à la documentation fournie par cette application, utilisez le menu de l'application du tableau de bord de l'interface Web du système. Les documents sont installés par les packages IPS dans l'emplacement suivant : `/usr/lib/webui/htdocs/solaris/apps/docs`.

Le tableau de bord de l'interface Web du système Oracle Solaris est le seul point d'accès pour la documentation d'API RAD. Pour les documents pouvant être disponibles dans plusieurs emplacements, le tableau de bord de l'interface Web du système s'avère très pratique.

Pour plus d'informations, reportez-vous aux pages de manuel `odoc-bundle`(5) et `odoctool`(1).

Filtre d'impression `paps`

`paps` convertit le texte en langage PostScript à l'aide de la bibliothèque Pango. `paps` lit un fichier d'entrée et écrit en langage PostScript ou dans un format spécifié par l'utilisateur le rendu du fichier dans la sortie standard. `paps` accepte le texte international de n'importe quel environnement linguistique et fournit une présentation de texte internationalisée incluant la mise en forme du texte et le rendu du texte bidirectionnel.

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

Modernisation de la structure `iconv`

La commande `iconv` et l'API `iconv()` d'Oracle Solaris ont été modernisées pour utiliser l'API `cconv` en interne pour la conversion. `cconv` est un mécanisme de conversion unifié qui utilise Unicode en tant qu'encodage intermédiaire. `cconv` prend en charge un large éventail d'ensemble de codes et fournit la commande `geniconvtbl` pour générer des tables de conversion avec des règles de conversion personnalisées.

Pour plus d'informations, reportez-vous aux pages de manuel `iconv`(1), `iconv`(3C), `cconv`(3C), `cconv_open`(3C), `cconv_close`(3C), `cconvctl`(3C), `geniconvtbl`(1) et `geniconvtbl-cconv`(5).

Mécanisme de secours du nom de l'environnement linguistique

Cette nouvelle fonction d'Oracle Solaris 11.4 étend la capacité de recherche de la commande `gettext` à des répertoires supplémentaires. Lors de la localisation d'un catalogue de message, la commande `gettext` lance

également une recherche dans les répertoires de secours en fonction de la langue et du territoire, tels que fr_FR et fr, en plus de fr_FR.UTF-8. Cette fonction permet à la commande `gettext` de se comporter comme d'autres systèmes d'exploitation de type UNIX.

Pour plus d'informations, reportez-vous à la page de manuel `gettext`(3C).

Prise en charge de la norme de produit UNIX V7 du consortium The Open Group

Oracle Solaris 11.4 est certifié comme étant conforme à la norme de produit UNIX V7 du consortium The Open Group. Cette certification apporte une amélioration considérable par rapport à la certification UNIX 03 précédente. La modification la plus importante réside dans l'alignement avec les spécifications SUS (Single UNIX Specification) version 4, incluant les spécifications de base du consortium The Open Group, Issue 7, et les rectificatifs techniques approuvés du corrigenda. Cette version permet également aux systèmes certifiés de prendre en charge le contrôle d'accès basé sur les rôles en tant qu'option.

Lors de l'utilisation du compilateur Oracle Developer Studio 12.5 ou 12.6 C, ou des dernières versions des commandes `gcc`, ou LLVM ou `clang` présents dans Oracle Solaris 11.4, Oracle Solaris 11.4 prend en charge les normes suivantes :

- Normes ANSI X3.159-1989 - Langage de programmation - C et ISO/IEC 9899:1990 Langage de programmation - C (C) interfaces
- Norme ISO/IEC 9899:1990 - Modification 1:1995 : Intégrité C
- Norme ISO/IEC 9899:1999 - Langages de programmation - C
- Norme INCITS/ISO/IEC 9899:2011 - Langages de programmation - C

Pour plus d'informations, reportez-vous à IEEE Std 1003.1TM-2008/The Open Group Technical Standard Base Specifications, Issue 7. Vous pouvez également vous reporter à la page de manuel `standards`(7).

Prise en charge d'Unicode 8.0

Les environnements linguistiques UTF-8 d'Oracle Solaris ont été mis à jour pour la version 8.0 de la norme Unicode. Unicode est une norme informatique pour l'encodage, la représentation et le traitement cohérents de texte exprimé dans la plupart des systèmes d'écriture du monde.

Mise à jour CLDR 28

Les environnements linguistiques d'Oracle Solaris ont été mis à jour vers la version 28 du CLDR, ce qui améliore la qualité des données de ces environnements. Pour plus d'informations, consultez le *Guide des environnements linguistiques internationaux pour Oracle Solaris 12*.

Nouveautés d'Oracle Solaris 11.4

Référence: E74962-01

Accessibilité de la documentation

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

Accès aux services de support Oracle

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

Part No: E74962-01