Tivoli System Automation for Multiplatforms
Version 4.1

Guide d'installation et de configuration

SC11-7498-04

Tivoli System Automation for Multiplatforms
Version 4.1

Guide d'installation et de configuration

SC11-7498-04

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations figurant dans la section «Remarques», à la page 143.

Cinquième édition - Février 2018

Cette édition du document *System Automation for Multiplatforms - Guide d'installation et de configuration* s'applique à la version 4.1.0 d'IBM Tivoli System Automation for Multiplatforms, numéro de programme 5724–M00 et à toutes les éditions et modifications suivantes, sauf indications contraires stipulées dans de nouvelles éditions.

Cette édition remplace le document SC11-7498-03.

Réf. US : SC34-2699-04

Compagnie IBM France
Direction Qualité
17, avenue de l'Europe
92275 Bois-Colombes Cedex

Table des matières

Figures

Tableaux

Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	**IBM Canada**
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

France	Canada	Etats-Unis
(Pos1)		Home
Fin	Fin	End
(PgAr)		PgUp
(PgAv)		PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
(Verr maj)	FixMaj	Caps Lock
AltGr	AltCar	Alt (à droite)

Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

Préface

Ce guide explique comment implémenter et utiliser les fonctions de reprise automatisée basées sur des règles fournies par IBM Tivoli System Automation for Multiplatforms (System Automation for Multiplatforms).

System Automation for Multiplatforms permet de garantir la haute disponibilité des ressources présentes dans des clusters AIX (sur IBM® System p), Linux (sur IBM System x, System z, System i et System p) et Windows (sur IBM System x).

A qui ce guide est-il destiné ?

Ce guide est destiné aux administrateurs système et aux opérateurs souhaitant exploiter les fonctions d'automatisation et de reprise en ligne de System Automation for Multiplatforms.

Où trouver des informations supplémentaires ?

La bibliothèque de Tivoli System Automation contient les manuels suivants, notamment la présente publication, qui décrivent Tivoli System Automation for Multiplatforms:

- *System Automation for Multiplatforms - Guide d'administration et d'utilisation*, SC11-7499-01
- *Tivoli System Automation for Multiplatforms Guide d'installation et de configuration*, SC11-7498-01
- *Tivoli System Automation for Multiplatforms Guide de référence Guide*, SC11-7500-01
- *Tivoli System Automation for Multiplatforms Guide des règles de haute disponibilité, SC11-7501-01*

Vous pouvez télécharger la documentation complète à l'adresse suivante :

`http://www.ibm.com/support/knowledgecenter/SSRM2X/welcome`

La bibliothèque Tivoli System Automation contient les documents suivants, y compris le présent document, décrivant System Automation Application Manager :

- *System Automation Application Manager - Guide d'utilisation et d'administration*, SC43-0643-00
- *System Automation Application Manager - Guide d'installation et de configuration*, SC43-0644-00
- *System Automation Application Manager - Guide de référence, d'identification des problèmes*, SC43-0645-00

Vous pouvez télécharger les manuels à l'adresse suivante :

`http://www.ibm.com/support/knowledgecenter/SSPQ7D/welcome`

La page d'accueil d'IBM Tivoli System Automation héberge les informations utiles les plus récentes sur le produit et contient notamment des liens permettant d'obtenir de l'aide et de télécharger des packages de maintenance. La page d'accueil d'IBM Tivoli System Automation est accessible à l'adresse suivante :

`www.ibm.com/software/tivoli/products/sys-auto-multi/`

Conventions

Les conventions suivantes de mise en évidence sont utilisées dans ce guide :

Tableau 1. Conventions de mise en évidence utilisées dans ce manuel

Gras	Identifie les commandes, les sous-routines, les mots clés, les fichiers, les structures, les répertoires ainsi que d'autres éléments dont les noms sont prédéfinis dans le système. Identifie également les objets graphiques tels que les boutons, les intitulés, et les icônes sélectionnés par l'utilisateur.
Italique	Identifie les paramètres dont les noms et valeurs en cours doivent être fournis par l'utilisateur.
`espacement fixe`	Identifie des exemples de valeurs de données spécifiques, des exemples de textes similaires à ceux pouvant apparaître, des exemples de morceaux de codes de programme semblables à ceux que vous pouvez rédiger en tant que programmeur, des messages provenant du système ou des informations que vous devez entrer.

Ce guide utilise des symboles pour l'affichage de ressources, de groupes de ressources, d'équivalences ou de relations. Les symboles sont utilisés comme suit :

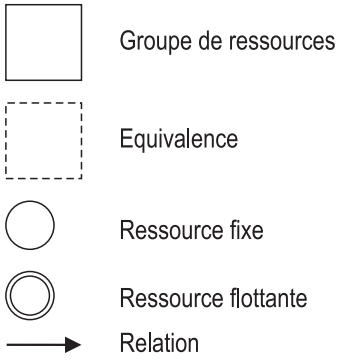

Figure 1. Symboles utilisés dans le document

ISO 9000

Des systèmes de qualités ISO 9000 ont été utilisés dans le développement et la fabrication de ce produit.

Informations RSCT connexes

Les publications IBM Reliable Scalable Cluster Technology (RSCT) suivantes sont disponibles sur le CD de System Automation for Multiplatforms :

- *RSCT Administration Guide*
- *RSCT for AIX 5L: Technical Reference*
- *RSCT for Multiplatforms: Technical Reference*
- *RSCT Messages*
- *RSCT Diagnosis Guide*

Pour plus d'informations sur RSCT, voir Systèmes de cluster IBM.

Pour plus d'informations, voir le Redpaper Linux on IBM zSeries et S/390: High Availability for z/VM et Linux IBM.

Comment obtenir des publications

Les publications System Automation for Multiplatforms sont également disponibles (valides ou moment de la parution) sur les sites Web :

```
www.ibm.com/servers/eserver/clusters/library/
www.ibm.com/servers/eserver/zseries/software/sa/
www.ibm.com/software/sysmgmt/products/support/
```

Comment nous contacter par e-mail

Si vous souhaitez nous contacter par e-mail, envoyez vos commentaires à l'adresse eservdoc@de.ibm.com

Nouveautés de cette édition

Voici une présentation rapide des nouvelles fonctionnalités de System Automation for Multiplatforms version 4.1.0.

Opérations améliorées sur la ligne de commande à l'aide de la commande `samcc`

Ajout d'une nouvelle commande `samcc` dans System Automation for Multiplatforms version 4.1.0.2, que vous pouvez utiliser en tant que console d'opérations sur l'interface de ligne de commande. Pour plus d'informations, voir .

Prise en charge de plateformes supplémentaires

System Automation for Multiplatforms version 4.1.0.1 prend en charge de nouvelles plateformes, telles que :
- SUSE SLES 12 (64 bits)
- Red Hat RHEL 7 (64 bits)
- Ubuntu 14.04 (64 bits) : System x, Power Systems (Little Endian uniquement)

System Automation for Multiplatforms version 4.1.0.2 prend en charge de nouvelles plateformes, telles que :
- Red Hat RHEL 7.1 on Power Systems Little Endian (64 octets)

System Automation for Multiplatforms version 4.1.0.3 prend en charge de nouvelles plateformes, telles que :
- AIX 7.2

Pour plus d'informations, voir *System Automation for Multiplatforms - Guide d'installation et de configuration*.

Règle de haute disponibilité pour SAP améliorée

La règle de haute disponibilité pour SAP Central Services est disponible en tant que fonction facultative System Automation for Multiplatforms qui fait l'objet d'un tarif distinct. Cette règle de haute disponibilité pour SAP Central Services est désormais adaptée à la technologie SAP Netweaver.

L'utilisateur peut démarrer et arrêter la pile SAP Netweaver à l'aide de l'interface utilisateur SAP sans interférer avec les règles de System Automation. SAP Software Update Manager permet de mettre à jour la solution Netweaver sans désactiver System Automation pendant le processus de mise à jour.

Les options de configuration SAP prises en charge sont les suivantes : prise en charge de la pile Java, ABAP et DUAL pour la reprise SAP Central Services. Les options de configuration suivantes sont également prises en charge :
- Serveur d'applications (redémarrage à la place des serveurs d'applications principal et supplémentaire)
- Reprise en ligne du routeur SAP
- Reprise en ligne du répartiteur Web SAP
- Démarrage après prise en charge de la dépendance vers la base de données

System Automation for Multiplatforms version 4.1.0.2 prend désormais en charge :

- La reprise de SAP HANA System Replication

Le noyau SAP version 7.20 ou ultérieure est pris en charge.

Pour plus d'informations, voir *System Automation for Multiplatforms - Guide des règles de haute disponibilité*.

Collecte d'informations concernant la collecte d'informations

Le programme `samwhy` est un outil simple et facile à utiliser qui permet la détection de défaillances d'application ainsi que leur analyse pour les applications contrôlées par System Automation. `samwhy` aide l'opérateur à comprendre ce qui s'est passé et fournit une explication de la réaction de System Automation.

Pour plus d'informations, voir *System Automation for Multiplatforms - Guide de référence*.

La haute disponibilité de l'adaptateur d'automatisation de bout en bout est simplifiée

Une règle d'automatisation ou une adresse IP virtuelle n'est plus requise.

Pour plus d'informations, voir System Automation for Multiplatforms - Guide d'installation et de configuration.

Exécution de l'adaptateur d'automatisation de bout en bout avec un utilisateur non superutilisateur

Par défaut, l'adaptateur d'automatisation de bout en bout s'exécute avec un superutilisateur. Désormais, l'adaptateur peut également être configuré avec un utilisateur non superutilisateur.

Pour plus d'informations, voir System Automation for Multiplatforms - Guide d'installation et de configuration.

Chapitre 1. Planification

L'évaluation de l'infrastructure en place et la vérification des prérequis font partie des tâches de planification.

Planification de l'installation

Avant d'installer System Automation for Multiplatforms dans vos environnements AIX et Linux, vous devez vérifier que les conditions requises sont respectées.

Conditionnement

System Automation for Multiplatforms peut être commandé auprès d'IBM® sur CD-ROM ou téléchargé sous la forme d'une image ESD (Electronic Software Distribution) depuis un site de téléchargement de distribution de logiciels IBM.

DVD du produit

Contenu du DVD de System Automation for Multiplatforms version 4.1.

Différents DVD contenant des scripts et des packages logiciels sont fournis pour chaque plateforme et l'architecture correspondante :

- Tivoli System Automation for Multiplatforms 4.1 - Linux on System x, Linux on POWER and Linux on System z
- Tivoli System Automation for Multiplatforms 4.1 - AIX

Pour installer System Automation for Multiplatforms, utilisez le script d'installation figurant dans la colonne de droite du tableau ci-dessous.

Tableau 2. Versions des DVD du produit

Système d'exploitation	**Nom du DVD du produit**	**Script d'installation**
Linux	Tivoli System Automation for Multiplatforms v4.1 - Linux on System x, Linux on POWER et Linux on System z	`SAM4100MPLinux/installSAM`
AIX	Tivoli System Automation for Multiplatforms v4.1 - AIX	`SAM4100MPAIX/installSAM`

Distribution électronique

Si vous préférez recevoir une copie électronique du logiciel au lieu d'un DVD, après avoir acheté System Automation for Multiplatforms, vous pouvez télécharger les fichiers archive correspondants depuis un site Web à l'aide de l'URL qui vous est fournie.

Linux

Tableau 3. Archive pour les plateformes Linux

Nom de l'archive	Description
`SA MP 4.1 Linux.tar`	Il s'agit de l'archive qui permet d'installer le produit. Pour extraire l'archive, vous devez utiliser GNU tar 1.13 ou une version ultérieure. Utilisez la commande **tar xf** pour extraire l'archive. Une fois les fichiers extraits, vous pouvez accéder au script d'installation `installSAM` dans le répertoire suivant : `SAM4100MPLinux`

AIX

Tableau 4. Archive pour les plateformes AIX

Nom de l'archive	Description
`SA MP 4.1 AIX.tar`	Il s'agit de l'archive qui permet d'installer le produit. Utilisez la commande **tar xf** pour extraire l'archive. Une fois les fichiers extraits, vous pouvez accéder au script d'installation `installSAM` dans le répertoire suivant : `SAM4100MPAIX`

Eléments prérequis

Veillez à ce que la configuration logicielle et matérielle requise pour System Automation for Multiplatforms soit satisfaite.

Prérequis pour les systèmes AIX

- Le droit d'accès root est nécessaire pour installer System Automation for Multiplatforms.
- Une version 32 bits de Java 6, Java 7 ou Java 7.1 est obligatoire avec les niveaux d'actualisation de service minimum suivants :
  - Java 6 SR9 groupe de correctifs 1 : package AIX Java6.sdk 6.0.0.265
  - Java 7.0 SR8 : package AIX Java7.jre/Java7.sdk 7.0.0.145
  - Java 7.1 SR2 : package AIX Java71.jre/Java71.sdk 7.1.0.25

Packages RSCT

Au cours de l'installation de System Automation for Multiplatforms sous AIX, une vérification a lieu. Elle vise à comparer les niveaux des packages RSCT requis par System Automation for Multiplatforms avec les niveaux des packages RSCT déjà installés en même temps que le système d'exploitation. Si nécessaire, les packages RSCT manquants ou de niveau supérieur sont alors installés. Selon les cas, il peut être nécessaire d'installer manuellement les niveaux supérieurs de certains packages RSCT. Par exemple, si le package de base RSCT n'est pas installé et que le niveau du package central RSCT installé est supérieur au niveau des packages RSCT fournis avec System Automation for Multiplatforms, l'installation du package de base RSCT est susceptible d'échouer, car les conditions requises par RSCT ne sont pas remplies. Vous devez alors télécharger et installer les ensembles de fichiers RSCT appropriés à partir du service d'assistance AIX pour faire en sorte que tous les packages RSCT installés soient au même niveau.

System Automation for Multiplatforms version 4.1.0.0 inclut RSCT niveau 3.1.5.3 (APAR IV52893).

Conditions requises sur Linux

Les conditions requises suivantes doivent être réunies pour pouvoir installer System Automation for Multiplatforms sur un système Linux :

- Le package suivant est requis dans chaque système RedHat version 7.1 :
  - `perl-Sys-Syslog`
- Le droit d'accès root est nécessaire pour installer System Automation for Multiplatforms.
- Pour pouvoir installer System Automation for Multiplatforms, vous devez avoir installé plusieurs bibliothèques 32 bits doivent être installées sur chaque système Red Hat 5, même si un noyau 64 bits est exécuté. Ces bibliothèques sont contenues dans les packages RPM Package Manager :
  - `compat-libstdc++- 33-3.2.3`
  - `xorg-x11-deprecated-libs-6.8.1`
- Pour pouvoir installer System Automation for Multiplatforms, vous devez avoir installé plusieurs bibliothèques 32 bits doivent être installées sur chaque système Red Hat 6, même si un noyau 64 bits est exécuté. Ces bibliothèques sont contenues dans les packages RPM Package Manager :
  - `libgcc-4.4.4`
  - `glibc-2.12`
  - `libstdc++-4.4.4`
  - `nss-softokn-freebl-3.12.7`
  - `audit-libs-2.0.4`
  - `cracklib-2.8.16`
  - `db4-4.7.25`
  - `libselinux-2.0.94`
  - `pam-1.1.1`
  - `compat-libstdc++-33-3.2.3`
- Pour pouvoir installer System Automation for Multiplatforms, vous devez avoir installé plusieurs bibliothèques 32 bits doivent être installées sur chaque système SLES 10 et SLES 11 Red Hat 10, même si un noyau 64 bits est exécuté. Ces bibliothèques sont contenues dans les packages RedHat Package Manager (RPM) suivants :
  - libstdc++33-32bit (SLES 10)
  - libstdc++43-32bit (SLES 11)
  - pam-32bit (SLES 11)

Conditions requises pour les environnements virtuels tels que KVM ou VMware

Les machines virtuelles ne disposant généralement pas de moyen fiable de conserver une trace du temps, les unités centrales qui comportent un compteur d'horodatage sont susceptibles d'expérimenter des erreurs de synchronisation. Pour éviter ces erreurs, configurez une synchronisation du temps appropriée, par exemple NTP, pour les noeuds s'exécutant dans des environnements virtuels.

Contrôle des prérequis

Exécutez un contrôle des prérequis.

Effectuez les opérations suivantes :

1.

Connectez-vous comme utilisateur root ou avec des droits équivalents.

2. Si vous avez téléchargé le fichier TAR depuis Internet, décompressez-le :

   ```
   tar -xvf <fichier tar>
   ```

   Si vous vous êtes procuré ce produit sur DVD, montez le DVD et accédez au répertoire correspondant.

3. Entrez la commande suivante :

   - **Linux : cd SAM4100MPLinux**
   - **AIX : cd SAM4100MPAIX**

   Pour plus d'informations sur les plateformes prises en charge, voir «Plateformes prises en charge», à la page 5.

4. Pour commencer le contrôle des prérequis, exécutez la commande suivante :

   ```
   ./prereqSAM
   ```

   Généralement, vous n'entrez aucune des options qui sont disponibles pour la commande **prereqSAM**. Pour une description détaillée de la commande, voir *Tivoli System Automation for Multiplatforms - Guide de référence* .

5. Une fois le contrôle terminé, recherchez des informations sur les prérequis manquants dans le fichier journal suivant :

   ```
   /tmp/prereqSAM.<#>.log
   ```

   La balise <#> est un nombre, le nombre le plus élevé identifiant le fichier journal le plus récent.

6. Si le contrôle des prérequis a échoué sur votre système, corrigez les incidents avant de commencer l'installation.

Conditions requises pour l'installation

Avant de commencer l'installation, vous devez vérifier que ces conditions sont remplies :

- Vous devez disposer des droits d'accès root pour pouvoir installer System Automation for Multiplatforms sur le système.
- Un shell Korn doit être installé.
- Perl est requis pour utiliser l'interface de la ligne de commande de System Automation for Multiplatforms y compris les commandes RSCT régionales. L'interface de ligne de commande est installée par défaut sur les systèmes Linux ou AIX avec le système d'exploitation. Si vous utilisez System Automation for Multiplatforms dans une langue autre que l'anglais, une version spéciale de Perl sera requise. En raison de certains problèmes rencontrés avec Perl 5.8.0 et de sa capacité à supporter les paramètres de lieu d'encodage UTF-8, certains caractères risquent de ne pas s'afficher correctement. Ce problème peut se produire sur des systèmes où la version Perl 5.8.0 est déjà installée, si vous utilisez les paramètres de lieu d'encodage UTF-8. Si vous utilisez une version précédente de Perl, ou un langage de programmation autre qu'UTF-8, ce problème ne se produira pas.

  Si vous décidez de mettre à niveau votre version Perl 5.8.0 sur une distribution Linux, effectuez les opérations suivantes :

  1.

Téléchargez le source Perl 5.8.1.

2. Extrayez le fichier dans n'importe quel répertoire à l'aide de **-xvf**.
3. Compilez et installez Perl sur le système UTF-8 en vous aidant les instructions fournies avec les fichiers téléchargés.
4. Modifiez le lien symbolique qui pointe vers le répertoire de la version Perl utilisée par System Automation for Multiplatforms

   Remplacez le lien :

   ```
   /usr/sbin/rsct/perl5/bin/perl->/usr/bin/perl
   ```

   par le répertoire dans lequel est installée la nouvelle version de Perl :

   ```
   /usr/sbin/rsct/perl5/bin/perl->/usr/local/bin/perl
   ```

- Assurez-vous aussi que les répertoires `/usr/sbin` et `/opt` disposent d'au moins 100 Mo d'espace disponible et que le répertoire `/var` dispose aussi de 100 Mo d'espace disponible.
- Au moins 128 Mo de mémoire vive doivent être disponibles sur chacun des nœuds configurés pour exécuter l'adaptateur d'automatisation de bout en bout.
- Au cours de l'installation de System Automation for Multiplatforms sous AIX, une vérification des niveaux des packages RSCT requis par System Automation for Multiplatforms par rapport aux niveaux des packages RSCT déjà installés est effectuée. Les packages RSCT manquants ou de niveau supérieur sont alors installés si nécessaire. Selon les cas, il peut être nécessaire d'installer manuellement les niveaux supérieurs de certains packages RSCT. Par exemple, si le package de base RSCT n'est pas installé et si le niveau du package central RSCT installé est supérieur au niveau des packages RSCT fournis avec System Automation for Multiplatforms, l'installation du package de base RSCT risque d'échouer, car les conditions requises par RSCT ne sont pas remplies. Vous devez alors télécharger et installer les ensembles de fichiers RSCT appropriés à partir du service d'assistance AIX pour faire en sorte que tous les packages RSCT installés soient au même niveau.
- Pour en savoir plus sur les conditions requises propres à chaque système d'exploitation, consultez la page des rapports de compatibilité logicielle.
- Pour les langues qui utilisent le jeu de caractères codé sur deux octets (DBCS), la taille de la mémoire tampon Telnet doit être suffisamment importante pour permettre à de longs messages de s'afficher correctement. Si tel n'est pas le cas, augmentez la taille de la mémoire-tampon Telnet.
- Dans certaines distributions RHEL, l'environnement SELinux est activé par défaut. Assurez-vous qu'il est désactivé pour que System Automation for Multiplatforms fonctionne correctement.

Plateformes prises en charge

Cette rubrique décrit les plates-formes qui sont prises en charge par System Automation for Multiplatforms.

System Automation for Multiplatforms prend en charge les environnements UNIX suivants :

- Linux on System z
- Linux on System x
- Linux on Power
- Ubuntu sur System x[4]
- Ubuntu sur Power[4]
- AIX

System Automation for Multiplatforms s'exécute sous :

- Toutes les machines IBM fonctionnant sous Linux.
- Les machines IBM System p fonctionnant sous AIX.

System Automation for Multiplatforms s'exécute sur :

- VMware sur IBM System x (sauf serveurs Intel IA64) ou autre serveur Intel 32 bits, AMD Opteron (64 bits) ou Intel EM64T (64 bits). La migration active des systèmes à l'aide de vMotion est prise en charge (voir «Prise en charge de VMware vMotion», à la page 8).
- L'hyperviseur RHEV-H/KVM version 5.4 ou ultérieure sur toutes les distributions Linux prises en charge sous IBM System x. La migration active des systèmes n'est pas prise en charge.

Le tableau ci-dessous répertorie les différentes versions prises en charge pour chaque système d'exploitation.

`www.ibm.com/software/tivoli/products/sys-auto-multi/`

Tableau 5. Prise en charge des plateformes UNIX et Linux d'System Automation for Multiplatforms

	IBM System x[1]	**IBM System z**	**Power Systems**	**Power Systems (Little Endian)**
SUSE SLES 10 (32 bits)3	x			
SUSE SLES 10 (64 bits)3	x	x	x	
SUSE SLES 11 (32 bits)	x			
SUSE SLES 11 (64 bits)	x	x	x	
SUSE SLES 12 (64 bits)[4]	x	x		x
Red Hat RHEL 5 (32 bits)	x			
Red Hat RHEL 5 (64 bits)	x	x	x	
Red Hat RHEL 6 (32 bits)	x			
Red Hat RHEL 6 (64 bits)	x	x	x	
Red Hat RHEL 7 (64 bits)	x[4]	x[4]	x[4]	x[5]

Tableau 5. Prise en charge des plateformes UNIX et Linux d'System Automation for Multiplatforms (suite)

	IBM System x[1]	IBM System z	Power Systems	Power Systems (Little Endian)
Ubuntu 14.04 (64 bits)[4]	x			x
AIX 6.1			x[2]	
AIX 7.1			x	
AIX 7.2			x[6]	

Tous les niveaux SP des versions SUSE prises en charge et les niveaux SP supérieurs aux niveaux SP/Red Hat répertoriés sont également pris en charge, sauf indication plus spécifique dans la configuration minimale requise.

Remarque :

1. System x (sauf serveurs Intel IA64) et tous les autres serveurs 32 bits Intel ou AMD Opteron (64 bits) ou Intel EM64T (64 bits).
2. Prise en charge sous AIX 6.1 de la mobilité et du déplacement WPAR (Workload Partition). System Automation for Multiplatforms et RSCT ne prennent pas en charge les domaines contenant des noeuds de type WPAR système.
3. Le SP1 doit être installé.
4. Le support de plate-forme est intégré dans le groupe de correctifs 4.1.0.1. Pour plus d'informations, voir «Installation sur de nouveaux systèmes d'exploitation» , à la page 39.
5. La prise en charge de la plateforme a été introduite avec le groupe de correctifs 4.1.0.2. Pour plus d'informations, voir «Installation sur de nouveaux systèmes d'exploitation», à la page 39.
6. La prise en charge de la plateforme a été introduite dans le groupe de correctifs 4.1.0.3. Pour plus d'informations, voir «Installation sur de nouveaux systèmes d'exploitation», à la page 39.

Interfaces de réseau prises en charge

Toutes les plateformes supportent Ethernet 10 Megabit, Fast Ethernet et Ethernet Gigabit. En outre, la plateforme System z prend également en charge HiperSockets, CTC et VM Guest LAN.

Prise en charge des systèmes NFS

System Automation for Multiplatforms prend en charge les systèmes de fichiers NFS sous Linux on POWER, Linux on System x, Linux on System z et AIX.

Les systèmes de fichiers NFS ne sont pas récoltés. Pour automatiser un système NFS, utilisez des ressources `IBM.AgFileSystem` définies par l'utilisateur.

Restriction :

- Les systèmes de fichiers NFS de classe `IBM.AgFileSystem` ne peuvent être automatisés et surveillés avec succès que si l'utilisateur `root` du système qui importe dispose d'un accès en écriture au système de fichiers.
- L'utilisation en cascade des systèmes de fichiers n'est pas possible :

System Automation for Multiplatforms permet de définir un serveur NFS à haute disponibilité, dans lequel les systèmes de fichiers exportés sont automatisés en tant que ressources de classe `IBM.AgFileSystem` qui résident sur un support de disque partagé. Le serveur NFS est lui-même automatisé en tant que ressource de la classe `IBM.Application`, capable de flotter sur les systèmes ayant accès au support de disque partagé. Cependant, lorsqu'un système supplémentaire importe les systèmes de fichiers NFS, les systèmes de fichiers importés ne doivent pas déjà résider en tant que ressources `IBM.AgFileSystem` définies par l'utilisateur sur le système qui importe. Sinon, la surveillance des systèmes de fichiers échoue et les ressources passent à l'état OpState 3 (`ECHEC HORS LIGNE`).

Conditions requises pour la prise en charge de Live Partition Mobility

Si AIX niveau 6100-00-01 (ou ultérieur) est installé sur les serveurs POWER6 source et cible, la fonction Live Partition Mobility peut être utilisée pour migrer une partition logique exécutée en tant que noeud System Automation for Multiplatforms. L'état ou le fonctionnement du cluster System Automation for Multiplatforms n'est pas affecté. Le cluster est configuré pour utiliser les paramètres de signal de présence standard (par défaut). Dans ce cas, pour les serveurs d'applications, cela se traduit par une courte interruption des opérations au cours de la migration. Il n'est pas nécessaire de redémarrer System Automation for Multiplatforms, ni les serveurs d'applications.

Vérifiez que la période d'interruption au cours de l'exécution de Live Partition Mobility n'engendre pas d'événements de cluster indésirables. Ceux-ci surviennent si un trop grand nombre de signaux de présence du noeud manquent pendant la période moyenne d'interruption. Dans ce cas, modifiez les paramètres de signaux de Live Partition Mobility.

Un autre moyen de limiter le risque de survenue d'événements de cluster indésirables lors du déplacement d'une partition logique consiste, avant le lancement de ce dernier, à forcer l'arrêt du domaine homologue à l'aide de la commande `stoprpdomain -f`, c'est-à-dire sans arrêter les applications gérées par les services de cluster. Une fois que le déplacement est terminé, redémarrez le domaine homologue.

Restriction : La condition de départage de disque n'est pas prise en charge par l'interface SCSI virtuelle, ce qui est prérequis par Live Partition Mobility.

Prise en charge de VMware vMotion

Lorsque VMware vSphere est configuré avec plusieurs serveurs ESX gérés par un serveur vCenter, la fonction vMotion peut être utilisée pour migrer des hôtes actifs exécutés en tant que noeud System Automation for Multiplatforms. La migration n'affecte pas l'état ou le fonctionnement du cluster System Automation for Multiplatforms, si ce cluster a été configuré pour utiliser des signaux de présence standard (c'est-à-dire, ceux par défaut). Pour les serveurs d'applications s'exécutant sous le contrôle de System Automation for Multiplatforms, cela se traduit par une courte interruption des opérations au cours de la migration. Ni System Automation for Multiplatforms ni les serveurs d'applications ne doivent être redémarrés.

Vérifiez que la période d'interruption au cours de l'exécution de vMotion n'engendre pas d'événements de cluster indésirables. Ceux-ci surviennent si un trop grand nombre de signaux du noeud manquent pendant la période moyenne de l'interruption. Dans ce cas, modifiez les paramètres de signaux de vMotion.

Un autre moyen de limiter le risque de survenue d'événements de cluster indésirables lors du déplacement d'un hôte virtuel consiste, avant le lancement de ce dernier, à forcer l'arrêt du domaine homologue à l'aide de la commande `stoprpdomain -f`, c'est-à-dire, sans arrêter les applications gérées par les services de cluster. Une fois que le déplacement est terminé, redémarrez le domaine homologue.

System Automation for Multiplatforms prend en charge vMotion pour les serveurs ESX et ESXi avec la version 3.5 ou ultérieure et les systèmes d'exploitation hôte suivants :

- RHEL 5 ou 6 (x86-64 ou x86-32)
- SLES 10 ou 11 (x86-64 ou x86-32)

Limitations : System Automation for Multiplatforms ne prend pas en charge la fonction vMotion des noeuds qui utilisent une mémoire partagée, car vMotion ne prend pas en charge les volumes de stockage virtuels ou réels (disques).

Prise en charge de l'Image système unique (SSI) z/VM et de Live Guest Relocation (LGR)

z/VM 6.2 introduit la prise en charge de l'image système unique (SSI), qui est une technologie de mise en cluster multi-systèmes. Vous pouvez mettre en cluster jusqu'à 4 images z/VM à l'aide de SSI. SSI permet le partage des ressources entre les membres du cluster. Vous pouvez déplacer un invité Linux on System z actif vers un autre système z/VM sans causer d'indisponibilité de l'invité. Cette fonction est appelée Live Guest Relocation (LGR) et est uniquement prise en charge pour les invités Linux sur System z.

Pour comprendre les concepts et les fonctions SSI et LGR de z/VM, voir An Introduction to z/VM Single System Image (SSI) and Live Guest Relocation (LGR) (SG24-8006).

Si le niveau requis de z/VM est installé sur les systèmes source et cible, la fonction Live Guest Relocation (LGR) z/VM peut être utilisée pour déplacer un système invité z/VM Linux. Si le niveau requis de System Automation for Multiplatforms est installé sur le système invité Linux, le déplacement de ce système invité n'affecte pas l'état ou le fonctionnement du cluster System Automation for Multiplatforms si les paramètres de signal de présence standard (valeur par défaut) sont configurés. Pour une application gérée par System Automation for Multiplatforms, le processus de déplacement entraîne une courte mise en suspend des opérations. Le redémarrage n'est pas requis pour System Automation for Multiplatforms et l'application.

Vérifiez que la période de mise en suspens au cours de l'exécution de Live Guest Relocation n'engendre pas d'événements de cluster indésirables. Ces derniers se produisent si le nombre configuré de signaux de présence est manquant sur le noeud concerné par une mise en suspens au cours de l'exécution de Live Guest Relocation. Si le test indique que la durée moyenne de mise en suspens peut entraîner la perte d'un trop grand nombre de signaux de présence, les paramètres de signal de présence doivent être assouplis pendant la durée d'exécution de Live Guest Relocation. Un autre moyen de limiter fortement le risque de survenue d'événements de cluster indésirables lors du déplacement d'un système invité z/VM consiste à forcer l'arrêt du domaine homologue avant le déplacement, à l'aide de la commande **`stoprpdomain -f`**. Par exemple, procédez sans arrêter les

applications gérées par les services de cluster. Une fois le déplacement terminé, il suffit ensuite de redémarrer le domaine homologue à l'aide de la commande **startrpdomain**.

Exigences

- System Automation for Multiplatforms version 3.2.2.4 (ou version ultérieure)
- z/VM version 6.2

Restrictions

Les conditions de départage du disque ECKD et SCSI PR ne peuvent pas être utilisées avec Live Guest Relocation, car des invités qui conservent une réservation d'un disque ne peuvent pas être déplacés.

Préparation de l'installation

System Automation for Multiplatforms est contenu dans différents packages devant être installés sur chaque noeud du cluster à automatiser. Le type de package et le contenu dépendent du système d'exploitation sur lequel vous installez System Automation for Multiplatforms.

Démarrage de la configuration

Effectuez les configurations initiales suivantes :

- Sur tous les noeuds, définissez la variable d'environnement `CT_MANAGEMENT_SCOPE` sur `2` (portée de domaine homologue) et exportez-la pour tous les utilisateurs de System Automation for Multiplatforms : `export CT_MANAGEMENT_SCOPE=2`

  Pour définir la variable de manière permanente, définissez-la et exportez-la dans le profil.

  Sur les systèmes SLES, vous pouvez créer des scripts dans `/etc/profile.d` avec le contenu suivant :

  ```
  sa_mp.sh:
  export CT_MANAGEMENT_SCOPE=2
  sap_mp.csh :
  setenv CT_MANAGEMENT_SCOPE 2
  ```

- Vérifiez que la variable d'environnement LANG est définie sur l'un des paramètres nationaux pris en charge pour l'utilisateur `root`. Pour définir la variable d'environnement, utilisez la commande suivante :

  ```
  export LANG=xx_XX
  ```

  `xx_XX` représente l'une des langues prises en charge.

Pour la liste des langues et des environnements locaux pris en charge, voir «Langues et paramètres nationaux pris en charge», à la page 26.

Charge sur les noeuds

Certains sous-systèmes de System Automation for Multiplatforms doivent faire l'objet d'un traitement permanent sur le noeud pour que les services de cluster puissent fonctionner correctement (transmission des signaux de présence et communication entre les sous-systèmes, par exemple). Si ce traitement ne peut pas être mis en oeuvre, System Automation peut déclencher des méthodes de protection des ressources critiques si ces sous-systèmes ne parvenaient plus à

communiquer pendant un court laps de temps. Ce mécanisme de protection peut provoquer un redémarrage du noeud sur lequel le problème survient.

Pour éviter un redémarrage inopportun du système, la charge constante d'entrée-sortie et de pagination doit être inférieure à 10 %.

Pour plus d'informations sur les méthodes de protection des ressources critiques, voir *Tivoli System Automation for Multiplatforms - Guide d'administration et d'utilisation*.

Nombre de noeuds dans un cluster

Linux Le nombre maximal de noeuds au sein d'un cluster est 32.

AIX Le nombre maximal de noeuds au sein d'un cluster est 130.

Remarque :

1. Les packages logiciels doivent être disponibles sur les noeuds sur lesquels vous souhaitez installer System Automation for Multiplatforms. Par exemple, vous pouvez monter le DVD sur un PC et utiliser FTP pour transférer les fichiers sur le noeud ; vous pouvez également installer les packages sur un système NFS (Network File System) partagé.
2. Pour que les packages logiciels soient installés et désinstallés dans le bon ordre, utilisez les scripts System Automation for Multiplatforms **installSAM** et **uninstallSAM**. Ils effectuent également des tâches de migration, d'installation de licence et de vérification des prérequis.
3. A l'exception des modules de langue, l'ensemble des packages sont requis pour que System Automation fonctionne. A partir de System Automation for Multiplatforms 4.1, il n'est plus possible de désinstaller le package RSCT `rsct.opt.storagerm` sans désinstaller le produit tout entier.

Planification pour un nouveau support de plateforme

Depuis le groupe de correctifs 4.1.0.1, System Automation for Multiplatforms propose différents packages d'installation pour les environnements de langage 32 bits et 64 bits.

Des packages correspondants sont également fournis pour tous les groupes de correctifs 4.1.0.x suivants. Les deux packages possèdent la même base de code.

- Le premier package, `4.1.0-TIV-SAMP-Linux-FP0001`, contient la génération du produit System Automation for Multiplatforms pour les environnements de langage 32 bits. Ces environnements de langage 32 bits sont requis par System Automation for Multiplatforms sur les systèmes d'exploitation Linux RHEL5/6 et SLES 10/11.
- Le deuxième package, `4.1.0-TIV-SAMP-Linux64-FP0001`, contient la génération du produit System Automation for Multiplatforms pour les environnements de langage 64 bits. Ces environnements de langage 64 bits sont requis par System Automation for Multiplatforms sur les systèmes d'exploitation Linux RHEL 7, SLES 12 et Ubuntu.

Il n'est pas possible d'utiliser ce deuxième package pour les systèmes d'exploitation Linux RHEL 5/6 ou SLES 10/11. System Automation for Multiplatforms 4.1.0.0 ou version antérieure n'est pas pris en charge sur SLES 12, RHEL 7 et Ubuntu.

Planification pour une infrastructure réseau hautement disponible

Cette section vous aide à mieux comprendre la complexité d'un réseau hautement disponible et à planifier sa configuration.

La figure suivante représente une infrastructure réseau sous Linux.

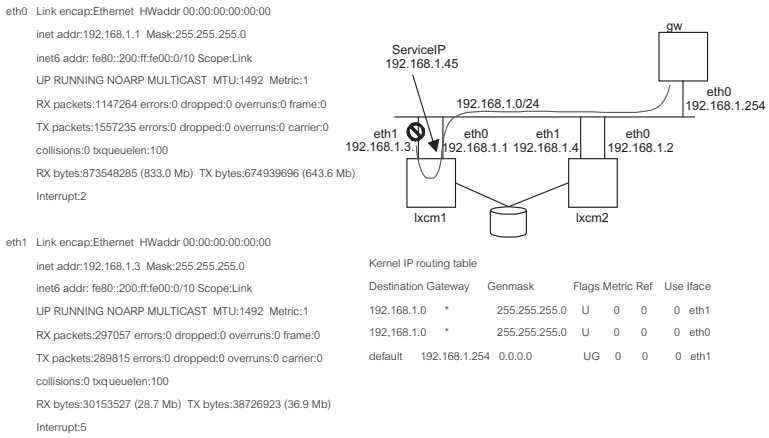

Figure 2. Problèmes lors de la planification d'un réseau hautement disponible

Chaque périphérique réseau statique configuré est identifié par une entrée dans la table de routage. L'algorithme de routage sélectionne la première route correspondante à partir de cette table de routage. Dans cet exemple, le périphérique `eth1` est en échec sur le noeud `lnxcm1`. Etant donné qu'`eth1` est la première entrée dans la table de routage, le noeud ne peut pas envoyer d'autres packages sur le réseau bien qu'il existe une autre interface réseau en fonction, `eth0`.

Répondez aux questions suivantes avant de lancer la planification d'un réseau hautement disponible :

1. De quel genre de réseau hautement disponible avez-vous besoin ?
   - Est-il nécessaire de déplacer la ressource `ServiceIP` d'une interface à une autre sur le même noeud ?
   - Est-il nécessaire d'utiliser un autre noeud connecté à une interface en fonctionnement dans le sous-réseau requis ?
2. Pouvez-vous implémenter des sous-réseaux supplémentaires IP ou utilisez-vous une infrastructure de réseau existante ?
3. Travaillez-vous exclusivement avec nos noeuds de cluster ou pouvez-vous implémenter ou déployer des services de réseau sur d'autres noeuds, en dehors du cluster d'automatisation ?
4. De quel matériel réseaux disposez-vous ?

En fonction des réponses, faites votre choix parmi l'une des configurations suivantes pour développer votre propre stratégie de réseau hautement disponible.

Planification pour les unités de stockage

Utilisation des unités de stockage à accès unique

La prise en charge des unités de stockage à accès unique diffère selon les environnements d'exploitation.

AIX

Une prise en charge complète est disponible pour les unités de stockage à accès unique :

- Les ressources `IBM.AgFileSystem` collectées peuvent être automatisées.

  Les ressources `IBM.AgFileSystem` sont collectées si elles sont de type `jfs` ou `jfs2` et résident sur des entités de stockage elles-mêmes collectées (entités de stockage de la classe `IBM.LogicalVolume`, `IBM.VolumeGroup`, `IBM.Disk`).
- Les ressources `IBM.AgFileSystem` définies par l'utilisateur peuvent être automatisées, par exemple, les systèmes de fichiers NFS).
- La réservation SCSI-2 n'est pas prise en charge.

Limitations :

- Pas de segmentation des données
- Les ressources `IBM.AgFileSystem` définies par l'utilisateur peuvent uniquement être automatisées si le disque hébergeant le système de fichiers possède le même nom sur tous les noeuds du cluster.

Linux on POWER et Linux on System x

Une prise en charge limitée est assurée :

- Les ressources `IBM.AgFileSystem` collectées peuvent être automatisées.

  Les ressources `IBM.AgFileSystem` sont collectées si elles sont du type `ext2`, `ext3` ou `reiserfs` et résident sur des entités de stockage elles-mêmes collectées (entités de stockage de la classe `IBM.LogicalVolume`, `IBM.Partition`, `IBM.VolumeGroup`, `IBM.Disk`.
- Les ressources `IBM.AgFileSystem` définies par l'utilisateur peuvent être automatisées, par exemple, les systèmes de fichiers NFS).

Limitations :

- La prise en charge de la réservation SCSI est limitée. Effectuez une opération de réservation de disque pour vérifier si la réservation SCSI est disponible.
- Les ressources `IBM.AgFileSystem` définies par l'utilisateur peuvent uniquement être automatisées si le disque hébergeant le système de fichiers possède le même nom sur tous les noeuds du cluster.

Linux on System z

Les unités fournies par l'associateur de périphériques ou les unités md sont collectées en tant que ressources `IBM.Disk` si un volume physique a été créé sur l'unité par bloc fournie à l'aide de la commande **`pvcreate`**.

Limitations :

- Seules les ressources `IBM.AgFileSystem` ou `IBM.AgFileSystem` définies par l'utilisateur qui résident sur les unités fournies par l'associateur de périphériques ou les unités md collectées peuvent être automatisées. La collecte de ressources

des autres disques n'est pas prise en charge. Même si la collecte sur les autres disques aboutit, les ressources collectées ne peuvent pas être automatisées.

- Les ressources IBM.AgFileSystem définies par l'utilisateur peuvent uniquement être automatisées si le disque hébergeant le système de fichiers possède le même nom sur tous les noeuds du cluster.
- La réservation SCSI n'est pas prise en charge.

Utilisation des unités de stockage multi-accès

Selon votre environnement, des limitations peuvent affecter la prise en charge des unités de stockage multi-accès.

AIX

Une prise en charge complète est disponible pour les unités de stockage SPIO et MPIO :

- Les ressources IBM.AgFileSystem collectées peuvent être automatisées.

  Les ressources IBM.AgFileSystem sont collectées si elles sont de type jfs ou jfs2 et résident sur des entités de stockage elles-mêmes collectées (entités de stockage de la classe IBM.LogicalVolume, IBM.VolumeGroup ou IBM.Disk).
- Les ressources IBM.AgFileSystem définies par l'utilisateur peuvent être automatisées (par exemple, les systèmes de fichiers NFS).
- La réservation SCSI-2 est prise en charge pour les unités de stockage SPIO et MPIO qui utilisent le pilote RDAC (Redundant Disk Array Controller).

Remarque : Ce pilote est uniquement disponible pour les familles IBM TotalStorage DS4k et DS6k.
Limitations :

- Pas de segmentation des données
- Les ressources IBM.AgFileSystem définies par l'utilisateur peuvent uniquement être automatisées si le disque hébergeant le système de fichiers possède le même nom sur tous les noeuds du cluster.

Linux on POWER et Linux on System x

Une prise en charge complète est assurée pour les unités de stockage SPIO (entrée-sortie à un accès) et pour les unités de stockage MPIO (entrée-sortie multi-accès) équipées de pilote d'unité RDAC (Redundant Disk Array Controller), ainsi que pour les unités md et les unités fournies par l'associateur de périphériques.

- Les ressources IBM.AgFileSystem collectées peuvent être automatisées.

  Les ressources sont collectées si elles sont du type ext2, ext3 ou reiserfs et résident sur des entités de stockage elles-mêmes collectées (entités de stockage de la classe IBM.LogicalVolume, IBM.Partition, IBM.VolumeGroup ou IBM.Disk.
- Les ressources IBM.AgFileSystem définies par l'utilisateur peuvent être automatisées (par exemple, les systèmes de fichiers NFS).
- La réservation SCSI-2 est prise en charge pour les disques collectés depuis le pilote RDAC.
- Linux RAID (/dev/device mapper unités fournies par l'associateur de périphériques ou les unités md devices) est pris en charge.
- Les unités gérées par l'associateur de périphériques sont prises en charge.

Limitations :

- Les systèmes de fichiers créés sur des unités fournies par l'associateur de périphériques ou des unités md sans LVM ne sont pas collectés, ils ne peuvent être automatisés qu'à l'aide des ressources `IBM.AgFileSystem`.
- Les unités fournies par l'associateur de périphériques ou les unités md sont uniquement collectées en tant que ressources `IBM.Disk` si un volume physique a été créé sur l'unité md à l'aide de la commande **`pvcreate`**.
- La réservation SCSI-2 n'est pas prise en charge pour les pilotes non RDAC, pour les unités fournies par l'associateur de périphériques ou pour les unités md elles-mêmes.
- Les ressources `IBM.AgFileSystem` définies par l'utilisateur peuvent uniquement être automatisées si le disque hébergeant le système de fichiers possède le même nom sur tous les noeuds du cluster.
- EVMS n'est pas pris en charge, y compris tous les groupes de volumes et les volumes logiques créés ou gérés par EVMS.
- Pour SLES 10 et RHEL 5, la collecte des entités de stockage de classes `IBM.Disk`, `IBM.VolumeGroup`, `IBM.LogicalVolume`, `IBM.Partition` et `IBM.AgFileSystem` est prise en charge. Les systèmes de fichiers peuvent être automatisés si les limitations s'appliquant aux unités fournies par l'associateur de périphériques ou aux unités md répertoriées ci-dessus sont respectées.

Linux on System z

Les unités fournies par l'associateur de périphériques ou les unités md sont collectées en tant que ressources `IBM.Disk` si un volume physique a été créé sur l'unité par bloc fournie à l'aide de la commande `pvcreate`. Cet aspect est indépendant de la technologie de disque sous-jacente, ECKD ou SCSI.

Limitations :

- Seules les ressources `IBM.AgFileSystems` ou `IBM.AgFileSystems` définies par l'utilisateur qui résident sur les unités fournies par l'associateur de périphériques ou les unités md collectées peuvent être automatisées. La collecte de ressources des autres disques n'est pas prise en charge. Même si la collecte sur les autres disques aboutit, les ressources collectées ne peuvent pas être automatisées.
- Les ressources `IBM.AgFileSystems` définies par l'utilisateur peuvent uniquement être automatisées si le disque hébergeant le système de fichiers possède le même nom sur tous les noeuds du cluster.
- La réservation SCSI n'est pas prise en charge.

Utilisation des interfaces réseau

Vous pouvez définir une configuration à haute disponibilité avec deux noeuds dans un cluster, chacun disposant de deux interfaces réseau.

Avant de démarrer cette configuration, ne perdez pas de vue qu'il est impossible d'avoir plus d'une interface réseau statique au sein du même sous-réseau IP. Vous devrez entrer chaque adresse IP dans la table de routage du noyau. Si deux interfaces se trouvent dans le même sous-réseau, deux routes permettent d'accéder au même réseau. Si l'interface, qui est à l'origine de la première entrée, échoue, la communication au sein de ce sous-réseau est interrompue même si une autre interface est toujours en fonctionnement.

Deux réseaux séparés physiquement, déplacement de ServiceIP entre les noeuds

La configuration réseau suivante concerne :

Tableau 6. Configuration réseau d'un cluster à deux noeuds avec des interfaces réseau

Ressource	Nom	Unité	IP
Noeud de cluster	lnxcm1	 eth0 eth1	 9.152.172.1/24 192.168.1.1/24
Noeud de cluster	lnxcm2	 eth0 eth1	 9.152.172.2/24 192.168.1.2/24
Routeur	gw	eth0	9.152.172.254/24
ServiceIP	-	–	9.152.172.3/24

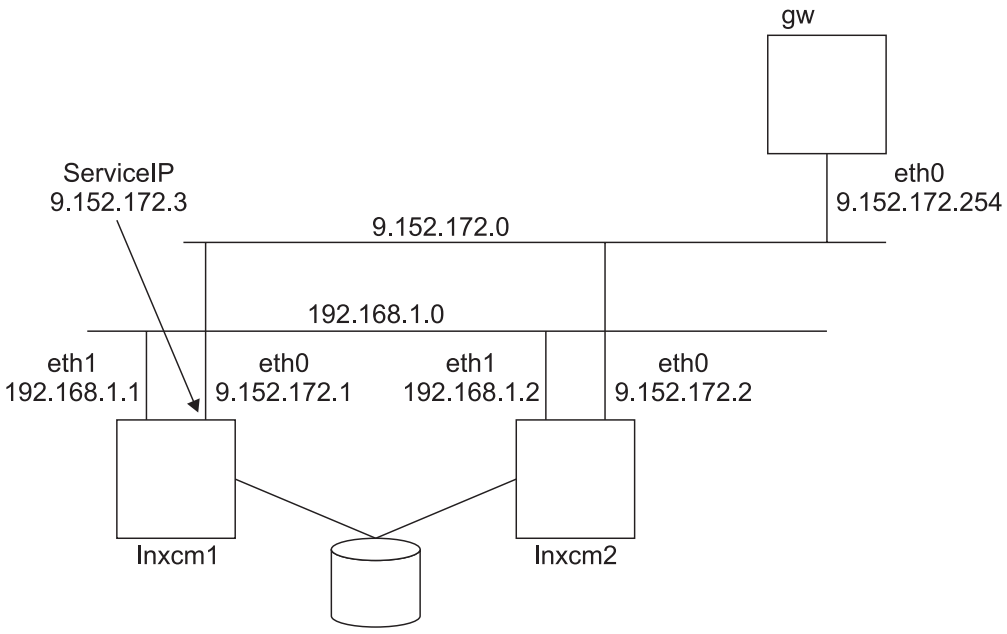

Figure 3. Deux interfaces à deux noeuds, deux réseaux séparés physiquement

Il existe maintenant deux réseaux 192.168.1.0 et 9.152.172.0 pour assurer les communications à l'intérieur du cluster. Si un incident se produit au niveau d'une interface réseau, le cluster ne sera pas rompu.

- Le réseau 9.152.172.0 représente le réseau pour le service informatique hautement disponible.
- Le réseau 192.168.1.0 rend la communication interne entre les clusters plus fiable.

Puisque seul le réseau du ServiceIP est connecté à la passerelle, un échec de l'interface eth0 au niveau de lnxcm1 provoquera le déplacement de ServiceIP vers l'interface eth0 au niveau de l'autre noeud lnxcm2. Puisque les deux réseaux sont séparés physiquement, il est impossible de déplacer ServiceIP depuis eth0 vers eth1 au sein du même noeud.

L'exemple de règle de System Automation for Multiplatforms est le même que celui décrit dans la figure 7, à la page 21.

Tableau 7. Avantages et inconvénients d'une configuration à deux noeuds avec des interfaces réseau

Avantage	Inconvénient
Configuration simplifiée.	ServiceIP se déplace uniquement entre les noeuds.
Redondance dans la communication à l'intérieur du cluster.	

Trois réseaux logiques dans un réseau physique, déplacement de `ServiceIP` entre les interfaces réseau

Il est nécessaire de procéder à une autre configuration réseau non seulement pour déplacer `ServiceIP` entre les noeuds au sein du cluster mais aussi entre les interfaces au sein d'un noeud.

Un réseau logique séparé est nécessaire pour chaque interface d'un noeud, ainsi qu'un réseau supplémentaire pour `ServiceIP`. Le fait de choisir un réseau existant (eth0 ou eth1) peut entraîner des problèmes de routage. Veillez à connecter toutes les interfaces au même réseau physique. Ceci permet à chaque interface de mettre en attente toutes les adresses des réseaux logiques.

La configuration réseau suivante concerne :

Tableau 8. Configuration réseau pour trois réseaux logiques dans un réseau physique

Ressource	Nom	Unité	IP
Noeud de cluster	lnxcm1	 eth0 eth1	 192.168.1.1/24 192.168.2.1/24
Noeud de cluster	lnxcm2	 eth0 eth1	 192.168.1.2/24 192.168.2.2/24
Routeur	gw	eth0	9.152.172.254/24
ServiceIP	-	–	9.152.172.3/24

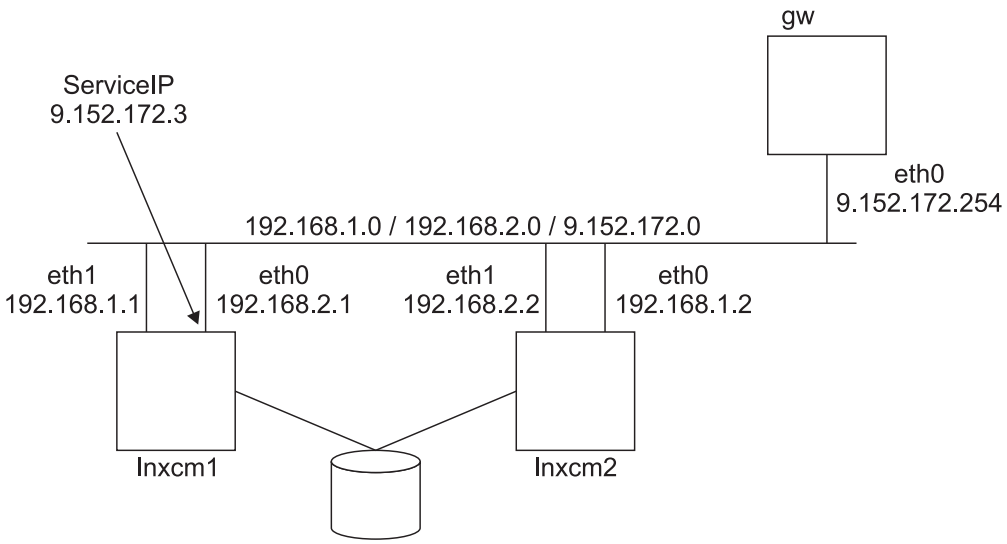

Figure 4. Un réseau physique à deux noeuds et deux interfaces

- Le réseau 9.152.172.0 représente le réseau pour le service informatique hautement disponible.
- Le réseau 192.168.1.0 représente le premier réseau de communication interne à l'intérieur du cluster.
- Le réseau 192.168.2.0 représente le deuxième réseau de communication interne à l'intérieur du cluster.

Exemple de règles de System Automation for Multiplatforms :

```
lnxcm1# mkequ NetInt
IBM.NetworkInterface:eth0:lnxcm1,eth1:lnxcm1,eth0:lnxcm2,eth1:lnxcm2
lnxcm1# mkrsrc IBM.ServiceIP Name="SIP" IPAddress="9.152.172.3"
NetMask="255.255.255.0" NodeNameList="{'lnxcm1','lnxcm2'}"
lnxcm1# mkrg rg
lnxcm1# addrgmbr -g rg IBM.ServiceIP:SIP
lnxcm1# mkrel -p dependson -S IBM.ServiceIP:SIP -G IBM.Equivalency:NetInt
```

Tableau 9. Avantages et inconvénients d'une configuration réseau pour trois réseaux logiques dans un réseau physique

Avantage	**Inconvénient**
Configuration simplifiée.	3 réseaux logiques dans 1 réseau physique.
Redondance dans la communication à l'intérieur du cluster.	Trafic entre trois réseaux sur 1 moyen physique.
`ServiceIP` peut se déplacer entre les interfaces et les noeuds.	

Deux réseaux séparés physiquement, routage dynamique et VIPA

La description détaillée de cette configuration n'est pas abordée dans ce manuel. `ServiceIP` est attribué à un réseau virtuel à l'intérieur du noyau d'un noeud de cluster. Le routage dynamique sur tous les noeuds de cluster et la passerelle assurent que l'établissement d'une route d'accès à `ServiceIP`.

La configuration réseau suivante concerne :

Tableau 10. Configuration réseau de deux réseaux séparés physiquement

Ressource	Nom	Unité	IP
Noeud de cluster	lnxcm1	 eth0 eth1	 9.152.170.1/24 9.152.171.1/24
Noeud de cluster	lnxcm2	 eth0 eth1	 9.152.170.2/24 9.152.171.2/24
Routeur	gw	 eth0 eth1	 9.152.170.254/24 9.152.171.254/24
ServiceIP	-	–	9.152.172.3/24

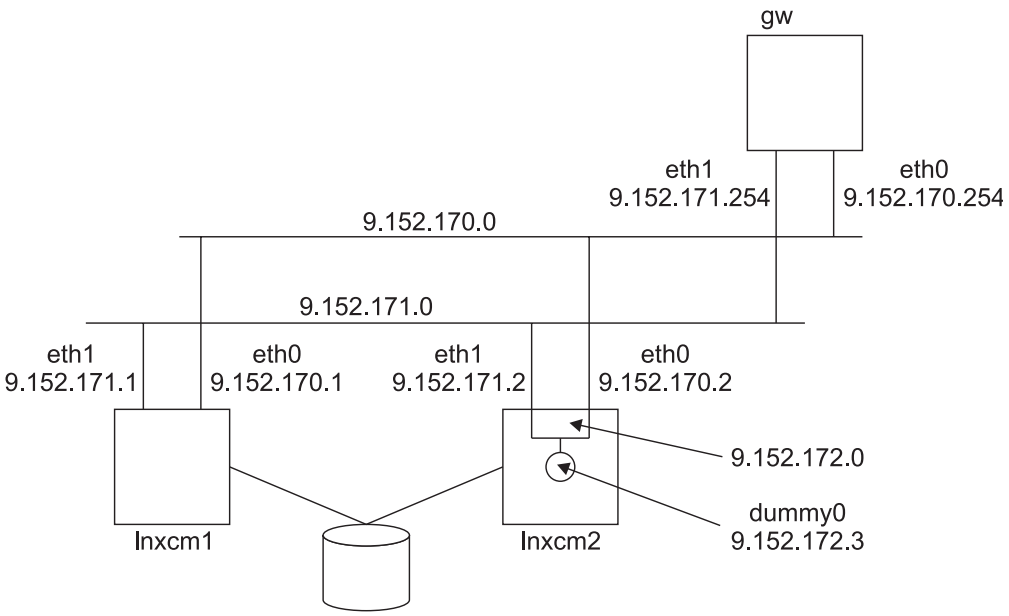

Figure 5. Deux réseaux séparés physiquement, routage dynamique et VIPA

Tableau 11. Avantages et inconvénients d'une configuration réseau de deux réseaux séparés physiquement

Avantage	Inconvénient
Il n'existe pas de dépendance au réseau physique.	Configuration complexe.
Concept permettant de trouver au sein d'un réseau dynamique un hôte (adresse IP)	Routage dynamique exigé.
Il est inutile de déplacer `ServiceIP` entre les périphériques sur le même noeud.	La configuration ne concerne pas uniquement les noeuds de cluster ; la passerelle doit elle-aussi prendre en charge le routage dynamique.

Association d'interfaces

Plusieurs interfaces de réseau physique sont reliées ensemble à un seul réseau logique. Le système d'exploitation doit supporter cette fonction au moyen d'un pilote de périphérique de connexion adéquat. Consultez le document sur votre

système d'exploitation pour savoir comment configurer la connexion à l'interface sur votre système. Assurez-vous d'avoir configuré la connexion HA (à haute disponibilité) et que vos cartes d'interface réseau prennent en charge le mécanisme de détection d'échecs de l'interface dont votre périphérique de connexion a besoin.

La configuration réseau suivante concerne :

Tableau 12. Configuration réseau pour des interfaces réseau physiques reliés ensemble

Ressource	**Nom**	**Unité**	**IP**
Noeud de cluster	lnxcm1	 eth0 eth1	 9.152.172.1/24 9.152.172.1/24
Noeud de cluster	lnxcm2	 eth0 eth1	 9.152.172.2/24 9.152.172.2/24
Routeur	gw	 eth0	 9.152.172.254/24
ServiceIP	-	-	9.152.172.3/24

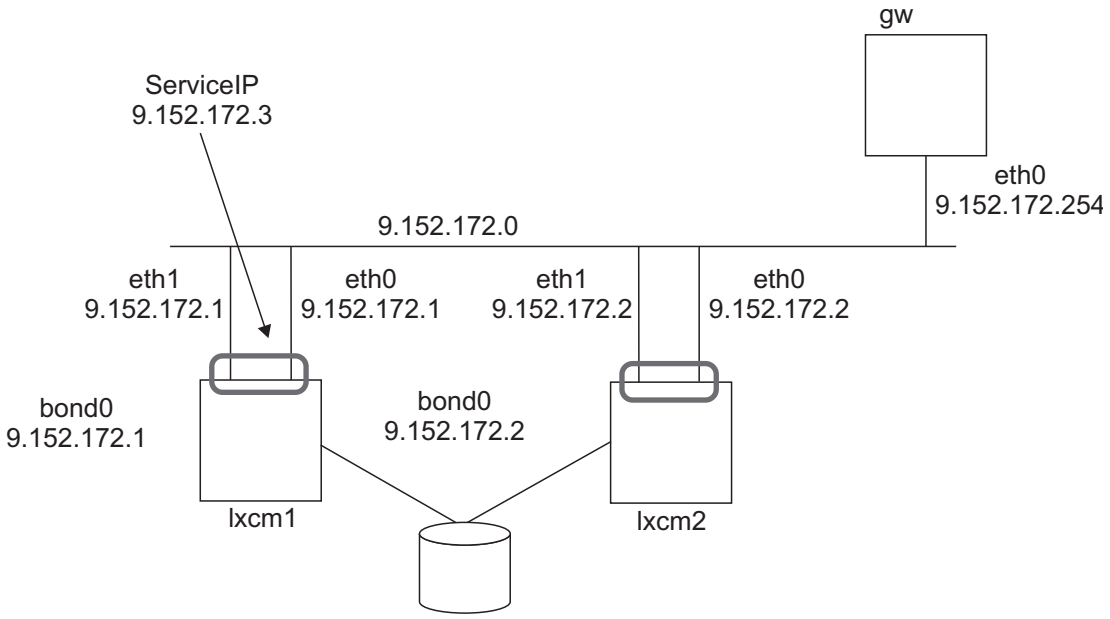

Figure 6. Interfaces de réseau connectées ensemble à un périphérique de réseau logique

Tableau 13. Avantages et inconvénients d'une configuration réseau pour des interfaces réseau physiques connectées ensemble

Avantage	**Inconvénient**
Configuration simplifiée.	Le système d'exploitation doit supporter l'interface de connexion.
Redondance dans la communication à l'intérieur du cluster.	Le matériel d'interface réseau devra prendre en charge la détection d'échecs d'interface (par exemple, le contrôle de connexion MII)
Il est inutile de déplacer ServiceIP entre les périphériques sur le même noeud.	

Utilisation d'une interface Ethernet

Vous pouvez définir une configuration à haute disponibilité avec deux noeuds dans un cluster, chacun disposant d'une interface Ethernet distincte.

La configuration du réseau suivante s'affiche :

Tableau 14. Configuration réseau d'un cluster à deux noeuds avec des interfaces Ethernet

Ressource	Nom	Unité	IP
Noeud de cluster	lnxcm1	eth0	9.152.172.1/24
Noeud de cluster	lnxcm2	eth0	9.152.172.2/24
Routeur	gw	eth0	9.152.172.254/24
ServiceIP	–	–	9.152.172.3/24

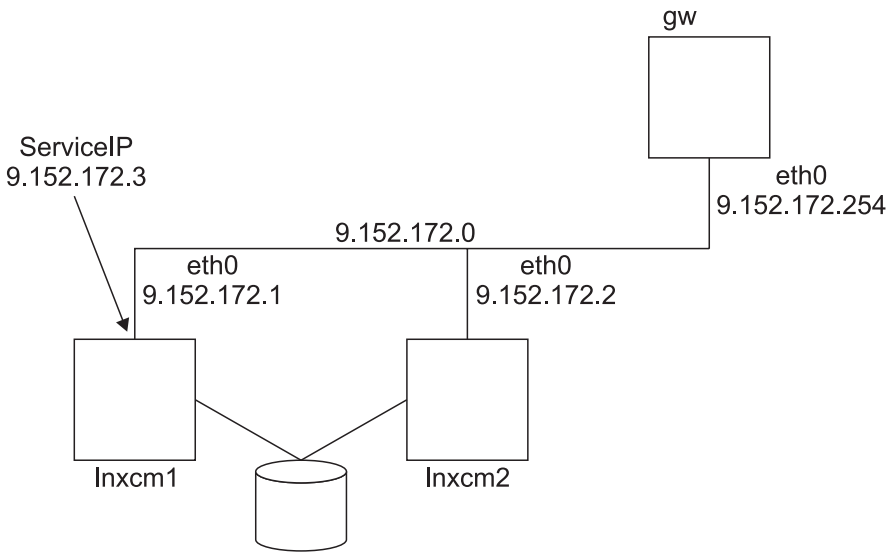

Figure 7. Une interface à deux noeuds

Lors de cette configuration, la communication à l'intérieur du cluster et la présentation du service informatique hautement disponible utilisent la même voie de communication, le réseau 9.152.172.0

ServiceIP peut être attribué automatiquement soit via l'interface eth0 lnxcm1 ou l'interface eth0 lnxcm2. Si une interface échoue, l'automatisation renvoie le ServiceIP vers l'autre noeud. Il répond ainsi aux exigences relatives à l'attribution d'une ressource ServiceIP au sein de l'interface réseau en fonction.

Dans cette configuration, l'échec de l'une des interfaces réseau entraîne une interruption de la communication à l'intérieur du cluster ainsi que l'ensemble des problèmes décrits dans System Automation for Multiplatforms - Guide d'administration et d'utilisation. Si la communication est interrompue, comme le montre à la figure 8, à la page 22, la condition de départage détermine quel noeud poursuit le processus d'automatisation. Si la condition de départage est réservée par le noeud lnxcm1, aucune interface réseau en ligne n'est disponible sur ce noeud pour attribuer ServiceIP.

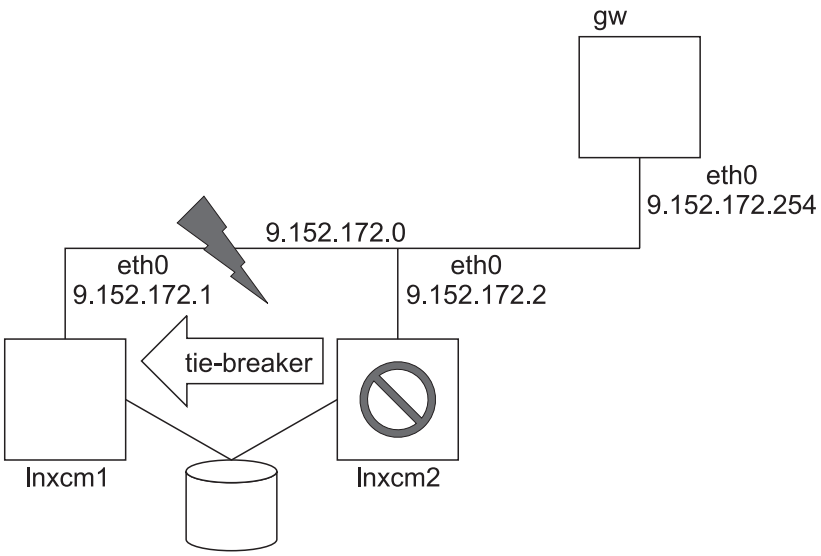

Figure 8. Deux noeuds, une interface – échec de l'interface

Dans cet exemple, le réseau 9.152.172.0 répond à deux objectifs :

1. Représenter le réseau pour le service informatique hautement disponible.
2. Utilisé pour la communication interne entre les clusters.

Exemple de règles de System Automation for Multiplatforms :

```
lnxcm1# mkequ NetInt IBM.NetworkInterface:eth0:lnxcm1,eth0:lnxcm2
lnxcm1# mkrsrc IBM.ServiceIP Name="SIP"
IPAddress="9.152.172.3"
NetMask="255.255.255.0"
NodeNameList="{'lnxcm1','lnxcm2'}"
lnxcm1# mkrg rg
lnxcm1# addrgmbr -g rg IBM.ServiceIP:SIP
lnxcm1# mkrel -p dependson -S IBM.ServiceIP:SIP -G IBM.Equivalency:NetInt
```

Tableau 15. Avantages et inconvénients d'un cluster à deux noeuds avec des interfaces Ethernet

Avantage	**Inconvénient**
La configuration est simple.	Chaque problème de communication entraîne le fractionnement du cluster.
Nécessite moins de matériel réseau.	ServiceIP se déplace uniquement entre les noeuds.

Chapitre 2. Installation

L'installation et la mise à niveau de System Automation for Multiplatforms comprennent la préparation du système et la réalisation d'un ensemble de tâches spécifiques à votre environnement.

Mise à niveau

Vous pouvez mettre à niveau System Automation for Multiplatforms soit à partir d'une version d'évaluation pour passer à une version complète du produit, soit à partir d'une version active pour obtenir la version la plus récente.

Migration d'une version d'évaluation à une version complète du produit

La version d'évaluation de System Automation for Multiplatforms est installée et vous avez acheté la version complète du produit. Vous recevez dans ce cas un autre exemplaire du support d'installation, qui contient le fichier de licence de la licence complète.

Le fichier de licence se trouve sur le support d'installation, dans le sous-répertoire `license`. Pour exécuter la mise à niveau de la licence, entrez :

```
samlicm -i <nom_fichier_licence>
```

Pour afficher la licence, entrez :

```
samlicm -s
```

Après avoir mis à niveau la licence, vous devez vérifier si des mises à jour de System Automation for Multiplatforms sont disponibles, puis installer le dernier niveau de service.

Mise à niveau à partir d'une version antérieure à la version 4.1

Vous pouvez effectuer une mise à niveau à la version 4.1 à partir d'une version antérieure du produit.

Lors de la mise à niveau de System Automation for Multiplatforms à partir d'une version antérieure à la version 4.1, conformez-vous aux recommandations suivantes :

Configuration de l'adaptateur en mode silencieux
Si vous utilisez l'utilitaire de configuration `cfgsamadapter` en mode silencieux pour configurer les paramètres de l'adaptateur d'automatisation de bout en bout, vous devez générer pour ce mode un nouveau fichier de propriétés en entrée, qui soit au niveau de la nouvelle version. Les paramètres de l'adaptateur d'automatisation de bout en bout sont configurés en mode silencieux lorsque vous lancez l'utilitaire `cfgsamadapter` avec l'option `-s`. Avant d'effectuer une configuration en mode silencieux, générez un nouveau fichier de propriétés en entrée en ouvrant l'utilitaire `cfgsamadapter` avec les options `-s [ -g | -gr ]`, plutôt que d'utiliser un fichier de propriétés en entrée existant.

Retrait de la console d'opérations
La console d'opérations et l'éditeur de règles ne sont pas fournis avec la

version 4.1. Vous pouvez cependant continuer à utiliser la console d'opérations pour faire fonctionner les domaines de premier niveau et l'éditeur de règles fourni par System Automation for Multiplatforms jusqu'à la version 3.2.2 pour réaliser la maintenance des règles.

Installation de System Automation for Multiplatforms

Vous pouvez installer System Automation for Multiplatforms dans votre environnement, ou effectuer une mise à jour à partir d'une version précédente du produit.

Les rubriques qui suivent expliquent comment installer ou mettre à jour System Automation for Multiplatforms dans les environnements AIX ou Linux.

Installation initiale
Si vous souhaitez exécuter l'installation initiale de System Automation for Multiplatforms, voir «Exécution de l'installation».

Installation existante
Si une ancienne version de System Automation for Multiplatforms est déjà installée, vous devez réaliser certaines opérations pour pouvoir installer la nouvelle version de System Automation for Multiplatforms. Pour savoir comment migrer une nouvelle version du produit, voir «Migration du domaine System Automation», à la page 27.

Exécution de l'installation

L'installation de System Automation for Multiplatforms s'effectue à l'aide d'un script d'installation.

Ce script d'installation effectue les actions suivantes :

- Un contrôle complet des prérequis pour vérifier qu'ils sont tous disponibles et au niveau demandé. Si ce contrôle échoue, l'installation ne démarre pas et vous devez fournir les prérequis manquants avant de redémarrer l'installation. Voir «Contrôle des prérequis», à la page 3
- Installez System Automation for Multiplatforms, y compris l'adaptateur d'automatisation de bout en bout.

Pour éviter d'avoir à redémarrer l'installation, vous pouvez lancer le contrôle des prérequis indépendamment, avant de commencer l'installation.

Si un domaine homologue IBM RSCT (Reliable Scalable Cluster Technology) existe, vérifiez que le noeud sur lequel vous exécutez le script est hors ligne dans le domaine. Autrement, l'installation est annulée.

Installez le produit, avec l'adaptateur d'automatisation :

1. Connectez-vous comme utilisateur root ou avec des droits équivalents.
2. Si vous avez téléchargé le fichier `.tar` depuis Internet, décompressez-le :
   ```
   tar -xvf <fichier tar>
   ```
   Si vous vous êtes procuré ce produit sur DVD, montez le DVD et accédez au répertoire correspondant.
3. Entrez la commande suivante :
   - Linux : `cd SAM4100MPLinux`

- AIX : `cd SAM4100MPAIX`

4. Lancez le script d'installation :

   `./installSAM`

   Généralement, vous n'avez pas besoin de spécifier d'options pour la commande **installSAM**. Par défaut, les packages correspondant à toutes les langues prises en charge sont installés. Si vous ne souhaitez pas installer l'ensemble des langues, mais seulement l'anglais, utilisez l'option `--nonls`. Pour une description détaillée de la commande **installSAM**, voir *Tivoli System Automation for Multiplatforms - Guide de référence* .

5. Lisez le contrat de licence et les iInformations sur la licence qui s'affichent. Vous pouvez faire défiler le texte ligne par ligne à l'aide de la touche Entrée, et page par page à l'aide de la barre d'espacement, ce qui correspond à l'option "more" sous UNIX. Lorsque vous êtes arrivé à la fin des informations sur la licence et que vous souhaitez les accepter, tapez 'y'. Toute autre entrée entraînera l'annulation de l'installation.

   L'installation est également annulée en cas d'absence de fichier de licence.

6. Une fois que vous avez accepté le contrat de licence, le programme d'installation effectue un contrôle des prérequis pour s'assurer qu'ils sont disponibles au niveau requis.

   Si ce contrôle échoue, l'installation ne démarre pas et vous devez fournir les prérequis manquants avant de redémarrer l'installation.

   Les résultats du contrôle des prérequis sont disponibles dans le fichier journal `/tmp/installSAM.<#>.log`.

   Si le contrôle a abouti sur votre système, le produit est installé, avec l'adaptateur d'automatisation.

7. Recherchez des informations sur l'installation dans le fichier journal suivant :

   `/tmp/installSAM.<#>.log`

   Le symbole de hachage <#> est un nombre, le nombre le plus élevé identifiant le fichier journal le plus récent.

   Les entrées du fichier journal possèdent les préfixes suivants :

   prereqSAM
   Entrées enregistrées lors du contrôle des prérequis.

   installSAM
   Entrées enregistrées lors de l'installation du produit.

8. Pour savoir quels packages ont été installés, examinez le fichier `/tmp/installSAM.<#>.log`, où <#> correspond au numéro de fichier journal le plus élevé de la liste.

Installation de la licence du produit

System Automation for Multiplatforms exige qu'une Licence de produit valide soit installée sur chaque système sur lequel il est exécuté.

La licence se trouve sur le support d'installation dans le sous-répertoire 'licence'. L'installation de la licence s'effectue lors du processus d'installation du produit. Si la licence ne s'est pas installée, exécutez la commande suivante pour l'installer :

`samlicm –i fichier_licence`

Pour afficher la licence, entrez :

`samlicm -s`

Pour une description détaillée de la commande, voir *Tivoli System Automation for Multiplatforms - Guide de référence* .

Langues et paramètres nationaux pris en charge

Si vous souhaitez utiliser System Automation for Multiplatforms dans une autre langue que l'anglais, consultez les sections ci-dessous pour connaître les langues et les paramètres régionaux pris en charge.

Linux

Le tableau 16 indique les combinaisons de langues et de paramètres régionaux pris en charge par System Automation for Multiplatforms sur les systèmes Linux pour l'affichage des messages traduits. Les nouvelles versions des systèmes d'exploitation Linux peuvent ne pas prendre en charge tous les codages répertoriés. Le codage UTF-8 est toujours pris en charge.

Tableau 16. Langues et paramètres régionaux pris en charge par System Automation for Multiplatforms sur les systèmes Linux.

Langue	UTF-8	ISO-8859-1	EUC/GBK	Euro	GB18030/BIG5
Allemand	de_DE.UTF-8	de_DE, de_DE.ISO-8859-1		de_DE@euro	
Espagnol	es_ES.UTF-8	es_ES, es_ES.ISO-8859-1		es_ES@euro	
Français	fr_FR.UTF-8	fr_FR, fr_FR.ISO-8859-1		fr_FR@euro	
Italien	it_IT.UTF-8	it_IT, it_IT.ISO-8859-1		it_IT@euro	
Japonais	ja_JP.UTF-8		ja_JP.eucJP		
Coréen	ko_KR.UTF-8		ko_KR.eucKR		
Portugais brésilien	pt_BR.UTF-8	pt_BR			
Chinois simplifié	zh_CN.UTF-8		zh_CN.GBK, zh_CN.GB2312		zh_CN.GB18030
Chinois traditionnel	zh_TW.UTF-8				zh_TW.Big5, zh_TW

AIX

Le tableau ci-dessous indique les combinaisons de langues et de paramètres régionaux pris en charge par System Automation for Multiplatforms sous AIX pour l'affichage des messages traduits.

Tableau 17. Langues et environnements locaux pris en charge par Tivoli System Automation sur les systèmes AIX

Langue	UTF-8	ISO-8859-1	EUC/GBK	SJIS/GB18030/BIG5
Allemand	DE_DE	de_DE		
Espagnol	ES_ES	es_ES		
Français	FR_FR	fr_FR		
Italien	IT_IT	it_IT		
Japonais	JA_JP		ja_JP	Ja_JP
Coréen	KO_KR		ko_KR	
Portugais brésilien	PT_BR	pt_BR		

Tableau 17. Langues et environnements locaux pris en charge par Tivoli System Automation sur les systèmes AIX (suite)

Langue	UTF-8	ISO-8859-1	EUC/GBK	SJIS/GB18030/BIG5
Chinois simplifié	ZH_CN		zh_CN	Zh_CN
Chinois traditionnel	ZH_TW		zh_TW	Zh_TW

Migration du domaine System Automation

Vous pouvez migrer vers System Automation for Multiplatforms version 4.1 si une version plus ancienne est déjà installée.

Avant de migrer un ou plusieurs noeuds vers un niveau plus récent, vous devez avoir bien assimilé les notions suivantes :

- Le processus de migration démarre lorsqu'un noeud à l'intérieur d'un cluster actif est mis à jour vers un niveau de code supérieur.
- Vous pouvez également effectuer une mise à niveau vers un niveau de code supérieur. En revanche, la migration descendante n'est pas possible.
- Le processus de migration n'est terminé qu'une fois que le numéro de version actif est égal au numéro de version le plus haut déjà installé. Jusque-là, plusieurs niveaux de version peuvent coexister.
- A partir de la version 4.1, l'activation de la haute disponibilité pour l'adaptateur d'automatisation de bout en bout ne nécessite plus de règle d'automatisation. Pour plus d'informations, voir «Migration d'un adaptateur d'automatisation de bout en bout hautement disponible», à la page 30.

Migration d'un domaine complet

Le domaine n'est pas disponible pendant la migration. Pour minimiser les temps d'arrêt, vous pouvez effectuer un contrôle des prérequis avant de commencer la migration.

Pour plus d'informations, voir «Contrôle des prérequis», à la page 3.

Migration d'un domaine entier :

1. Vérifiez que toutes les ressources sont hors ligne :
   a. Vérifiez que adaptateur d'automatisation de bout en bout est actif :
      ```
      samadapter status
      ```
      S'il fonctionne, arrêtez-le :
      ```
      samadapter stop
      ```
   b. Arrêtez l'ensemble des groupes de ressources en ligne en définissant leur état nominal sur hors ligne :
      ```
      chrg -o Offline <nom_groupe_ressources>
      ```
2. Si le domaine est en ligne, arrêtez le domaine :
   ```
   stoprpdomain <nom_domaine>
   ```
3. Sous AIX, exécutez la commande suivante après l'arrêt du cluster et avant le lancement de l'installation :
   ```
   # /usr/sbin/slibclean
   ```
4. Exécutez le script `./installSAM` depuis le répertoire d'installation sur le DVD du produit ou depuis le livrable obtenu par voie électronique et décompressé

sur tous les noeuds. Pour plus d'informations sur le script `installSAM`, voir«Exécution de l'installation», à la page 24.

5. Démarrez le domaine :

   ```
   startrpdomain <nom_domaine>
   ```

6. Vérifiez les niveaux de code avec la commande `lssrc –ls IBM.RecoveryRM` (voir l'exemple dans «Vérification du numéro de version d'installation et du numéro de version active», à la page 29). Tous les noeuds doivent comporter le nouveau niveau de code, mais le niveau de code actif doit correspondre au précédent.

7. Pour activer la nouvelle version, voir «Exécution de la migration», à la page 29.

Migration noeud par noeud

La migration noeud par noeud est prise en charge uniquement lors de la migration à partir de System Automation for Multiplatforms version 2.3 ou d'une version ultérieure. La migration individuelle des noeuds d'un domaine présente l'avantage de maintenir System Automation for Multiplatforms disponible pendant l'opération.

Pour savoir comment réduire le temps d'indisponibilité, voir «Contrôle des prérequis», à la page 3.

Exécutez une migration noeud par noeud :

1. Excluez le noeud de l'automatisation pour vérifier que les ressources devant rester disponibles sont déplacées vers un autre noeud du domaine homologue :

   ```
   samctrl -u a <noeud>
   ```

   Remarque : La commande peut être exécutée pendant une durée très importante jusqu'à ce que toutes les opérations de transfert soient terminées.

2. Arrêtez le noeud depuis un autre noeud dans le domaine et vérifiez qu'il est bien arrêté :

   ```
   stoprpnode <noeud>; lsrpnode
   ```

3. Pour mettre à niveau le noeud, exécutez le script `./installSAM` depuis le répertoire d'installation sur le CD du produit ou depuis le livrable obtenu par voie électronique et décompressé. Pour plus d'informations sur le script `installSAM`, voir«Exécution de l'installation», à la page 24.

4. Démarrez le noeud :

   ```
   startrpnode <noeud>
   ```

5. Ajoutez de nouveau le noeud mis à niveau à l'automatisation :

   ```
   samctrl -u d <noeud>
   ```

6. Le noeud mis à jour peut dorénavant rejoindre le domaine existant. Utilisez la commande `lssrc –ls IBM.RecoveryRM` (voir l'exemple dans «Vérification du numéro de version d'installation et du numéro de version active», à la page 29) pour afficher la version installée et la version active du produit. Les nouvelles fonctions du code ne seront pas activées tant que le numéro de version actif de System Automation for Multiplatforms n'est pas égal au numéro de version le plus élevé de System Automation for Multiplatforms installé à l'intérieur du

cluster. Vous ne pourrez pas utiliser pleinement ces nouvelles fonctions de code tant que tous les noeuds n'ont pas été mis à niveau.

7. Renouvelez les étapes 1 à 6 pour les autres noeuds du cluster.

8. Pour activer la nouvelle version, voir «Exécution de la migration».

Vérification du numéro de version d'installation et du numéro de version active

Après la mise à niveau, les nouvelles fonctions ne sont pas encore activées. Les niveaux de version précédente et les nouveaux niveaux de version peuvent coexister jusqu'au terme de la migration.

La commande **lssrc –ls IBM.RecoveryRM** indique le numéro de la version active, AVN, ainsi que le numéro de la version installée, IVN, du produit. Lorsque les numéros IVN et AVN sont identiques, la migration est terminée. Sortie :

```
Sous-système         : IBM.RecoveryRM
PID               : 31163
Nom de l'ensemble de clusters      : xdr43
Numéro du noeud       : 1
Heure de début du démon : 02/19/13 15:12:00

Etat du démon :
   Nom du noeud         : lnxxdr43
   Nom du noeud maître  : lnxxdr43 (numéro du noeud = 1)
   Notre IVN            : 4.1.0.0
   Notre AVN            : 4.1.0.0
   Notre CVN            : d4b7e876c (4b7e876c)
   Nombre total de noeuds: 2
   Nombre de membre associé  : 2
   Nombre de quorum de configuration : 2
   Nombre de quorum au démarrage : 1
   Etat du quorum opérationnel : HAS_QUORUM
   Dans Quorum de configuration : TRUE
   Dans Etat de configuration  : TRUE
   Remplacement de l'état de configuration : FALSE
```

Figure 9. Vérification du numéro de version active et du numéro de version d'installation

Pour activer la nouvelle version, voir «Exécution de la migration».

Exécution de la migration

Vérifiez si la migration s'est déroulée correctement.

Vérifiez et exécutez la migration :

1. Vérifiez que le domaine est démarré et que tous les noeuds du domaine sont en ligne.

2. Exécutez la commande **lsrpdomain** pour afficher la version de RSCT active dans le domaine homologue et l'état de la version mixte :

   ```
   Name        OpState  RSCTActiveVersion  MixedVersions  TSPort GSPort
   SA_Domain  Online   2.5.5.1           Yes            12347   12348
   ```

3. Exécutez la commande **lsrpnode** pour afficher la version de RSCT installée sur les noeuds. Gardez à l'esprit que tous les noeuds doivent être en ligne :

```
Nom     EtatOp Version RSCT
node01 Online  2.5.5.1
node02 Online  2.5.5.1
node03 Online  2.5.5.1
```

4. Si le domaine homologue RSCT est exécuté en mode version mixte (`MixedVersions = Yes`) et si tous les noeuds ont été mis à niveau vers la nouvelle version, vous devez mettre à jour la version active RSCT en exécutant l'action RSCT `CompleteMigration` sur l''un des noeuds. Avant d'exécuter l'action, consultez les procédures de préparation à la migration de RSCT dans le manuel *IBM RSCT Administration Guide*.

   Pour mettre à jour `RSCTActiveVersion`, vérifiez que tous les noeuds sont en ligne. Exécutez la commande suivante sur l'un des noeuds :

   ```
   runact -c IBM.PeerDomain CompleteMigration Options=0
   ```

   Pour vérifier que la version active de RSCT a bien été mise à jour, exécutez à nouveau la commande **`lsrpdomain`** :

   ```
   Name        OpState  RSCTActiveVersion  MixedVersions  TSPort GSPort
   SA_Domain   Online   2.5.5.1            No             12347  12348
   ```

5. Exécutez la commande **`samctrl -m`** pour activer les nouvelles fonctions et finaliser la migration. Pour plus d'informations sur cette commande, voir *System Automation for Multiplatforms - Guide de référence*.

6. Si la migration a été effectuée à partir de la version 3.1 de System Automation for Multiplatforms release 3.1, vous devez ajuster la valeur de l'attribut `OperationalFlags` en entrant la commande suivante sur l'un des noeuds :

   ```
   chrsrc -c IBM.CHARMControl OperationalFlags=8088
   ```

   Pour afficher la valeur réelle de cet attribut, tapez :

   ```
   lsrsrc -c IBM.CHARMControl
   ```

Les nouvelles fonctions de code sont actives si la valeur de `ActiveVersion` et de `InstalledVersion` de System Automation for Multiplatforms est la même pour tous les noeuds.

Migration d'un adaptateur d'automatisation de bout en bout hautement disponible

Découvrez comment mettre à niveau un adaptateur d'automatisation de bout en bout hautement disponible vers la version 4.1.

A partir de System Automation for Multiplatforms version 4.1, une règle d'automatisation n'est plus requise pour rendre l'adaptateur d'automatisation de bout en bout hautement disponible. Sous Windows, cette implémentation était déjà disponible avant la version 4.1, mais elle l'est désormais pour tous les autres systèmes d'exploitation.

System Automation for Multiplatforms version 3.2 ou ou version antérieure :

La figure 10, à la page 31 présente l'environnement dans lequel l'adaptateur d'automatisation de bout en bout fonctionnait dans des clusters UNIX et Linux.

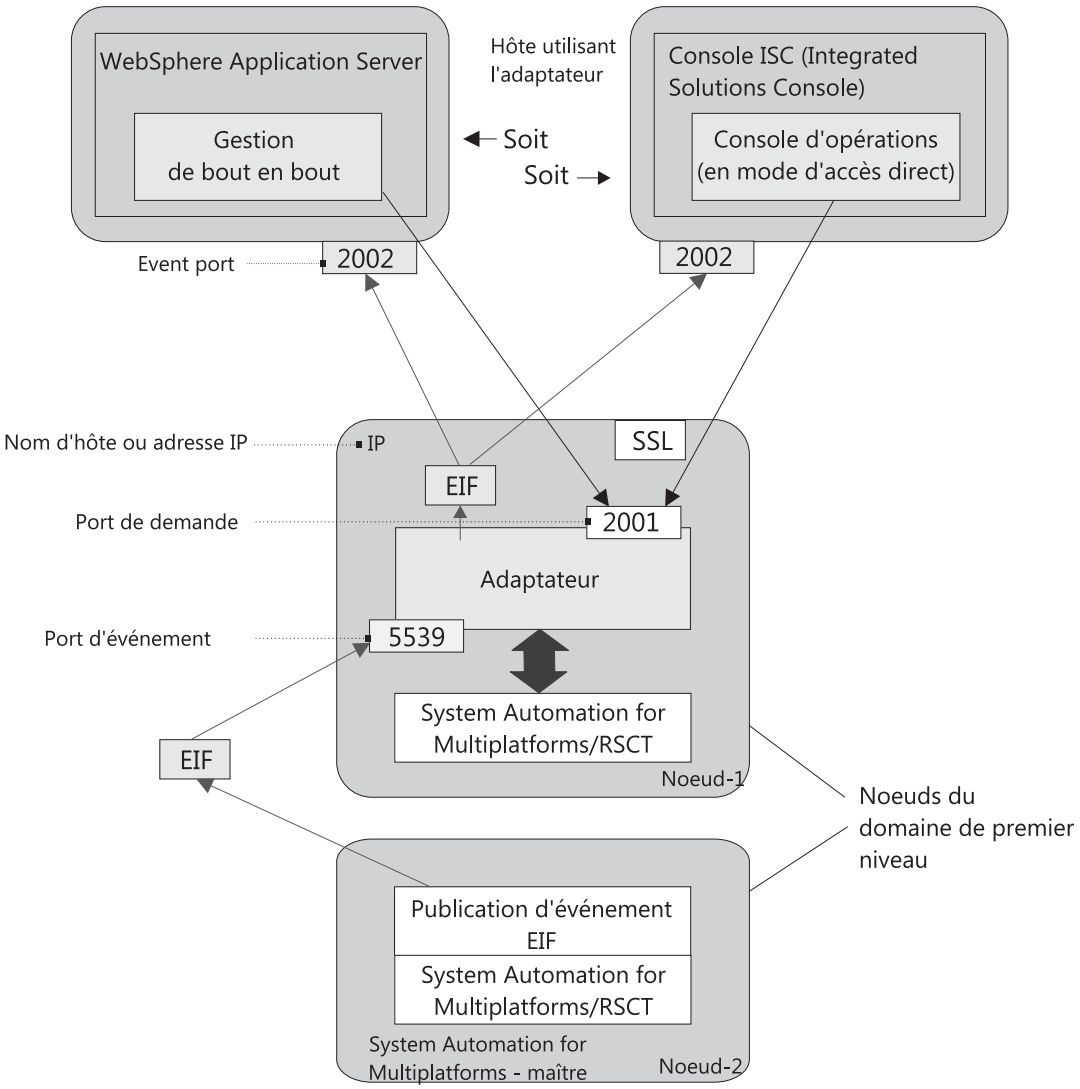

Figure 10. Environnement de l'adaptateur d'automatisation de bout en bout dans des clusters UNIX et Linux avant la version 4.1

System Automation for Multiplatforms version 4.1 :

La figure 11, à la page 32 présente l'environnement dans lequel l'adaptateur fonctionne à partir de la version 4.1.

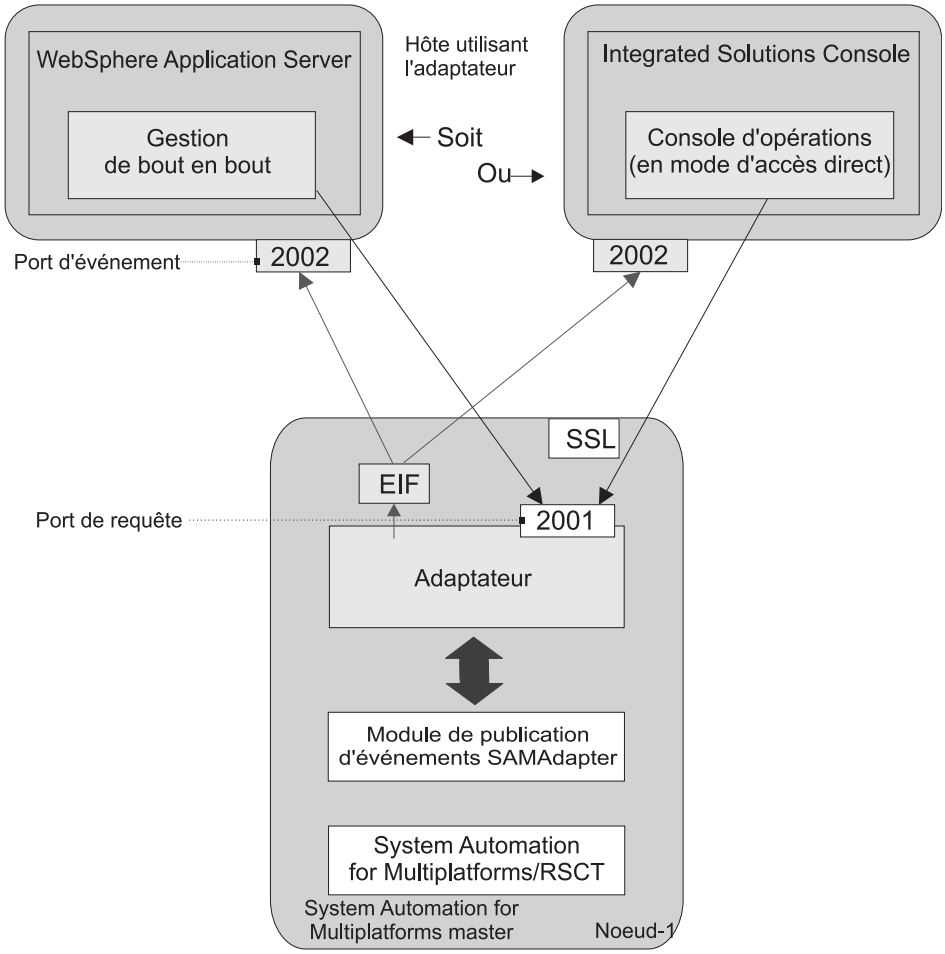

Figure 11. Environnement de l'adaptateur d'automatisation de bout en bout à partir de la version 4.1

A partir de la version 4.1, l'adaptateur d'automatisation est connecté au nœud maître de System Automation. L'infrastructure de cluster vérifie que le nœud maître de System Automation for Multiplatforms et l'adaptateur sont toujours disponibles. Aucune règle d'automatisation supplémentaire n'est requise pour rendre l'adaptateur hautement disponible. L'adresse IP virtuelle, qui est une ressource critique de System Automation, n'est plus nécessaire dans ce scénario.

La modification de l'implémentation haute disponibilité pour l'adaptateur d'automatisation de bout en bout a les implications suivantes si vous mettez à niveau votre cluster nœud par nœud, conformément à la description figurant dans «Migration noeud par noeud», à la page 28.

L'ancienne implémentation est active lors du processus de migration
Tant que la migration n'est pas terminée, différentes versions du code sont actives sur les différents nœuds du cluster. Au cours de cette période, l'ancienne implémentation de la haute disponibilité est toujours active. La nouvelle implémentation entre en vigueur dès que la version active est définie sur la version 4.1.0.0 (ou ultérieure). Pour plus d'informations, voir «Exécution de la migration», à la page 29.

La configuration de la règle d'automatisation est toujours possible lors du processus de migration
Une règle d'automatisation n'est plus requise pour rendre l'adaptateur hautement disponible. Néanmoins, l'ancienne implémentation est toujours

prise en charge tant que vous n'avez pas terminé une migration nœud par nœud. Les tâches de configuration des règles d'automatisation d'adaptateur sont toujours disponibles et prises en charge au cours du processus de migration. La documentation relative à ces tâches de configuration a été supprimée. Si vous avez encore besoin de consulter la description de ces tâches, reportez-vous à la documentation de la version précédente du produit.

Remarque : Si vous souhaitez modifier la configuration haute disponibilité lors d'une migration nœud par nœud, veillez à exécuter l'utilitaire de configuration sur un nœud de cluster en ligne. En effet, le numéro de la version active ne peut pas être déterminé sur un nœud hors ligne. L'ancienne implémentation de la configuration de la haute disponibilité de l'adaptateur n'est pas disponible dans un cluster ou hors ligne sur un nœud hors ligne. C'est le cas même si le numéro de la version active est antérieur à la 4.1.0.0.

Avant de terminer la migration vers la version 4.1, vérifiez toutes vos règles d'automatisation pour le domaine entier et la migration nœud par nœud. Les règles d'automatisation peuvent contenir des ressources qui sont liées à la haute disponibilité de l'adaptateur d'automatisation de bout en bout. Supprimez toutes ces ressources :

- Vérifiez le préfixe de ressource que vous utilisez lors de la configuration de l'automatisation de l'adaptateur. Le préfixe par défaut est `samadapter-`.
- Supprimez l'ensemble des relations, ressources et groupes de ressources dont le nom commence par ce préfixe.
- Si vous utilisez le format `xml` pour définir vos règles, supprimez l'ensemble des relations, ressources et groupes de ressources dont le nom commence par le préfixe des fichiers `xml`.

Actions requises une fois la migration terminée

Si l'adaptateur fonctionne au moment du lancement de la migration du cluster, il est arrêté et n'est pas redémarré une fois la migration terminée.

Dans le cadre de la migration, les opérations manuelles suivantes doivent obligatoirement être réalisées avant le démarrage de l'adaptateur :

1. A l'aide de l'utilitaire de configuration `cfgsamadapter`, modifiez le nom d'hôte ou l'adresse IP de l'adaptateur. Sélectionnez le nom de l'hôte local de chaque cluster comme par défaut, ou entrez un autre nom d'hôte ou une autre adresse IP.
2. Si vous avez sélectionné l'hôte par défaut pour l'adaptateur, répliquez la configuration sur les autres nœuds du cluster. Sinon, configurez explicitement un nom d'hôte ou une adresse IP sur chaque nœud du cluster.

Vous pouvez maintenant démarrer l'adaptateur. Vous pouvez utiliser la boîte de dialogue de configuration comme décrit dans System Automation for Multiplatforms - Guide d'administration et d'utilisation ou utiliser la commande `samadapter start`.

L'ancienne implémentation haute disponibilité de l'adaptateur continue à être utilisée

Dans de rares cas, il peut être impossible d'utiliser la nouvelle implémentation haute disponibilité de l'adaptateur. Par exemple, si vous souhaitez que l'adaptateur s'exécute uniquement sur un sous-ensemble des nœuds disponibles dans le cluster. Ce scénario est possible avec l'ancienne

règle d'automatisation. Cependant, avec la nouvelle approche, l'adaptateur peut s'exécuter sur n'importe quel nœud de cluster.

Dans un tel cas, vous pouvez faire appliquer obligatoirement la règle d'automatisation pour activer la haute disponibilité de l'adaptateur, si vous utilisez la version 4.1. Même si vous exécutez déjà un cluster à l'aide de la nouvelle ou de l'ancienne approche, vous pouvez basculer vers l'autre approche respective. Les scénarios suivants sont pris en charge :

1. **Continuez à utiliser l'ancienne implémentation lors de la migration vers la version 4.1.**

   Si vous migrez votre cluster à partir d'une version antérieure vers la version 4.1, la nouvelle implémentation à haute disponibilité de l'adaptateur est activée. Si vous souhaitez utiliser l'ancienne implémentation à la place, procédez comme suit après avoir mis à niveau le code du produit vers la version 4.1 sur tous les nœuds de cluster :

   a. Editez le fichier des propriétés de configuration `/etc/opt/IBM/tsamp/sam/cfg/sam.adapter.properties` et remplacez la valeur `false` du paramètre `use-adapter-ha-policy` par `true` dans chaque nœud du cluster.
   b. Lancez la commande **`samctrl -m`**.

2. **Basculement vers la nouvelle implémentation haute disponibilité de l'adaptateur après la migration.**

   Si vous avez migré votre cluster à partir d'une version antérieure vers la version 4.1, et appliqué la procédure du scénario 1 décrite ci-dessus, l'ancienne implémentation à haute disponibilité de l'adaptateur est toujours utilisée. Pour basculer vers la nouvelle implémentation haute disponibilité de l'adaptateur, procédez comme suit :

   a. Arrêtez le domaine à l'aide de la commande **`stoprpdomain`**.
   b. Editez le fichier des propriétés de `/etc/opt/IBM/tsamp/sam/cfg/sam.adapter.properties` et remplacez la valeur `true` du paramètre `use-adapter-ha-policy` par `false` dans chaque nœud du cluster.
   c. Démarrez le domaine à l'aide de la commande **`startrpdomain`**.

3. **Retour à l'ancienne implémentation haute disponibilité de l'adaptateur après la migration.**

   Si vous avez migré votre cluster à partir d'une version antérieure vers la version 4.1, mais sans appliquer la procédure du scénario 1 décrite ci-dessus, la nouvelle implémentation à haute disponibilité de l'adaptateur est utilisée. Il en va de même si vous avez suivi la procédure décrite pour le scénario 2. Pour revenir à l'ancienne implémentation haute disponibilité de l'adaptateur, procédez comme suit :

   a. Arrêtez l'adaptateur à l'aide de la commande **`samadapter stop`**.
   b. Editez le fichier des propriétés de configuration `/etc/opt/IBM/tsamp/sam/cfg/sam.adapter.properties` et remplacez la valeur `false` du paramètre `use-adapter-ha-policy` par `true` dans chaque nœud du cluster.
   c. Démarrez l'utilitaire de configuration en entrant la commande **`cfgsamadapter`** puis procédez comme suit :
      1) Dans la fenêtre principale de la boîte de dialogue de configuration, cliquez sur **Configurer**.

2) Cliquez sur **Enregistrer** pour enregistrer les modifications de configuration. L'entrée du diffuseur EEZ qui est requise pour l'ancienne implémentation est alors ajoutée au fichier de propriétés de configuration /etc/Tivoli/tec/samPublisher.conf dans tous les cas. Cette opération est obligatoire car l'entrée du diffuseur peut être supprimée par l'adaptateur lorsqu'il utilise la nouvelle implémentation à haute disponibilité de l'adaptateur.
3) Dans l'écran principal de la boîte de dialogue de configuration, cliquez sur **Répliquer** pour répercuter les modifications de configuration aux autres nœuds du cluster.
4) Dans la fenêtre principale de la boîte de dialogue de configuration, cliquez sur **Définir** pour réactiver la règle de haute disponibilité de l'adaptateur. Elle est supprimée par la System Automation for Multiplatforms lors de l'exécution de la commande **samctrl -m**.

d. Démarrez l'adaptateur à l'aide de la commande **samadapter start**.

4. **Utilisation de l'implémentation à haute disponibilité de l'adaptateur dans un nouveau cluster de la version 4.1.0.0**

   Si vous exécutez une installation initiale de la version 4.1.0.0, vous utilisez la nouvelle implémentation à haute disponibilité de l'adaptateur. Si vous souhaitez utiliser à la place l'ancienne implémentation à haute disponibilité de l'adaptateur, procédez comme suit :

   a. Arrêtez l'adaptateur à l'aide de la commande **samadapter stop**.
   b. Editez le fichier des propriétés de configuration /etc/opt/IBM/tsamp/sam/cfg/sam.adapter.properties et remplacez la valeur false du paramètre use-adapter-ha-policy par true dans chaque nœud du cluster.
   c. Démarrez l'utilitaire de configuration en entrant la commande **cfgsamadapter** puis procédez comme suit :
      1) Dans la fenêtre principale de la boîte de dialogue de configuration, cliquez sur **Configurer**.
      2) Dans l'onglet Automatisation, configurez la règle de haute disponibilité de l'adaptateur.
      3) Cliquez sur **Enregistrer** pour enregistrer les modifications de configuration.
      4) Dans l'écran principal de la boîte de dialogue de configuration, cliquez sur **Répliquer** pour répercuter les modifications de configuration aux autres nœuds du cluster.
      5) Dans la fenêtre principale de la boîte de dialogue de configuration, cliquez sur **Définir** pour activer la règle de haute disponibilité de l'adaptateur.
   d. Démarrez l'adaptateur à l'aide de la commande **samadapter start**.

Scénarios 3 et 4 : voir la tâche **Définir** et l'onglet Automatisation. La documentation correspondante est supprimée dans la version 4.1. Si vous avez encore besoin de consulter la description de ces tâches, reportez-vous à la documentation de la version précédente du produit.

Post-installation

Pour pouvoir obtenir les données de débogage, vous devez configurer le programme de journalisation système.

Après avoir installé System Automation for Multiplatforms sous AIX, vous devez effectuer la tâche suivante :

Configurez le programme de journalisation système sous AIX

Le programme de journalisation système n'est pas configuré par défaut. Les messages sont écrits dans le journal d'erreurs.

Pour pouvoir obtenir les données de débogage, vous devez configurer le programme de journalisation système dans le fichier `/etc/syslog.conf`. Lorsque vous avez effectué les modifications nécessaires, vous devez régénérer `syslogd` à l'aide de la commande **`refresh –s syslogd`**. L'emplacement du fichier journal est défini dans `/etc/syslog.conf`.

Aucune action supplémentaire n'est requise pour Linux.

Activation de la compatibilité avec le mode d'accès simultané optimisé sur les groupes de volumes partagés sous AIX

Si la fonction d'accès simultané optimisé n'est pas activée sur vos groupes de volumes partagés, la défaillance d'un noeud provoque le verrouillage des disques et le noeud distant ne peut plus accéder au disque. Pour éviter cette situation, vous devez activer l'accès simultané optimisé sur le groupe de volumes partagés.

Remarque :

1. Vérifiez que le package `bos.clvm.enh` est installé sur votre système.
2. System Automation for Multiplatforms prend en charge des groupes de volumes compatibles avec le mode d'accès simultané dans un mode non simultané lorsque la règle utilise des ressources de classes `IBM.AgFileSystem` ou `IBM.VolumeGroup`. System Automation for Multiplatforms ne prend en charge ni les groupes de volume, ni le système de fichiers, en tant que ressources dans la règle. La prise en charge de groupes de volumes compatibles avec le mode d'accès simultané améliorés peut être fournie de façon explicite par un fournisseur de règles via les ressources `IBM.Application` afin de gérer le système de fichiers en plus des groupes de volumes.

Avant d'activer la compatibilité avec le mode d'accès simultané optimisé sur le groupe de volumes, exécutez la commande `lsvg` pour afficher des informations sur le groupe de volumes partagés :

```
# lsvg vgERSTZ0
VOLUME GROUP:       vgERSTZ0                 VG IDENTIFIER:
00c31bfe00004c0000000118c2f1ead2
VG STATE:           active                   PP SIZE:        4 megabyte(s)
VG PERMISSION:      read/write               TOTAL PPs:      255 (1020
megabytes)
MAX LVs:            256                      FREE PPs:       14 (56 megabytes)
LVs:                2                        USED PPs:       241 (964 megabytes)
OPEN LVs:           2                        QUORUM:         2 (Enabled)
TOTAL PVs:          1                        VG DESCRIPTORS: 2
STALE PVs:          0                        STALE PPs:      0
ACTIVE PVs:         1                        AUTO ON:        no
MAX PPs per VG:     32512
MAX PPs per PV:     1016                     MAX PVs:        32
LTG size (Dynamic): 256 kilobyte(s)          AUTO SYNC:      no
HOT SPARE:          no                       BB POLICY:      relocatable
```

Pour activer la compatibilité avec le mode d'accès simultané optimisé sur un groupe de volumes à l'aide de l'interface SMIT, procédez comme suit :

1. Entrez la commande suivante :

   ```
   # smitty vg
   ```

Un texte de ce type s'affiche :

```
      Set Characteristics of a Volume Group
          Change a Volume Group

* VOLUME GROUP name                                    vgERSTZ0
* Activate volume group AUTOMATICALLY                  no                    +
    at system restart?
* A QUORUM of disks required to keep the volume       yes                   +
   group on-line ?
  Convert this VG to Concurrent Capable?              enhanced concurrent
```

2. Appuyez sur Entrée.

Pour activer la compatibilité avec le mode d'accès simultané optimisé sur le groupe de volumes à partir de la ligne de commande, entrez la commande suivante :

```
# /usr/sbin/chvg -a'n' -Q'y' '-C' <NOM_GROUPE_VOLUMES>
```

Lorsque le groupe de volumes est compatible avec le mode d'accès simultané optimisé, le résultat renvoyé par la commande `lsvg` est semblable à ceci :

```
# lsvg vgERSTZ0
VOLUME GROUP:       vgERSTZ0                 VG IDENTIFIER:
00c31bfe00004c0000000118c2f1ead2
VG STATE:           active                   PP SIZE:        4 megabyte(s)
VG PERMISSION:      read/write               TOTAL PPs:      255 (1020
megabytes)
MAX LVs:            256                      FREE PPs:       14 (56 megabytes)
LVs:                2                        USED PPs:       241 (964 megabytes)
OPEN LVs:           2                        QUORUM:         2 (Enabled)
TOTAL PVs:          1                        VG DESCRIPTORS: 2
STALE PVs:          0                        STALE PPs:      0
ACTIVE PVs:         1                        AUTO ON:        no
Concurrent:         Enhanced-Capable         Auto-Concurrent: Disabled
VG Mode:            Non-Concurrent
MAX PPs per VG:     32512
MAX PPs per PV:     1016                     MAX PVs:        32
LTG size (Dynamic): 256 kilobyte(s)          AUTO SYNC:      no
HOT SPARE:          no                       BB POLICY:      relocatable
```

Procédure d'annulation de la mise à niveau

Procédez comme indiqué dans cette section pour annuler votre installation et revenir à la version précédente.

Pour annuler l'installation et revenir à l'édition précédente de System Automation for Multiplatforms, procédez comme suit :

1. Enregistrez la règle d'automatisation :

   ```
   sampolicy -s file.xml
   ```

2. Mettez hors ligne tous les groupes de ressources. Sinon, si vous ne souhaitez pas impacter les ressources, arrêtez le domaine :

   ```
   stoprpdomain –f nom_domaine
   ```

3. Supprimez également le domaine si vous devez annuler la mise à niveau de RSCT. Sinon, mettez le domaine hors ligne.
4. System Automation for Multiplatforms peut être rétrogradée à l'aide de la commande `./installSAM --forceAll`. La commande installe les livrables System Automation for Multiplatforms et RSCT au même emplacement que celui de `installSAM`, quelle que soit la version déjà installée.
5. Si vous aviez supprimé le domaine, vous pouvez le recréer maintenant. Sinon, démarrez le domaine à l'aide de la commande `startrpdomain -w nom_domaine`.

6. Si le domaine a été recréé, vous pouvez lui appliquer la règle enregistrée à l'aide de la commande `sampolicy -a file.xml`.

Désinstallation

Pour désinstaller System Automation for Multiplatforms dans un environnement AIX ou Linux, suivez la procédure documentée.

Prenez connaissance des remarques suivantes avant de démarrer la procédure de désinstallation :

- Utilisez le script **uninstallSAM** correspondant à votre système d'exploitation pour désinstaller System Automation for Multiplatforms. Pour désinstaller proprement le produit, exécutez par exemple **./uninstallSAM** à partir du répertoire d'installation.
- Avant de procéder à la désinstallation, enregistrez toujours votre configuration à l'aide de la commande **sampolicy -s**. Pour plus d'informations sur l'enregistrement d'une configuration System Automation for Multiplatforms, voir *Tivoli System Automation for Multiplatforms - Guide d'administration et d'utilisation*.

  Description de la commande **sampolicy** dans le manuel *System Automation for Multiplatforms - Guide de référence*.
- La commande **uninstallSAM** supprime toutes les informations de configuration que vous avez définies pour le domaine. Par conséquent, n'utilisez jamais la commande **uninstallSAM** si vous souhaitez procéder à une mise à niveau vers une version plus récente.

Pour désinstaller System Automation for Multiplatforms, procédez comme suit :

1. Vérifiez que le domaine est hors ligne :
   - Pour vérifier si un domaine est en ligne, exécutez la commande :

     ```
     lsrpdomain
     ```
   - Pour arrêter le domaine, exécutez la commande :

     ```
     stoprpdomain <domaine>
     ```
2. Désinstallez le produit à l'aide du script `uninstallSAM` figurant dans le répertoire `/opt/IBM/tsamp/sam/uninst/` :

   ```
   ./uninstallSAM
   ```

   Généralement, vous n'avez pas besoin de spécifier d'options pour la commande `uninstallSAM`. Pour obtenir une description détaillée de la commande, consultez le manuel System Automation for Multiplatforms - Guide de référence.

   Redhat Package Manager s'assure que RSCT et SRC ne sont pas désinstallés avec System Automation for Multiplatforms, si CSM ou GPFS est installé sur le même système Linux. CFM ou GPFS utilisent également les modules RSCT et System Resource Controller (SRC). Les messages Redhat Package Manager indique cette condition.
3. Recherchez des informations sur la désinstallation dans le fichier journal suivant :

   ```
   /tmp/uninstallSAM.<#>.log
   ```

   Le symbole de hachage <#> correspond à un nombre. Le nombre le plus élevé identifie le fichier journal le plus récent.
4. Pour savoir quels packages ont été désinstallés, examinez le fichier `/tmp/uninstallSAM.<#>.log`, où <#> correspond au numéro de fichier journal le plus élevé.

Remarque : La commande `uninstallSAM` supprime également tous les paramètres stockés sous `/etc/opt/IBM/tsamp/sam`.

Installation sur de nouveaux systèmes d'exploitation

Une prise en charge de nouveaux systèmes d'exploitation est possible avec un correctif 4.1.0.<f>, où <f> est le numéro de groupe de correctifs

Une installation de System Automation for Multiplatforms 4.1.0.0 telle qu'elle est décrite dans «Installation de System Automation for Multiplatforms», à la page 24 est possible uniquement sur l'ensemble de plateformes et de systèmes d'exploitation initialement pris en charge avec la présente version 4.1. Néanmoins, la prise en charge de plateformes ou de versions de système d'exploitation supplémentaires peut être ajoutée ultérieurement à l'aide de groupes de correctifs. Cette possibilité est désignée comme "prise en charge de la nouvelle plateforme" dans ce qui suit. Si vous souhaitez installer un groupe de correctifs sur un système d'exploitation déjà pris en charge, effectuez une mise à niveau de l'installation.

Pour savoir quelles sont les nouvelles plateformes prises en charge et par quels groupes de correctifs, voir «Plateformes prises en charge», à la page 5.

Si un groupe de correctifs permet la prise en charge d'un nouveau système d'exploitation, vous devez installer ce groupe de correctifs en tant que première installation et non en tant que mise à niveau. Vous devez donc copier le fichier de licence 4.1 dans le répertoire `SAM410<f>MP<plateforme>/license` avant de commencer l'installation du groupe de correctifs. Procédez comme suit :

1. Procurez-vous un fichier de licence System Automation for Multiplatforms. Il se trouve dans l'un des livrables de la version 4.1 :

   DVD du produit
   Utilisez l'un des DVD répertoriés dans «DVD du produit», à la page 1 pour obtenir la licence. Vous trouverez le fichier de licence nommé `sam41.lic` dans le répertoire `SAM4100MP<plateforme>/license`.

   Distribution électronique
   Utilisez l'un des fichiers archive répertoriés dans «Distribution électronique», à la page 1 pour obtenir la licence. Extrayez le fichier archive. Dans l'arborescence de répertoires étendue, vous trouverez le fichier de licence nommé `sam41.lic` dans le répertoire `SAM4100MP<plateforme>/license`.
2. Extrayez la version 4.1.0. <f> du fichier archive du groupe de correctifs contenant la prise en charge des nouveaux systèmes d'exploitation, comme indiqué dans «Instructions d'utilisation des archives spécifiques aux plateformes», à la page 41. Dans l'arborescence de répertoires étendue, le répertoire `SAM410<f>MP<plateforme>/license` est vide.
3. Copiez le fichier de licence obtenu à l'étape 1 dans le répertoire `SAM410<f>MP<plateforme>/license` de l'arborescence de répertoires étendue du groupe de correctifs.
4. Démarrez l'installation de System Automation for Multiplatforms comme indiqué dans «Exécution de l'installation», à la page 24. Le programme d'installation exécute une installation initiale du produit sur le nouveau système d'exploitation.

Migration depuis SLES 11 vers SLES 12 ou depuis RHEL 6 vers RHEL 7

Vous pouvez procéder à la migration depuis SLES 11 vers SLES 12 ou depuis RHEL 6 vers RHEL 7 avec des clusters System Automation for Multiplatforms existants.

Procédez comme suit pour migrer votre cluster :

1. Sauvegardez la règle avec la commande `sampolicy -s`. Arrêtez les ressources et retirez le domaine.
2. Installez la nouvelle plateforme SLES 12 ou RHEL 7.
3. Installez le package System Automation for Multiplatforms prenant en charge SLES 12 et RHEL 7 : `4.1.0-TIV-SAMP-Linux64-FP000x`. Pour plus d'informations, voir «Installation sur de nouveaux systèmes d'exploitation», à la page 39.
4. Créez le domaine à nouveau et activez la règle : `sampolicy -a`

Remarque :

1. La fonction de migration noeud par noeud permet uniquement de mettre à niveau le niveau de produit System Automation for Multiplatforms et non de mettre à niveau la version du système d'exploitation.
2. Il n'est pas possible d'avoir un domaine comportant des niveaux de système d'exploitation différents, par exemple SLES 11/12 ou RHEL 6/7. Des environnements de langage 32 bits et 64 bits ne peuvent pas être utilisés dans un même domaine.

Installation des groupes de correctifs de service

L'installation du service consiste à appliquer les groupes de correctifs de services à la version 4.1 de System Automation for Multiplatforms ou à mettre à niveau le niveau de version du logiciel depuis la version 4.1. Ces groupes de correctifs de service sont aussi appelés groupes de correctifs de produit.

Des groupes de correctifs sont disponibles pour System Automation for Multiplatforms au format suivant :

Linux Archives au format `.tar` compressé.

AIX Archives au format `.tar` compressé.

Obtention des groupes de correctifs

Pour plus d'informations, reportez-vous à la page du produit System Automation for Multiplatforms.

Les archives des groupes de correctifs de produit peuvent être téléchargées à partir du portail de support System Automation for Multiplatforms. Téléchargez l'archive dans un répertoire temporaire. Généralement, une archive est disponible pour chaque système d'exploitation. Pour plus d'informations sur les conventions de dénomination qui s'appliquent aux archives de groupe de correctifs du produit, voir «Conventions de dénomination des archives».

Conventions de dénomination des archives

Informations supplémentaires sur la syntaxe des noms d'archive.

Les archives des groupes de correctifs de produit de System Automation for Multiplatforms possèdent la syntaxe suivante :

4.1.0-TIV-SAMP-<plateforme>-FP<numéro_groupe_correctifs>.<type_archive> contient le correctif de service de System Automation for Multiplatforms.

Explication :

<plateforme>
Système d'exploitation sur lequel System Automation for Multiplatforms est installé.

<numéro_groupe_correctifs>
Numéro du groupe de correctifs.

<type_archive>
tar.gz ou tar.Z.

Exemple :

Archive tar.Z utilisée pour l'installation du groupe de correctifs 1 de System Automation for Multiplatforms 4.1.0 sur les systèmes d'exploitation AIX :

4.1.0-TIV-SAMP-AIX-FP0001.tar.Z

Instructions d'utilisation des archives spécifiques aux plateformes

Informations supplémentaires sur le téléchargement et l'installation du groupe de correctifs.

Les tableaux contiennent la liste des fichiers archive que vous pouvez télécharger pour appliquer une mise à jour de service sur les systèmes d'exploitation Linux et AIX. i Pour chaque archive, suivez les instructions de la colonne Description.

Linux

Tableau 18. Archive pour les systèmes d'exploitation Linux

Nom de l'archive	Description
4.1.0-TIV-SAMP-Linux-FP<numéro_groupe_correctifs>.tar.gz	Utilisez la commande tar -zxf pour décompresser et extraire l'archive. Lorsque l'archive est extraite, le script d'installation installSAM est stocké dans SAM41<niveau_maintenance>MPLinux/installSAM

Depuis le groupe de correctifs 4.1.0.1, la prise en charge de versions de système d'exploitation supplémentaires a été introduite comme décrit dans «Plateformes prises en charge», à la page 5. Les versions de ces systèmes d'exploitation ne prennent plus en charge le mode de compatibilité 32 bits. Le tableau suivant décrit le fichier archive System Automation for Multiplatforms contenant le livrable du service 64 bits correspondant. Pour plus d'informations, voir «Installation sur de nouveaux systèmes d'exploitation», à la page 39.

Tableau 19. Archive pour les systèmes d'exploitation Linux 64 bits

Nom de l'archive	Description
4.1.0-TIV-SAMP-Linux64-FP<numéro_groupe_correctifs>.tar.gz	Utilisez la commande tar -zxf pour décompresser et extraire l'archive. Lorsque l'archive est extraite, le script d'installation installSAM est stocké dans SAM41<niveau_maintenance>MPLinux64/installSAM

AIX

Tableau 20. Archive pour les systèmes d'exploitation AIX

Nom de l'archive	Description
4.1.0-TIV-SAMP-AIX-FP<numéro_groupe_correctifs>.tar.Z	Utilisez la commande **uncompress** pour décompresser l'archive, puis utilisez la commande tar -xf pour extraire l'archive. Vous trouvez le script d'installation installSAM après avoir extrait l'archive : SAM41<niveau_maintenance>MPAIX/installSAM

Installation du service pour System Automation for Multiplatforms

L'installation du service consiste à effectuer une mise à niveau de System Automation for Multiplatforms à partir de la version 4.1. Par conséquent, la version 4.1 doit avoir été installée pour que vous puissiez appliquer un service.

Avant de commencer :

- Les groupes de correctifs de produit sont toujours cumulatifs.
- Vous devez disposer des droits de l'administrateur root pour installer un groupe de correctifs produit.
- Une fois que vous avez téléchargé les archives depuis le site de support System Automation for Multiplatforms (voir «Obtention des groupes de correctifs», à la page 40), décompressez l'archive du groupe de correctifs de produit dans un répertoire temporaire. Pour plus d'informations sur la manière de décompresser l'archive pour votre système d'exploitation, reportez-vous à la rubrique «Instructions d'utilisation des archives spécifiques aux plateformes», à la page 41.
- Sauvegardez votre configuration système avant d'installer le groupe de correctifs de service. Pour plus d'informations, voir *Tivoli System Automation for Multiplatforms - Guide d'administration et d'utilisation*.
- Pour minimiser les temps d'arrêt, vous pouvez effectuer un contrôle des prérequis avant de commencer l'installation. Pour plus d'informations, voir «Contrôle des prérequis», à la page 3.

Effectuez les étapes suivantes sur chaque noeud du domaine homologue :

1. Vérifiez que toutes les ressources sont en ligne sur le noeud sur lequel vous souhaitez intervenir :
   - Si des ressources sont en ligne et doivent rester disponibles, excluez le noeud de l'automatisation à l'aide de cette commande :
     ```
     samctrl -u a <noeud>
     ```
     System Automation for Multiplatforms arrête les ressources sur le noeud et, si possible, les redémarre sur un autre noeud du domaine homologue.
   - Si les ressources n'ont pas besoin de rester disponibles lors de la maintenance, mettez les groupes de ressources hors ligne.
2. Arrêtez le noeud depuis un autre noeud dans le domaine et vérifiez qu'il est bien arrêté :
   ```
   stoprpnode <noeud>; lsrpnode
   ```
3.

Après avoir reçu les archives, extrayez-les. Cette opération crée une arborescence dans le répertoire principal SAM41mcMP, où mc correspond au niveau de modification et de correction.

4. Installez le groupe de correctifs de service à l'aide du script `installSAM`. Pour des informations détaillées sur le script, reportez-vous à la rubrique «Exécution de l'installation», à la page 24.
5. Démarrez le noeud :
   ```
   startrpnode <noeud>
   ```
6. Si vous avez exclu le noeud au cours de l'étape 2, incluez le noeud dans l'automatisation à l'aide de la commande suivante :
   ```
   samctrl -u d <noeud>
   ```
7. Si les groupes de ressources doivent être en ligne, mettez les groupes de ressources sur en ligne. Sinon, vous pouvez exécuter cette étape après être intervenu sur le dernier noeud du domaine homologue.
8. Lorsque vous êtes intervenu sur tous les noeuds, exécutez les étapes décrites dans «Exécution de la migration», à la page 29. Les modifications deviennent effectives dans tout le domaine et la version correcte est affichée.

Désinstallation du service

Pour désinstaller un groupe de correctifs, vous devez désinstaller l'intégralité du produit.

Pour désinstaller System Automation for Multiplatforms, suivez la procédure décrite dans «Désinstallation», à la page 38.

Une fois que la désinstallation est terminée, vous pouvez réinstaller System Automation for Multiplatforms et le niveau de service requis (niveau de groupe de correctifs).

Installation de la fonction xDR de reprise après incident étendue

De nos jours, les marchés et les entreprises dépendent des solutions de reprise sur incident afin de récupérer des données vitales. Pour résoudre ce problème, System Automation for Multiplatforms prend en charge GDPS/PPRC Multiplatform Resiliency on System z (xDR).

Geographically Dispersed Parallel Sysplex (GDPS) est une solution de mise à disposition des applications et de reprise sur incident, très personnalisée qui fonctionne avec votre environnement z/OS. Elle permet d'effectuer une reprise sur incident et de défaillance à partir d'un point de contrôle unique et d'assurer la cohérence des données. Pour plus d'informations sur GDPS, voir le document IBM Redbooks *GDPS Family - An Introduction to Concepts and Capabilities*, qui peut être téléchargé à l'adresse IBM Redbooks.

System Automation for Multiplatforms étend GDPS/PPRC pour les systèmes Linux qui s'exécutent sur System z. Il fournit une solution coordonnée de reprise sur incident, exécutée sur

- zSeries, y compris z/OS
- Linux on System z sous z/VM

- Linux on System z s'exécutant en mode natif dans la partition logique

Conditionnement xDR

Le code de la fonction xDR est fourni avec le produit System Automation for Multiplatforms. Vous ne pouvez pas utiliser la fonction correspondante, sauf si vous avez installé une licence distincte permettant l'activation du code.

La licence vous est fournie lorsque vous commandez la fonction xDR. Le nom du fichier de licence est `sam41XDR.lic` :

DVD Installez la fonction xDR à partir du DVD System Automation for Multiplatforms v4.1 – xDR for Linux on System z. Le fichier de licence se trouve dans le répertoire `SAM4100FeatXDR/license`.

Distribution électronique
Si vous avez obtenu la fonction xDR par voie électronique, le fichier de licence se trouve dans le fichier de distribution électronique `CIVG7ML.txt`. Ce fichier est identique au fichier de licence. Renommez le fichier de distribution électronique ou copiez-le et renommez la copie `sam41XDR.lic`.

Prérequis pour xDR

Pour installer la licence de la fonction xDR, vous devez installer le produit de base System Automation for Multiplatforms.

xDR est prise en charge uniquement sous Linux on System z.

Les distributions Linux suivantes sont prises en charge pour xDR :

- xDR for Linux on System z sous z/VM nécessite l'un des systèmes d'exploitation suivants :
  - SUSE SLES 10 (64 bits)
  - SUSE SLES 11 (64 bits)
  - SUSE SLES 12 (64 bits)
  - Red Hat RHEL 5 (64 bits)
  - Red Hat RHEL 6 (64 bits)
  - Red Hat RHEL 7 (64 bits)
- xDR for Linux on System z s'exécutant en mode natif dans une partition logique utilisant des disques ECKD requiert l'un des systèmes d'exploitation suivants :
  - SUSE SLES 10 SP4
  - SUSE SLES 11 SP1
  - SUSE SLES 11 SP2
  - SUSE SLES 11 SP3 avec la dernière mise à jour Maintweb. La version de Kernel doit être 3.0.101-0.40 ou une version ultérieure ; la version des outils multi-accès doit être 0.4.9-0.95.1 ou une version ultérieure.

Remarque :

1. Si vous souhaitez utiliser la fonctionnalité xDR, des versions particulières de z/VM, Linux on System z, GDPS et System Automation for Multiplatforms doivent être installées. Pour plus d'informations sur la fonctionnalité disponible et les versions nécessaires, reportez-vous aux manuels GDPS. System Automation for Multiplatforms s'exécute uniquement sur Linux sous System z.
2. Les conventions de nommage xDR nécessitent que le nom des clusters et des noeuds ne dépasse pas 32 caractères. Les noms de cluster et de noeud ne doivent pas contenir de points (.) ou des tirets (-) et ne doivent pas être identiques. Pour xDR, les noms de clusters ne dépendent pas des

minuscules/majuscules. Pour utiliser xDR, System Automation for Multiplatforms doit être personnalisé selon les indications des manuels GDPS.

3. L'anglais est la seule langue prise en charge par xDR et GDPS.

Installation de la licence de la fonction xDR

Utilisez la commande **samlicm** pour installer la licence.

Le fichier de licence doit être accessible depuis le système sur lequel System Automation for Multiplatforms est installé. Copiez le fichier `sam41XDR.lic` à un emplacement d'où il sera accessible lors du démarrage de **samlicm**.

Installez la licence :

```
samlicm -i  <emplacement du fichier de licence>/sam41XDR.lic
```

Vérifiez que la licence de la fonction est correctement installée :

```
samlicm -s
```

Le nom de la fonction xDR doit apparaître comme valeur de la zone `Product Annotation` dans le résultat de la commande. Par exemple :

```
...
Product ID: 101
Product Annotation: SA for MP xDR for Linux on System z
...
```

Pour plus d'informations sur la commande **samlicm**, reportez-vous au manuel *System Automation for Multiplatforms - Guide de référence*.

Mise à niveau de la fonction xDR depuis une version antérieure à 4.1

A compter de la version 4.1, la licence de la fonction xDR est installée dans un répertoire cible différent.

Si vous effectuez une mise à niveau de la fonction xDR depuis une version antérieure à 4.1, la licence installée auparavant est supprimée. Installez à nouveau la licence de la fonction comme décrit dans «Installation de la licence de la fonction xDR». Vous pouvez utiliser soit le fichier de licence de la version de System Automation for Multiplatforms dont vous avez mis à niveau le code produit, soit celui de la version vers laquelle vous avez effectué la mise à niveau.

A partir de la version 4.1, xDR for Linux on System z s'exécutant sous z/VM autorise uniquement que le stockage de tous les noeuds proxy soit verrouillé de manière permanente. Les clients qui utilisent actuellement un cluster de serveurs proxy à deux noeuds avec l'option de verrouillage du stockage pour le proxy maître doivent effectuer une migration en exécutant le script `enableErpd`. Pour verrouiller le stockage, ajoutez la commande `LOCK` au fichier `boot.local` ou `rc.local` des deux noeuds proxy. Pour plus d'informations, voir les manuels GDPS.

Désinstallation de la fonction xDR

Il n'existe pas de procédure de désinstallation propre à la fonction xDR. Cette fonction est désinstallée de manière implicite lors de la désinstallation de System Automation for Multiplatforms.

Installation de la règle de haute disponibilité SAP

La fonction de règle de haute disponibilité SAP Central Services est fournie dans le cadre de System Automation for Multiplatforms mais requiert une licence distincte.

La fonction de règle de haute disponibilité SAP est fournie dans le cadre de System Automation for Multiplatforms mais requiert une licence distincte.

Pour plus d'informations sur l'installation de la fonction de règle de haute disponibilité SAP, voir le document System Automation for MultiplatformsGuide des règles de haute disponibilité.

Chapitre 3. Configuration

Une fois que vous avez correctement installé System Automation for Multiplatforms, traitez les tâches de configuration qui dépendent des composants et des fonctions de System Automation for Multiplatforms dont vous avez besoin.

Remarque : Vous devez disposer d'un serveur X11 pour utiliser la boîte de dialogue de configuration de l'adaptateur d'automatisation. Pour pouvoir utiliser la boîte de dialogue de configuration, vous devez disposer de la version 32-bit bits des modules d'installation X11. Sur certains systèmes d'exploitation Linux, ces modules figurent sur les supports d'installation, mais ne font pas partie de l'installation standard. Assurez-vous que la version 32 bits des modules d'installation X11 a été installée.

Vous pouvez également configurer l'adaptateur d'automatisation en mode silencieux à l'aide d'un fichier d'entrée de propriétés. Si aucun serveur X11 n'est disponible, la configuration en mode silencieux est la seule méthode prise en charge sur ce système. Pour plus d'informations, voir «Configuration en mode silencieux», à la page 88.

Configuration du comportement de l'adaptateur d'automatisation de bout en bout

Vous pouvez gérer et contrôler System Automation for Multiplatforms en modifiant un ensemble d'attributs qui affectent le comportement du produit.

Vous pouvez lancer ou arrêter la fonction d'automatisation, définir des expirations ou exclure des noeuds de l'automatisation, par exemple, pour des raisons de maintenance.

Vous pouvez modifier les attributs suivants :

TimeOut
: Indique la valeur du délai d'attente en secondes pour une opération de contrôle de démarrage exécuté par System Automation for Multiplatforms. Lorsque le délai d'attente expire, l'opération est répétée si le nombre de tentatives autorisé (RetryCount) n'est pas dépassé.

RetryCount
: Nombre de fois qu'une opération de contrôle peut être retentée si elle échoue ou arrive à expiration.

Automatisation
: Indicateur qui active ou désactive l'automatisation par System Automation for Multiplatforms.

ExcludedNodes
: Liste de noeuds sur lesquels System Automation for Multiplatforms exclut de manière active les ressources ou les arrête. Peut être utilisé à des fins de maintenance, par exemple.

ResourceRestartTimeOut
: Délai en secondes au cours duquel System Automation for Multiplatforms attend avant de redémarrer les ressources qui étaient situées sur un noeud défectueux dans un autre noeud.

TraceLevel
Le niveau de trace peut être utilisé pour contrôler le nombre d'entrées de trace écrites. La valeur maximale est de 255 résultats pour la trace détaillée et la valeur 0 supprime l'écriture des différentes classes d'entrées de trace. La réduction du niveau de trace est recommandée pour les règles d'automatisation avec un grand nombre de ressources.

Vous pouvez répertorier les valeurs en cours des attributs à l'aide de la commande **lssamctrl**. Les attributs sont modifiés à l'aide de la commande **samctrl**. Pour plus d'informations, voir le document *IBM Tivoli System Automation for Multiplatforms - Guide de référence* dans lequel vous trouverez la liste et la description de ces commandes.

TimeOut et RetryCount

L'attribut `TimeOut` est toujours utilisé en association avec l'attribut `RetryCount` :

TimeOut
Indique le délai d'attente au cours duquel System Automation for Multiplatforms attend que le gestionnaire de ressources entreprenne une action.

RetryCount
Indique le nombre de tentatives d'opérations de contrôle possibles que System Automation for Multiplatforms effectuera au cours du délai de `TimeOut` si l'opération de contrôle échoue. En général, si la première tentative échoue, les chances que l'opération aboutisse à la seconde tentative ou aux suivantes sont relativement faibles.

Opérations de démarrage

Le temporisateur des opérations est lancé lorsque System Automation for Multiplatforms envoie la première opération de contrôle de démarrage pour une ressource. Une fois qu'il est lancé, il existe plusieurs possibilités :

1. La ressource est modifiée avec l'état souhaité (en ligne ou hors ligne) au cours du délai d'attente. Dans ce cas, aucune autre action n'est déclenchée car la ressource possède l'état que System Automation for Multiplatforms lui a affecté.
2. La ressource rejette le contrôle de démarrage au cours du délai d'attente. Ce qui se produit ensuite dépend du code de refus :
   - Si ce code indique que l'erreur est remédiable, System Automation for Multiplatforms continue de lancer des opérations de contrôle de démarrage sur la ressource. Chaque tentative d'opération de contrôle est comptée. Lorsque la valeur de RetryCount est dépassée, System Automation for Multiplatforms arrête de lancer d'autres opérations de contrôle.
   - Si l'erreur n'est pas remédiable, la ressource entrera dans un état de défectuosité. Que cet incident déclenche ou non d'autres actions d'automatisation dépend du type de ressource sur laquelle l'opération de démarrage a été lancée :
     – Si une ressource fixe est affectée, aucune autre action n'est déclenchée.
     – Si l'opération de contrôle a été lancée sur la constituante d'une ressource flottante et cette constituante a l'état Hors ligne ou Echec hors ligne, System Automation for Multiplatforms tentera de lancer les opérations de contrôle sur une autre constituante de la ressource. Notez que la constituante ayant rejeté l'opération de contrôle restera dans un état d'erreur irrémédiable tant que vous n'aurez pas lancé une opération de réinitialisation sur elle.

3. La ressource n'atteint pas l'état souhaité (en ligne) à la fin du délai d'attente. Dans ce cas, System Automation for Multiplatforms émet tout d'abord une opération de réinitialisation sur la ressource et attend jusqu'à ce que l'opération de réinitialisation ait été acceptée et que la ressource ait été mise en ligne. Ensuite, System Automation for Multiplatforms émet une autre opération de contrôle de démarrage sur la ressource. Chaque tentative d'opération de contrôle est comptabilisée et System Automation for Multiplatforms arrête d'émettre des opérations de contrôle lorsque le nombre de tentatives autorisées (RetryCount) est dépassé ou que le délai d'attente maximal (TimeOut * RetryCount) expire, quel que soit le premier des deux cas de figure qui se produit en premier.

Si System Automation for Multiplatforms arrête d'émettre des opérations de contrôle pour une ressource fixe ou un composant de la ressource flottante, l'état opérationnel de cette ressource est défini sur Echec hors ligne. Cela indique que la ressource ne peut plus être utilisée et qu'un intervention manuelle est nécessaire pour corriger la cause de l'échec. Une fois le problème résolu, la ressource doit être réinitialisée à l'aide de la commande RMC **resetrsrc**.

Le compteur de tentatives est réinitialisé lorsque les ressources atteignent l'état souhaité car aucun seuil n'a été mis en oeuvre. Cela signifie, par exemple, que si une ressource est lancée, reste en ligne pendant une courte période, puis s'arrête, elle est relancée par System Automation for Multiplatforms dans une boucle.

Les valeurs par défaut sont les suivantes :

- TimeOut = 60
- RetryCount = 3

Vous pouvez utiliser la commande **samctrl –t Timeout** pour modifier la valeur du délai d'expiration et la commande **samctrl –r Retry_count** pour modifier la valeur du nombre de tentatives.

La classe `IBM.Application` fournit sa propre valeur de délai d'expiration. Si vous ajoutez une ressource de classe `IBM.Application` à un groupe, la valeur générale du délai d'expiration `TimeOut` n'est pas utilisée pour cette ressource. La valeur du délai d'expiration `TimeOut` utilisé pour ce membre du groupe est la valeur la plus grande de l'attribut `StartCommandTimeout` ou `MonitorCommandPeriod` (qui sont des attributs de la ressource `IBM.Application`.

Opérations d'arrêt

Le temporisateur des opérations est lancé lorsque System Automation for Multiplatforms envoie, pour la première fois, une opération de contrôle d'arrêt de ressource à une ressource. Une fois qu'il est lancé, il existe plusieurs possibilités :

1. La ressource change et prend l'état souhaité (hors ligne) au cours de la période d'expiration. Aucune autre action n'est déclenchée.
2. La ressource refuse le contrôle d'arrêt au cours de la période d'expiration. Ce qui se produit ensuite dépend du code de refus :
   - Si le code indique que l'erreur peut être récupérée, System Automation for Multiplatforms émet une autre opération de contrôle d'arrêt pour la ressource.
   - Si l'erreur ne peut pas être récupérée, la ressource se trouve dans un état d'erreur. Une intervention manuelle est nécessaire pour que la ressource ne soit plus dans l'état d'erreur.

3. La ressource n'atteint pas l'état souhaité (hors ligne) au cours de la période d'expiration. Dans ce cas, System Automation for Multiplatforms émet d'abord une opération de réinitialisation pour la ressource et attend que la ressource atteigne l'état souhaité (hors ligne).

Automatisation

Cet indicateur indique si la fonction d'automatisation d'System Automation for Multiplatforms est activée ou non. Si l'automatisation est désactivée, System Automation for Multiplatforms arrête les opérations de contrôle d'arrêt. L'état des ressources restera inchangé.

La valeur par défaut est le mode AUTO qui indique que l'automatisation est activée.

Utilisez la commande **samctrl –M F** pour activer l'automatisation et la commande **samctrl –M T** pour la désactiver.

ExcludedNodes

Liste des noeuds dans laquelle System Automation for Multiplatforms arrête toutes les ressources et les déplace dans un autre noeud, si cette opération est possible.

Prenons par exemple, une ressource flottante A qui peut fonctionner sur quatre noeuds : node05, node06, node07 et node08. Il s'agit d'un membre du groupe de ressources RG_A. Lorsque le groupe est en ligne, il est démarré sur le noeud node05. Si vous ajoutez le noeud node05 dans la liste des noeuds exclus, System Automation for Multiplatforms arrête la ressource sur le noeud node05. Les ressources sont ensuite redémarrées sur l'un des autres noeuds.

Avertissement : si vous excluez un noeud, il se peut qu'un ou plusieurs membres obligatoires du groupe ne puissent être redémarrés dans un autre noeud et que le groupe entier soit arrêté.

Par défaut, la liste est vide, ce qui signifie que tous les noeuds situés dans le domaine homologue peuvent être utilisés.

Utilisez **samctrl -u a** pour ajouter un ou plusieurs noeuds indiqués à la liste des noeuds exclus. **samctrl -u d** supprime les noeuds de la liste. **samctrl -u r** remplace les noeuds dans la liste.

ResourceRestartTimeout

La valeur `ResourceRestartTimeout` indique le délai d'attente en secondes d'System Automation for Multiplatforms avant de redémarrer les ressources situées dans un noeud ayant échoué sur un autre noeud. Les ressources ou le noeud défectueux peuvent effectuer un nettoyage avant de déplacer les ressources vers un autre système.

La durée par défaut est 5 secondes.

Vous indiquez la valeur de délai d'attente de redémarrage des ressources à l'aide de la commande **samctrl –o**.

Vous pouvez indiquer le niveau de trace à l'aide de la commande **samctrl -l** . Le niveau de trace (TraceLevel) détermine le nombre d'entrées de trace écrites. La valeur par défaut est 127. La valeur maximale est de 255 résultats pour une trace

détaillée. Si la valeur est sur 0, les différentes classes d'entrées de trace ne sont pas écrites. La réduction du niveau de trace est recommandée pour les règles d'automatisation ayant un grand nombre de ressources.

Exemples

Pour répertorier les paramètres de contrôle courants d'System Automation for Multiplatforms, utilisez la commande **lssamctrl**.

Informations de contrôle System Automation for Multiplatforms :

```
SAMControl:
    TimeOut                = 60
    RetryCount = 3
    Automation             = Auto
    ExcludedNodes          = {}
    ResourceRestartTimeOut = 5
    ActiveVersion      = [4.1.0.0,Thu Sept 27 11:10:58 METDST 2012]
    EnablePublisher     = XDR_GDP2 XDR_GDP1
    TraceLevel = 31
    ActivePolicy           = []
    CleanupList            = {}
    PublisherList          = {}
```

Pour ajouter le noeud node05 à la liste des noeuds exclus, entrez cette commande :

```
samctrl -u a node05
```

Pour définir le paramètre `RetryCount` sur 5, entrez :

```
samctrl –r 5
```

Configuration de la condition de départage

Configurez une condition de départage pour les environnements en cluster avec un nombre de noeuds pair.

Pour que System Automation for Multiplatforms commence les opérations d'automatisation, la majorité des noeuds du domaine doivent être en ligne. Si le domaine comprend un nombre pair de noeuds, il est possible que précisément la moitié des noeuds du domaine soient en ligne. Si tel est le cas, System Automation utilise une condition de départage pour déterminer l'état du quorum, lequel détermine quelles actions peuvent être démarrées (**HAS_QUORUM**), ou si aucune action d'automatisation n'est possible (**PENDING_QUORUM, NO_QUORUM**).

Configurez une condition de départage de disque partagé tel que ECKD ou SCSI avec la classe de ressource **IBM.TieBreaker**. De plus, deux autres conditions de départage sont prédéfinies, operator et fail. La condition de départage de type Operator donne un résultat indéterminé lorsqu'une situation de parité se produit. Il incombe à l'administrateur de résoudre cette situation de parité en autorisant ou en refusant le quorum opérationnel. Lorsqu'une situation de parité se produit et qu'une situation de départage du type "Fail" est active, la tentative de réservation de la condition de départage est toujours refusée. Le type de départage par défaut est défini sur Operator.

D'autres implémentations d'une condition de départage peuvent être ajoutées à l'aide du type de condition de départage **EXEC**. System Automation for Multiplatforms fournit deux autres implémentations de conditions de départage : réseau et NFS.

Liste le type de condition de départage disponible :

```
lsrsrc -c IBM.TieBreaker
```

Sortie :

```
Attributs persistants d'une classe de ressources pour : IBM.TieBreaker
        resource 1:
                  AvailableTypes ={["SCSI",""],["EXEC",""],["Operator",""],["Fail",""]}
```

Liste le nom de la condition de départage :

```
lsrsrc IBM.TieBreaker
```

Sortie :

```
Attributs persistants de ressource pour : IBM.TieBreaker
        resource 1:
            Name                = "FAIL"
            Type                = "FAIL"
            DeviceInfo          = ""
            ReprobeData         = ""
            ReleaseRetryPeriod  = 0
            HeartbeatPeriod     = 0
            PreReserveWaitTime  = 0
            PostReserveWaitTime = 0
            NodeInfo            = {}

        resource 2:
            Name                = "Operator"
            Type                = "Operator"
            DeviceInfo          = ""
            ReprobeData         = ""
            ReleaseRetryPeriod  = 0
            HeartbeatPeriod     = 0
            PreReserveWaitTime  = 0
            PostReserveWaitTime = 0
            NodeInfo            = {}

resource 3:
           Name                = "myTieBreaker"
           Type                = "SCSI"
           DeviceInfo          = "ID=0 LUN=0 CHAN=0 HOST=2"
           ReprobeData         = ""
           ReleaseRetryPeriod  = 0
           HeartbeatPeriod     = 5
           PreReserveWaitTime  = 0
           PostReserveWaitTime = 0
           NodeInfo            = {}

ressource 4:
           Name                = "mytb"
           Type                = "EXEC"
           DeviceInfo          = "PATHNAME=/usr/sbin/rsct/bin/samtb_net
                                          Address=192.168.177.2"
           ReprobeData         = ""
           ReleaseRetryPeriod  = 0
           HeartbeatPeriod     = 30
           PreReserveWaitTime  = 0
           PostReserveWaitTime = 30
           NodeInfo            = {}
           ActivePeerDomain    = "21"
```

Bien que vous puissiez définir plusieurs ressources de condition de départage dans la classe de ressources IBM.TieBreaker, seule l'une de ces conditions peut être active au sein du cluster en même temps. Exécutez la commande suivante pour répertorier la condition de départage qui est actuellement active dans le cluster :

```
lsrsrc -c IBM.PeerNode OpQuorumTieBreaker
```

Sortie :

```
Attributs persistants de la classe de ressources pour : IBM.PeerNode
        resource 1:
          OpQuorumTieBreaker = "Operator"
```

Définissez la condition de départage active :

```
chrsrc -c IBM.PeerNode OpQuorumTieBreaker="Operator"
```

Entrez la commande suivante pour accorder ou refuser le quorum opérationnel lorsque la condition de départage est Operator :

```
runact -c IBM.PeerDomain ResolveOpQuorumTie Ownership=1 (0 pour refuser)
```

Remarque : Pour éviter les conditions d'indétermination, la condition de départage Operator doit être refusée pour le sous-cluster perdant. Ensuite, la condition de départage Operator peut être accordée au sous-cluster, qui est censé continuer.

Condition de départage de disque partagé

Configurez une condition de départage dans un cluster possédant un nombre pair de noeuds. Le disque sur lequel s'applique la condition de départage est partagé entre tous les noeuds du cluster.

Un disque peut être utilisé comme ressource de condition de départage à l'ai de la classe de ressource `IBM.TieBreaker`. Lorsque seulement la moitié des noeuds d'un sous-domaine sont en ligne, System Automation for Multiplatforms tente de réserver la condition de départage à l'aide de la fonction or réservation/libération. Si la réservation réussit, le sous-domaine obtient le quorum, et System Automation for Multiplatforms peut continuer à automatiser des ressources. La réservation du disque est libérée lorsqu'un autre noeud rejoint le domaine, de sorte que plus de la moitié des noeuds sont en ligne dans ce domaine.

Remarque : Lorsque vous définissez la condition de départage, vérifiez que la disque indiqué pour la ressource `IBM.TieBreaker` n'est pas aussi utilisé pour stocker des systèmes de fichiers.

Les trois exemples suivants montrent comment utiliser une condition de départage avec un périphérique ECKD, SCSI ou DISK. La condition de départage n'a pas besoin d'être formatée ou partitionnée.

Configuration d'une condition de départage ECKD pour un cluster à deux nœuds

Configurez une condition de départage ECKD sur Linux on System z.

Si les noeuds s'exécutent sous z/VM, voir «Condition de départage ECKD dans les environnements z/VM», à la page 64 pour en savoir plus sur les implications en termes de configuration de la définition d'une unité de stockage à accès direct ECKD en tant que condition de départage.

Le type de condition de départage s'appliquant à ECKD est spécifique à Linux sur System z. Si vous souhaitez créer un objet condition de départage ECKD, vous devez configurer l'attribut persistant de ressource `DeviceInfo` pour indiquer le numéro du périphérique ECKD. Ce type de condition de départage utilise un mécanisme de réservation/libération et doit être réservé de nouveau périodiquement pour mettre la réservation en suspens. Pour cette raison, vous

pouvez aussi indiquer l'attribut persistant de ressource HeartbeatPeriod lors de la création d'une condition de départage de ce type. Cet attribut définit l'intervalle d'émission de la demande de réservation.

Collectez les informations système suivantes(Linux noyau v2.4) :

```
node01:~ # cat /proc/subchannels
Device sch. Dev Type/Model CU in use PIM PAM POM CHPIDs
------------------------------------------------------------------------
50DE 0A6F 3390/0A 3990/E9 F0 A0 FF 7475E6E7 FFFFFFFF
```

```
node01:~ # cat /proc/dasd/devices
50dc(ECKD) at ( 94:  0) is            : active at blocksize: 4096, 601020 blocks, 2347 MB
50dd(ECKD) at ( 94:  4) is            : active at blocksize: 4096, 601020 blocks, 2347 MB
50de(ECKD) at ( 94:  8) is            : active at blocksize: 4096, 601020 blocks, 2347 MB
50df(ECKD) at ( 94: 12) is            : active at blocksize: 4096, 601020 blocks, 2347 MB
```

Pour le noyau Linux v2.6, utilisez la commande **lscss** au lieu de la commande cat /proc/subchannels. Procédez comme suit afin d'utiliser la condition de départage :

1. Créez un objet de ressource à départager dans IBM.TieBreaker class. DeviceInfo indique le numéro du périphérique ECKD. Vous pouvez l'obtenir dans le fichier /proc/dasd/devices.

```
node01:~ # mkrsrc IBM.TieBreaker Name=myTieBreaker \
   Type=ECKD DeviceInfo="ID=50de" HeartbeatPeriod=5
```

```
node01:~ # lsrsrc IBM.TieBreaker
Attributs persistants de ressource pour : IBM.TieBreaker
resource 1:
        Name                = "Operator"
        Type                = "Operator"
        DeviceInfo          = ""
        ReprobeData         = ""
        ReleaseRetryPeriod  = 0
        HeartbeatPeriod     = 0
        PreReserveWaitTime  = 0
        PostReserveWaitTime = 0
        NodeInfo            = {}
resource 2:
        Name                = "Fail"
        Type                = "Fail"
        DeviceInfo          = ""
        ReprobeData         = ""
        ReleaseRetryPeriod  = 0
        HeartbeatPeriod     = 0
        PreReserveWaitTime  = 0
        PostReserveWaitTime = 0
        NodeInfo            = {}
resource 3:
        Name                = "myTieBreaker"
        Type                = "ECKD"
        DeviceInfo          = "ID=50de"
        ReprobeData         = ""
        ReleaseRetryPeriod  = 0
        HeartbeatPeriod     = 5
        PreReserveWaitTime  = 0
        PostReserveWaitTime = 0
        NodeInfo            = {}
```

2. Remplacez l'attribut OpQuorumTieBreaker dans IBM.PeerNode par l'un des objets de ressource à départager.

```
node01:~ # chrsrc -c IBM.PeerNode OpQuorumTieBreaker="myTieBreaker"
```

```
node01:~ # lsrsrc -c IBM.PeerNode
Attributs persistants de la classe de ressources pour : IBM.PeerNode
resource 1:
        CommittedRSCTVersion  = ""
        ActiveVersionChanging = 0
```

```
OpQuorumOverride      = 0
CritRsrcProtMethod    = 1
OpQuorumTieBreaker    = "myTieBreaker"
```

Redémarrage manuel d'un noeud

Si un noeud d'un cluster à deux noeuds est réinitialisé, le noeud de réinitialisation peut revenir rapidement. Cette opération risque de perturber la méthode de départage et entraîner une réinitialisation intempestive du noeud restant. Si un noeud appartenant à un cluster doit être réinitialisé manuellement, utilisez la commande **halt -nf** au lieu de **reboot -nf**.

Interruption manuelle d'une réservation de disque

Si le nœud réservant une condition de départage est hors service ou ne peut être réinitialisé, vous devez accéder manuellement à un nœud fonctionnant correctement pour interrompre la réservation et la basculer sur ce nœud.

- Le disque de départage peut être soit encore rattaché au noeud fonctionnant correctement, à condition que ce noeud n'ait pas été réinitialisé dans l'intervalle :

  ```
  node01:~ # cat /proc/subchannels
  Device sch. Dev Type/Model CU in use PIM PAM POM CHPIDs
  ------------------------------------------------------------
  50DE 0A6F 3390/0A 3990/E9 F0 A0 FF 7475E6E7 FFFFFFFF

  node01:~ # cat /proc/dasd/devices
  50de(ECKD) at ( 94: 8) is dasdc: active at blocksize: 4096,601020 blocks, 2347 MB
  ```

- Le disque de la condition de départage peut être réinitialisé si ce noeud est réinitialisé et ne peut plus reconnaître le disque de départage :

  ```
  node01:~ # cat /proc/subchannels
  Device sch. Dev Type/Model CU in use PIM PAM POM CHPIDs
  ------------------------------------------------------------
  50DE   0A6F            FFFF/00          F0  A0  FF  7475E6E7 FFFFFFFF

  node01:~ # cat /proc/dasd/devices
  50de(ECKD) at ( 94: 8) is dasdc : boxed
  ```

  Pour rompre la réservation au niveau du disque à départager, entrez la commande `/usr/sbin/rsct/bin/tb_break`:

  ```
  tb_break -t ECKD /dev/dasdc
  ```

  Le disque de départage est maintenant réservé par le noeud en bon état de fonctionnement.

Remarque : Si la commande **tb_brk** ne fonctionne pas la première fois, exécutez-la de nouveau.

Configuration d'une condition de départage SCSI pour un cluster à deux nœuds

Configurez une condition de départage SCSI sur Linux on System x ou Linux on POWER.

Le type de condition de départage SCSI est spécifique à Linux sur System x et Linux on POWER. Si vous souhaitez créer un objet SCSI à départager, vous devez définir le périphérique SCSI à l'aide de l'attribut de ressource persistant `DeviceInfo`. Si la configuration SCSI diffère selon les noeuds du cluster, vous

pouvez également utiliser l'attribut de ressource persistant NodeInfo pour refléter ces différences. Ce type de condition de départage utilise un mécanisme de réservation/libération et devra être réservé périodiquement pour maintenir la réservation. Lorsque vous créez une condition de départage de ce type, vous pouvez également définir l'attribut de ressource persistant HeartbeatPeriod. Cet attribut définit l'intervalle d'émission de la demande de réservation.

Sous Linux, les unités peuvent être identifiées par les quatre valeurs entières des attributs HOST, CHAN, ID et LUN :

```
node1:~# dmesg | grep "Attached scsi disk"
```

Généralement, ces paramètres sont identiques sur chaque noeud du cluster. Par exemple, pour les noeuds 1 et 2, on obtient HOST=0 CHAN=0 ID=4 LUN=0.

Dans ce cas, utilisez la commande suivante pour créer l'objet de la condition de départage :

```
mkrsrc IBM.TieBreaker Name=myTieBreaker Type=SCSI DeviceInfo=" HOST=0 CHAN=0 ID=4 LUN=0"
```

Ces quatre valeurs peuvent aussi être différentes sur les noeuds (même si le périphérique cible est le même). Dans ce cas, utilisez la zone NodeInfo en plus de la zone DeviceInfo.

Utilisez les quatre valeurs entières issues du résultat de la commande :

```
# dmesg | grep "Attached scsi disk"
Attached scsi disk sdf at scsi2, channel 2, id 4, lun 0
```

Pour le disque sdf, les valeurs de l'attribut de l'identificateur SCSI sont HOST=2, CHAN=2, ID=4, LUN=0. Par exemple, un périphérique SCSI est connecté à deux noeuds appelés node1 et node2 et comporte les identificateurs SCSI suivants :

```
node1:  HOST=0 CHAN=0 ID=4 LUN=0
node2:  HOST=2 CHAN=2 ID=4 LUN=0
```

Créez l'objet de la condition de départage en utilisant DeviceInfo pour spécifier des valeurs d'attribut communes et NodeInfo pour spécifier des valeurs d'attribut spécifiques au noeud :

```
# mkrsrc IBM.TieBreaker Name=scsi Type=SCSI DeviceInfo="ID=4 LUN=0"
NodeInfo='{["node1", "HOST=0 CHAN=0"], ["node2", "HOST=2 CHAN=2"]}'
```

System Automation for Multiplatforms traite DeviceInfo et NodeInfo de telle manière qu'il fusionne les deux chaînes, en commençant par DeviceInfo puis NodeInfo. Par exemple, pour le noeud "node1", la chaîne fusionnée est

```
"ID=4 LUN=0 HOST=0 CHAN=0"
```

Cette chaîne est ensuite analysée.

Tous les mots clés en double sont autorisés et le dernier est utilisé. Par conséquent, la même commande peut être indiquée en tant que

```
# mkrsrc IBM.TieBreaker Name=myTieBreaker Type=SCSI DeviceInfo="ID=4 LUN=0
HOST=0,CHAN=0"  NodeInfo='{["node2", "HOST=2 CHAN=2"]}'
```

Cette simplification peut être utile puisque l'ID SCSI est le même pour la plupart des noeuds.

Interruption manuelle d'une réservation de disque

Si le nœud réservant une condition de départage est hors service ou ne peut être réinitialisé, vous devez accéder manuellement à un nœud fonctionnant correctement pour libérer le disque SCSI à départager. Pour libérer un disque, exécutez la commande **tb_break [–f] HOST CHAN ID LUN**, par exemple

```
/usr/sbin/rsct/bin/tb_break –f HOST=0 CHAN=0 ID=4 LUN=0
```

Configuration d'une condition de départage DISK AIX pour un cluster à deux nœuds

Configurez un départage AIX DISK sur les systèmes AIX.

Le type de départage de DISK s'applique à AIX. Si vous souhaitez créer un objet condition de départage DISK, vous devez définir un attribut persistant `DeviceInfo` pour indiquer le nom de l'unité sous AIX. Le nom de l'unité sous AIX doit indiquer un disque SCSI ou un disque physique de type SCSI partagé par tous les nœuds dans le domaine homologue.

Les disques physiques rattachés via Fibre Channel, iSCSI, et Serial Storage Architecture peuvent servir de condition de départage de DISK. Toutefois, les disques durs IDE ne prennent pas en charge le protocole SCSI, en conséquence ils ne peuvent être départagés. Les volumes logiques ne peuvent pas non plus servir de départage DISK. Ce type de condition de départage utilise un mécanisme de réservation/libération et doit être réservé de nouveau périodiquement pour mettre la réservation en suspens. C'est pour cette raison que nous vous recommandons fortement d'indiquer l'attribut persistant de ressource `HeartbeatPeriod` lors de la création d'une condition de départage de ce type. Cet attribut définit l'intervalle d'émission de la demande de réservation.

Pour imprimer tous les volumes physiques connus présents dans le système ainsi que le nom du disque physique de chaque volume, entrez la commande suivante :

```
lspv
```

Un résultat similaire au résultat suivant s'affiche :

```
hdisk0 000000371e5766b8 rootvg active
hdisk1 000069683404ed54 None
```

Utilisez la commande **lsdev** afin de vérifier qu'il s'agit d'un disque SCSI ou de type SCSI. Ce disque est une bonne option pour une condition de départage DISK. Par exemple :

```
lsdev -C -l hdisk1
```

Un résultat similaire au résultat suivant s'affiche :

```
hdisk1 Available 10-60-00-0,0 16 Bit SCSI Disk Drive
```

Pour servir de disque de départage, le disque doit être partagé par tous les nœuds dans le domaine homologue. Vérifiez l'ID du volume physique issu de la commande **lspv** pour déterminer si le disque est partagé par plusieurs nœuds. Dans le résultat précédent issu de la commande **lspv**, l'ID du volume physique est répertorié dans la seconde colonne ; l'ID du volume de hdisk1 est 000069683404ed54. AIX se souvient de tous les disques qui ont été attachés au système. Les disques répertoriés par la commande **lspv** ne peuvent plus être attachés. Si ce disque a été déplacé vers un autre système, il apparaîtra en tant que disque partagé, alors qu'en réalité il n'est plus rattaché au système d'origine.

Vérifiez que le disque sur lequel les ressources IBM.TieBreaker sont stockées ne stocke pas aussi des systèmes de fichiers. Si les nœuds dans le cluster partagent plus d'un disque, il peut s'avérer difficile de déterminer quel est le disque sur lequel s'applique la condition de départage et quel est le disque réservé aux données applicatives. La sortie issue de la commande **lsdev** affiche l'adresse SCSI associée au disque. (Dans le résultat précédent issu de la commande **lsdev**, l'adresse SCSI est répertoriée dans la troisième colonne ; l'adresse SCSI de hdisk0 est 10-60-00-0,0). Ces informations vous aideront à identifier le disque approprié si vous connaissez l'adresse du disque avant son installation.

Une fois que vous avez déterminé le nom de l'unité, lancez la commande **mkrsrc** pour définir l'objet de départage :

```
mkrsrc IBM.TieBreaker Name=myTieBreaker \
Type=DISK DeviceInfo="DEVICE=/dev/hdisk1" HeartbeatPeriod=5
```

Vérification de la fonction de réservation SCSI

La condition de départage s'appuie sur la réservation SCSI-2, qui n'est pas forcément prise en charge par toutes les combinaisons de configuration de système de stockage et de pilote. Pour vérifier que la configuration prend en charge la réservation SCSI-2, RSCT est livré avec l'utilitaire **disk_reserve**, qui doit être appelé en spécifiant son chemin d'accès complet /usr/sbin/rsct/bin/disk_reserve.

La condition de départage fonctionne correctement si son disque peut être réservé et déverrouillé par l'un des deux nœuds et si le disque ne peut pas être réservé depuis un nœud lorsqu'il est verrouillé par l'autre nœud.

Syntaxe :

```
/usr/sbin/rsct/bin/disk_reserve [-l | -u | -b] [-h] [-v] [-f] [-d nom_disque_serveur]
/usr/sbin/rsct/bin/disk_reserve [-l | -u | -b] [-h] [-v] [-f] [-g nom_unité_grpe_serveurs]
```

-h - affiche ce texte d'aide

-v - prolixe

-f - réserve après la rupture (pour l'option **-l** ou **-b**)

-d nom_disque_serveur - disque à utiliser, par exemple, /dev/sdb

-l - verrouile (réserve)

-u - déverrouille (libère)

-b - interrompre

-g nom_unité_grpe_serveurs, par exemple, /dev/sg1

Exemples :

```
/usr/sbin/rsct/bin/disk_reserve -l -f -d /dev/sde
/usr/sbin/rsct/bin/disk_reserve -l -g /dev/sg3
```

Interruption manuelle d'une réservation de disque

Si le nœud réservant une condition de départage est hors service ou ne peut être réinitialisé, vous devez accéder manuellement à un nœud fonctionnant

correctement pour libérer le disque SCSI à départager. Pour libérer le disque, utilisez la commande **tb_break**, par exemple :

```
/usr/sbin/rsct/bin/tb_break –f –t DISK "DEVICE=/dev/hdisk1"
```

Ci-dessous figure un exemple de disque ne répondant pas aux critères lui permettant de servir de disque de départage. Entrez la commande **lspath**, par exemple :

```
lspath -l hdisk2
lspath: 0514-538 Impossible d'effectuer la fonction demandée car l'unité spécifiée
                 ne prend pas en charge plusieurs chemins d'accès.
```

Exemple de sortie :

```
#lspath -l hdisk2
Enabled hdisk2 fscsi0
Failed  hdisk2 fscsi0
Failed  hdisk2 fscsi0
Failed  hdisk2 fscsi0
Failed  hdisk2 fscsi0
Enabled hdisk2 fscsi0
Enabled hdisk2 fscsi0
Enabled hdisk2 fscsi1
Failed  hdisk2 fscsi1
Failed  hdisk2 fscsi1
Failed  hdisk2 fscsi1
Failed  hdisk2 fscsi1
Enabled hdisk2 fscsi1
Enabled hdisk2 fscsi1
```

Cet exemple de résultat indique que le disque ne prend pas en charge la réservation SCSI-2 et ne peut pas être utilisé en tant que condition de départage.

Réservation persistante de type SCSI pour la condition de départage de disque

Vous pouvez configurer une condition de départage de disque pour utiliser la réservation persistante SCSI sous Aix et Linux for System x. A partir de System Automation for Multiplatforms version 3.2.1.3, cette fonctionnalité est étendue à Linux for System z.

Condition de départage SCSI-3 sous AIX :

Par défaut, la condition de départage de type DISK sous AIX utilise la réservation ou la libération SCSI-2, qui n'est pas forcément prise en charge par toutes les combinaisons de configuration de système de stockage et de pilote. En règle générale, les solutions de virtualisation du stockage telles que le contrôleur de volume SAN ne prennent pas en charge la réservation SCSI-2. Dans ces environnements, le système d'exploitation AIX peut être configuré pour transformer les commandes de réservation ou de libération SCSI-2 en commandes de réservation persistante SCSI-3.

Utilisez la commande suivante pour configurer la réservation ou la libération SCSI-2 en transformation de réservation persistante sous AIX :

```
chdev -l <nom_vol_phys> -a PR_key_value=0x<clé_unique> -a reserve_policy=PR_exclusive
```

<nom_vol_phys>
: Nom du volume physique sur le système AIX à utiliser pour la condition de départage.

<clé_unique>
: Clé numérique arbitraire unique pour chaque noeud dans le cluster.

Exécutez cette commande sur chaque système homologue distant du domaine et indiquez une clé unique différente sur chaque système. Pour savoir si un disque SCSI devant être utilisé par la condition de départage de disque prend en charge cette approche, exécutez

```
lsattr -El <nom_vol_phys>
```

Recherchez les attributs `valeur_clé_nom_vol_phys` et `règle_réservation`. Si les attributs ne peut pas être modifiés comme indiqué dans les paragraphes précédents, recherchez les pilotes de périphérique manquants dans Host Attachment for SDDPCM on AIX.

Les disques sur les composants blade POWER dans un environnement zBX peuvent être uniquement définis en tant que `disque SCSI virtuel`. Ils ne peuvent pas être configurés pour prendre en charge la réservation ou la libération SCSI-2 ou une réservation persistante SCSI-3. Par conséquent, ces disques ne peuvent pas être utilisés comme condition de départage du disque.

Condition de départage SCSIPR dans Linux for System x :

System Automation for Multiplatforms version 3.2.1.2 a introduit le type de condition de départage SCSIPR destiné à être utilisé avec Linux on System x. Il est pris en charge sous RHEL 5, RHEL 6, SLES 10 et SLES 11.

La condition de départage SCSIPR utilise les réservations persistantes SCSI-3 sur une unité de stockage de disque SCSI comme mécanisme de condition de départage. S'il existe une situation de parité dans laquelle le domaine homologue est partitionné en deux sous-domaines, chaque sous-domaine contenant exactement la moitié du noeud défini, le sous-domaine qui parvient à obtenir une réservation persistante exclusive de l'unité de stockage du disque SCSI partagé obtient alors le quorum opérationnel.

Eléments prérequis

L'unité de stockage du disque SCSI devant être utilisée par la condition de départage SCSI-3 doit prendre en charge le protocole de réservation persistante avec le type de réservation `Write Exclusive Registrants Only`. Cette unité doit être partagée entre tous les systèmes du domaine homologue et tous les systèmes doivent pouvoir la réserver à l'aide du protocole de réservation persistante SCSI-3.

La condition de départage SCISPR utilise l'utilitaire `sg_persist`. Utilisez les commandes suivantes pour vérifier qu'il est déjà installé sur tous les systèmes du domaine homologue :

```
which sg_persist
rpm -qf /usr/bin/sg_persist
```

Si l'utilitaire `sg_persist` n'est pas installé, vous devez installer le module Linux approprié :

- RHEL5, RHEL6, SLES 11 : `sg3_utils*.rpm`
- SLES 10 : `scsi*.rpm`

Définition

Lorsque vous créez une condition de départage de type SCSIPR, utilisez l'attribut de ressource persistant `DeviceInfo` pour indiquer l'unité de stockage du disque

SCSI devant être utilisée par la condition de départage. Si la configuration SCSI diffère selon les noeuds des systèmes des domaines homologues, vous pouvez également utiliser l'attribut de ressource persistant `NodeInfo` pour tenir compte de ces différences.

La condition de départage SCSIPR utilise un mécanisme de réservation/libération et doit être réservée de nouveau périodiquement pour mettre la réservation en suspens. Pour cette raison, indiquez l'attribut persistant de ressource `HeartbeatPeriod` lors de la création d'une condition de départage de ce type. L'attribut de ressource persistant `HeartbeatPeriod` définit l'intervalle de renouvellement de la demande de réservation.

Remarque : Lors de la définition des ressources à départager, gardez toujours à l'esprit que le disque sur lequel les ressources `IBM.Tiebreaker` sont stockées ne doit pas aussi être utilisé pour stocker les systèmes de fichiers.

Utilisez l'une des options suivantes pour identifier l'unité de stockage du disque SCSI devant être utilisée par la condition de départage dans l'attribut de ressource persistant `DeviceInfo`.

- `DEVICE=<nom générique ou nom d'unité de disque>`
- `HOST=<h> CHAN=<c> ID=<i> LUN=<I>`
- `WWID=<wwid affiché par le système>`
- `RDAC.WWN=<wwn affiché par le système lors de l'utilisation du pilote multi-chemins LSI RDAC>`

Exemple :

```
mkrsrc IBM.TieBreaker Name="mySCSIPRTieBreaker" Type=SCSIPR DeviceInfo="DEVICE=/dev/sdx" HeartbeatPeriod=5
```

Vérification

Procédez comme suit sur tous les systèmes homologues distants pour vérifier que tous les systèmes prennent correctement en charge la condition de départage SCSIPR avec l'unité de stockage du disque SCSI choisie :

- Réservez l'unité de disque à l'aide de la commande **tb_break** :

```
/usr/sbin/rsct/bin/tb_break -l -t SCSIPR <spécification de l'unité DeviceInfo pour ce système>
```

  Cette commande doit être en mesure de réserver l'unité de disque.

- Tentez de réserver l'unité de disque à l'aide de la commande **tb_break** sur tous les autres tous les systèmes de domaines homologues :

```
/usr/sbin/rsct/bin/tb_break -l -t SCSIPR <spécification de l'unité DeviceInfo pour ce système>
```

  Cette commande ne doit pas parvenir à réserver l'unité de disque, car cette dernière est déjà exclusivement réservée par le premier système.

- Libérez l'unité de disque à l'aide de la commande **tb_break** :

```
/usr/sbin/rsct/bin/tb_break -u -t SCSIPR <spécification de l'unité DeviceInfo pour ce système>
```

  Cette commande doit être en mesure de libérer l'unité de disque.

Vérification de l'état de mise en suspens d'une réservation :

Utilisez la commande suivante pour vérifier si une réservation est en suspens sur l'unité de stockage du disque SCSI :

```
sg_persist --read-reservation <nom générique ou nom d'unité de disque>
```

Exemple : aucune réservation n'est en suspens :

```
sg_persist --read-reservation /dev/sdx
IBM 2145 0000
Peripheral device type: disk
PR generation=0x5, there is NO reservation held
```

Example: reservation is held:

```
sg_persist --read-reservation /dev/sdx
IBM 2145 0000
Peripheral device type: disk
PR generation=0x5, Reservation follows:
Key=0x11293693fa4d5807
scope: LU_SCOPE, type: Write Exclusive, registrants only
```

Lorsque vous réservez une unité de disque, chaque système homologue distant utilise son identificateur de noeud RSCT comme clé de réservation. Pour afficher l'identificateur de noeud RSCT d'un système homologue distant, lancez la commande **/usr/sbin/rsct/bin/lsnodeid**. Si une unité de stockage du disque SCSI est réservée par la condition de départage SCSIPR, vous pouvez déterminer le système qui détient la réservation. Déterminez la clé de réservation en cours et comparez-la à l'identificateur de noeud RSC de tous les systèmes homologues distants.

Interruption d'une réservation :

Si un système homologue distant possède une réservation sur l'unité de stockage du disque SCSI, il est possible d'interrompre cette réservation à partir d'un autre système homologue distant. Utilisez la commande suivante pour forcer l'interruption d'une réservation existante et obtenir une nouvelle réservation :

```
/usr/sbin/rsct/bin/tb_break -f -t SCSIPR <spécification de l'unité DeviceInfo pour ce système>
```

Condition de départage SCSIPR dans Linux for System z :

System Automation for Multiplatforms version 3.2.1.3 a introduit le type de condition de départage SCSIPR destiné à être utilisé avec Linux on System z. Il est pris en charge sous SLES 10 et SLES 11.

La condition de départage SCSIPR utilise les réservations persistantes SCSI-3 sur une unité de stockage de disque SCSI comme mécanisme de condition de départage. S'il existe une situation de parité dans laquelle le domaine homologue est partitionné en deux sous-domaines, chaque sous-domaine contenant exactement la moitié du noeud défini, le sous-domaine qui parvient à obtenir une réservation persistante exclusive de l'unité de stockage du disque SCSI partagé obtient alors le quorum opérationnel.

Eléments prérequis

L'unité de stockage du disque SCSI devant être utilisée par la condition de départage SCSI-3 doit prendre en charge le protocole de réservation persistante avec le type de réservation `Write Exclusive Registrants Only`. Cette unité doit être partagée entre tous les systèmes du domaine homologue et tous les systèmes doivent pouvoir la réserver à l'aide du protocole de réservation persistante SCSI-3. La condition de départage SCISPR utilise l'utilitaire `sg_persist`. Utilisez les commandes suivantes pour vérifier qu'il est déjà installé sur tous les systèmes du domaine homologue :

```
which sg_persist
rpm -qf /usr/bin/sg_persist
```

Si l'utilitaire sg_persist n'est pas installé, vous devez installer le module Linux approprié :

- SLES 11 : sg3_utils*.rpm
- SLES 10 : scsi*.rpm

La virtualisation d'identificateur de port N doit être activée sur le disque utilisé comme condition de départage. Sinon, chaque réservation est exécutée pour le compte de l'ensemble des CEC, le boîtier physique du zSeries, au lieu d'une seule partition logique sur ce CEC. Pour plus d'informations sur la virtualisation de l'identificateur de port N sous zSeries, voir :

- Redpaper : Introducing N_Port Identifier Virtualization for IBM System z9®
- Redbooks : Fibre Channel Protocol for Linux and z/VM on IBM System z

Définition

Lorsque vous créez une condition de départage de type SCSIPR, utilisez l'attribut de ressource persistant DeviceInfo pour indiquer l'unité de stockage du disque SCSI devant être utilisée par la condition de départage. Si la configuration SCSI diffère selon les noeuds des systèmes des domaines homologues, vous pouvez également utiliser l'attribut de ressource persistant NodeInfo pour tenir compte de ces différences.

La condition de départage SCSIPR utilise un mécanisme de réservation/libération et doit être réservée de nouveau périodiquement pour mettre la réservation en suspens. Pour cette raison, indiquez l'attribut persistant de ressource HeartbeatPeriod lors de la création d'une condition de départage de ce type. L'attribut de ressource persistant HeartbeatPeriod définit l'intervalle de renouvellement de la demande de réservation.

Remarque : Lors de la définition des ressources à départager, gardez toujours à l'esprit que le disque sur lequel les ressources IBM.Tiebreaker sont stockées ne doit pas être utilisé pour stocker les systèmes de fichiers.

Utilisez l'une des options suivantes pour identifier l'unité de stockage du disque SCSI devant être utilisée par la condition de départage dans l'attribut de ressource persistant DeviceInfo.

- DEVICE=<nom générique ou nom d'unité de disque>
- HOST=<h> CHAN=<c> ID=<i> LUN=<l>
- WWID=<wwid affiché par le système>
- RDAC.WWN=<wwn affiché par le système lors de l'utilisation du pilote multi-chemins LSI RDAC>

Exemple :

```
mkrsrc IBM.TieBreaker Name="mySCSIPRTieBreaker" Type=SCSIPR DeviceInfo="DEVICE=/dev/sdx" HeartbeatPeriod=5
```

Vérification

Procédez comme suit sur tous les systèmes homologues distants pour vérifier que tous les systèmes prennent correctement en charge la condition de départage SCSIPR avec l'unité de stockage du disque SCSI choisie :

- Réservez l'unité de disque à l'aide de la commande tb_break :

```
/usr/sbin/rsct/bin/tb_break -l -t SCSIPR <spécification de l'unité DeviceInfo pour ce système>
```

Cette commande doit être en mesure de réserver l'unité de disque.

- Tentez de réserver l'unité de disque à l'aide de la commande `tb_break` sur tous les autres tous les systèmes de domaines homologues :

```
/usr/sbin/rsct/bin/tb_break -l -t SCSIPR <spécification de l'unité DeviceInfo pour ce système>
```

Cette commande ne doit pas parvenir à réserver l'unité de disque, car cette dernière est déjà exclusivement réservée par le premier système.

- Libérez l'unité de disque à l'aide de la commande `tb_break` :

```
/usr/sbin/rsct/bin/tb_break -u -t SCSIPR <spécification de l'unité DeviceInfo pour ce système>
```

Cette commande doit être en mesure de libérer l'unité de disque.

Vérification de l'état de mise en suspens d'une réservation :
Utilisez la commande suivante pour vérifier si une réservation est en suspens sur l'unité de stockage du disque SCSI :

```
sg_persist --read-reservation <nom générique ou nom d'unité de disque>
```

Exemple : aucune réservation n'est en suspens :

```
sg_persist --read-reservation /dev/sdx
IBM 2145 0000
Peripheral device type: disk
PR generation=0x5, there is NO reservation held
```

Exemple : une réservation est en suspens :

```
sg_persist --read-reservation /dev/sdx
IBM 2145 0000
Peripheral device type: disk
PR generation=0x5, Reservation follows:
Key=0x11293693fa4d5807
scope: LU_SCOPE, type: Write Exclusive, registrants only
```

Lorsque vous réservez une unité de disque, chaque système homologue distant utilise son identificateur de noeud RSCT comme clé de réservation. Pour afficher l'identificateur de noeud RSCT d'un système homologue distant, lancez la commande **/usr/sbin/rsct/bin/lsnodeid**. Si une unité de stockage du disque SCSI est réservée par la condition de départage SCSIPR, vous pouvez déterminer le système qui détient la réservation en vérifiant quelle est la clé de réservation. Comparez la clé de réservation avec tous les identificateurs de noeud RSCT des systèmes homologues distants.

Interruption d'une réservation :
Si un système homologue distant possède une réservation sur l'unité de stockage du disque SCSI, il est possible d'interrompre cette réservation à partir d'un autre système homologue distant. Utilisez la commande suivante pour forcer l'interruption d'une réservation existante et obtenir une nouvelle réservation :

```
/usr/sbin/rsct/bin/tb_break -f -t SCSIPR <spécification de l'unité DeviceInfo pour ce système>
```

Condition de départage ECKD dans les environnements z/VM

Sous Linux on System z®, une unité de stockage à accès direct ECKD™ peut être utilisée comme ressource de condition de départage.

La condition de départage ECKD utilise la fonction de réservation et de libération, ce qui peut impliquer des étapes de configuration supplémentaires. z/VM® ne peut pas accéder à un stockage à accès direct ECKD. En conséquence, z/VM ne peut pas connecter ni mettre en fonction un périphérique de ce type réservé par un

autre système. Pour pallier cette situation, un ensemble d'actions de configuration est requis. Les exigences correspondantes sont décrites dans les sections suivantes.

Exigences relatives aux unités de stockage à accès direct ECKD pour les domaines s'exécutant dans un seul système z/VM : Si tous les noeuds du domaine System Automation sont des invités de ce même système z/VM, les définitions suivantes sont requises pour l'unité de stockage à accès direct ECKD :

- Un mini-disque complet doit être défini.
- Si la mémoire cache du mini-disque est utilisée, sa valeur doit être définie sur `off`.
- L'unité de stockage à accès direct ECKD est partagée entre les deux invités dans le z/VM.

Exigences relatives aux unités de stockage à accès direct ECKD pour les domaines couvrant deux systèmes z/VM : Si les noeuds du domaine System Automation sont des invités de deux systèmes z/VM différents, les définitions suivantes sont requises pour l'unité de stockage à accès direct ECKD :

- Le disque de départage doit être défini en tant que disque DEVNO dans une instruction de minidisque dans le profil d'utilisateur (aucun minidisque, aucun minidisque complet, aucune unité de stockage à accès direct dédiée ou connectée)
- Le disque ECKD (DEVNO) est partagé entre les deux noeuds.
- L'unité de stockage à accès direct ECKD ne doit pas être connectée au système lorsque le système z/VM fait l'objet d'un IPL.

La connexion aux invités Linux affiche la relation d'unité suivante, une unité virtuelle (291 dans l'exemple) avec l'adresse réelle (4a82 dans l'exemple). L'unité devient partagée, dans l'exemple, grâce à la commande `cp set shared on 4a82`. L'unité doit être partagés des deux côtés.

```
00: CP Q 4A82
00: DASD 4A82 CP SYSTEM DEVNO   1     SHARED
00:
00: CP Q V 291
00: DASD 0291 3390 VM4A82 R/W      3339 CYL ON DASD 4A82 SUBCHANNEL = 000F
```

Si l'un des systèmes z/VM est arrêté, l'unité de stockage à accès direct ECKD est réservée par l'invité Linux conservé sur l'autre système z/VM. Dans le côté qui subsiste, vous pouvez voir ce qui suit :

```
00: CP Q DA RESERVE
00: DASD 4A82 CP SYSTEM DEVNO    1     RESERVED BY USER test1
```

Une fois que z/VM est redémarré, l'unité de stockage à accès direct 4A82 est toujours hors ligne et ne peut pas être mise en ligne du fait qu'elle est toujours réservée par l'autre système. Un délai d'attente de 20 à 30 minutes se produit à la place.

Il est recommandé de démarrer Linux sur le système z/VM qui a été redémarré sans utiliser l'unité de stockage à accès direct de départage. Cette méthode réussira étant donné que l'unité de stockage à accès direct n'est pas requise pour démarrer Linux. Une fois que Linux est démarré, System Automation va démarrer automatiquement sur l'invité Linux, puis Linux va de nouveau rejoindre le domaine System Automation. La réservation de l'unité de stockage à accès direct ECKD est alors libérée. Il est possible de mettre en fonction l'unité du disque de départage (4a82 dans notre exemple). Lancez la commande **`share`** liez l'adresse virtuelle du disque de départage (291 dans notre exemple) sur le système qui vient

de faire l'objet d'un IPL. Entrez la commande **chccwdev -e 291** sur le système Linux redémarré. Une fois la commande terminée, tout est opérationnel. Aucune interaction supplémentaire sur le système Linux qui subsiste n'est nécessaire.

Toutes les commandes requises sont des commandes CP. Par conséquent, un script qui émet ces commandes à l'aide de VMCP peut être écrit pour automatiser la restauration du système Linux défaillant.

Pour l'exemple ci-dessus, le script pourrait contenir les commandes suivantes :

```
vmcp vary on 4a82
vmcp set shared on 4a82
vmcp link * 291 291 mr
chccwdev -e 291
```

System Automation reconnaîtra automatiquement l'unité de stockage à accès direct nouvellement définie.

Condition de départage de réseau

La condition de départage du réseau est une alternative aux conditions de départage du disque et de l'opérateur. Elle utilise une (instance de réseau) IP externe pour résoudre une situation de parité.

Il existe plusieurs cas dans lesquels l'utilisation d'une condition de départage du réseau est recommandée. Par exemple :

- Un disque partagé utilisable comme disque de départage n'est pas disponible.
- La priorité supérieure est de permettre à l'environnement à haute disponibilité de communiquer avec les instances en dehors du cluster.

Exemple : Les fonctions essentielles d'un serveur Web sont de délivrer des pages Web aux clients en dehors du cluster. Pour rendre ce service hautement disponible, la condition de départage ne doit pas autoriser l'accès à un noeud incapable de communiquer avec les instances en dehors du cluster.

Utilisez la condition de départage du réseau uniquement pour les domaines dans lesquels tous les noeuds se trouvent dans le même sous-réseau IP. Si les noeuds se trouvent dans des sous-réseaux IP différents, le risque de voir les deux noeuds envoyer des commandes ping à la condition de départage de réseau est plus élevé, alors même qu'ils ne peuvent pas communiquer entre eux. Par ailleurs, l'adresse IP de la passerelle par défaut ne doit pas être utilisée si elle est virtualisée par l'infrastructure du réseau. Choisissez une adresse IP accessible exclusivement par le biais d'un chemin unique à partir de chaque noeud du domaine.

Dans la configuration par défaut, la condition de départage du réseau effectue deux tentatives pour atteindre (via une commande ping) l'adresse IP de la condition de départage du réseau. Le nombre par défaut de commandes ping peut être trop faible dans des environnements virtualisés ou des environnements ayant une connexion réseau lente ou peu fiable. Pour ces environnements, vous pouvez augmenter jusqu'à 9 le nombre de commandes ping exécutées par la condition de départage du réseau. Cela garantit un résultat correct de l'opération de réservation de la condition de départage.

Conditions requises pour la condition de départage du réseau

Pour assurer la fonction de condition de départage du réseau, l'instance de réseau IP externe doit pouvoir être atteinte par tous les noeuds au sein d'un cluster hautement disponible. L'instance du réseau IP externe doit pouvoir répondre aux

demandes d'écho dans ICMP (ping). Si vous définissez une règle de pare-feu qui a pour effet de bloquer le trafic dans ICMP entre les noeuds du cluster et l'instance IP externe, la condition de départage du réseau ne fonctionne pas. Dans ce cas, les noeuds du cluster risquent de ne plus communiquer avec leurs homologues (fractionnement du cluster), mais les deux sous-clusters peuvent atteindre l'instance IP externe. Normalement, le protocole IP s'assure que si les deux sous-clusters peuvent atteindre la passerelle externe, ils peuvent aussi communiquer avec leurs homologues. Si cette règle ne peut pas être garantie, par exemple en raison des paramètres du pare-feu, vous ne pouvez pas utiliser la condition de départage réseau.

Le tableau suivant présente les avantages et les inconvénients des conditions de départage disque et réseau :

Tableau 21. Comparaison entre une condition de départage du réseau et une condition de départage du disque

Condition de départage réseau	Condition de départage de disque
• + : Pas de dépendance matérielle. • + : Evalue la disponibilité de communication.	• + : Condition de départage la plus sûre. Le matériel veille à ce qu'une seule instance (noeud) puisse être soumise à une condition de départage.
• - : Si l'instance IP externe n'est pas disponible en cas de fractionnement d'un cluster, aucun sous-cluster n'aura de quorum. • -: Il peut y avoir des conditions d'erreur dans lesquelles une situation de parité se produit mais où plusieurs noeuds peuvent communiquer. Dans ce cas, les deux sous-clusters peuvent alors être soumis à la condition de départage.	• Si la communication est interrompue, cette condition de départage peut garantir l'accès à un noeud qui ne parvient pas à communiquer avec les instances situées en dehors du cluster.

Configuration d'une condition de départage de réseau

Définissez une condition de départage de réseau comme une ressource `IBM.TieBreaker` de type `EXEC`. Pour plus d'informations sur la condition de départage `EXEC`, consultez la documentation de RSCT. Les fichiers exécutables de la condition de départage de réseau, `samtb_net` et `samtb_net6`, se trouvent dans le répertoire `/usr/sbin/rsct/bin`. Lors de l'implémentation en cours, les options suivantes devront être spécifiées en tant que mots clés `key=value` pendant la création de la condition de départage RSCT d'une commande `EXEC` :

`Address=<adresse IP>`
: Adresse de l'instance IP externe qui est utilisée pour résoudre une situation de parité. Dans un réseau IPv6, indiquez une adresse au format IPv6. N'utilisez pas de nom DNS. En cas de problèmes de communication, survenant généralement lors du fractionnement du cluster, DNS ne pourra fonctionner correctement. L'adresse est une option obligatoire. Il n'y a pas de valeur par défaut.

`Log=<1/0>`
: Indiquez 1 si vous souhaitez que la condition de départage du réseau rédige des journaux systèmes dans la fonction journal système (syslog). Sinon, indiquez 0.

`Count=<nombre>`
: Nombre de demandes d'écho dans ICMP envoyées pour déterminer le

quorum. Si la première demande obtient une réponse, aucune autre demande n'est envoyée. La valeur par défaut est 2. La gamme de valeurs autorisée est comprise entre 1 et 9. Augmentez la valeur de Nombre pour les environnements virtuels ou les environnements ayant une connexion réseau lente ou peu fiable.

En fonction de la version IP, il existe différents fichiers exécutables de la condition de départage réseau que vous devez utiliser lorsque vous définissez la condition de départage.

La commande suivante crée une nouvelle condition de départage de réseau pour une adresse IPv4 :

```
# mkrsrc IBM.TieBreaker Type="EXEC" Name="mynetworktb" \
DeviceInfo='PATHNAME=/usr/sbin/rsct/bin/samtb_net Address=<adresse IPv4> \
Log=1' PostReserveWaitTime=30;
```

La commande suivante crée une nouvelle condition de départage de réseau pour une adresse IPv6 :

```
# mkrsrc IBM.TieBreaker Type=EXEC Name="mynetworktb" \
DeviceInfo='PATHNAME=/usr/sbin/rsct/bin/samtb_net6 Address=<adresse IPv6> \
Log=1' PostReserveWaitTime=30;
```

Activez votre condition de départage du réseau comme suit :

```
# chrsrc -c IBM.PeerNode OpQuorumTieBreaker="mynetworktb"
```

Utilisez la commande **chrsrc** pour modifier la définition de la condition de départage de réseau. Par exemple, si vous devez augmenter la valeur pour le nombre de commandes ping, utilisez les commandes suivantes :

```
chrsrc -c IBM.PeerNode OpQuorumTieBreaker="Operator"
chrsrc -s "Name = 'your_tiebreaker_name'" IBM.TieBreaker \
DeviceInfo="PATHNAME=/usr/sbin/rsct/bin/samtb_net Address=<ip_départage_réseau> \
Count=<nouvelle_valeur> Log=1"
chrsrc -c IBM.PeerNode OpQuorumTieBreaker="nom_départage"
```

Pour supprimer la définition de la condition de départage, utilisez la commande **rmrsrc**.

Comportement de réservation d'une condition de départage de réseau

Lorsqu'un noeud réserve une condition de départage, celle-ci n'est plus disponible et ne peut pas être réservée par un autre noeud. Ce dispositif n'est pas possible pour une condition de départage réseau. Par conséquent, le comportement de réservation d'une condition de départage de réseau présente les différences décrites ci-dessous.

Après l'échec d'une tentative de réservation, aucune autre réservation n'est autorisée tant que le noeud n'a pas rejoint le cluster. Un fichier est enregistré dans `/var/ct/` afin d'indiquer que la réservation a échoué. Si ce fichier est présent, toute commande de réservation de condition de départage échoue obligatoirement. Un processus supplémentaire est engendré et observe le quorum et supprime le fichier des blocs si le noeud a été de nouveau ajouté au domaine.

L'exemple de fichier suivant a été créé par la condition de départage du réseau suite à l'échec d'une opération de réservation de la condition de départage vers l'instance du réseau IP externe 123.456.789.1. Il comprend l'horodatage de l'échec de l'opération de réservation.

```
# cat /var/ct/samtb_net_blockreserve_123.456.789.1
Mo Jul 4 08:38:40 CEST 2005
```

Configuration d'une ressource de condition de départage dans le cadre du départage du réseau

Cette rubrique décrit les options de configuration de la condition de départage qui doivent être prises en compte lorsque vous définissez une condition de départage réseau.

PostReserveWaitTime=30

PostReserveWaitTime définit le délai entre la réservation réussie de la condition de départage et le moment où le quorum est accordé. Un noeud qui réserve la condition de départage du réseau n'obtient pas le quorum opérationnel tant que le délai défini par l'attribut PostReserveWaitTime n'est pas écoulé. Indiquez une valeur de 30 secondes pour définir une durée d'indisponibilité suffisante. Ce délai est nécessaires pour que les noeuds puissent détecter l'inactivité de l'autre noeud et restaurer immédiatement la communication. Dans ce cas, les deux noeuds sont en mesure de réserver la condition de départage du réseau. En raison du délai d'attente plus long, la communication entre les noeuds est également rétablie et le risque que les deux noeuds obtiennent le quorum et démarrent les ressources en parallèle est minimisé.

HeartbeatPeriod=30

Après la réussite d'une réservation, ConfigRM commence à appeler périodiquement l'opération de signal de présence de la condition de départage. Pour que le système ne soit par surchargé lors du fractionnement du cluster, augmentez le délai entre les signaux de présence de la condition de départage ou mettez-les hors fonction en définissant l'attribut HeartbeatPeriod sur 0.

Révision des journaux système d'un scénario de condition de départage du réseau

Cette rubrique montre un exemple du journal système dans un scénario de condition de départage de réseau au sein d'un cluster à deux noeuds (n1 et n2).

Dans la figure 12, à la page 70, vous voyez les journaux système d'un cluster à deux noeuds (noeud n1 et noeud n2). Ce scénario d'erreur part du principe qu'aucune ressource critique ne s'exécute sur les deux noeuds. Un problème de réseau interrompt tous les chemins de communication disponibles entre les homologues, mais un homologue (n2) peut encore communiquer avec sa passerelle (123.456.789.1). Après un certain temps et une fois la communication rétablie, les deux noeuds peuvent être ajoutés au cluster.

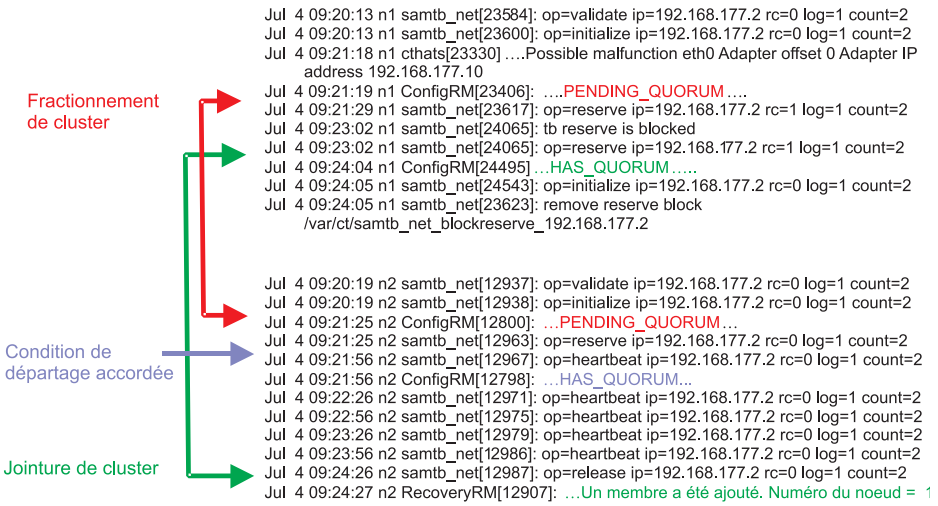

Figure 12. Journaux système d'un cluster à deux noeuds

Condition de départage NFS

La condition de départage NFS résout les situations de parité basées sur les fichiers de réserve stockés sur un serveur NFS v4. Le serveur NFS peut être utilisé pour plusieurs clusters System Automation for Multiplatforms. Si le même serveur est utilisé pour plusieurs séparateurs de la condition de départage NFS, chaque réservation a besoin d'un fichier avec un nom unique.

Dans une situation de fractionnement de cluster, un seul noeud peut disposer du quorum ou être en attente de celui-ci à un moment donné. Si le noeud qui a obtenu le quorum tombe en panne, les autres noeuds tentent automatiquement de l'obtenir à leur tour en s'appuyant sur le protocole challenger-défenseur.

Le serveur NFS peut se trouver sur n'importe quel système exécutant NFS v4. Si vous utilisez un serveur NFS conforme au dernier standard v4.1 ou pNFS pour la conditions de départage de System Automation for Multiplatforms vérifiez que les fonctions de réplication et de basculement du serveur NFS sont désactivées. Utilisez le serveur NFS uniquement pour la condition de départage de System Automation for Multiplatforms.

Les bibliothèques client NFS v4 doivent être installées sur tous les noeuds des clusters de System Automation for Multiplatforms.

Un exemple de scénario d'utilisation d'une condition de départage NFS est une configuration sur trois sites. Deux sites hébergent un ensemble de clusters à deux noeuds, et la condition de départage se trouve sur le troisième site. La condition de départage de disque ne peut pas être utilisée, car elle requiert une configuration de réseau de stockage SAN qui n'est pas nécessairement commune aux trois sites. Il n'est pas non plus possible de prévoir la topologie du réseau. Aucun périphérique réseau du troisième site ne peut être choisi comme adresse de destination pour la condition de départage du réseau. Dans ce cas, la troisième site peut être utilisé pour héberger le serveur NFS v4 utilisé en tant que condition de départage.

Si le serveur de quorum NFS n'est pas joignable ou est en panne dans une situation de fractionnement de cluster, les noeuds du cluster n'obtiennent pas le

quorum. Cette situation est semblable à une condition de départage de disque, où aucun des noeuds n'obtient le quorum si le disque est en panne ou non joignable. Vérifiez que le serveur de quorum NFS fonctionne de manière permanente et fiable.

System Automation monte le système de fichiers NFS à divers stades sur les noeuds de cluster, mais pas régulièrement.

Initialize
Le montage est établi lorsque la condition de départage du système NFS est définie comme condition de départage active, au cours de l'opération `Initialize`, ainsi qu'au cours du démarrage du domaine ou du noeud. En cas d'échec, il se peut que le noeud ne parvienne pas à rejoindre le domaine.

Reserve
Au cours de l'opération `Reserve`, avant l'accès au fichier de réservation, le montage du système NFS est vérifié et (r)établi si nécessaire.

Terminate
Le système de fichiers NFS est démonté au cours de l'opération `Terminate`, qui s'exécute lorsque la condition de départage du système NFS n'est pas la condition de départage active ou lorsque le domaine ou le noeud est arrêté.

System Automation for Multiplatforms monte le système de fichiers NFS à divers stades sur les noeuds de cluster, mais pas régulièrement :

- Au départ, le montage est établi lorsque la condition de départage du système NFS est définie comme la `condition de départage active` au cours de l'opération `Initialize` ou au démarrage du domaine ou du noeud. Si le montage échoue, il se peut que le noeud ne parvienne pas à rejoindre le domaine.
- Au cours de l'opération `Reserve`, avant l'accès au `fichier de réservation`, le montage du système NFS est vérifié et (r)établi si nécessaire.

Le système de fichiers NFS est démonté au cours de l'opération `Terminate`, qui est exécutée lorsque la condition de départage du système NFS n'est pas la condition de départage active ou lorsque le domaine ou le noeud est arrêté.

Remarque : Le fichier de réserve jouant un rôle primordial en cas de fractionnement de cluster. Sa suppression peut permettre à deux noeuds d'un cluster d'obtenir le quorum. Utilisez un schéma de désignation pour ces fichiers permettant une association directe entre le fichier de réserve et le cluster à l'aide du fichier de réserve. Par exemple, `NFS_reserve_file_SAP_HA_sapnode1_sapnode2_DO_NOT_REMOVE` indique clairement l'objectif du fichier, le nom du cluster et le nom des noeuds qui utilisent le fichier de réserve. Si le fichier a été supprimé, activez la condition de départage de l'opérateur par défaut, créez à nouveau le fichier, puis activez à nouveau la condition de départage NFS. Pour plus d'informations sur la condition de départage Operator, voir «Configuration de la condition de départage», à la page 51.

Activation du serveur NFS sous Linux

Découvrez comment activer la prise en charge NFS v4 si vous exécutez System Automation for Multiplatforms sous Linux.

Activez la prise en charge NFS v4 :

1. Ajoutez la ligne suivante au fichier /etc/exports pour le système de fichiers du serveur de quorum :

   ```
   </votre/rép_serveur_quorum> *(fsid=0,rw,sync,no_root_squash)
   ```

   Le nom du répertoire </your/quorumserverDir> est un exemple. Vous pouvez utiliser n'importe quel nom de répertoire. Vérifiez que fsid=0 n'entraîne l'exportation que d'un seul chemin.
2. Créez le répertoire <rép_serveur_quorum> et définissez la valeur a+rwxt pour son masque de bit d'autorisation.
3. Pour permettre le montage automatique des systèmes de fichier rpc_pipefs et nfsd, vous devez peut-être ajouter les lignes suivantes à /etc/fstab :
   a. `rpc_pipefs /var/lib/nfs/rpc_pipefs rpc_pipefs defaults 0 0`
   b. `nfsd /proc/fs/nfsd nfsd defaults 0 0`
4. Il est possible que les modifications apportées aux fichiers config du répertoire /etc ne soient prises en compte qu'au redémarrage du serveur. Pour plus d'informations, reportez-vous à la documentation relative à votre distribution Linux.
5. Vérifiez que les répertoires /var/lib/nfs/v4recovery/ et /var/lib/nfs/rpc_pipefs/ ont bien été créés. Selon la distribution utilisée, vous devez peut-être charger le module du noyau NFS avec la commande modprobe nfs.
6. Selon la distribution que vous utilisez, les démons sont démarrés différemment. Ainsi, la commande /etc/init.d/idmapd start ou service idmapd start peut démarrer le démon rpc.idmapd. Les démons suivants doivent être démarrés :
   a. rpc.idmapd
   b. rpc.gssd
   c. rpc.nfsd
7. Régénérez la liste d'exportation à l'aide de la commande exportfs –r.
8. Vérifiez que les démons rpc.nfsd et rpc.idmapd sont actifs.
   a. rpc.nfsd : A l'aide de la commande ps –ef | grep nfsd, vérifiez qu'un processus nommé nfsd est actif.
   b. rpc.idmapd : Utilisez la commande ps –ef | grep rpc.idmapd.
   c. A l'aide de la commande rpcinfo –p, vérifiez les versions de tous les programmes RPC enregistrés.

L'ID NFS v4 du démon de mappage rpc.idmapd est requis pour une exécution sur le noeud System Automation for Multiplatforms, qui exécute la condition de départage NFS. Reportez-vous à la documentation de votre distribution sur la façon de démarrer le démon idmapd.

Pour vérifier qu'un noeud System Automation for Multiplatforms peut accéder correctement au serveur NFS, entrez la commande suivante :

```
mount –t nfs4 <nom_serveur_nfs>:/<nom_répertoire_quorum>/<répertoire_local>
```

L'installation est vérifiée avec succès, si la commande de montage aboutit et s'il est possible de créer des fichiers dans le répertoire monté NFS v4.

Si l'opération de montage n'aboutit pas, corrigez votre installation avec l'aide de la documentation de votre système d'exploitation.

Pour plus d'informations, reportez-vous à la documentation relative à votre distribution Linux.

Activation du serveur NFS sous AIX

Découvrez comment activer la prise en charge NFS v4 si vous exécutez System Automation for Multiplatforms sous AIX.

Assurez-vous que les démons NFS v4 sont démarrés sur votre serveur:

1. A l'aide de la commande `lssrc –g nfs`, vérifiez que les démons NFS v4 sont démarrés sur votre serveur.
2. Si le serveur NFS n'est pas démarré, démarrez-le à l'aide de la commande suivante :
   a. `mknfs`
   b. `chnfsdom <nom_domaine_nfs>`
   c. `startsrc –s nfsrgyd`
3. Créez le répertoire `<serveur_quorum>` et définissez la valeur `a+rwxt` pour son masque de bit d'autorisation.
4. Exportez ce répertoire vers les clients NFS v4 à l'aide de la commande `mknfsexp –v 4 –d <serveur_quorum> [ -h <hôte>]`.
5. Pour des raisons de sécurité, vous pouvez restreindre la liste des hôtes qui sont autorisés à monter le répertoire. Restreignez la liste des hôtes à tous les noeuds System Automation for Multiplatforms utilisant le serveur NFS en indiquant l'option `–h`.

Démarrez et configurez les démons NFS requis sur le client NFS en exécutant la commande `mknfs`. Si le serveur NFS utilisé fonctionne sous Linux, le message d'erreur suivant peut figurer dans le journal système après l'initialisation d'une condition de départage :

```
vmount: operation not permited (opération non autorisée)
```

Le serveur Linux NFS vérifie si le port du client NFS est un port réservé. Si vous recevez ce message d'erreur, lancez la commande suivante sur chaque système AIX sur lequel la condition de départage NFS s'exécute.

```
nfso -p -o nfs_use_reserved_ports=1
```

Pour vérifier qu'un noeud System Automation for Multiplatforms peut accéder correctement au serveur NFS, entrez :

```
mount –o vers=4 <nom_serveur_nfs>:/<nom_répertoire_quorum>/<répertoire_local>
```

L'installation est vérifiée avec succès si la commande de montage aboutit et s'il est possible de créer des fichiers dans le répertoire monté NFS v4.

Si l'opération de montage n'aboutit pas, corrigez votre installation avec l'aide de la documentation de votre système d'exploitation.

Configuration de la condition de départage NFS

Définissez une condition de départage de réseau comme une ressource `IBM.TieBreaker` de type `EXEC`.

L'exécutable de la condition de départage NFS `samtb_nfs` se trouve dans le répertoire `/usr/sbin/rsct/bin`. Lors de l'implémentation en cours, les options suivantes devront être spécifiées en tant que mots clés `key=value` pendant la création de la condition de départage d'une commande exec RSCT :

`nfsQuorumServer`
: Nom d'hôte du serveur NFS v4 utilisé. Cette option est obligatoire.

localQuorumDirectory
Répertoire utilisé par la condition de départage NFS sur le noeud System Automation for Multiplatforms. Ce répertoire est créé automatiquement s'il n'existe pas. Si cette option n'est pas spécifiée, c'est le répertoire par défaut `/var/ct/nfsTieBreaker/` qui est utilisé.

remoteQuorumDirectory
Répertoire est exporté par `nfsQuorumServer` et utilisé par la condition de départage NFS de System Automation for Multiplatforms. Si cette option n'est pas spécifiée, c'est l'option par défaut `/` qui est utilisée.

nfsOptions
Options utilisées pour la commande de montage. Utilisez l'option par défaut documentée dans «Options de montage NFS par défaut», à la page 75.

Elle est nécessaire pour remplacer tous les caractères `'='` par `'::'` et tous les caractères `','` par `'..'`. Par exemple, `vers::4..fg..soft..retry::1..timeo::10` est transformé en `vers=4,fg,soft,retry=1,timeo=10` avant que l'option de montage soit passée à la commande de montage du système d'exploitation.

Si `nfsOptions` n'est pas spécifié, les options de montage par défaut sont :

AIX `vers::4..fg..soft..retry::1..timeo::10`

Linux `rw..soft..intr..noac..fg..retry::0`

reserveFileName
Nom de fichier créé par la condition de départage NFS dans le répertoire `remoteQuorumDirectory` de `nfsQuorumServer` pour stocker des informations liées à la condition de départage. Cette option est obligatoire.

Si plusieurs clusters utilisent le même serveur NFS v4 pour la condition de départage NFS, assurez-vous que chaque cluster utilise un nom `reserveFileName` distinct. Si deux clusters utilisent le même fichier de réserve, un seul sous-cluster peut inutilement perdre le quorum en cas de fractionnement de cluster. Pour garantir le caractère unique des noms de fichier de réserve, vous pouvez envisager un schéma de dénomination utilisant le nom du cluster et au moins certains noms de noeud au sein des clusters.

Log Utilisé pour activer ou désactiver l'écriture des informations de journal dans `syslog`.

- `Log=0` : Aucune information de journal n'est collectée.
- `Log=1` : Des informations importantes sont écrites dans `syslog`.
- `Log=2` : Des informations de niveau de débogage et de trace sont générées.

La valeur par défaut est 1.

HeartbeatPeriod
Après la réussite d'une réservation, `ConfigRM` commence à appeler périodiquement l'opération heartbeat à départager. Pour la condition de départage NFS, indiquez une valeur supérieure à 15.

PostReserveWaitTime
L'attribut `PostReserveWaitTime` définit le délai entre la réservation réussie de la condition de départage et le moment où le quorum est accordé. Un noeud qui réserve la condition de départage du réseau n'obtient pas le quorum opérationnel tant que le délai défini par l'attribut

PostReserveWaitTime n'est pas écoulé. Pour la condition de départage NFS, la valeur PostReserveWaitTime doit être égale à 15.

Pour créer une condition de départage NFS myNFSTiebreaker sur le serveur NFS my.nfs.server.com avec localQuorumDirectory /my/quorumServer, niveau de journalisation 2, et les valeurs par défaut pour les autres options, la commande suivante peut être utilisée :

```
mkrsrc IBM.TieBreaker Type="EXEC" Name="myNFSTie breaker"
DeviceInfo='PATHNAME=/usr/sbin/rsct/bin/samtb_nfs
nfsQuorumServer="my.nfs.server.com" reserveFileName=<nom_fichier_unique>
localQuorumDirectory "/my/quorumServer" Log=2'
HeartbeatPeriod=30 PostReserveWaitTime=15'
```

Lorsque la condition de départage NFS est activée, une logique de validation s'assure que le serveur NFS fonctionne comme prévu.

Les erreurs de configuration suivantes ne peuvent pas être détectées par la logique de validation :

- Si la valeur HeartbeatPeriod est inférieure à 15.
- Si reserveFileName n'est pas unique pour le serveur NFS v4 utilisé.
- Si PostReserveWaitTime est différent de 15.

Pour plus d'informations sur la condition de départage EXEC, consultez la documentation de RSCT.

Options de montage NFS par défaut : Les options de montage suivantes sont utilisées :

rw Indique que le répertoire monté est accessible en lecture et en écriture.

soft Renvoie une erreur si le serveur NFS est inaccessible.

intr Autorise des signaux d'interruption.

noac Les attributs de fichier ne sont pas mis en cache. Force le caractère synchrone de la demande d'écriture du client.

fg Exécute la commande de montage et échoue si cette commande n'aboutit pas.

retry=0
Le système abandonne immédiatement si une commande de montage échoue.

Si vous utilisez d'autres options de montage, il n'est pas garanti que la condition de départage NFS fonctionne toujours dans tous les cas.

Protection des opérations de départage NFS par le délai d'expiration : Il est important de s'assurer que les opérations soumises à une condition de départage EXEC ne subissent pas de blocage, pour les raisons suivantes :

- Les opérations RSCT telles que **lsrsrc**, **lsrpnode** et **lssam** sont bloquées pendant l'exécution des opérations soumises à une condition de départage.
- Si une opération de réservation sur un noeud avec une ressource critique en cours d'exécution se bloque, le noeud reste à l'état PENDING_QUORUM alors qu'un autre noeud peut parvenir à la valeur HAS_QUORUM. Par conséquent une ressource critique est exécutée simultanément sur plusieurs noeuds du cluster.

La condition de départage NFS comporte deux processus qui sont définis. Il s'agit d'un processus agent et d'un deuxième processus qui active le temporisateur et arrête l'agent s'il n'est pas terminé dans le délai imparti :

- `samtb_nfs_worker` : exécute les opérations réelles de condition de départage.
- `samtb_nfs` : initialise un temporisateur, puis exécute `samtb_nfs_worker` à partir d'une unité d'exécution générée. Si `samtb_nfs_worker` se termine dans le délai imparti, `samtb_nfs` se termine avec le code retour `samtb_nfs_worker`. Si `samtb_nfs_worker` ne se termine pas dans le délai imparti, le gestionnaire d'alarmes s'assure que `samtb_nfs_worker` est terminé, écrit un message d'erreur dans `syslog` et s'arrête avec la valeur -1 (FAILED).

Les valeurs de délai d'expiration suivantes sont possibles :

Opération de réservation
13 secondes après le fractionnement du cluster.

Opération de validation
60 secondes au moment de la définition de la condition de départage.

Opération d'initialisation
20 secondes après le réamorçage d'un noeud au moment de l'initialisation du cluster.

Toutes les autres opérations
15 secondes.

Remplacement du quorum opérationnel

Remplacez l'état de quorum opérationnel si le nombre de noeuds permettant d'atteindre un quorum opérationnel est insuffisant.

Pour supprimer des noeuds du cluster, au moins un des noeuds présents dans le cluster doit être en ligne pour exécuter la commande **rmrpnode**. Le quorum opérationnel est obligatoire pour exécuter cette commande. Si le nombre de noeuds permettant d'atteindre un quorum opérationnel est insuffisant, vous ne pouvez pas ajuster la taille du cluster pour rétablir le quorum.

Si pour une raison ou pour une autre, la fonction de quorum opérationnel doit être désactivée, l'attribut persistant `OpQuorumOverride` doit être défini sur 1 :

```
chrsrc –c IBM.PeerNode OpQuorumOverride=1
```

Dans ce cas, l'état de quorum opérationnel est toujours `HAS_QUORUM` et la protection de la ressource n'est plus assurée.

Configuration de l'adaptateur d'automatisation de bout en bout

Si vous souhaitez intégrer un domaine System Automation for Multiplatforms à l'environnement d'automatisation de bout en bout System Automation Application Manager, vous devez configurer l'adaptateur d'automatisation.

Pour intégrer un domaine System Automation for Multiplatforms à l'environnement d'automatisation de bout en bout System Automation Application Manager,vous devez respecter les conditions suivantes :

- Noms d'objet System Automation for Multiplatforms. Par exemple, les noms de groupes, les noms de ressources et les descriptions ne peuvent pas contenir les caractères suivants :
  - " : Guillemets doubles

- ' : Guillemet simple
- ; : Point-virgule
- $: Symbole du dollar
- / : Barre oblique

- Les noms de domaine System Automation for Multiplatforms doivent être uniques dans la portée des domaines d'automatisation qui se connectent au même gestionnaire d'automatisation de bout en bout.

La figure 13 présente l'environnement dans lequel fonctionne l'adaptateur d'automatisation de bout en bout, et les éléments à configurer pour l'adaptateur :

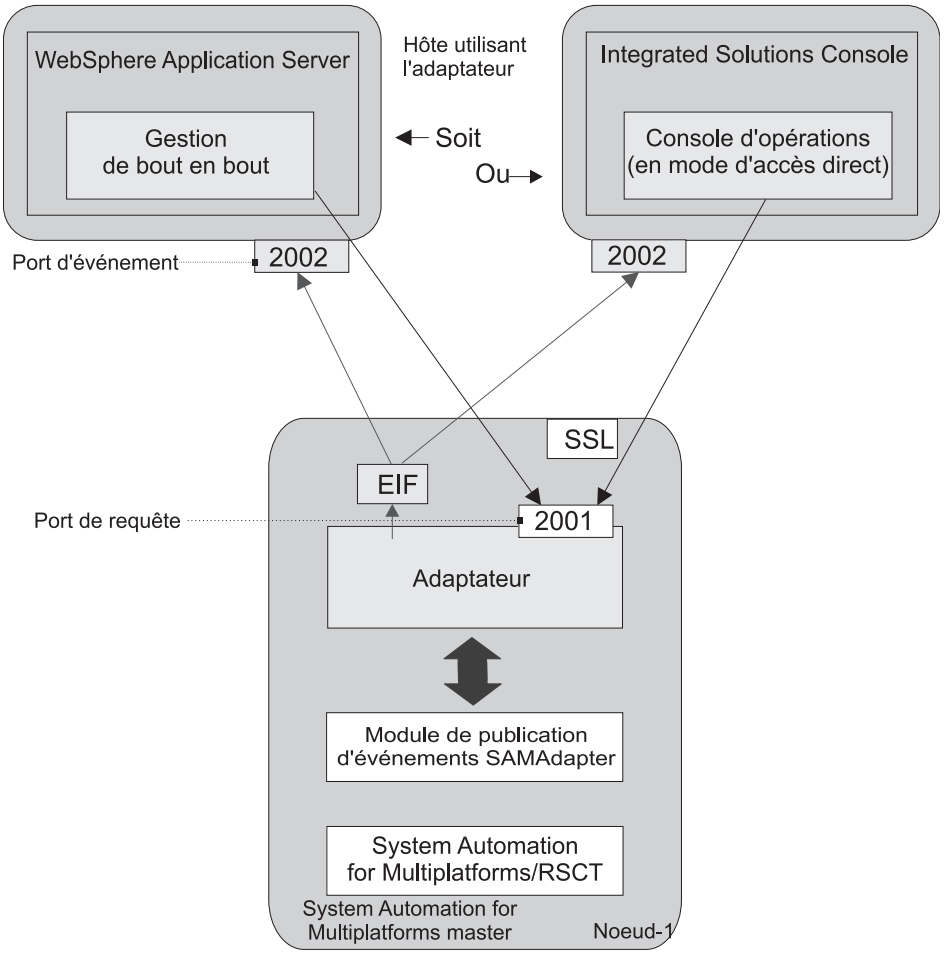

Figure 13. Présentation de l'environnement de l'adaptateur d'automatisation de bout en bout dans un cluster System Automation for Multiplatforms

Pour intégrer un domaine System Automation for Multiplatforms à l'environnement d'automatisation de bout en bout System Automation Application Manager, le produit System Automation Application Manager doit être installé. Pour plus d'informations sur la gestion de l'automatisation de bout en bout, voir le *System Automation for Multiplatforms - Guide d'administration et d'utilisation*.

Démarrage de la boîte de dialogue de configuration de l'adaptateur d'automatisation de bout en bout

Utilisez la commande `cfgsamadapter` pour démarrer la boîte de dialogue de configuration.

Remarque :

1. L'utilitaire `cfgsamadapter` est une application X Window System et doit être utilisé à partir d'un poste de travail intégrant des fonctions de serveur X Window System. Pour pouvoir utiliser la boîte de dialogue de configuration, vous devez disposer de la version 32-bit bits des modules d'installation X11. Sur certains systèmes d'exploitation, ces modules figurent sur les supports d'installation, mais ne font pas partie de l'installation standard.
   - Installez la version 32 bits des modules d'installation X11 sur les systèmes d'exploitation AIX et Linux, où la version 32 bits de System Automation for Multiplatforms est installée.
   - Installez la version 64 bits des modules d'installation X11 sur les systèmes d'exploitation Ubuntu et Linux, où la version 64 bits de System Automation for Multiplatforms est installée.
2. Sur les systèmes AIX, les conditions préalables à l'installation de adaptateur d'automatisation de bout en bout doivent être respectées : les modules **`SSL/SSH`** doivent être installés et le sous-système **`sshd`** doit être actif pour que la tâche de **Réplication** de la configuration de l'adaptateur soit réalisée.
3. Vous pouvez également configurer l'adaptateur d'automatisation de bout en bout en mode silencieux à l'aide d'un fichier d'entrée de propriétés. Si aucun serveur X11 n'est disponible, la configuration en mode silencieux est la seule méthode prise en charge sur ce système. Pour plus d'informations, voir «Configuration en mode silencieux», à la page 88.
4. Pour pouvoir utiliser la boîte de dialogue de configuration, vous devez vous connecter au système avec l'ID utilisateur `root` ou disposer des droits d'écriture dans les répertoires `/etc/opt/IBM/tsamp/sam/cfg` et `/etc/Tivoli`.

Exécutez la commande **`cfgsamadapter`** pour ouvrir la boîte de dialogue Configuration de l'adaptateur Tivoli System Automation. Le panneau principal de la boîte de dialogue s'affiche :

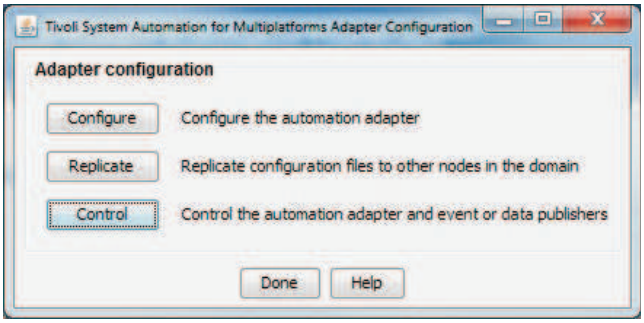

Figure 14. Panneau principal de la boîte de dialogue de configuration de l'adaptateur de bout en bout

Tâches de configuration :

1. Configuration de l'adaptateur d'automatisation de bout en bout (voir page «Configuration des paramètres de l'adaptateur d'automatisations», à la page 79)

2. Réplication des fichiers de configuration de l'adaptateur d'automatisation de bout en bout sur d'autres noeuds (voir page «Réplication des fichiers de configuration de l'adaptateur d'automatisation de bout en bout», à la page 87)
3. Contrôle de l'adaptateur d'automatisation et des diffuseurs de publications d'événements ou de données. Démarrage ou arrêt de l'adaptateur d'automatisation de bout en bout, du diffuseur de publications d'événements Tivoli Netcool/OMNIbus ou du diffuseur de publications de données de rapport. Pour plus d'informations sur l'adaptateur et les diffuseurs de publications, reportez-vous à la rubrique System Automation for Multiplatforms - Guide d'administration et d'utilisation.

Configuration des paramètres de l'adaptateur d'automatisations

Dans l'écran principal de la boîte de dialogue de configuration, cliquez sur **Configurer** pour afficher les onglets de configuration décrits dans les sections suivantes.

Onglet Adaptateur

Utilisez l'onglet Adaptateur pour configurer l'hôte de l'adaptateur.

Zones et commandes de l'onglet Adaptateur :

Nom d'hôte ou adresse IP
Nom d'hôte ou adresse IP du noeud sur lequel s'exécute l'adaptateur. Le nom est l'hôte local est utilisé par défaut. Pour utiliser une valeur différente du nom d'hôte local, désélectionnez la case **Utiliser le nom d'hôte local** pour autoriser l'édition de la zone d'entrée. Cela est par exemple utile si vous utilisez un deuxième réseau.

Impact sur la réplication des fichiers de configuration : Si vous utilisez le nom de l'hôte local, la fonction **Répliquer** vérifie que les noms d'hôte local respectifs sont utilisés sur chaque noeud cible de la réplication. Si vous entrez un autre nom d'hôte ou une autre adresse IP, la fonction **Répliquer** réplique cette valeur sur les autres nœuds du cluster. Dans ce cas, vous devez configurer l'hôte de l'adaptateur individuellement sur chaque noeud si vous ne voulez pas qu'il utilisent tous la même valeur. Pour plus d'informations, voir «Réplication des fichiers de configuration de l'adaptateur d'automatisation de bout en bout», à la page 87.

Numéro de port de demande
Spécifiez le numéro du port sur lequel l'adaptateur écoute les demandes de l'hôte de gestion d'automatisation de bout en bout. Le port par défaut est 2001.

Emplacement du pool de règles
Spécifiez le nom de chemin complet qualifié du répertoire contenant tous les fichiers de règles XML. Si vous utilisez System Automation Application Manager pour activer une règle d'automatisation System Automation for Multiplatforms, le pool de règles est requis. Définissez et créez le répertoire de pool de règles sur tous les nœuds du cluster. Ce paramètre est facultatif.

Cliquez sur **Avancé** pour spécifier le comportement de l'adaptateur lorsqu'il est en cours d'exécution :

Différé de l'arrêt de l'adaptateur
Définissez la plage de temps exprimée en secondes. L'arrêt de l'adaptateur est différé pendant cette plage de temps pour permettre à l'adaptateur de

transmettre correctement l'événement de retrait de domaine. La valeur par défaut est 5. Vous pouvez augmenter cette valeur pour les systèmes plus lents. Elle doit être comprise entre 3 et 60 secondes.

Intervalle d'activité du contact distant
Définissez la plage de temps, exprimée en secondes, au terme de laquelle l'adaptateur s'arrête si aucune connexion n'est établie avec l'hôte de gestion d'automatisation de bout en bout. L'hôte contacte régulièrement l'adaptateur pour vérifier si ce dernier est toujours en cours d'exécution. La valeur par défaut est 360. Si une valeur autre que 0 est indiquée, l'intervalle doit être un multiple de l'intervalle de vérification.

Si la valeur est définie sur 0, l'adaptateur est exécuté en continu et ne s'arrête jamais.

Intervalle entre les nouvelles tentatives de contact initial
Définissez la plage de temps exprimée en minutes. Dans cette plage de temps, l'adaptateur tente de contacter l'hôte de gestion de l'automatisation de bout en bout jusqu'à ce qu'il y parvienne ou que le temps imparti soit écoulé. La valeur par défaut est 0, ce qui signifie que l'adaptateur tente de contacter l'hôte indéfiniment.

Activer la mise en cache d'événements EIF
Cochez cette case pour activer la mise en cache d'événements.

Intervalle de tentative de reconnexion EIF
Définissez la plage de temps exprimée en secondes. Il s'agit du délai observé par l'adaptateur avant de tenter de rétablir la connexion à l'hôte de gestion d'automatisation de bout en bout après l'interruption de la connexion. La durée par défaut est 30.

Onglet Hôte utilisant l'adaptateur

L'onglet Hôte utilisant l'adaptateur permet de configurer l'hôte du gestionnaire d'automatisation de bout en bout auquel se connecte l'adaptateur.

Zones de l'onglet Hôte utilisant l'adaptateur :

Nom d'hôte ou adresse IP
Nom ou adresse IP de l'hôte sur lequel le gestionnaire d'automatisation de bout en bout s'exécute.

Autre hôte
Une valeur pour cette zone est facultative. Si vous avez défini une configuration de reprise après incident sur deux sites différents pour System Automation Application Manager, le gestionnaire d'automatisation de bout en bout peut s'exécuter sur l'un ou l'autre site. Pour prendre en charge une telle configuration, indiquez également le nom d'hôte ou l'adresse IP du second site. En cas de basculement du site d'Application Manager, cela permet de s'assurer que l'adaptateur permute de manière transparente vers la nouvelle instance active du gestionnaire d'automatisation de bout en bout qui deviendra alors la cible de l'envoi d'événements.

Numéro de port d'événement
Port sur lequel le gestionnaire d'automatisation de bout en bout écoute les événements de l'adaptateur d'automatisation. Le numéro de port doit correspondre au numéro de port spécifié comme numéro de port d'événement lors de la configuration du domaine du gestionnaire d'automatisation de bout en bout. Le port par défaut est 2002.

Remarque : Si la communication entre l'adaptateur d'automatisation de bout en bout et l'hôte du gestionnaire d'automatisation de bout en bout utilise la version IPv6, les restrictions ci-dessous s'appliquent.

Pour la communication de l'adaptateur vers l'hôte utilisant l'adaptateur :

1. Si un nom d'hôte IPv6 est spécifié dans la configuration de l'hôte du gestionnaire d'automatisation de bout en bout, le serveur DNS doit être configuré pour renvoyer des enregistrements IPv6 uniquement.
2. Si le serveur DNS est configuré pour renvoyer des enregistrements IPv4 et IPv6, seule l'adresse IPv4 est utilisée. Si vous souhaitez utiliser IPv6, spécifiez de manière explicite l'adresse IPv6 à la place du nom d'hôte dans la configuration de l'hôte du gestionnaire d'automatisation de bout en bout.

Pour la communication de l'hôte du gestionnaire d'automatisation de bout en bout vers l'adaptateur :

1. Si un nom d'hôte IPv6 est spécifié dans la configuration de l'hôte utilisant l'adaptateur, le serveur DNS doit être configuré pour le renvoi des enregistrements IPv6 uniquement.
2. Si le serveur DNS est configuré pour renvoyer des enregistrements IPv4 et IPv6, seule l'adresse IPv4 est utilisée. Si vous souhaitez utiliser IPv6, vous devez spécifier explicitement l'adresse IPv6 et non le nom d'hôte lors de la configuration de l'hôte utilisant l'adaptateur.

Utilisez la commande `host -n -a <ipv6_hostname>` pour vérifier les enregistrements de recherche DNS.

Onglet Génération de rapports

L'onglet Génération de rapports permet de configurer les paramètres permettant de collecter les données de rapport dans la base de données System Automation Application Manager.

Une fois que vous avez configuré la base de données des rapports, vous devez démarrer le diffuseur de publications de données de rapport.

Remarque :

1. La fonction de génération de rapports fait partie intégrante du produit System Automation Application Manager jusqu'à la version 3.2.2.
2. Veillez à désactiver la génération de rapports avant de désinstaller System Automation Application Manager de l'hôte de gestion de l'automatisation de bout en bout.

   Les installations de bases de données locales de System Automation Application Manager sont supprimées pendant la désinstallation. Dans ce cas, arrêtez le diffuseur de publications de données de rapport.

Pour démarrer ou arrêter le diffuseur de publications de données de rapport, reportez-vous à la rubrique *System Automation for Multiplatforms - Guide d'administration et d'utilisation* ou utilisez les commandes suivantes :

```
samctrl -e JDBC or samctrl -d JDBC
```

Si vous souhaitez collecter les données de rapport dans la base de données DB2 deSystem Automation Application Manager, cochez la case **Activer la collecte de données de rapport**. Sinon, désélectionnez cette case. Les zones de saisie de cet onglet sont alors désactivées.

Zones de l'onglet Génération de rapports :

Nom ou adresse IP du serveur DB2

Nom d'hôte ou adresse IP du serveur DB2 qui héberge la base de données des données de rapport. La véritable fonction de génération de rapports fait partie intégrante du produit System Automation Application Manager. Le serveur DB2 doit se trouver sur le système sur lequel se trouve la base de données DB2 de System Automation Application Manager.

Si vous ne précisez pas cette valeur, la valeur indiquée pour l'hôte System Automation Application Manager utilisant l'adaptateur dans l'onglet Hôte utilisant l'adaptateur est utilisée par défaut. Si vous utilisez une base de données DB2 éloignée pour la base de données du System Automation Application Manager, spécifiez le nom d'hôte ou l'adresse IP de ce système DB2 éloigné.

Remarque : Si le serveur DB2 s'exécute sous z/OS, vérifiez que le fichier `db2jcc_license_cisuz.jar` est disponible sur chaque noeud du cluster System Automation for Multiplatforms. En effet, ce fichier contient la licence de connexion à DB2 sous z/OS à partir de machines non-z/OS.

Il se trouve dans le répertoire WebSphere Application Server utilisé pour System Automation Application Manager. Recherchez le fichier dans l'arborescence suivante :

```
<RACINE_INSTALLATION_WAS>/deploytool/itp/plugins
```

Copiez le fichier dans le répertoire `/opt/IBM/tsamp/sam/lib` sur chaque noeud du cluster System Automation for Multiplatforms. Vérifiez que vous disposez d'un contrat de licence DB2.

Autre serveur DB2

Une valeur pour cette zone est facultative. Si vous avez configuré une configuration de reprise après incident sur deux sites différents pour System Automation Application Manager, le gestionnaire d'automatisation de bout en bout peut être exécuté sur l'un ou l'autre de ces sites. Pour prendre en charge une telle configuration, indiquez dans cette zone le nom d'hôte ou l'adresse IP de System Automation Application Manager sur le second site. En cas de basculement du site d'Application Manager, l'adaptateur passe automatiquement à la nouvelle instance active du gestionnaire d'automatisation de bout en bout qui deviendra alors la cible des données de rapport collectées. Les valeurs des paramètres ci-après sont utilisées pour les deux serveurs DB2. Si la base de données se trouve sur le même système que le gestionnaire d'automatisation de bout en bout, spécifiez la valeur que vous avez utilisée pour l'autre hôte System Automation Application Manager qui utilise l'adaptateur.

Si vous utilisez une base de données DB2 éloignée comme base de données du System Automation Application Manager, ne renseignez pas cette zone.

Remarque : Si vous spécifiez un autre serveur DB2, vous devez configurer la fonction DB2 Automatic Client Reroute. Cela permettra à la fonction de génération de rapports de toujours alimenter en données de rapport l'instance principale de la fonction de reprise sur incident haute disponibilité de DB2. Pour savoir comment configurer cette fonction, reportez-vous à la documentation de DB2.

Exemple :

La fonction de reprise sur incident haute disponibilité de DB2 est configurée pour la base de données `eautodb` sur les hôtes `lnxcm5x` et `lnxcm6x`. Les ports DB2 sont les port 50000 sur ces deux hôtes. Pour configurer la fonction Automatic Client pour les deux hôtes, exécutez les commandes suivantes :

- Sur lnxcm5x :

  ```
  db2 update alternate server for database eautodb using host name
  lnxcm6x port 50001
  ```

- Sur lnxcm6x :

  ```
  db2 update alternate server for database eautodb using host name
  lnxcm5x port 50001
  ```

Nom de la base de données DB2
Nom de la base de données DB2 de System Automation Application Manager, dans laquelle les données de rapport sont stockées.

Nom du schéma DB2
Nom du schéma utilisé pour les tables de base de données utilisées pour stocker les données de rapport. Modifiez la valeur de ce paramètre uniquement si la base de données DB2 de System Automation Application Manager se trouve sur un système z/OS. Il peut être nécessaire de contrôler le nom du schéma afin d'identifier de manière unique les tables de base de données de votre installation DB2.

Port DB2
Numéro du port utilisé pour accéder à la base de données DB2 de System Automation Application Manager dans laquelle sont stockées les données de rapport. Le port par défaut est 50001.

ID utilisateur
ID utilisateur permettant d'accéder à la base de données DB2 de System Automation Application Manager,dans laquelle les données de rapport sont stockées.

Mot de passe
Mot de passe permettant d'accéder à la base de données DB2 de System Automation Application Manager, dans laquelle les données de rapport sont stockées.

Cliquez sur **Modifier** pour modifier le mot de passe.

Remarque : Pensez à mettre à jour le mot de passe configuré chaque fois que le mot de passe associé à la base de données DB2 est modifié. Si mot de passe configuré ne correspond pas au mot de passe de la base DB2, les événements ne seront pas enregistrés dans la base de données.

Onglet Publication d'événement

L'onglet Publication d'événement permet de configurer les paramètres de publication des événements EIF vers Tivoli Netcool/Omnibus.

Commandes et zones de l'onglet Publication d'événement :

Publication des événements OMNIbus

Activer la publication des événements EIF par OMNIbus
Cochez cette case pour que les événements EIF soient envoyés à l'hôte où s'exécute OMNIbus Probe for Tivoli EIF. Si cette case n'est pas cochée, les autres zones de cet onglet sont toutes désactivées. Si vous activez ou désactivez la publication d'événement EIF, veillez à démarrer ou arrêter le

diffuseur de publications d'événements correspondant. Pour démarrer ou arrêter le diffuseur de publications d'événements EIF, reportez-vous à la rubrique *System Automation for Multiplatforms - Guide d'administration et d'utilisation* ou utilisez les commandes suivantes :

```
samctrl -e TEC or samctrl -d TECs
```

Remarque : Pour des raisons de compatibilité, un serveur Tivoli Enterprise Console et un port peuvent également être configurés.

Serveur d'événements

Nom d'hôte ou adresse IP
Nom d'hôte ou adresse IP de l'hôte où OMNIbus Probe for Tivoli EIF s'exécute. Vous pouvez spécifier jusqu'à huit valeurs séparées par une virgule. Le premier emplacement correspond au serveur d'événements principal, tandis que les autres correspondent à des serveurs secondaires à utiliser dans l'ordre indiqué lorsque le serveur principal est arrêté.

Numéro de port
Numéro de port utilisé par OMNIbus Probe for Tivoli EIF pour écouter les événements EIF. Si vous utilisez le mappage des ports, vous pouvez spécifier `0` comme numéro de port.

Filtre d'événements

Publier les événements EIF causés par :

Modifications de configuration des relations
Cochez cette case pour que tous les événements EIF causés par l'ajout, la suppression et la modification de relations soient envoyés au serveur d'événements. Sinon, les événements de modification de configuration pour les relations sont filtrés.

Modifications de configuration des ressources
Cochez cette case pour que tous les événements EIF causés par l'ajout, la suppression et la modification de ressources soient envoyés au serveur d'événements. Sinon, les événements de modification de configuration pour les ressources sont filtrés.

Ajout et suppression de demandes
Cochez cette case pour que les événements EIF causés par l'ajout et la suppression de demandes soient envoyés au serveur d'événements. Sinon, les événements pour l'ajout ou la suppression de demandes sont filtrés.

Modifications d'état des ressources pour
Cochez cette case pour que les événements EIF liés aux modifications d'état des ressources soient envoyés au serveur d'événements. Sinon, tous les événements de modification d'état des ressources sont filtrés. Suivant la gravité, sélectionnez l'un des boutons d'option pour définir les événements de modification d'état qui seront publiés.

Définition de filtres supplémentaires :

Les filtres d'événements que vous pouvez activer ou désactiver dans cet onglet sont les filtres prédéfinis qui sont fournis avec System Automation for Multiplatforms. Pour définir des filtres supplémentaires, modifiez manuellement le fichier de propriétés de configuration correspondant :

```
/etc/Tivoli/TECPublisher.conf
```

Pour modifier un filtre prédéfini, ajoutez un filtre et désactivez le filtre prédéfini. Si les modifications de configuration sont appliquées par l'utilitaire de configuration `cfgsamadapter`, les filtres que vous avez ajoutés sont conservés.

Onglet Sécurité

L'onglet Sécurité vous permet de configurer la sécurité de l'interface entre l'hôte utilisant l'adaptateur et l'hôte de gestion de bout en bout.

Sélectionnez **Activer SSL** si vous souhaitez utiliser le protocole SSL (Secure Socket Layer) pour les communications entre l'adaptateur d'automatisation et l'hôte qui utilisant l'adaptateur. Si vous cochez cette case, les zones de saisie suivantes doivent être complétées.

Commandes et zones de l'onglet Sécurité :

Magasin de certificats
: Nom du fichier de stockage des certificats pour la couche SSL. Le nom du fichier peut contenir plusieurs caractères point. Cliquez sur **Parcourir** pour sélectionner un fichier.

Magasin de clés
: Nom du fichier de stockage de clés utilisé pour la couche SSL. Le nom du fichier peut contenir plusieurs caractères point. Cliquez sur **Parcourir** pour sélectionner un fichier.

Mot de passe du magasin de clés
: Mot de passe du fichier de stockage de clés. Cliquez sur **Modifier** pour modifier le mot de passe.

  Remarque : Si le fichier de clés certifiées est situé dans un autre fichier que le fichier de clés, les mots de passe des fichiers doivent être identiques.

Alias de certificat
: Nom d'alias du certificat que le serveur doit utiliser.

Appliquer l'authentification des utilisateurs
: Cochez la case **Appliquer l'authentification des utilisateurs** pour activer l'authentification des utilisateurs avec le `module PAM (Pluggable Access Module)`.

  Si vous utilisez System Automation Application Manager pour gérer aussi les règles XML de System Automation for Multiplatforms, vous devez obligatoirement sélectionner **Appliquer l'authentification des utilisateurs.**

Service PAM
: Nom du service Pluggable Access Module qui détermine les vérifications effectuées pour valider les utilisateurs, selon le système d'exploitation sur lequel s'exécute l'adaptateur.
  - Pour toute distribution Linux SUSE, un fichier dans le répertoire `/etc/pam.d`
  - Pour toute distribution Linux RedHat, une entrée dans le fichier `/etc/pam.conf`
  - Pour AIX, une entrée dans le fichier `/etc/pam.conf`

Onglet Journal d'événements

L'onglet Journal d'événements permet de spécifier le niveau de consignation des messages, le niveau de traçage ainsi que les premières options des paramètres FFDC (First Failure Data Capture). Vous pouvez modifier les paramètres de manière permanente ou temporaire.

L'onglet Journal d'événements affiche toujours les valeurs définies dans le fichier de configuration.

L'onglet Journal d'événements permet d'effectuer les tâches suivantes :

Modifier temporairement les paramètres
Suivez cette procédure :

1. Effectuez les changements nécessaires dans l'onglet.
2. Cliquez sur **Sauvegarder**.

Résultats : Les paramètres du fichier de configuration sont mis à jour. Redémarrez l'adaptateur pour que les modifications soient prises en compte.

Modifier provisoirement les paramètres
Procédez comme suit après s'être assuré que l'adaptateur est exécuté :

1. Effectuez les changements nécessaires dans l'onglet.
2. Cliquez sur **Appliquer**.

Résultats : Les nouveaux paramètres prennent effet immédiatement. Ils ne sont pas enregistrés dans le fichier de configuration. Si l'adaptateur n'est pas actif, vous recevez un message d'erreur.

Rétablir les paramètres permanents
Si vous avez modifié les paramètres de manière provisoire, effectuez les opérations suivantes pour rétablir les paramètres permanents définis dans le fichier de configuration ou si vous n'êtes pas sûr des paramètres actifs pour l'adaptateur :

1. Appelez la boîte de dialogue de configuration et ouvrez l'onglet Journal d'événements. L'onglet Journal d'événements affiche les valeurs qui sont actuellement définies dans le fichier de configuration.
2. Cliquez sur **Appliquer** pour activer les paramètres.

Résultats : Les paramètres prennent effet immédiatement. Si l'adaptateur n'est pas actif, vous recevez un message d'erreur.

Commandes et zones de l'onglet Journal d'événements :

Taille maximale du fichier de trace/journal
Espace disque maximal exprimé en Ko que peut occuper un fichier journal. Si la limite est atteinte, un autre fichier journal est créé. Il peut exister au maximum deux fichiers journaux. Par conséquent, le fichier le moins récent est remplacé lorsque les deux fichiers sont saturés. La taille de fichier maximale par défaut est de 1024 Ko.

Niveau de consignation des messages
Sélectionnez le **Niveau de consignation des messages**, selon la gravité des messages que vous souhaitez consigner.

Niveau de consignation de la fonction de trace
Sélectionnez le **Niveau de consignation de la fonction de trace**, selon la gravité des incidents que vous souhaitez consigner.

Niveau d'enregistrement FFDC
Sélectionnez le niveau d'enregistrement FFDC, selon la gravité des incidents pour lesquels vous souhaitez collecter les données FFDC.

Espace disque maximum FFDC
Indiquez l'espace disque maximal en octets utilisé par les traces d'outil de

diagnostic de premier niveau (FFDC) écrites dans le répertoire de trace FFDC. L'espace par défaut est de 10485760 octets (10 Mo).

Règle en cas d'espace dépassé FFDC
Sélectionnez l'une des options suivantes :

Ignorer
Envoyer un avertissement, mais ne pas appliquer la limitation d'espace disque FFDC.

Suppression automatique
Supprime automatiquement les fichiers FFDC afin d'appliquer la limitation de l'espace disque FFDC. Il s'agit de la règle de dépassement d'espace par défaut.

Suspendre
Interrompre les actions FFDC jusqu'à ce que de l'espace disque soit libéré manuellement.

Mode de filtrage des ID message FFDC
Sélectionnez l'une des options suivantes :

Passthru
Tous les événements à enregistrer qui comportent des messages spécifiés dans la liste des ID de message passeront à travers le filtre et les données FFDC seront enregistrées. Il s'agit du mode de filtrage par défaut.

Bloquer
Tous les événements à enregistrer qui comportent des messages spécifiés dans la liste des ID de message seront bloqués.

Liste des ID de message FFDC
ID de message qui détermine les événements de journal pour lesquels des données FFDC sont enregistrées en fonction du mode de filtrage défini. La comparaison des ID de message tient compte de la casse. Chaque ID de message doit se trouver sur une nouvelle ligne. Les caractères génériques, comme *E (pour tous les messages d'erreur), sont admis.

Sauvegarde de la configuration

Cliquez sur **Enregistrer** dans la fenêtre de configuration pour sauvegarder vos modifications dans les fichiers de configuration de l'adaptateur.

Si des entrées sont manquantes ou si une valeur n'est pas comprise dans la plage admise (par exemple, un numéro de port), un message d'erreur est affiché. Une fois cette opération terminée, la fenêtre Etat de mise à jour de la configuration affiche la liste des fichiers de configuration et leur état de mise à jour. Redémarrez l'adaptateur pour que les modifications prennent effet.

Réplication des fichiers de configuration de l'adaptateur d'automatisation de bout en bout

Répliquez les fichiers de configuration de l'adaptateur d'automatisation de bout en bout sur les autres noeuds du domaine.

Cliquez sur **Répliquer** dans le panneau principal de la boîte de dialogue de configuration (voir «Démarrage de la boîte de dialogue de configuration de l'adaptateur d'automatisation de bout en bout», à la page 78). La fenêtre Réplication des fichiers de configuration s'affiche.

Pour distribuer (répliquer) les fichiers de configuration de l'adaptateur d'automatisation sur les noeuds restants du domaine homologue RSCT, procédez de la manière suivante :

1. Sélectionnez les fichiers de configuration que vous souhaitez répliquer ou cliquez sur **Sélectionner tout** pour sélectionner tous les fichiers de configuration de la liste.
   - Si (1) le fichier `sam.adapter.ssl.properties` se trouve parmi les fichiers sélectionnés et (2) que les fichiers de clés et les fichiers de clés certifiées SSL que vous avez configurés dans l'onglet Sécurité de la configuration de l'adaptateur existent sur le noeud source de réplication, ces fichiers sont également répliqués.
   - Vérifiez que le répertoire dans lequel se trouvent les fichiers sur le noeud source de réplication existent aussi sur tous les noeuds cible.
2. Cliquez sur **Sélectionner tout** sous la liste des noeuds cible de la réplication pour vous assurer que la configuration de l'adaptateur soit identique sur tous les noeuds.
3. Entrez l'ID utilisateur et le mot de passe des noeuds cible dans lesquels vous souhaitez répliquer les fichiers.
4. Démarrez le processus en cliquant sur **Répliquer**.

La réplication peut prendre un certain temps. Lors de cette opération, le bouton **Répliquer** est en retrait et grisé. Lorsque la réplication est terminée, l'état de réplication de chaque fichier de configuration est affiché.

Mise en œuvre de la haute disponibilité de l'adaptateur d'automatisation de bout en bout

Dans un cluster Tivoli System Automation contenant plusieurs nœuds, l'adaptateur d'automatisation de bout en bout doit être en mode haute disponibilité.

La communication vers la console d'opérations System Automation Application Manager reste opérationnelle pendant les périodes d'indisponibilité et de maintenance des nœuds du cluster.

Comme le montre la rubrique «Configuration de l'adaptateur d'automatisation de bout en bout», à la page 76, l'adaptateur d'automatisation est connecté au noeud maître de System Automation. Grâce à l'infrastructure des clusters, le noeud maître est toujours disponible, et par conséquent, de manière implicite, l'adaptateur l'est toujours aussi sur le noeud maître. A partir de la version 4.1.0.0 de System Automation for Multiplatforms, aucune configuration de règle d'automatisation n'est nécessaire pour rendre l'adaptateur hautement disponible.

Configuration en mode silencieux

Vous pouvez configurer l'adaptateur d'automatisation de bout en bout à l'aide de la configuration en mode silencieux.

L'outil de configuration en mode silencieux permet de configurer l'adaptateur d'automatisation de bout en bout sans passer par la boîte de dialogue de configuration. Dans ce cas, vous n'avez pas besoin d'une session X Windows.

Configurez l'adaptateur d'automatisation de bout en bout en modifiant les valeurs des paramètres de configuration dans le fichier de propriétés associé. Si vous utilisez la configuration en mode silencieux, il n'est pas nécessaire qu'une session X Window soit disponible.

Vous devez d'abord démarrer l'outil de configuration pour générer un fichier de propriétés en entrée destiné au mode silencieux avant de pouvoir effectuer une mise à jour de la configuration. Pour plus d'informations, voir «Configuration de l'adaptateur d'automatisation de bout en bout», à la page 76.

Utilisation du mode silencieux

Informations supplémentaires sur les principales tâches si vous travaillez dans le mode de configuration en mode silencieux.

Pour utiliser l'outil de configuration en mode silencieux, suivez la procédure ci-après pour chacun des composants à configurer :

1. Générez le fichier de propriétés d'entrée en mode silencieux ou localisez-le s'il existe déjà (voir «Fichier de propriétés d'entrée en mode silencieux», à la page 90).
2. Modifiez les valeurs des paramètres dans le fichier (voir «Modification du fichier de propriétés d'entrée», à la page 91).
3. Lancez l'outil de configuration en mode silencieux pour mettre à jour les fichiers de configuration cible (voir «Démarrage de la configuration en mode silencieux».
4. Si la configuration dans l'outil de configuration ne se termine pas correctement, corrigez les éventuelles erreurs signalées (voir «Résultat du mode silencieux», à la page 91) et lancez à nouveau l'outil de configuration.

Pour certaines tâches, la charge de configuration en mode silencieux n'existe pas. Si vous ne souhaitez pas utiliser les boîtes de dialogue de configuration, vous devez effectuer ces tâches manuellement. Pour plus d'informations, voir «Tâches de configuration à accomplir manuellement».

Tâches de configuration à accomplir manuellement

Certaines tâches de configuration appelées en mode dialogue en cliquant sur le bouton de fonction correspondant dans la fenêtre du tableau de bord ne sont pas prises en charge par le mode de configuration silencieux.

Si vous ne souhaitez pas utiliser la boîte de dialogue de configuration, vous devez effectuer manuellement les tâches suivantes :

1. **Repliquer les fichiers de configuration**

   Si le domaine System Automation for Multiplatforms est constitué de plusieurs noeuds, répliquez manuellement les fichiers de configuration de l'adaptateur d'automatisation de bout en bout sur les autres noeuds du domaine. Répliquez les fichiers de configuration en exécutant l'outil de configuration en mode silencieux avec des fichiers de propriétés en entrée identiques sur chaque noeud du domaine.
2. **Contrôler l'adaptateur d'automatisation et les diffuseurs de publications.**
   - Utiliser la commande `samadapter {start|stop}` pour démarrer ou arrêter l'adaptateur d'automatisation de bout en bout.
   - Utiliser la commande TEC `samctrl {-e|-d}` pour démarrer ou arrêter le diffuseur de publications d'événements Tivoli Netcool/OMNIbus.
   - Utiliser la commande JDBC `samctrl {-e|-d}` pour démarrer ou arrêter le diffuseur de publications de données de rapport.

Démarrage de la configuration en mode silencieux

Lancez la commande **`cfgsamadapter -s`** pour démarrer la configuration en mode silencieux.

Démarrez la configuration en mode silencieux pour l'adaptateur d'automatisation de bout en bout :

- Pour utiliser l'outil de configuration de l'adaptateur System Automation en mode silencieux, vous devez avoir accès en écriture aux répertoires `/etc/opt/IBM/tsamp/sam/cfg` et `/etc/Tivoli`.
- Entrez la commande `cfgsamadapter -s`.

Pour plus d'informations sur la commande `cfgsamadapter`, voir *Tivoli System Automation for Multiplatforms Guide de référence*.

Fichier de propriétés d'entrée en mode silencieux

Générez un fichier d'entrée de propriétés en mode silencieux à partir des valeurs actuellement définies. Utilisez ce fichier pour modifier les paramètres de configuration en mode silencieux.

Générez un fichier d'entrée de propriétés en mode silencieux à partir des valeurs actuellement définies dans les fichiers de configuration cible correspondants. Les avantages sont les suivants :

- Vous pouvez générer des fichiers de propriétés immédiatement après l'installation, et avant de commencer la personnalisation.
- Si vous effectuez la personnalisation à l'aide de la boîte de dialogue de configuration et en mode silencieux, vous pouvez commencer par générer un fichier d'entrée à jour avant d'appliquer les modifications en mode silencieux.
- Vous pouvez rétablir facilement la configuration après une suppression accidentelle du fichier de propriétés d'entrée en mode silencieux.

Pour générer un fichier de propriétés d'entrée en mode silencieux, utilisez l'une des options suivantes lorsque vous démarrez la configuration en mode silencieux :

-g Génère le fichier d'entrée de propriétés uniquement s'il n'existe pas déjà.

-gr
Génère le fichier d'entrée de propriétés en le remplaçant s'il existe déjà.

-l *emplacement*
Le fichier de propriétés d'entrée pour la configuration en mode silencieux se trouve dans le répertoire qui est spécifié avec *emplacement*. Si `-l` est omis, le fichier de propriétés en entrée se trouve dans le répertoire par défaut `/etc/opt/IBM/tsamp/sam/cfg`.

Tableau 22. Fichiers de propriétés en entrée générés.

Commande de configuration	Fichier de propriétés en entrée pour le mode silencieux	
cfgsamadapter -s -g | -gr	`/etc/opt/IBM/tsamp/sam/cfg/silent.samadapter.properties`	
cfgsamadapter -s -g | -gr -l *emplacement*	*emplacement*`/silent.samadapter.properties`	

Si vous mettez à jour les paramètres de configuration en mode silencieux, le fichier de propriétés du mode silencieux est utilisé comme fichier d'entrée pour la tâche de mise à jour. Si vous souhaitez que l'utilitaire de configuration extraie le fichier en entrée d'un emplacement autre que le répertoire `etc/opt/IBM/tsamp/sam/cfg`, utilisez l'option **-l** *emplacement*.

Modification du fichier de propriétés d'entrée

Modifiez les valeurs du fichier de propriétés en entrée pour faire passer la configuration en mode silencieux.

Les fichiers de propriétés d'entrée qui sont créés pour chaque composant contiennent des paires mot clé-valeur de paramètres de configuration. Pour faciliter le passage d'un noeud à l'autre et limiter le risque d'erreur lors de la modification du fichier de propriétés, la structure, la terminologie et les formulations utilisées dans le fichier de propriétés en mode silencieux sont identiques à la structure, à la terminologie et aux formulations de la boîte de dialogue de configuration.

Le nom des onglets, par exemple Adaptateur, ou des boutons, par exemple **Avancé...**, de la boîte de dialogue de configuration sont utilisés comme identificateurs dans le fichier de propriétés. Exemple :

```
# ============================================================================
# ... Adaptateur
⋮
# ============================================================================
# ... Avancé
```

Tous les noms de zone figurant dans la boîte de dialogue de configuration, par exemple **Numéro de port de requête**, sont présents dans le fichier de propriétés. Ils sont suivis d'une courte description de la zone et de son mot clé. Exemple :

```
#     ----------------------------------------------------------------------
#     ... Numéro de port de demande
#         Port de l'adaptateur d'automatisation utilisé pour recevoir les
#         demandes de l'hôte qui utilise l'adaptateur
adapter-request-port=2001
#
```

Pour modifier le fichier de propriétés, repérez les mots clés associé à la valeur à modifier et effectuez la modification.

Si vous indiquez une valeur vide pour un mot clé obligatoire ou mettez le mot clé en commentaire, la valeur actuellement définie dans le fichier de configuration cible reste inchangée.

Remarque :

1. Si un mot clé est spécifié à plusieurs reprises, la valeur de sa dernière occurrence dans le fichier est utilisée.
2. Chaque valeur doit être définie sur une seule ligne.

Résultat du mode silencieux

Examinez la sortie qui est générée par l'outil de configuration en mode silencieux.

Le lancement de l'outil de configuration en mode silencieux génère un résultat proche de celui affiché par la boîte de dialogue de configuration. Les types de sortie suivants peuvent être générés :

Pas de mise à jour

Il n'existe aucune mise à jour de configuration à enregistrer. Tous les paramètres de tous les fichiers de configuration cible correspondent déjà aux paramètres d'entrée en mode silencieux spécifiés. Aucune erreur n'a été détectée lors de la vérification des paramètres d'entrée en mode silencieux. Si des informations supplémentaires sont disponibles ou si des conditions d'avertissement sont détectées, les informations et les alertes sont signalées. Si des avertissements sont signalés, l'outil de configuration

émet le code retour "1" au lieu de "0". Vous pouvez être amené à faire ces observations lors du démarrage d'une configuration en mode silencieux, par exemple dans un script de shell.

Opération réussie
Au moins un des fichiers de configuration cible est mis à jour et tous les fichiers de configuration et leur état de mise à jour sont répertoriés. Aucune erreur n'a été détectée lors de la vérification des paramètres d'entrée en mode silencieux. Si des informations supplémentaires sont disponibles ou si des conditions d'avertissement sont détectées, les informations et les alertes sont signalées. Si des avertissements sont signalés, l'outil de configuration émet le code retour "1" au lieu de "0". Vous pouvez être amené à faire ces observations lors du démarrage d'une configuration en mode silencieux, par exemple dans un script de shell.

Echec de l'opération
Aucun fichier de configuration cible n'est mis à jour. Toute erreur détectée lors de la vérification des paramètres d'entrée en mode silencieux est signalée. L'outil de configuration s'arrête lorsque le code retour "2" est renvoyé.

Génération d'un fichier de propriétés d'entrée en mode silencieux
Les valeurs des fichiers de configuration cible sont utilisées pour générer le fichier d'entrée. Aucun fichier de configuration cible n'est mis à jour.

Erreur irréparable
Des messages d'erreur indiquant la raison de l'erreur sont générés. L'outil de configuration s'arrête lorsqu'un code retour supérieur à "2" est renvoyé.

Détection des incidents liés aux interfaces réseau

Si vous exécutez un cluster à un noeud ou à deux noeuds, une configuration supplémentaire est nécessaire pour détecter les incidents liés à l'interface de réseau.

Le logiciel du cluster essaie périodiquement de contacter chaque interface réseau du cluster. Si la tentative de contact d'une interface échoue sur un noeud d'un cluster à deux noeuds, l'interface située sur l'autre noeud est également marquée comme hors ligne, car elle ne reçoit pas de réponse de la part de son homologue.

Pour éviter tout comportement de ce type, le logiciel du cluster devra être configuré pour contacter une instance du réseau hors du cluster. Vous pouvez utiliser la passerelle de noeud par défaut du sous-réseau dans lequel se trouve l'interface.

Créez le fichier suivant sur chaque noeud :

```
/var/ct/cfg/netmon.cf
```

Chaque ligne de ce fichier contient le nom système ou l'adresse IP de l'instance du réseau externe. Les adresses IP peuvent être exprimées en notation décimale.

Exemple d'un fichier `netmon.cf` :

```
# Passerelle par défaut pour toutes les interfaces du sous-réseau 192.168.1.0
192.168.1.1

# Passerelle par défaut pour toutes les interfaces du sous-réseau 192.168.2.0
gw.de.ibm.com
```

Utilisation d'Ethernet virtuel sur des systèmes Power Systems

La décision concernant l'état des adaptateurs réseau est prise selon que le trafic réseau peut être détecté ou non sur l'adaptateur local, par exemple si la carte locale ou distante est endommagée. Le trafic réseau est reflété par le nombre d'octets entrants de l'interface.

Si VIO (Virtual I/O) est utilisé, le test n'est plus fiable parce qu'il n'est pas possible de distinguer si le trafic entrant vient du serveur ou du client VIO. La partition logique n'est pas capable de distinguer une carte virtuelle d'une carte réelle. Pour résoudre ce problème, la bibliothèque `netmon` prend en charge jusqu'à 32 cibles par adaptateur réseau local. Si vous pouvez envoyer une commande ping à l'une de ces cibles, l'adaptateur local est considéré comme opérationnel. Les cibles peuvent être indiquées dans le fichier `netmon.cf` avec le mot clé `!REQD`.

```
!REQD <propriétaire><cible>
```

- `!REQD` : Valeur de chaîne. Pas d'espaces à gauche. Toujours au début d'une ligne.
- `<propriétaire>` : Définit l'interface. Le `<propriétaire>` surveille l'adaptateur et détermine l'état selon qu'il peut envoyer une commande ping à l'une des cibles définies sur une ligne sous le `<propriétaire>`. Le `<propriétaire>` peut être défini sous la forma d'un nom d'hôte, d'une adresse IP ou d'un nom d'interface. Si le nom d'hôte ou l'adresse IP est spécifié, il doit faire référence au nom ou à l'adresse IP de départ. Aucun alias de service n'est autorisé. Si le nom d'hôte est défini, il doit pouvoir être résolu en adresse IP. Sinon, la ligne est ignorée. Le mot-clé `!ALL` désigne tous les adaptateurs.
- `<cible>` : Adresse IP ou nom d'hôte à laquelle le `<propriétaire>` doit envoyer une commande ping. La cible d'un nom d'hôte doit pouvoir être résolue en adresse IP pour être utilisée pour les entrées de `netmon.cf` .

Exécution sous Linux on System z sous z/VM

Outre la création du fichier `netmon.cf`, vous devez désactiver la diffusion pour tous les groupes de communication lorsque le système utilise System Automation for Multiplatforms on Linux on System z dans un environnement z/VM. Le mécanisme de signal de présence RSCT exécute régulièrement des commandes ping de diffusion, en particulier lorsqu'aucune interface réseau n'est disponible. Cette fonction permet de savoir si l'interface réseau envoyant les commandes ping de diffusion est toujours opérationnelle. Vérifiez si d'autres systèmes répondent à cette commande ping de diffusion ou non. Cette fonction n'est pas nécessaire si le fichier `netmon.cf` est configuré correctement. Dans ce cas, la disponibilité d'autres adaptateurs d'interface réseau connus doit être testée. Une commande ping de diffusion sur un système autonome n'affecte pas les performances. En revanche, elle aura un impact négatif sur les performances si les systèmes fonctionnent dans un environnement z/VM. Cet impact sur la performance se produit parce que tous les autres systèmes exécutés dans cet environnement z/VM et situés dans le même segment de réseau (même réseau IP et masque de réseau) répondent à cette demande ping de diffusion. Par conséquent, même les systèmes VM invités inactifs et paginés sont chargés dans l'environnement z/VM simplement pour répondre à cette commande ping. Selon le nombre de systèmes invités exécutés sous z/VM, les performances de l'ensemble du système z/VM peuvent être réduites.

Pour éviter cet impact négatif sur les performances, apportez les modifications suivantes à la configuration :

- Obtenez la liste de tous les groupes de communication du cluster :

  ```
  # lscomg
  ```

- Désactivez la diffusion pour tous les groupes de communication :

```
# chcomg -x b <groupe de communication> ...
```

Par exemple :

```
chcomg -x b CG1
```

- Utilisez à nouveau la commande **lscomg** pour vérifier que la diffusion est désactivée.

Activation du signal de présence d'un disque

Vous pouvez activer le signal de présence d'un disque pour garantir l'intégrité des données dans les environnements en cluster.

Le signal de présence d'un disque réduit les risques de fractionnement d'un cluster, car il permet de faire la distinction entre une défaillance du réseau et un dysfonctionnement du noeud.

Une défaillance du réseau se produit si la connexion réseau entre les noeuds et entre un noeud et le disque partagé échoue, comme illustré à la figure 15.

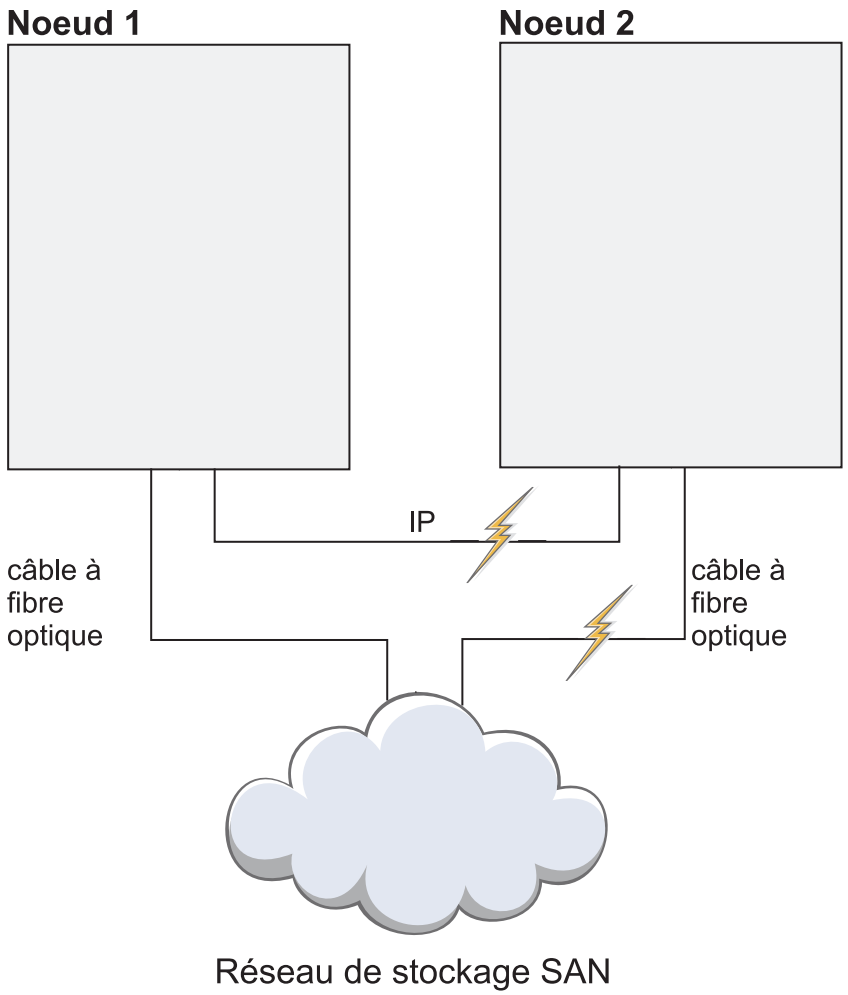

Figure 15. Défaillance du réseau dans un scénario à deux noeuds avec un disque partagé

Un dysfonctionnement du noeud se produit si un noeud n'est plus accessible, comme illustré à la figure 16.

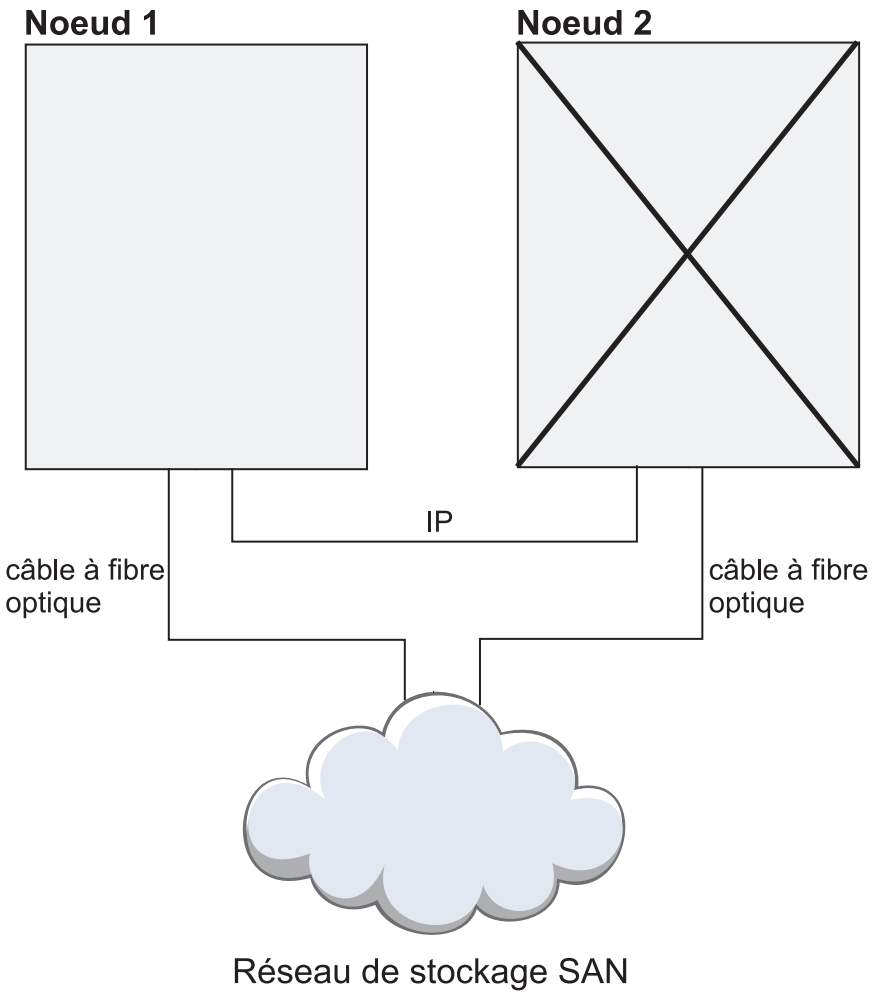

Figure 16. Dysfonctionnement d'un noeud dans un scénario à deux noeuds avec un disque partagé

Si un fractionnement de cluster peut être évité, aucune protection des ressources critiques n'est requise. Les systèmes n'ont pas besoin d'être redémarrés. Les problèmes d'intégrité des données sont également évités.

En cas de fractionnement d'un cluster, l'ensemble de noeuds qui a perdu l'accès au disque émettant le signal de présence perd également l'accès à des données vitales. La protection des ressources critiques sert à éviter l'altération de données. Le signal de présence de disque permet de moduler les règles de protection des ressources critiques, car les noeuds ne pouvant pas accéder au disque ne peuvent pas en modifier les données.

Remarque :

1. Le signalement de présence d'un disque peut uniquement être activé lorsque le domaine homologue est déjà en ligne.
2. Le signalement de présence d'un disque peut uniquement être défini entre deux noeuds. En présence de plus de deux noeuds, chaque paire doit être connectée séparément.

Trouvez un volume physique, un volume logique ou une unité md multi-accès adaptés sous Linux. Les données de ce volume sont effacées. Créez une ressource d'interface de signal de présence à l'aide de

```
CT_MANAGEMENT_SCOPE=2
mkrsrc IBM.HeartbeatInterface attributes [Force=0|1]
```

Attributs

Name Nom arbitraire d'un maximum de 36 caractères

DeviceInfo
Disque ou ID de volume valides :

- `/dev/hdisk` : disques de données brutes
- LVID : volumes logiques
- MPATH : unités multi-accès
- PVID : volumes physiques

CommGroup
Nom de l'instance dans `IBM.CommunicationGroup`. Est créé si le paramètre `Force` a pour valeur 1.

NodeNameList
Paire de noeuds pour cette interface de signal de présence, par exemple {'node1','node2'}.

MediaType
2 (disque)

Pour chaque anneau de signal de présence, un groupe de communication est créé. Cela est également vrai pour le signalement de présence conventionnel basé sur le réseau. Le groupe de communication est créé en même temps que l'unité de signal de présence. Le groupe de communication peut être réglé de façon similaire aux groupes de réseau. `PingGracePeriodMilliSec` ne peut pas être modifié pour le signal de présence d'un disque.

Procédez comme suit pour vérifier votre configuration de signal de présence du disque :

- Dans la configuration du système, vérifiez que le disque utilisé pour le signalement de présence d'un disque n'est pas réservé par les noeuds homologues.
- Le signalement de présence d'un disque peut être testé à l'aide des commandes suivantes :

  ```
  dhb_read -p <nom-unité> -t    # exécutez cette commande sur le noeud expéditeur
  dhb_read -p <nom-unité> -r   # exécutez cette commande sur le noeud destinataire
  ```

  Pour exécuter une vérification complète, relancez les commandes, en échangeant le noeud expéditeur et le noeud récepteur. Si ce test ne fonctionne pas, il se peut qu'il ne soit pas pris en charge en raison de la réservation de disque ou que la configuration du système ne soit pas compatible.
- Vérifiez que les appels système suivants entre les noeuds fonctionnent correctement :

  ```
  open("<dev>", O_RDWR|O_DIRECT), pread() and pwrite();
  ```

Protection des ressources critiques (indicateur de présence)

Activation de l'indicateur de présence (DMS) dans un environnement à haute disponibilité.

Dans un environnement à haute disponibilité, il est essentiel qu'une seule instance de ressource critique fonctionne à un moment donné. Un exemple classique de ressource critique est l'accès en écriture à un disque partagé. Lorsque l'accès en lecture-écriture est octroyé à plusieurs noeuds simultanément, il provoque une altération totale de la structure du système de fichiers.

Les algorithmes de quorum de RSCT `ConfigRM` évitent ce scénario, à condition que `ConfigRM`, `HATS` et `HAGS` reçoivent suffisamment de ressources pour exécuter leurs calculs. L'indicateur de présence intervient si les composants de cette infrastructure RSCT ne peuvent plus assurer la gestion des ressources critiques, par exemple en cas de carence des processus ou d'interblocage. L'indicateur de présence nécessite un accès à intervalle régulier sur une période donnée. Si l'accès échoue, le noyau de système d'exploitation déclenche lui-même un redémarrage immédiat du système, afin d'éviter le double démarrage d'une ressource critique.

Sur les systèmes Linux, cette fonctionnalité est mise en œuvre à l'aide de la commande `reboot` et de l'appel système `halt`, a ainsi que d'un module `softdog`. Sous AIX, le pilote de périphérique `haDMS` est utilisé à cet effet.

Valeurs du quorum opérationnel

Si des ressources critiques sont actives sur un sous-cluster dépourvu d'un quorum, `ConfigRM` détermine la façon dont le système doit être arrêté. Six méthodes de protection différentes peuvent être configurées par l'attribut `CritRsctProtMethod` sur chaque noeud.

Le tableau suivant liste les méthodes d'arrêt du système en fonction de la valeur de l'attribut `CritRsctProtMethod` qui les représente.

Tableau 23. Méthodes de protection du quorum opérationnel.

Signification	**Valeur**	
Réinitialisation à froid et redémarrage du système d'exploitation (par défaut)	1	
Arrêt du système d'exploitation	2	
Réinitialisation à froid et redémarrage du système d'exploitation avec `sync`	3	
Arrêt avec `sync`	4	
Aucune protection. Le système continue de fonctionner	5	
Quitte et redémarre les sous-systèmes RSCT	6	

Activation du support IPv6

Pour utiliser IPv6 avec System Automation, vous devez configurer votre système d'exploitation pour IPv4 et IPv6. Les opérations courantes du cluster RSCT utilisent des connexions IPv4, mais les ressources `IBM.ServiceIP` peuvent être définies pour utiliser des adresses IPv6.

Pour activer le support IPv6 dans RSCT et System Automation for Multiplatforms, exécutez la commande suivante :

```
chrsrc -c IBM.NetworkInterface IPv6Support=1
```

La commande **chrsrc** crée également davantage de ressources `IBM.NetworkInterface` pour les interfaces IPv6. Vous disposez désormais de deux ressources `IBM.NetworkInterface` par interface physique : une pour IPv4 et une pour IPv6. Pour des exemples de création de ressources `IBM.ServiceIP` avec des adresses IPv6, voir System Automation for Multiplatforms - Guide d'administration et d'utilisation. Un nouvel attribut de classe `IBM.ServiceIP` intitulé Netprefix est défini pour être utilisé avec IPv6.

Configuration de l'adaptateur d'automatisation à l'aide d'un compte utilisateur non superutilisateur

Par défaut, l'adaptateur d'automatisation de bout en bout System Automation for Multiplatforms s'exécute avec un superutilisateur. Cette section décrit comment cet adaptateur peut être configuré avec un utilisateur non superutilisateur.

Avant de configurer l'adaptateur avec un utilisateur non superutilisateur, configurez-le avec le compte superutilisateur :

- Créez et lancez le domaine System Automation.
- Configurez l'adaptateur avec l'utilitaire `cfgsamadapter`.
- Configurez la connectivité SSL avec System Automation Application Manager (facultatif).
- Vérifiez la fonction de l'adaptateur avec la console des opérations System Automation Application Manager.

L'exécution à l'avance de cette procédure permet de garantir que la procédure de configuration non superutilisateur de l'adaptateur ne doive être effectuée qu'une seule fois.

Pour effectuer la configuration avec un utilisateur non superutilisateur, procédez comme suit :

1. Effectuez les préparations de sécurité spécifiques au système d'exploitation, par exemple la création d'un utilisateur et d'un groupe dédiés pour l'adaptateur. Pour avoir une description des actions correspondantes que vous devez effectuer manuellement, voir «Configuration de la sécurité pour des systèmes d'exploitation spécifiques», à la page 99.
2. Modifiez la propriété du groupe et les droits d'accès de certains fichiers et répertoires créés par l'installation par défaut. Définissez les droits d'accès System Automation et RSCT appropriés pour l'utilisateur de l'adaptateur. Les actions en rapport avec cette étape s'exécutent automatiquement via le script `setupAdapterNonRoot.sh`. Toutes les actions exécutées par le script sont décrites à la rubrique «Exécution du script de configuration de l'adaptateur utilisateur non root», à la page 100.

Configuration de la sécurité pour des systèmes d'exploitation spécifiques

Informations sur les préparations de la sécurité propres au système d'exploitation qui sont obligatoires avant le lancement du script `setupAdapterNonRoot.sh`. Exécutez les actions décrites dans cette section sur tous les noeuds du cluster.

Création de compte d'utilisateur et de groupe

Le même groupe et compte d'utilisateur doit être créé sur chaque noeud du cluster. Ils seront transmis en tant que paramètres d'entrée au script `setupAdapterNonRoot.sh`.

Créez un groupe qui sera le groupe principal pour le compte utilisateur de l'adaptateur. Le nom de groupe `sagroup` est utilisé dans la section suivante. Tout autre nom est également valide. `sagroup` est utilisé lors de la modification de l'appartenance au groupe de plusieurs fichiers et répertoires de System Automation for Multiplatforms, ce qui accorde des droits d'accès au compte utilisateur de l'adaptateur.

Créez le compte utilisateur pour l'exécution de l'adaptateur à l'aide de l'ID de groupe `sagroup` en tant que groupe principal de l'utilisateur. Le nom de groupe `samadapt` est utilisé dans la section suivante. Le compte utilisateur `samadapt` peut être un compte utilisateur technique qui n'est pas destiné à être utilisé dans un shell de connexion. Dans de cas, un mot de passe n'est pas requis. Vérifiez que le répertoire de base existe et qu'il possède des droits d'accès corrects.

L'utilisateur `samadapt` peut être un administrateur ou un opérateur System Automation for Multiplatforms. Vous devez suivre les instructions fournies dans la rubrique Chapitre 5, «Sécurisation», à la page 131 pour configurer les droits appropriés.

Pour un opérateur, affectez le rôle `sa_operator`. Pour un administrateur, affectez le rôle `sa_admin`. Avec le rôle `sa_operator`, l'adaptateur peut démarrer et arrêter des ressources et des groupes de ressources, et avec le rôle `sa_admin` il peut en plus activer et désactiver des règles.

Remarque : Si vous souhaitez activer des utilisateurs non root supplémentaires pour l'administration et l'exécution de System Automation, voir Chapitre 5, «Sécurisation», à la page 131. Utilisez le groupe `sagroup` également pour ces utilisateurs.

Etapes de configuration si l'authentification d'utilisateur est activée

Des étapes supplémentaires doivent être exécutées si l'authentification d'utilisateur avec PAM (Pluggable Authentication Modules) est activée dans la configuration de l'adaptateur d'automatisation.

Commandes spécifiques Linux (SLES)

Le compte utilisateur `samadapt` doit être ajouté à l'image de l'ID de groupe, ce qui autorise `samadapt` à lire le fichier `/etc/shadow` qui contient des utilisateurs et leurs mots de passe chiffrés. Le fichier `/etc/shadow` a l'appartenance `root:shadow` avec les paramètres de bit de droit standard 640. L'accès au fichier `/etc/shadow` est requis pour autoriser l'authentification d'utilisateur PAM (Pluggable Access Module) à partir d'un compte utilisateur non root. Cela se produit lorsque PAM est utilisé pour vérifier les données d'identification d'utilisateur pour accéder au

domaine System Automation for Multiplatforms à partir du moteur d'automatisation ou de la console d'opérations de System Automation Application Manager.

Commandes spécifiques AIX

Le compte utilisateur `samadapt` doit être ajouté à l'ID de groupe `security`, ce qui autorise `samadapt` à utiliser la fonctionnalité PAM et à accéder au répertoire `/etc/security`. Cela est obligatoire pour vérifier les données d'identification d'utilisateur lors de l'accès au domaine System Automation for Multiplatforms à partir du moteur d'automatisation ou de la console d'opérations de System Automation Application Manager. De plus, les paramètres ACL doivent être modifiés pour le fichier `/etc/security/password`.

Sous AIX, le fichier `/etc/security/passwd` contient les comptes utilisateur et leurs mots de passe chiffrés. Le fichier `/etc/security/passwd` a l'appartenance `root:security` avec les paramètres de bit de droit standard 600. Ce paramètre refuse l'accès à partir du compte utilisateur `samadapt`, même s'il est membre du groupe de sécurité. L'accès peut être accordé en modifiant les ACL dans le fichier, ce qui évite de modifier l'appartenance et les bits de droit.

Les ACL peuvent être modifiés à l'aide de l'utilitaire `acledit` ou `aclget/aclput`. Exemple de sortie :

```
*
* ACL_type   AIXC
*
attributes:
base permissions
    owner(root):  rw-
    group(security):  ---
    others:  ---
extended permissions
    enabled                      <== activer les droits étendus
    permit   r--     u:samadapt  <== autoriser l'accès en lecture à samadapt
```

Fusionnez ces modifications avec d'autres modifications qui ont pu être appliquées précédemment.

Activez le compte utilisateur `samadapter` qui doit être utilisé par System Automation Application Manager

Si vous avez activé l'authentification de l'utilisateur de l'adaptateur d'automatisation et souhaitez utiliser le compte utilisateur `samadapt` pour accéder au cluster System Automation for Multiplatforms à partir de System Automation Application Manager, vous devez définir un mot de passe pour cet ID utilisateur. Vous pouvez spécifier ses données d'identification pour l'accès à un domaine d'automatisation de premier niveau dans l'utilitaire de configuration `cfgeezdm`. Vous pouvez aussi utiliser les données d'identification pour accéder au domaine System Automation Application Manager à partir de la console des opérations.

Exécution du script de configuration de l'adaptateur utilisateur non root

Exécutez le script `setupAdapterNonRoot.sh` pour effectuer les actions restantes de la configuration de l'adaptateur non root.

Le script se trouve dans le répertoire `/opt/IBM/tsamp/sam/bin`. Avant l'exécution du script, les conditions suivantes doivent être remplies :

- Si vous mettez à niveau System Automation for Multiplatforms à partir d'une version antérieure à 4.1 vers la version 4.1, tous les noeuds du cluster sont mis à niveau vers la nouvelle version. La migration du cluster est terminée. La commande `samctrl –m` a été exécutée avec succès.
- L'adaptateur est arrêté.
- Toutes les étapes manuelles décrites dans «Configuration de la sécurité pour des systèmes d'exploitation spécifiques», à la page 99 ont abouti.
- Le cluster System Automation est défini, mais n'est pas obligatoire pour arrêter le cluster. Les étapes de configuration n'interfèrent pas avec les opérations du cluster.

Exécutez le script `setupAdapterNonRoot.sh` sur tous les noeuds du cluster.

La liste suivante présente l'utilisation du script `setupAdapterNonRoot.sh` :

```
setupAdapterNonRoot.sh

Nom
setupAdapterNonRoot.sh  - configure l'adaptateur d'automatisation de bout en bout
pour l'exécuter avec un compte utilisateur non root

Synopsis
      setupAdapterNonRoot.sh [–x] userName [groupName]

Description
      Script permettant de configurer l'adaptateur d'automatisation de bout en bout
pour l'exécuter avec un compte utilisateur non root.
      Il adapte l'appartenance au groupe et les droits d'accès, ainsi que les définitions de sécurité RSCT.

Options
      -x  Définit les droits ACL pour le rôle sa_admin. En cas d'omission, ils sont définis sur ACL par défaut
          pour le rôle sa_operator.

Paramètres
      userName  - nom du compte utilisateur sous lequel doit s'exécuter l'adaptateur
      groupName - nom du groupe principal du compte utilisateur de l'adaptateur

Codes de sortie
 0 toutes les configurations ont abouti
 1 au moins une tâche de configuration a échoué - pour plus de détails, voir la sortie
 2 prérequis non satisfaits - pour plus de détails, voir la sortie
```

Exécutez le script sous le nom d'un utilisateur ayant des droits root :

Vérification de la configuration requise
Le système vérifie si un cluster existe, si l'adaptateur d'automatisation est arrêté et si le compte utilisateur existe. Il vérifie également si le groupe indiqué est le groupe principal du compte utilisateur.

Modification des appartenances au groupe et des droits
Plusieurs appartenances et droits de fichiers et de répertoires doivent être modifiés, car ils ont été créés initialement pour autoriser l'accès à un utilisateur root uniquement. Pour plus d'informations, voir «Modification des appartenances au groupe et des droits», à la page 102.

Remarque : Le script modifie le groupe auquel appartient le fichier `/etc/ibm/tivoli/common/cfg/log.properties`. Ce fichier peut être utilisé également par d'autres produits Tivoli. Si l'un de ces produits est exécuté également avec un compte utilisateur non root, vérifiez que le fichier `log.properties` est toujours lisible pour ces produits.

Définition des droits System Automation et RSCT appropriés
Pour autoriser le compte utilisateur non root `samadapt` à utiliser RSCT Resource Management Control (RMC), des droits doivent être attribués par le biais du fichier `/var/ct/cfg/ctrmc.acls`. Pour plus d'informations, voir «Définition des droits System Automation et RSCT appropriés», à la page 103.

Adaptation de la configuration de l'adaptateur d'automatisation
L'utilisateur non root et le groupe sont ajoutés aux propriétés de configuration de l'adaptateur. Pour plus d'informations, voir «Adaptation de la configuration de l'adaptateur d'automatisation», à la page 104.

Exemple de sortie :

```
root@p6sa13 /opt/IBM/tsamp/sam/bin# ./setupAdapterNonRoot.sh -x samadapt
------------------------------------------------------------------------------
Vérification de l'userid samadapt.
Groupe non défini comme paramètre. Extraction du groupe principal pour l'utilisateur de samadapt.
------------------------------------------------------------------------------
Vérification du groupe sagroup pour l'userid samadapt.
Compte utilisateur samadapt et groupe sagroup vérifiés avec succès. Le traitement continue...
------------------------------------------------------------------------------
Vérification s'il existe un domaine homologue  ...
Le domaine homologue existe. Le traitement continue ...
------------------------------------------------------------------------------
Vérification si l'adaptateur existe et s'il est hors ligne ...
samadapter n'est pas en cours d'exécution.
L'adaptateur existe et il est hors ligne. Le traitement continue ...
------------------------------------------------------------------------------
Recherche d'une configuration d'adaptateur non root précédente ...
------------------------------------------------------------------------------
Modifiez différents droits. Appuyez sur Entrée pour continuer ...

PolicyPool : /etc/opt/IBM/tsamp/sam/policyPool
Tivoli Common Directory : /var/ibm/tivoli/common
KeyStore non défini.
TrustStore non défini.
------------------------------------------------------------------------------
Remplacement de la strophe DEFAULT dans le fichier /var/ct/cfg/ctrmc.acls.
Appuyez sur Entrée pour continuer ...

Ajout des entrées suivantes à la strophe DEFAULT de /var/ct/cfg/ctrmc.acls
DEFAULT
   samadapt@0xc3d084925f78e253   *   rw
------------------------------------------------------------------------------
La commande 'refresh -s ctrmc' va être émise. Appuyez sur Entrée pour continuer ...

0513-095 La demande de régénération du sous-système a abouti.
------------------------------------------------------------------------------
Adaptation du fichier sam.adapter.properties
 Appuyez sur Entrée pour continuer ...

Remplacement des lignes dans le fichier de propriétés
------------------------------------------------------------------------------
Toutes les configurations ont abouti.
Exécutez ce script, y compris les préparations de compte utilisateur
et de groupe sur tous les noeuds du cluster.
S'il s'agit du dernier noeud du cluster sur
lequel vous avez exécuté le script, vous pouvez maintenant
démarrer l'adaptateur.
```

Modification des appartenances au groupe et des droits

Le script `setupAdapterNonRoot.sh` applique différentes modifications à l'appartenance au groupe des fichiers et répertoires de System Automation for

Multiplatforms en utilisant le groupe sagroup. Aucun ID utilisateur propriétaire du fichier n'est modifié. Si nécessaire, les droits d'accès sont également modifiés au niveau du groupe.

Des modifications sont apportées au système de fichiers :

- Configurez l'adaptateur de sorte qu'il puisse accéder en lecture et écriture à son répertoire de cache /var/opt/IBM/tsamp.
- Modifiez les droits et l'appartenance du fichier /etc/ibm/tivoli/common/cfg/log.properties. Ce fichier contient l'emplacement du répertoire commun Tivoli qui est utilisé par l'adaptateur.
- Accordez des droits d'accès en lecture, écriture ou exécution au répertoire commun Tivoli. Le nom du répertoire est stocké dans le fichier /etc/ibm/tivoli/common/cfg/log.properties. Le répertoire par défaut est /var/ibm/tivoli/common.
- Autorisez la lecture des fichiers de configuration de l'adaptateur dans les répertoires /etc/opt/IBM/tsamp/sam/cfg et /etc/Tivoli/tec.
- Accordez l'accès au pool de règles de l'adaptateur. L'emplacement peut être configuré à l'aide de l'outil cfgsamadapter. Le répertoire par défaut est : /etc/opt/IBM/tsamp/sam/policyPool.
- Modifiez le groupe des fichiers binaires de l'adaptateur dans les répertoires /opt/IBM/tsamp/sam/bin, /usr/sbin/rsct/bin, et les fichiers JAR associés dans /opt/IBM/tsamp/sam/lib.

Pour plus de détails, voir la source du script setupAdapterNonRoot.sh.

Définition des droits System Automation et RSCT appropriés

Pour autoriser le compte utilisateur non root samadapt à exécuter RSCT Resource Management Control (RMC), le script setupAdapterNonRoot.sh accorde des droits par le biais du fichier /var/ct/cfg/ctrmc.acls.

Pour plus d'informations sur la sécurité RSCT, voir le document RSCT Technical Reference. Ce dernier est fourni avec les logiciels System Automation.

Le fichier ctrmc.acls est composé de plusieurs blocs (strophes) qui décrivent le droit d'accès pour une classe de ressource RSCT. De plus, le contenu de la strophe DEFAULT est ajouté à toutes les autres strophes. Il est utilisé par défaut pour les classes de ressources RSCT qui ne possèdent pas leur propre strophe dans ctrmc.acls. Pour accorder un accès aux classes de ressources RSCT pour le compte utilisateur non root de l'adaptateur, la strophe DEFAULT est modifiée en conséquence.

L'exemple suivant de Linux SLES présente les entrées qui sont ajoutées à la strophe DEFAULT ctrmc :

```
DEFAULT
samadapt@0xabac71a5e6f0c07b  * rw
samadapt@0xc8981082ad2616dd  * rw
root@LOCALHOST       *    rw
LOCALHOST    * r
none:clusteruser   * r // added by preprpnode
none:root    * rw // added by preprpnode
```

Les nouvelles entrées sont de type userid@RSCT-nodeid :

userid Compte utilisateur non root prêt à exécuter l'adaptateur.

RSCT-nodeid
ID de noeud RSCT contenu dans le fichier /var/ct/cfg/ct_node_id sur chaque noeud du cluster.

Une entrée est ajoutée pour chaque noeud du cluster au début de la strophe DEFAULT. Celle-ci prévaut par rapport aux entrées existantes moins spécifiques.

Il se peut que la strophe DEFAULT pour les systèmes d'exploitation AIX soit beaucoup plus grande que l'exemple Linux présenté plus haut. En revanche, les modifications apportées sont identiques.

Une fois la modification ctrmc.acls terminée, RSCT RMC est déclenché pour lire à nouveau le fichier. Cela s'effectue par le biais de la commande suivante :

```
refresh -s ctrmc
```

Après avoir exécuté le script setupAdapterNonRoot.sh, recherchez la modification appropriée dans le contenu de ctrmc.acls.

Adaptation de la configuration de l'adaptateur d'automatisation

Lorsque l'adaptateur est démarré, il doit connaître l'utilisateur non root et le groupe.

Ainsi, le script setupAdapterNonRoot.sh s'assure que le fichier de propriétés /etc/opt/IBM/tsamp/sam/cfg/sam.adapter.properties de configuration de l'adaptateur contient le paramètre suivant :

```
non-root-user=samadapt
non-root-group=sagroup
```

Activité et maintenance

Si vous installez un groupe de correctifs ou ajoutez des noeuds au cluster, les étapes d'application de la configuration non root de l'adaptateur doivent être partiellement répétées.

Scénarios et étapes à répéter.

Installation des groupes de correctifs
L'installation des groupes de correctifs System Automation for Multiplatforms peut remplacer des fichiers, ainsi que les appartenances au groupe et droits correspondants dans le répertoire /opt/IBM/tsamp/sam.

Exécutez à nouveau le script setupAdapterNonRoot.sh sur chaque noeud juste après avoir installé un groupe de correctifs sur le noeud. Spécifiez les mêmes paramètres d'entrée pour le script que ceux utilisés lors de son appel initial.

Ajout de nouveaux noeuds
Ajoutez un noeud au cluster à l'aide des commandes preprpnode et addrpnode.

Exécutez les étapes décrites dans «Configuration de la sécurité pour des systèmes d'exploitation spécifiques», à la page 99 sur le nouveau noeud après avoir ajouté ce dernier au cluster. Exécutez le script setupAdapterNonRoot.sh comme indiqué dans «Exécution du script de configuration de l'adaptateur utilisateur non root», à la page 100 sur tous les noeuds du cluster (anciens et nouveaux). Spécifiez les mêmes paramètres d'entrée pour le script que ceux utilisés lors de son appel initial sur les anciens noeuds du cluster.

Modification de l'ID utilisateur de l'adaptateur non root

Si vous voulez modifier l'ID utilisateur utilisé pour la configuration de l'adaptateur non root, supprimez la configuration existante. Vous pouvez ensuite définir la configuration pour le nouvel utilisateur.

Supprimez la configuration existante en exécutant le script `setupAdapterNonRoot.sh` avec les paramètres suivants :

```
setupAdapterNonRoot.sh -x root
```

Exécutez ensuite à nouveau le script avec le nouvel ID utilisateur et groupe voulus.

Suppression de la configuration de l'adaptateur non root

Supprimez la configuration de l'adaptateur non root en redéfinissant tous les droits et autorisations sur root.

Exécutez le script `setupAdapterNonRoot.sh` avec les paramètres suivants :

```
setupAdapterNonRoot.sh -x root system
```

Restrictions

Les restrictions sont liées aux problèmes qui peuvent survenir lors de l'accès aux règles XML dans le pool de règles System Automation for Multiplatforms. Des restrictions peuvent se produire lorsque vous répliquez les fichiers de configuration sur les autres noeuds du cluster.

Démarrage de l'adaptateur avec une règle active qui n'est pas lisible par le compte utilisateur non root

Lorsque la règle est chargée à partir d'un fichier de règles XML, le nom et l'emplacement de ce fichier peut s'afficher si vous entrez la commande `lssamctrl` à partir d'un interpréteur de commandes sur l'un des noeuds du cluster. Le fichier de règles ne doit pas forcément se trouver dans le pool de règles car la commande `sampolicy -a` peut utiliser des fichiers de règles situés à n'importe quel emplacement.

```
node:~ # lssamctrl
Displaying SAM Control information:

SAMControl:
TimeOut                 = 60
RetryCount = 3
Automation              = Auto
ExcludedNodes           = {}
ResourceRestartTimeOut = 5
ActiveVersion = [3.2.2.2,Mon Apr 8 15:49:33 2013]
EnablePublisher         = Désactivé
TraceLevel = 31
ActivePolicy = [/etc/opt/IBM/tsamp/sam/policyPool/nonRootAdapter-testuser-2.xml,20130415143902+0200,0]
CleanupList             = {}
PublisherList           = {}
```

Lorsque ce fichier de règles XML existe mais n'est pas lisible par le compte utilisateur non root, l'adaptateur ne peut pas démarre sur ce noeud et la connexion à System Automation Application Manager n'est pas établie.

Résolution : Modifiez le droit du fichier de règles XML ou placez ce fichier dans le pool de règles.

Lecture et activation des règles System Automation for Multiplatforms à partir du pool de règles. Ces opérations sont impossibles si `samadapt` a le rôle opérateur.

Pour activer une règle d'automatisation nouvelle ou modifiée à partir de la console d'opérations System Automation Application Manager, l'ID utilisateur `samadapt` doit avoir le droit de lire le fichier XML correspondant dans le pool de règles. Les règles XML dont les paramètres de bit de droit ou d'appartenance sont inappropriés ne s'affichent pas dans les boîtes de dialogue de sélection des règles de la console d'opérations.

Résolution : Les étapes de configuration non root ajustent l'appartenance et le droit des fichiers de règles XML existants. Vérifiez que les fichiers de règles XML qui seront stockés ultérieurement dans le pool de règles, par exemple en sauvegardant les règles à l'aide de la commande `sampolicy -s`, auront les droits appropriés.

Réplication des fichiers de configuration

Répliquez les fichiers de configuration sur d'autres noeuds du cluster à l'aide de la fonction **Répliquer** de l'utilitaire `cfgsamadapter`. Des droits en écriture pour l'ID utilisateur root uniquement sont définis pour certains fichiers remplacés. Par conséquent, La fonction **Répliquer** ne peut donc être exécutée qu'avec un ID utilisateur root.

Résolution : Exécutez la commande `setupAdapterNonRoot.sh sript` sur les noeuds cible, dès que la réplication est terminée. Spécifiez les mêmes paramètres d'entrée pour le script que ceux utilisés lors de son appel initial. Il existe une alternative à la fonction **Répliquer**. La commande `cfgsamadapter` permet d'effectuer les mêmes modifications de configuration de manière explicite sur chaque noeud du cluster.

Chapitre 4. Intégration

System Automation for Multiplatforms intègre d'autres applications Tivoli pour constituer une solution complète. L'intégration d'applications Tivoli et de votre environnement implique des tâches de configuration spécifiques pour adapter l'infrastructure en place.

Les configurations requises pour les intégrations ci-dessous sont décrites :

- Réacheminement d'événements System Automation for Multiplatforms à IBM Tivoli Enterprise Console (TEC).
- Réacheminement d'événements System Automation for Multiplatforms à IBM Tivoli Netcool/OMNIbus.
- Enrichissement des vues TBSM avec des informations provenant des ressources et des événements System Automation for Multiplatforms.

Consoles d'événements

System Automation for Multiplatforms envoie des événements EIF à Tivoli Enterprise Console (TEC) ou bien à Tivoli Netcool/OMNIbus (OMNIbus). TEC et OMNIbus sont des applications de gestion d'événements basées règles qui utilisent un serveur central pour le traitement des événements entrants.

Ils collectent des alertes et des événements depuis diverses sources :

- Applications Tivoli
- Applications partenaires Tivoli
- Applications client
- Plateformes de gestion de réseau
- Système de gestion de bases de données relationnelles

Pour IBM Tivoli System Automation for Multiplatforms, un événement est généré et envoyé à la console d'événements TEC ou OMNIbus dans les circonstances suivantes :

- Changement de la configuration de IBM Tivoli System Automation for Multiplatforms ou de l'état d'une ressource automatisée.
- Détection de problèmes.

Si vous désirez utiliser les événements System Automation avec Tivoli Business Service Manager (TBSM), vous devez réacheminer les événements à OMNIbus.

IBM Tivoli System Automation for Multiplatforms peut générer les types d'événements suivants :

Tableau 24. Types de classe d'événements de System Automation Application Manager

Classe d'événements / Groupe d'alertes	Description
SystemAutomation_Resource_Status_Change	L'état d'une ressource automatisée a été modifié.
SystemAutomation_Resource_Configuration_Change	Une nouvelle ressource automatisée a été ajoutée ou une ressource existante a été supprimée ou modifiée.
SystemAutomation_Relationship_Configuration_Change	Une nouvelle relation a été ajoutée ou une relation existante a été supprimée ou modifiée.

Tableau 24. Types de classe d'événements de System Automation Application Manager (suite)

Classe d'événements / Groupe d'alertes	Description
SystemAutomation_Domain_Status_Change	L'état du domaine a été modifié. Par exemple : • Le gestionnaire ou l'adaptateur d'automatisation du domaine démarre ou est arrêté. • Une nouvelle règle d'automatisation est activée.
SystemAutomation_Request_Configuration_Change	Une nouvelle demande a été émise vis à vis d'une ressource automatisée ou une demande existante a été annulée.

Les rubriques ci-après décrivent la configuration de IBM Tivoli System Automation for Multiplatforms et des consoles d'événements pour l'activation du transfert d'événements à TEC ou OMNIbus :

- Configuration d'OMNIbus pour son utilisation avec IBM Tivoli System Automation for Multiplatforms : «Tivoli Netcool/OMNIbus»
- Configuration de TEC pour son utilisation avec IBM Tivoli System Automation for Multiplatforms : «Tivoli Enterprise Console», à la page 116.

Après avoir préparé la console d'événements de votre choix, vous devez activer la génération des événements, comme indiqué à la rubrique «Activation de la génération d'événements», à la page 116.

Tivoli Netcool/OMNIbus

Les rubriques de cette section expliquent comment configurer IBM Tivoli Netcool/OMNIbus pour réacheminer des événements System Automation à la console d'événements OMNIbus. Cette configuration OMNIbus constitue également un prérequis pour l'intégration de IBM Tivoli System Automation for Multiplatforms avec Tivoli Business Service Manager.

Eléments prérequis

Etant donné que System Automation for Multiplatforms utilise des événements Tivoli Event Integration Facility (EIF) pour la communication, les composants suivants sont requis :

- IBM Tivoli Netcool/OMNIbus (OMNIbus)
- OMNIbus Probes Library for Nonnative Base
- OMNIbus Probe for Tivoli EIF (Sonde EIF). Cette sonde peut recevoir des événements EIF envoyés par System Automation et les réacheminer à l'ObjectServer.

Les versions suivantes sont requises, au minimum :

- OMNIbus Probe for Tivoli EIF V.9.0
- IBM Tivoli Netcool/OMNIbus 7.2.1

Remarque : Si vous exécutez IBM Tivoli Netcool/OMNIbus V7.2.1, installez le correctif temporaire 3 (7.2.1.5-IF0003). Si vous exécutez IBM Tivoli Netcool/OMNIbus V7.3, ou une version ultérieure, aucun groupe de correctifs supplémentaire n'est requis.

Installez et configurez ces composants conformément à la documentation disponible dans le centre de documentation d'IBM Tivoli Netcool/OMNIbus.

Variables d'environnement

$NCHOME

Correspond au répertoire de base Netcool dans lequel sont installés les modules. Répertoire par défaut sous Linux : `/opt/IBM/tivoli/netcool`.

$OMNIHOME

La variable `$OMNIHOME` est utilisée à des fins de compatibilité descendante avec des scripts, des applications d'éditeurs tiers et des sondes qui continuent à utiliser la variable d'environnement `$OMNIHOME`. `$OMNIHOME` se réfère à `$NCHOME/omnibus`.

Zones d'événement dans la base de données OMNIbus

Les nouvelles colonnes ci-dessous comportant des informations propres à System Automation for Multiplatforms vont être ajoutées à la table OMNIbus `alerts.status`. Elles seront remplies dans le fichier de règles OMNIbus propre à System Automation for Multiplatforms lors du traitement d'un événement.

Tableau 25. Attributs de statut de System Automation for Multiplatforms utilisés dans les événements de modification de statut d'une ressource (alerts.status)

Nom d'attribut	Type	Description
SADesiredState	varchar(16)	Etat souhaité reflétant l'objectif d'automatisation d'une ressource automatisée. Les valeurs possibles sont : • Online (En ligne) • Offline (Hors ligne) • NoChange (Pas de changement) Indique que l'objectif d'automatisation de la ressource ne peut pas être modifié par un opérateur.
SAObservedState	varchar(16)	Etat actuel observé d'une ressource automatisée. Valeurs possibles : • Unknown (Inconnu) • Online (En ligne) • Offline (Hors ligne) • Starting (Démarrage en cours) • Stopping (Arrêt en cours) • NotApplicable (Non applicable) **Remarque :** Correspond à l'état `c_status_observed` dans les événements TEC
SAOperationalState	varchar(255)	Liste des valeurs d'état opérationnel donnant des informations de granularité plus fine sur l'état courant de la ressource. Pour consulter la liste des valeurs possibles, reportez-vous au fichier `SystemAutomation.baroc`. **Remarque :** Correspond à l'état `c_status_operational` dans les événements TEC.
SACompoundState	varchar(16)	Etat composé indiquant si la ressource fonctionne comme prévu ou a rencontré une erreur. Les valeurs possibles sont : • Ok • Warning (Avertissement) • Error (Erreur) • Fatal **Remarque :** Correspond à l'état `c_status_compound` dans les événements TEC.

Tableau 26. Identification de ressource, de domaine et d'événement (alerts.status)

SADomainName	varchar(64)	Nom du domaine d'automatisation. Partie de la clé permettant d'identifier une ressource. **Remarque :** Correspond à l'état `sa_domain_name` dans les événements TEC.

SAResourceName	varchar(255)	Nom de la ressource. Ce nom est composé du nom de la ressource elle-même concaténé avec la classe de la ressource et éventuellement avec son noeud. L'ordre des parties du nom et le caractère de séparation dépendent du produit System Automation en émission.
		Dans le cas de SA MP et de SA AM :
		`<nom_classe>:<nom_ressource>:<nom_noeud>`
		Dans le cas de SA z/OS :
		`<nom_ressource>:<nom_classe>:<nom_noeud>`
		Remarque : `<nom_noeue>` est défini uniquement s'il existe. Pour les références de ressource System Automation Application Manager, le nom du noeud contient le domaine d'automatisation de premier niveau référencé. Correspond à l'état `sa_resource_name` dans les événements TEC.

SAEventReason	varchar(255)	Causes de l'événement. Un événement peut avoir des causes multiples dans un événement TEC. Exemples de causes d'événement : • StatusCommonObservedChanged • ConfigurationDeleted • PreferredMemberChanged **Remarque :** Correspond à l'état `sa_event_reason` dans les événements TEC.
SAReferencedResource	varchar(255)	Pour les références de ressources System Automation Application Manager de bout en bout, contient la clé de la ressource référencée.

Tableau 27. Autres attributs utilisés dans les événements de modification de statut d'une ressource (alerts.status)

SAExludedFromAutomation	varchar(16)	Indicateur signalant si la ressource est exclue de l'automatisation (c.a.d. que l'automatisation est suspendue). Utilisé dans les événements de changement d'état des ressources. Les valeurs possibles sont : • NotExcluded • Excluded **Remarque :** Correspond à `sa_flag_excluded` dans les événements TEC.
SADesiredRole	varchar(16)	Rôle souhaité. Utilisé pour les références de réplication indiquant la direction de réplication du stockage souhaitée (SA AM uniquement). Utilisé dans les événements de changement d'état des ressources. **Remarque :** Correspond à `sa_role_desired` dans les événements TEC.
SAObservedRole	varchar(16)	Rôle observé. Utilisé pour les références de réplication indiquant la direction de réplication du stockage observée (SA AM uniquement). Utilisé dans les événements de changement d'état des ressources. **Remarque :** Correspond à `sa_role_observed` dans les événements TEC.

Tableau 28. Evénements de modification de statut d'une ressource (alerts.status)

SADomainState	varchar(16)	Statut dui domaine d'automatisation. Valeurs possibles : • Online (En ligne) • Offline (Hors ligne) • Unknown (Inconnu) **Remarque :** Correspond à `sa_domain_state` dans les événements TEC.
SACommunicationState	varchar(32)	Indique l'état de connexion et de disponibilité du domaine si celui-ci est connecté à System Automation Application Manager. Les valeurs possibles sont : • Ok • AsyncTimeout • AsyncMissedEvent • SyncFailed • SyncFailedAndAsyncMissedEvent • SyncFailedAndAsyncTimeout • DomainHasLeft **Remarque :** Correspond à `sa_communication_state` dans les événements TEC.

Parallèlement aux nouvelles zones destinées aux événements System Automation, les zones existantes suivantes seront définies dans le fichier de règles pour les événements System Automation lors du traitement de l'événement.

Tableau 29. Zones existantes dans le fichier de règles pour les événements System Automation

Nom d'attribut	**Description**
Manager (Gestionnaire)	Nom descriptif de la sonde ayant collecté et réacheminé l'alerte à l'ObjectServer. Valeur pour les événements SA : `tivoli_eif on <nom_hôte>`.
Agent	Nom descriptif du gestionnaire ayant généré l'événement. Valeur pour les événements System Automation for Multiplatforms : `SystemAutomation`.
Node (Noeud)	Identifie le nom d'hôte d'où provient l'événement.
AlertGroup (Groupe d'alerte)	Identifie le type d'événement émis par System Automation. Voir le tableau 24, à la page 107 pour la liste des classes d'événement possibles.
AlertKey (Clé d'alerte)	Clé descriptive indiquant la ressource ayant déclenché l'événement. Dans le cas d'événements de ressource, contient la clé de la ressource sous forme de jeton source System Automation, par exemple : `EEZResourceKey,DN={DB2Cluster},NN={},RN={db2rs},RC={IBM.Application}`. Dans le cas d'événements de domaine, contient le nom du domaine sous forme de jeton source System Automation, par exemple : `EEZDomain,DN={Db2Cluster}`
Severity (Gravité)	Indique le niveau de gravité de l'événement. Dans le cas d'événements de ressource, l'état composé de la ressource détermine le niveau de gravité. La couleur de l'événement dans la liste des événements est contrôlée par la valeur de la gravité : • 0 : Vide • 1 : Indéterminée • 2 : Avertissement • 3 : Mineure • 4 : Majeure • 5 : Critique Voir «Mappage de l'état composé et de la gravité», à la page 112.

Tableau 29. Zones existantes dans le fichier de règles pour les événements System Automation (suite)

Nom d'attribut	Description
Summary (Récapitulatif)	Texte récapitulatif décrivant l'événement.
Service	Nom du service affecté par cet événement. Correspond à la zone `SAResourceName`.
Identifier (Identificateur)	Identificateur qui identifie de manière unique la cause du problème et contrôle la déduplication ObjectServer. Le module ObjectServer utilise la déduplication pour garantir que les informations d'événement générées depuis la même source ne soient pas dupliquées dans la liste des événements. Les événements répétitifs sont identifiés à l'aide de cet attribut et stockés en tant qu'événement unique afin de réduire le volume de données dans le module ObjectServer. Dans le cas d'événements System Automation, la zone Identifier est définie à `AlertKey + ":" + AlertGroup`. Par conséquent, la console d'événements affiche toujours le dernier événement d'une même ressource et du même AlertGroup.
Class	Classe unique des événements System Automation. La valeur correspond à 87725 (Tivoli System Automation).
ExtendedAttr (Attribut étendu)	Contient les paires nom-valeur des attributs internes propres à System Automation supplémentaires, pour lesquels il n'existe pas de colonne dédiée dans la table `alerts.status`.

En plus des attributs stockés dans la table OMNIbus `alerts.status`, des informations supplémentaires sont consignées dans la table `alerts.details`. Dans le cas d'événements de domaine, par exemple, le nom du produit et la version du produit d'automatisation correspondant au domaine sont stockés dans le tableau `alerts.details`.

Mappage de l'état composé et de la gravité

Dans le cas d'événements contenant une valeur `SACompoundState`, (par exemple, tous les événements de changement d'état de ressources) le tableau suivant est utilisé :

Tableau 30. Mappage de l'état composé et de la gravité

SACompoundState	Zone Gravité OMNIbus
Fatale	5 (Critique)
Erreur	4 (Majeure)
Avertissement	3 (Mineure)
OK	1 (Indéterminée)

Pour les autres événements qui ne contiennent pas la valeur `SACompoundState`, comme les événements de demande ou les événements de domaine, la zone de gravité de la fonction d'intégration d'événements (EIF) est utilisée pour déterminer la gravité OMNIbus.

Tableau 31. Mappage de gravité EIF à OMNIbus

Gravité EIF	Zone Gravité OMNIbus
60 (FATALE)	5 (Critique)
50 (CRITIQUE)	5 (Critique)
40 (MINEURE)	4 (Majeure)
30 (AVERTISSEMENT)	3 (Mineure)
20 (INOFFENSIVE)	2 (Avertissement)
Autre	1 (Indéterminée)

Remarque : La valeur de la gravité EIF de l'événement EIF originel peut être consultée dans la zone `ExtendedAttr` de l'événement.

Configuration d'OMNIbus pour traitement des événements System Automation

La configuration d'OMNIbus comprend la mise à jour de la base de données OMNIbus et l'activation du fichier de règles.

Mise à jour de la base de données OMNIbus :

La base de données OMNIbus ObjectServer inclut la table `alerts.status` qui contient toutes les zones affichées et sélectionnées par une liste d'événements.

Pour les événements System Automation for Multiplatforms, les colonnes supplémentaires décrites dans la rubrique «Zones d'événement dans la base de données OMNIbus», à la page 109 doivent être créées dans la table `alerts.status`.

Le fichier `sa_db_update.sql` génère les nouvelles colonnes dans la table `alert.status`. La classe d'événements pour les événements de Tivoli System Automation est également créée. System Automation for Multiplatforms utilise pour ses événements la classe d'événement 87725. Cette classe est utilisée afin d'associer des outils (par exemple, l'outil de lancement en contexte) à un type spécifique d'événement.

Entrez la commande suivante sur le serveur OMNIbus :

UNIX :

```
$OMNIHOME/bin/nco_sql -server NCOMS -username root < sa_db_update.sql
```

Windows :

```
%NCHOME%\bin\redist\isql -S NCOMS -U root < sa_db_update.sql
```

A l'invite, entrez votre mot de passe.

Le fichier `sa_db_update.sql` est situé sur le DVD du produit System Automation for Multiplatforms sous le répertoire `/integration`.

Remarque : La classe d'événement 87725 est prédéfinie dans OMNIbus version 7.3.1 ou ultérieure. Si vous lancez le script `sa_db_update.sql` alors que vous utilisez OMNIbus version 7.3.1, le message d'erreur suivant est renvoyé :

```
ERREUR=Tentative d'insertion d'une ligne en double à la
ligne 2 de l'instruction 'Insertion dans les valeurs
alerts.conversions ( 'Class87725','Class',87725,'Tivoli System
Automation' );...'
```

Vous pouvez ignorer ce message d'erreur.

Vérifiez que l'ajout à OMNIbus des colonnes spécifiques à SA et de la classe d'événement a abouti :

1. Ouvrez la fenêtre d'administration de Netcool/OMNIbus à l'aide de la commande `nco_config`.
2. Depuis la fenêtre d'administration de Netcool/OMNIbus, sélectionnez le bouton de menu **Système**.
3. Cliquez sur **Bases de données**. Le panneau Bases de données s'ouvre.

4. Sélectionnez la table **alerts.status**. La sous-fenêtre de la table `alerts.status` s'ouvre.
5. Vérifiez que les colonnes suivantes sont répertoriées :
   a. SACompoundState
   b. SADesiredState
   c. SAObservedState
   d. SAOperationalState
   e. SADomainName
   f. SAResourceName
   g. SAReferencedResource
   h. SAEventReason
   i. SAExludedFromAutomation
   j. SADesiredRole
   k. SAObservedRole
   l. SADomainState
   m. SACommunicationState
6. Depuis la fenêtre d'administration de Netcool/OMNIbus, sélectionnez le bouton de menu **Visuel**.
7. Cliquez sur **Classes**. Le panneau Classes s'ouvre.
8. Vérifiez que la classe portant l'ID **87725** et le libellé **Tivoli System Automation** es répertoriée dans la table.

Activation du fichier de règles :

Le fichier de règles OMNIbus définit comment la sonde traite les données d'événement afin de créer une alerte. Pour chaque alerte, le fichier de règles crée également un identificateur identifiant de manière unique la source du problème.

La sonde pour Tivoli EIF utilise un fichier de règles standard nommé `tivoli_eif.rules`. System Automation for Multiplatforms est livré avec le fichier de règles `tivoli_eif_sa.rules` spécifique à System Automation. Ce fichier doit être inclus dans le fichier `tivoli_eif.rules` par défaut à l'aide d'une instruction 'include'. Le fichier de règles `tivoli_eif_sa.rules` traite un événement EIF reçu par la sonde pour Tivoli EIF si la zone d'événement `source` contient la valeur `System Automation`.

Le fichier `tivoli_eif.rules` par défaut est situé sous le répertoire suivant du système sur lequel la sonde Tivoli EIF est installée :

```
Windows : %OMNIHOME%\probes\<os_dir>\tivoli_eif.rules
UNIX : $OMNIHOME/probes/<os_dir>/tivoli_eif.rules
```

Procédez comme suit pour activer le fichier `tivoli_eif_sa.rules` :

1. Copiez le fichier `tivoli_eif_sa.rules`, situé sous le répertoire `/integration` du CD du produit System Automation for Multiplatforms vers le système sur lequel la sonde OMNIbus Tivoli EIF est installée. Comme répertoire cible, choisissez le répertoire dans lequel se trouve le fichier `tivoli_eif.rules`.
2. Activez le fichier de règles livré `tivoli_eif_sa.rules`. Modifiez le fichier `tivoli_eif.rules` utilisé par la sonde pour Tivoli EIF en lui ajoutant une instruction "include" au fichier `tivoli_eif_sa.rules`.

   Le contenu du fichier `tivoli_eif.rules` est différent selon le type d'installation OMNIbus :

a. Si vous utilisez une installation OMNIbus autonome :

   Ouvrez le fichier `tivoli_eif.rules` dans un éditeur texte et ajoutez-lui l'instruction 'include' après le bloc `switch($source)` :

```
:
else
{
        switch($source)
        {
                case "dummy case statement": ### Ceci empêchera des erreurs de syntaxe au cas où
       aucune instruction include ne serait ajoutée ci-dessous.

                        include "tivoli_eif_tpc.rules"
                        include "tivoli_eif_tsm.rules"

                        # Annulez la mise en commentaire de la ligne suivante
                        # en cas d'utilisation de l'intégration TADDM
                        # ce fichier de règles est disponible uniquement dans OMNIbus 7.3
                        # et versions ultérieures
                        # include "tivoli_eif_taddm.rules"

                default:
                        # Mettez en commentaire la ligne suivante si vous ne recevez pas d'événements de TEC
                        include "tivoli_eif_default.rules"
        }
        include "tivoli_eif_sa.rules"
}
```

b. Si vous effectuez une intégration avec Tivoli Business Service Manager (TBSM) et que vous utilisez la version OMNIbus livrée avec TBSM :

   Ouvrez le fichier `tivoli_eif.rules` dans un éditeur de texte et ajoutez l'instruction include dans le bloc où sont inclus les fichiers de règles prédéfinis. Recherchez la ligne `# Inclusion des règles client qui se substitueraient aux règles antérieures` et ajoutez l'instruction 'include' pour `tivoli_eif_sa.rules` avant la ligne suivante :

```
:
:
 ###
 ### Gestion des événements TEC
 ###
 include "tec_event.rules"

 ###
 ### Gestion des événements Z
 ###
 # include "zos_event.rules"

 ###
 ### Gestion des événements Z définis par l'utilisateur.
 ###
 # include "zos_event_user_defined.rules"

 ###
 ### Gestion des affectations d'identité Z.
 ###
 # include "zos_identity.rules"

 ###
 ### Gestion des événements EE( Activation d'événements).
 ###
 # include "tivoli_eif_ee.rules"

   include "tivoli_eif_sa.rules"
```

```
 # Inclusion des règles client qui se substitueraient aux règles antérieures.
 # include "customer_override.rules"
:
:
```

3. Arrêtez la sonde EIF.
   - Sous Windows : sélectionnez **Panneau de configuration > Outils d'administration > Services**. Dans la liste des services, effectuez un double-clic sur **Sonde EIF** , puis cliquez sur **Arrêter**.
   - Sous UNIX : Entrez la commande suivante sur la ligne de commande

     `$OMNIHOME/bin/nco_pa_stop -process <nom_sonde>`
4. Redémarrez la sonde EIF.
   - Sous Windows : Dans la liste des services, cliquez deux fois sur **Sonde OMNIbus EIF**, puis cliquez sur **Démarrer**
   - Sous UNIX : Entrez la commande suivante sur la ligne de commande :

     `$OMNIHOME/bin/nco_pa_start -process <nom_sonde>`

Remarque :

1. Vous pouvez tester les modifications apportées au fichier de règles avec l'outil de vérification de syntaxe `nco_p_syntax` livré avec le serveur OMNIbus. Utilisez le fichier de règles racine `tivoli_eif.rules`. Les fichiers inclus sont vérifiés automatiquement.

   Exemple :

```
$OMNIHOME/probes/nco_p_syntax -rulesfile $OMNIHOME/probes/linux2x86/tivoli_eif.rules
```

2. Si vous voulez forcer la sonde à lire le fichier de règles à nouveau sans que des événements ne soient perdus, entrez la commande suivante :

   `kill -HUP <pid>`

   `pid` représente l'ID de processus de la sonde. Vous pouvez déterminer le `pid` avec la commande `nco_pa_status`.

Tivoli Enterprise Console

Vous pouvez configurer Tivoli Enterprise Console de manière à lui réacheminer les événements System Automation.

Configuration de TEC pour le traitement des événements System Automation

Le langage de programmation BAROC (Basic Recorder of Objects in C) est utilisé pour définir la structure des événements et leurs propriétés. Ces définitions sont stockées dans des fichiers portant l'extension `.baroc`. Le fichier baroc pour les événements System Automation se nomme `SystemAutomation.baroc` et est situé dans le répertoire `/usr/sbin/rsct/samples/tec/SystemAutomation.baroc` au terme de l'installation. Pour préparer TEC en vue d'une utilisation avec System Automation for Multiplatforms, importez, compilez, chargez et activez le fichier `baroc`, `SystemAutomation.baroc`, sur le serveur TEC. Pour plus d'informations sur cette procédure, reportez-vous au manuel IBM Tivoli Enterprise Console Rule Builder's Guide , GC32–0669.

Activation de la génération d'événements

Si vous désirez envoyer des événements à TEC ou à OMNIbus, activez le réacheminement d'événements dans System Automation for Multiplatforms.

Activez et configurez la génération d'événement EIF et la fonction de réacheminement en activant le diffuseur d'informations TEC. Procédez comme suit :

1. Configurez la publication d'événements à l'aide de l'utilitaire de configuration `cfgsamadapter`. Pour plus d'informations sur la configuration de la publication d'événements, voir «Onglet Publication d'événement», à la page 83.
2. Activez le diffuseur de publications sur chaque noeud du cluster System Automation for Multiplatforms. Par défaut, le diffuseur de publications est désactivé. Vous pouvez l'activer soit par la boîte de dialogue de configuration (voir *System Automation for Multiplatforms - Guide d'administration et d'utilisation*), soit à l'aide de la commande `samctrl`, comme indiqué à la rubrique «Activation du diffuseur de publications à l'aide de l'interface de ligne de commande».
3. Configurez un nouvel environnement local de langue pour les messsages des événements TEC si vous ne souhaitez pas utiliser l'environnement local du système par défaut.

Activation du diffuseur de publications à l'aide de l'interface de ligne de commande

Vous pouvez utiliser l'interface de ligne de commande (CLI) ou la boîte de dialogue de configuration `cfgsamadapter` de System Automation for Multiplatforms pour contrôler le diffuseur de publications.

Cette section explique comment contrôler le diffuseur de publications par l'interface de ligne de commande. Pour utiliser la boîte de dialogue de configuration `cfgsamadapter`, voir *System Automation for Multiplatforms - Guide d'administration et d'utilisation*.

Par défaut, la fonction de diffuseur de publications est désactivée. Pour connaître l'état du diffuseur de publications, exécutez la commande suivante :

```
node1:/usr/sbin/rsct/samples/tec # lssamctrl
```

Les données de contrôle suivantes de Tivoli System Automation s'affichent :

```
SAMControl:
 TimeOut   = 60
 RetryCount  = 3
 Automation  = Auto
 ExcludedNodes  = {}
 ResourceRestartTimeOut = 5
 ActiveVersion      = [3.2.0.0,Wed Feb 17 20:19:07 2010]
 EnablePublisher     = XDR_GDP2 XDR_GDP1
 TraceLevel  = 31
 ActivePolicy  = []
 CleanupList  = {}
 PublisherList  = {}
```

Pour activer le diffuseur de publications de TEC, exécutez la commande suivante sur un noeud :

```
node1:/usr/sbin/rsct/samples/tec # samctrl –e TEC
```

Pour désactiver le diffuseur de publications de TEC, exécutez la commande suivante sur un noeud :

```
node1:/usr/sbin/rsct/samples/tec # samctrl –d TEC
```

Pour activer tous les diffuseurs de publications définis, exécutez la commande suivante sur un noeud :

```
node1:/usr/sbin/rsct/samples/tec # samctrl –e P
```

Pour désactiver tous les diffuseurs de publications définis, exécutez la commande suivante sur un noeud :

```
node1:/usr/sbin/rsct/samples/tec # samctrl –d P
```

Configuration d'un nouvel environnement local de langue pour les messages d'événement TEC ou OMNIbus

Les messages d'événement TEC ou OMNIbus sont toujours dans la langue de l'environnement local système du noeud sur lequel System Automation for Multiplatforms maître s'exécute.

Remarque : Le nom des ressources dans les messages d'événement TEC ou OMNIbus peuvent être endommagés si l'utilisateur a créé les ressources (mkrg, mkrsrc) dans un shell dont le paramètre d'environnement local est différent du paramètre par défaut du système, ou si le transcodage de caractères utilisé par le programme du terminal est différent de celui de l'environnement local du shell. Pour résoudre ce problème, l'environnement local du système et du shell doivent être configurés de manière identique, et le transcodage de caractères du programme du terminal doit être défini en conséquence. Si l'environnement local du shell est modifié alors que les ressources ont déjà été créées à l'aide de l'ancien paramétrage, toutes les ressources devront être supprimées et recréées à l'aide des nouveaux paramètres d'environnement local.

Si l'utilisateur décide de remplacer l'environnement local par défaut du système par celui qu'il préfère pour le shell, il lui faudra effectuer cette modification sur tous les noeuds du cluster. Pour ce faire, procédez comme suit :

1. Arrêtez le cluster à l'aide de la commande **stoprpdomain**.
2. Editez le fichier qui contient les paramètres d'environnement local par défaut du système, définissez les nouvelles valeurs et enregistrez le fichier.

   SUSE Linux

   Fichier : `/etc/sysconfig/language`

   Mots-clés : `RC_LANG="<NewLocale>"`

   Remplacez `<NewLocale>` par votre paramètre d'environnement local.

   `ROOT_USES_LANG="yes"`

   Tous les mots clés commençant par `RC_LC_` doivent être définis pour les chaînes vides "", par exemple `RC_LC_ALL=""`.

   Exécutez `/etc/SUSEconfig` pour appliquer les modifications apportées à votre système. Vous pouvez également utiliser l'outil de configuration système `yast2 sysconfig` pour appliquer ces modifications.

   RedHat Linux

   Fichier : `/etc/sysconfig/i18n`

   Mots-clés : `LANG="<NewLocale>"`

   Remplacez `<NewLocale>` par votre paramètre d'environnement local.

   AIX

   Fichier : `/etc/environment`

   Mots-clés : `LANG="<NewLocale>"`

Remplacez `<NewLocale>` par votre paramètre d'environnement local.

3. Redémarrez le système.
4. Renouvelez ces étapes sur tous les noeuds du cluster.
5. Démarrez le cluster à l'aide de la commande **startrpdomain**.

Tivoli Business Service Manager (TBSM)

TBSM fournit les informations en temps réel dont vous avez besoin pour réagir aux alertes efficacement et conformément à vos exigences métier, et éventuellement pour vous conformer aux accords sur les niveaux de service (SLA).

Les outils TBSM permettent de construire un modèle de service s'intégrant avec les alertes d'IBM Tivoli Netcool®/OMNIbus™ ou éventuellement avec des données d'une source de données SQL.

Le serveur de données TBSM analyse les événements d'IBM Netcool/OMNIbus ObjectServer ou les données SQL pour identifier des correspondances avec les règles d'état en entrée configurées pour vos modèles de service. Si les données correspondantes changent l'état du service, l'état du modèle de service TBSM est modifié en conséquence. Lorsque l'état d'un service change, TBSM renvoie les événements de service correspondants à l'ObjectServer.

Le kit de la bibliothèque de reconnaissance vous permet de créer des objets de service TBSM à l'aide de données de livres de l'adaptateur de bibliothèque de reconnaissance ou depuis IBM Tivoli Application Dependency Discovery Manager.

La console TBSM fournit une interface graphique (GUI) s'exécutant sous Tivoli Integrated Portal (TIP) qui vous permet d'associer sur une base logique des services et des exigences métier dans le modèle de service. Le modèle de service fournit à un opérateur une vue du fonctionnement de l'entreprise à n'importe quel moment ou de son fonctionnement au cours d'une période donnée.

Le diagramme suivant illustre l'architecture TBSM élémentaire :

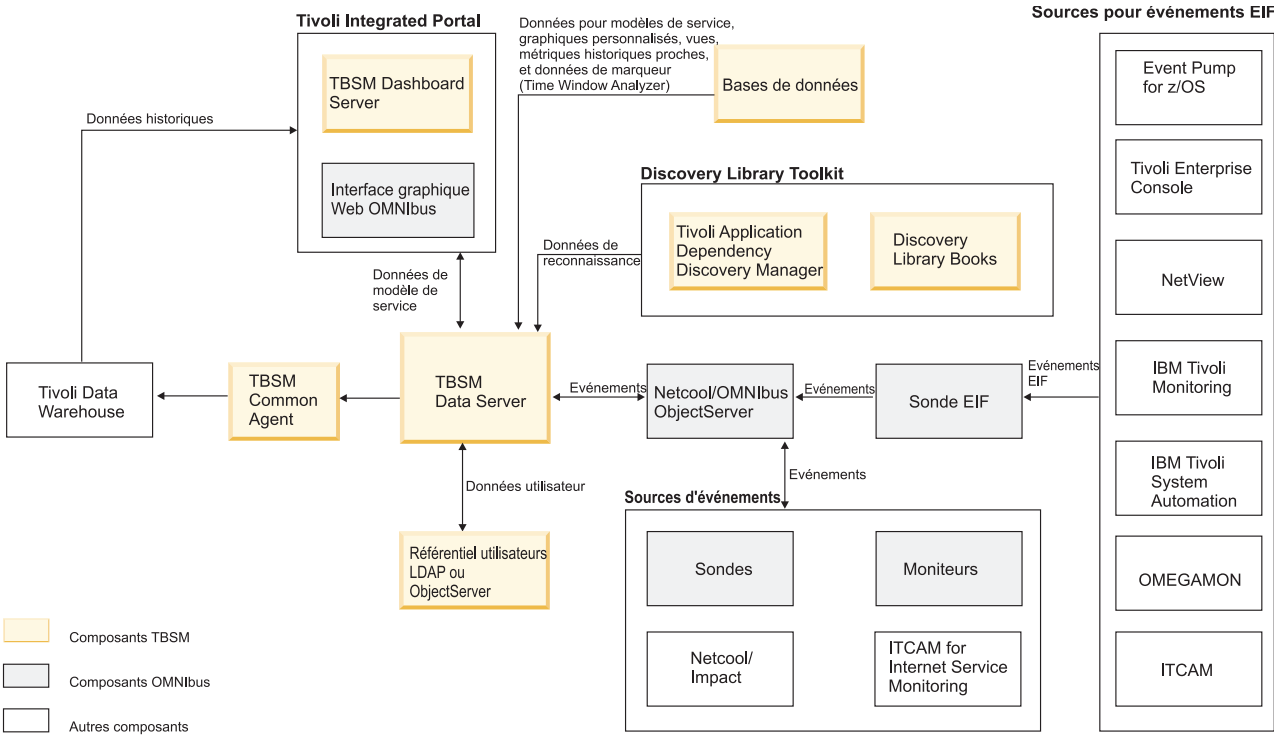

Figure 17. Architecture TBSM élémentaire

Composants principaux

Tivoli Integrated Portal

Tivoli Integrated Portal active l'interaction et la transmission sécurisée de données entre les produits Tivoli via un portail commun. Vous pouvez lancer une application depuis une autre et depuis la même vue de tableau de bord examiner différents aspects de votre entreprise gérée.

Tivoli Netcool/OMNIbus

TBSM effectue un suivi de Tivoli Netcool/OMNIbus ObjectServer pour détecter des événements entrants. L'ObjectServer collecte des événements depuis des sondes, des moniteurs et d'autres applications, telles qu'IBM Tivoli Monitoring. TBSM permet de créer des modèles de service qui répondent aux données reçues dans les événements entrants. Les données d'événement entrant peuvent, par exemple, changer l'état d'un service ou déclencher un contrôle d'une violation potentielle d'un accord sur les niveaux de service.

Tivoli Netcool/Webtop (GUI OMNIbus Web)

Netcool/Webtop est la console du navigateur pour Netcool/OMNIbus et TBSM utilise des composants Netcool/Webtop pour afficher des événements associés aux modèles de service. La liste des événements actifs et le portlet Détails du service dans TBSM sont des composants Netcool/Webtop et sont installés de pair avec TBSM. Tivoli Integrated Portal inclut également des composants Netcool/Webtop.

Serveur TBSM Dashboard

Le serveur TBSM Dashboard gère l'affichage de la console TBSM et communique avec le serveur TBSM Data pour prendre en charge la création et la visualisation de modèles de service via les consoles TBSM connectées. Au fur et à mesure que des utilisateurs visualisent des portions

du modèle de service, le serveur de tableau de bord acquiert et mémorise l'état des services depuis le serveur de données.

Serveur TBSM Data
Le serveur TBSM Data effectue un suivi de l'ObjectServer et de bases de données externes pour détecter des données affectant l'état des services que vous avez configurés dans la console TBSM ou à l'aide de l'outil de ligne de commande radshell. Le serveur calcule l'état de ces services en appliquant des règles aux données externes. Vos modèles de service et les règles sont stockés dans la base de données TBSM.

Intégration de System Automation for Multiplatforms

Les applications métier sont généralement constituées de différents composants middleware, sont multiniveaux et s'exécutent sur des plateformes hétérogènes. Tivoli Business Service Manager (TBSM) fournit des informations sur l'état de l'application multiniveau. TBSM surveille également les accords sur les niveaux de service à partir d'informations provenant de nombreuses sources. Netcool/OMNIbus est utilisé pour collecter tous les événements associés au périmètre de l'application de gestion et TBSM utilise ces événements pour déterminer l'état de ces applications de gestion.

System Automation for Multiplatforms automatise les dépendances de démarrage ou d'arrêt dans les applications de gestion, fournit une opération commune, une reprise automatique en situation d'échec et une vue agrégée de l'état de disponibilité. System Automation for Multiplatforms and System Automation for z/OS permet une haute disponibilité des composants individuels de l'application métier, par exemple une base de données critique.

System Automation for Multiplatforms peut être utilisé dans une intégration avec TBSM, pour enrichir les vues du service TBSM avec les données des événements de System Automation. System Automation for Multiplatforms intègre un modèle de service TBSM contenant des règles préconfigurées pour le mappage des états de System Automation aux instances de service TBSM.

Eléments prérequis

Avant de commencer, installez et configurez les produits suivants, puis testez votre installation :

- Configurez et activez le réacheminement d'événements vers OMNIbus pour les événements System Automation for Multiplatforms. Pour plus d'informations, voir «Configuration d'OMNIbus pour traitement des événements System Automation», à la page 113 et «Activation de la génération d'événements», à la page 116.
- Tivoli Business Service Manager (TBSM) version 4.2.1 ou ultérieure
- Mettez à jour le schéma Netcool OMNIbus ObjectServer pour TBSM.
  - Si vous disposez d'un serveur OMNIbus existant, importez les fichiers de schéma `tbsm_db_update.sql` et `ClearServiceDeps.auto`.
  - Si OMNIbus est installé avec TBSM, le programme d'installation de TBSM procède aux mises à jour des schémas requises.

Vous pouvez trouver des informations produit spécifiques à TBSM dans le centre de documentation de TivoliBusiness Service Manager. Pour plus d'informations sur l'installation du produit, consultez Tivoli Business Service Manager Knowledge Center.

Configuration de TBSM

Pour simplifier le processus de définition et de configuration des services dans TBSM, vous pouvez définir des modèles de service pour les instances de service avec un comportement identique. Au lieu de définir individuellement chaque service et ses dépendances, un modèle de service peut être créé pour un type de service, puis affecté aux services concernés.

Les instances de service représentent des services effectifs auxquels un modèle est affecté. Le modèle définit comment un service doit répondre à des données entrantes et à l'état des autres services. Les services du même type devraient être affectés à un modèle commun. Ceci permet d'utiliser les mêmes règles de modèle pour évaluer l'état de multiples services.

Lorsque vous affectez un modèle à un service, vous marquez le service avec le modèle concerné. Les modèles évitent d'avoir à créer à plusieurs reprises les mêmes règles pour un service.

Modèle de service pour TBSM

System Automation for Multiplatforms un modèle de service TBSM qui est utilisé pour les ressources System Automation affichées dans une arborescence de services TBSM.

Ce modèle de service se nomme `EEZ_SystemAutomationResource`. Il fournit :

- Une règle de statut entrant appelée `SACompoundState`, qui utilise des événements de modification d'état provenant de ressources System Automation for Multiplatforms afin de déterminer l'état général des services
- Des règles de statut entrant textuelles qui exportent l'état observé dans System Automation et d'autres états de ressource propres à System Automation en vue de leur utilisation dans des vues TBSM. Pour plus d'informations sur l'utilisation des règles de statut entrant textuelles, voir «Personnalisation des vues TBSM pour l'ajout d'informations provenant de System Automation», à la page 126.

Le modèle de service `EEZ_SystemAutomationResource` comporte une règle d'état entrant nommée `SACompoundState` qui détermine l'état global d'un service. Si le modèle de service a été associé à une instance de service spécifique, les événements de modification d'état de ressource provenant de System Automation for Multiplatforms auront un impact sur l'état général du service. Des événements sont associés à une instance de service si la valeur `AlertKey` de l'événement correspond à la valeur `AlertKey` définie comme identificateur pour l'instance de service.

Trois états globaux sont disponibles dans TBSM : Bon, Marginal et Mauvais. Le mappage suivant est défini dans la règle `SACompoundState` pour mapper les événements de modification d'état de ressource à partir de System Automation vers un état TBSM général pour une instance de service :

Tableau 32. Mappage des événements de changement d'état de ressources System Automation aux états TBSM

Gravité de l'événement	Etat TBSM
5 (Critique)	Mauvais (rouge)
4 (Majeure)	Mauvais (rouge)
3 (Mineure)	Marginal (jaune)
1 (Indéterminée)	Bon (vert)

Etant donné le mappage un à un de l'état composé d'une ressource avec la gravité de l'événement, l'état composé System Automation détermine directement l'état TBSM. Pour plus d'informations sur le mappage de l'état composé avec la gravité de l'événement, reportez-vous à la section «Mappage de l'état composé et de la gravité», à la page 112.

Définition d'un modèle de service System Automation dans TBSM

Le modèle `EEZ_SystemAutomationResource` est requis pour utiliser des événements System Automation dans TBSM. Importez le modèle `EEZ_SystemAutomationResource` dans TBSM en procédant comme suit :

1. Copiez le fichier `EEZ_SystemAutomationResource.radsh` depuis le répertoire `/integration` sur le CD du produit System Automation for Multiplatforms vers un répertoire temporaire où le serveur de données TBSM est installé.
2. Ouvrez une invite de commande sur le système du serveur de données TBSM. Placez-vous dans le répertoire dans lequel vous avez copié `EEZ_SystemAutomationResource.radsh` et émettez la commande suivante :
   - **UNIX :**

     ```
     cat EEZ_SystemAutomationResource.radsh  |
     $TBSM_HOME/bin/rad_radshell
     ```

   - **Windows :**

     ```
     type EEZ_SystemAutomationResource.radsh |
     %TBSM_HOME%\bin\rad_radshell
     ```

Le modèle de service fourni par System Automation for Multiplatforms est désormais défini dans TBSM.

Définition d'un déclencheur dans Netcool/OMNIbus

Sur le serveur d'objets OMNIbus, un nouvel événement de modification d'état d'une ressource remplace l'événement précédent (dédoublonnage d'événement).

Par défaut, TBSM traite uniquement un événement dédoublonné si la valeur de la zone **Gravité** a changé. Dans ce cas, TBSM traite les événements dédoublonnés et met à jour le statut du service en conséquence. Une modification de statut est possible pour une ressource qui met à jour les zones de statut utilisées dans les règles de statut entrant textuelles contenues dans le modèle de service `EEZ_SystemAutomationResource`. Mais la valeur de la gravité ne change pas puisque l'état composé de la ressource reste inchangé. Définissez dans OMNIbus un déclencheur de sorte que TBSM mette également les services à jour dans ces circonstances.

Le fichier `sa_db_tbsm_update.sql` est utilisé pour définir le déclencheur appelé `update_tbsm_service_on_sa_events` dans OMNIbus. Ce déclencheur veille à ce que TBSM traite à nouveau les événements si l'un des états utilisés dans les règles d'état entrant basées texte est modifié et ce, même si la valeur de la gravité reste inchangée. Créez cette définition de déclencheur chaque fois que vous désirez utiliser les règles d'état entrant basées texte inclues dans le modèle de service `EEZ_SystemAutomationResource`.

Entrez la commande suivante sur le serveur OMNIbus pour définir le déclencheur :

UNIX :

```
$OMNIHOME/bin/nco_sql -server NCOMS -username root < sa_db_tbsm_update.sql
```

Windows :

```
%NCHOME%\bin\redist\isql -S NCOMS -U root < sa_db_tbsm_update.sql
```

Entrez votre mot de passe et votre ID utilisateur lorsque vous y êtes invité.

`sa_db_tbsm_update.sql` est livré avec System Automation for Multiplatforms et se trouve dans le répertoire `/integration` sur le DVD du produit.

Intégration de ressources System Automation et de TBSM

Si vous désirez ajouter des ressources System Automation à une arborescence de services TBSM, vous devez créer celle-ci manuellement dans TBSM, puis lui affecter le modèle de service System Automation. Cette opération est décrite à la rubrique «Affectation du modèle de service à une instance de service». Vous devez également effectuer cette opération si vous désirez enrichir des instances de service existant déjà dans une arborescence de services TBSM avec des informations provenant d'événements System Automation.

Remarque : Si vous utilisez également System Automation Application Manager, vous pouvez exploiter son adaptateur de bibliothèque de reconnaissance afin de créer automatiquement des instances de service pour les ressources gérées par System Automation Application Manager.

Affectation du modèle de service à une instance de service

Un modèle de service est composé de règles pouvant être appliquées à des instances de service. Un modèle peut être utilisé pour plusieurs instances. Si vous désirez affecter le modèle `EEZ_SystemAutomationResource` à un service, vous pouvez marquer ce service avec le modèle.

Procédez comme suit :

1. Marquez les services utilisant le modèle `EEZ_SystemAutomationResource` pour rendre les règles d'état entrant définies disponibles pour ces services.
   a. Dans le portlet Service Navigation, sélectionnez le **nom du service** auquel associer le modèle de service spécifique de System Automation `EEZ_SystemAutomationResource`.
   b. Sélectionnez l'onglet **Edition du service** dans l'Editeur de service afin d'éditer le service.
   c. Sélectionnez l'onglet **Modèles**. Vous pouvez distinguer les deux listes suivantes :
      - **Modèles disponibles** : affiche tous les modèles que vous pouvez associer à l'instance de service sélectionnée.
      - **Modèles sélectionnés** : Affiche tous les modèles affectés au service.
   d. Pour affecter le modèle System Automation à un service, sélectionnez le modèle `EEZ_SystemAutomationResource` dans la liste **Modèles disponibles**. Cliquez sur la bouton fléché >> pour déplacer le modèle dans la liste **Modèles sélectionnés**.
2. Configurez les valeurs **Identification Field** pour ce service. TBSM utilise les zones d'identification pour mapper les événements entrants à une instance de service.
   a. Sélectionnez l'onglet **Edition du service**.
   b. Sélectionnez l'onglet **Zones d'identification** qui fournit les règles définies dans le modèle `EEZ_SystemAutomationResource` et les valeurs de zone d'identification requises pour mapper un événement à l'instance de service sélectionnée.

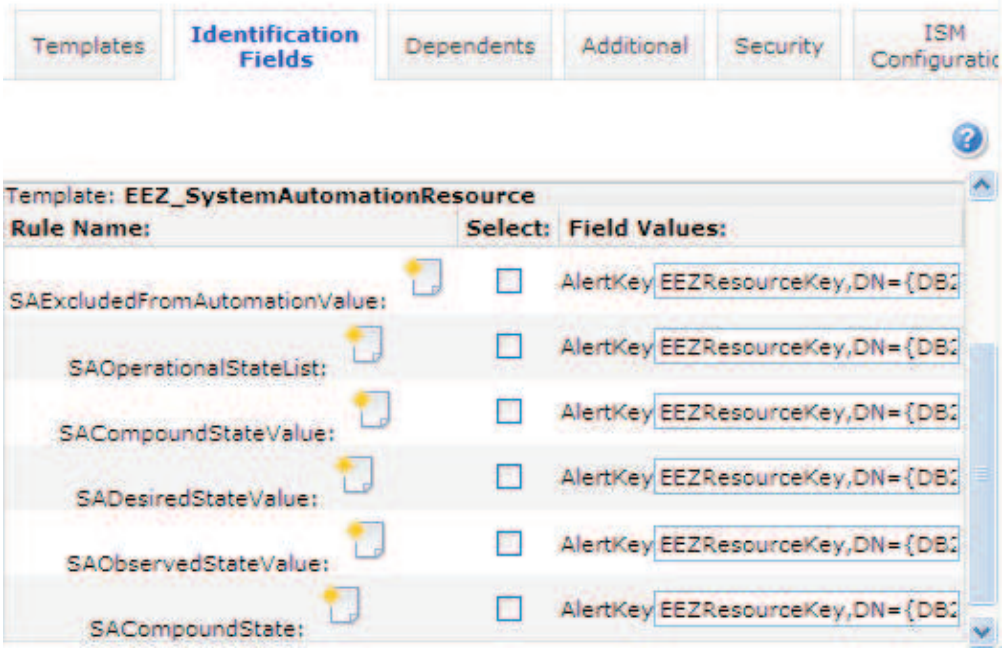

Figure 18. Onglet Zones d'identification

Les règles contenues dans le modèle `EEZ_SystemAutomationResource` utilisent l'attribut d'événement `AlertKey` comme identificateur. Par défaut, la valeur de chaque zone d'identification est celle saisie dans la zone **Nom du service**.

c. Entrez la valeur d'attribut `AlertKey` correcte qui correspond au service sélectionné. La valeur `AlertKey` doit contenir la clé de ressource System Automation unique au format CDM `SourceToken`. La structure est définie comme ceci :

```
EEZResourceKey,DN={NomDomaine},NN={NomNoeud},
RN={NomRessource},RC={ClasseRessource}
```

Vous pouvez ouvrir l'un des événements de la ressource et copier et coller la valeur `AlertKey` d'un événement pour éviter les erreurs de saisie. Exemples de valeurs AlertKey `AlertKey` valides :

Ressource

Ressource fixe , affichée par `lssam` en tant que `IBM.Application:db2-rs:saxb32c`.

AlertKey :

```
EEZResourceKey,DN={DB2Cluster},NN={saxb32c},RN={db2- rs},
RC={IBM.Application}
```

Déplacer le groupe

Ressource flottante. Le domaine `DB2Cluster` est affiché par `lssam` comme suit : `IBM.Application:db2-rs`

AlertKey :

```
EEZResourceKey,DN={DB2Cluster},NN={},RN={db2- rs},
RC={IBM.Application}
```

Groupe de ressources

Le domaine `DB2Cluster` qui est affiché par `lssam` comme suit : `IBM.ResourceGroup:DB2`.

AlertKey :

```
EEZResourceKey,DN={DB2Cluster},NN={},RN={DB2},
RC={IBM.ResourceGroup}
```

d. Cliquez sur **Enregistrer** pour appliquer vos modifications.

A chaque fois que de nouveaux événements de modification d'état de System Automation for Multiplatforms sont reçus pour le service et correspondent à la valeur `AlertKey` spécifiée, TBSM traitera les règles de statut entrant et pourra changer l'état général du service en fonction de la gravité de l'événement.

Personnalisation des vues TBSM pour l'ajout d'informations provenant de System Automation

Le modèle de service `EEZ_SystemAutomationResource` contient des règles de statut entrant textuelles qui extraient l'état observé dans System Automation et d'autres états de ressource propres à System Automation. Ces informations peuvent être utilisées dans les vues TBSM afin d'enrichir des instances de service avec des informations provenant de System Automation for Multiplatforms.

Les règles de texte d'état entrant suivantes sont disponibles :

Tableau 33. Règles d'état entrant basées texte pour TBSM

Nom de la règle	Description
SAObservedStateValue	Extrait la zone `SAObservedState` d'un événement de modification de statut d'une ressource. Les valeurs possibles sont : • Inconnu • En ligne • Hors ligne • Démarrage en cours • Arrêt en cours • Non applicable
SADesiredStateValue	Extrait la zone `SADesiredState` d'un événement de modification de statut d'une ressource. Les valeurs possibles sont : • En ligne • Hors ligne • NoChange (c'est-à-dire que l'opérateur ne peut pas changer l'objectif d'automatisation de la ressource)
SAOperationalStateValue	Extrait la zone `SAOperationalStateValue` d'un événement de changement d'état d'une ressource. Liste de valeurs d'état opérationnel fournissant des informations plus affinées sur l'état actuel de la ressource. Pour consulter la liste des valeurs possibles, reportez-vous au fichier `SystemAutomation.baroc`.

Tableau 33. Règles d'état entrant basées texte pour TBSM (suite)

Nom de la règle	Description
SACompoundStateValue	Extrait la zone `SACompoundStateValue` d'un événement de changement d'état d'une ressource. Etat composé indiquant si la ressource fonctionne correctement ou a rencontré une erreur. Les valeurs possibles sont : • Ok • Avertissement • Erreur • Fatale
SAExcludedFromAutomationValue	Extrait la zone `SAExcludedFromAutomationValue` d'un événement de changement d'état d'une ressource. Indicateur signalant si la ressource est exclue de l'automatisation (c.a.d. que l'automatisation est suspendue). Les valeurs possibles sont : • NotExcluded • Excluded

Ajout de colonnes d'informations System Automation supplémentaires à une arborescence de services TBSM

Vous pouvez modifier les colonnes des arborescences personnalisées affichées dans TBSM dans :

- Portlet de navigation des services Service Navigation
- Portlet d'arborescence des servicesService Tree

Le portlet Service Navigation par défaut comporte trois colonnes :

- **Etat**
- **Heure**
- **Evénements**

Vous pouvez modifier, supprimer et ajouter des colonnes d'arborescence dans l'Editeur de modèle d'arborescence. L'Editeur de modèle d'arborescence est disponible dans la barre d'outils **Services** du portlet Service Navigation. Vous pouvez ajouter un nouveau modèle d'arborescence au portlet Service Navigation. Pour chaque colonne personnalisée, utilisez l'Editeur de modèle d'arborescence afin de spécifier les données de règle à afficher dans la colonne.

Ajout de colonnes :

Cette fonction permet d'ajouter des colonnes à n'importe quelle règle de texte d'état entrant définie par le modèle `EEZ_SystemAutomationResource`. Par exemple, vous pouvez définir une colonne affichant l'état observé actuel provenant de System Automation pour chaque instance de service à laquelle le modèle `EEZ_SystemAutomationResource` est associé. Procédez comme suit :

1. Cliquez sur le bouton **Editeur de modèle d'arborescence** dans la barre d'outils du portlet de navigation des services.
2. Sélectionnez le modèle d'arborescence à modifier dans la liste déroulante **Tree Template Name**.

3. Cliquez sur le bouton **Ajouter une nouvelle colonne à l'arborescence** dans la section Configuration des colonnes.
4. Entrez le nom que vous voulez utiliser dans la zone vierge pour la nouvelle colonne, par exemple “Etat de disponibilité”.
5. Ajustez la position et la largeur de la colonne.
6. Dans la section **Sélection du modèle de service**, sélectionnez le modèle `EEZ_SystemAutomationResource`.
7. Sous **Mappage de règle de modèle de service**, sélectionnez le modèle `EEZ_SystemAutomationResource` dans la liste Modèle actif.
8. Pour chaque règle que vous voulez afficher dans une colonne d'arborescence de services, cochez la case **Afficher** et choisissez une colonne dans la zone déroulante pour afficher la valeur de sortie. Dans cet exemple, cochez la case **Display** pour l'attribut `@SAObservedStateValue` et choisissez la colonne **Availability State** dans la boîte déroulante de cette ligne.
9. Cliquez sur **OK** pour enregistrer les modifications du modèle d'arborescence.

L'illustration ci-dessous présente une capture d'écran de l'éditeur de modèle d'arborescence. Une nouvelle colonne, **Etat de disponibilité** a été ajoutée et indique l'état observé de System Automation :

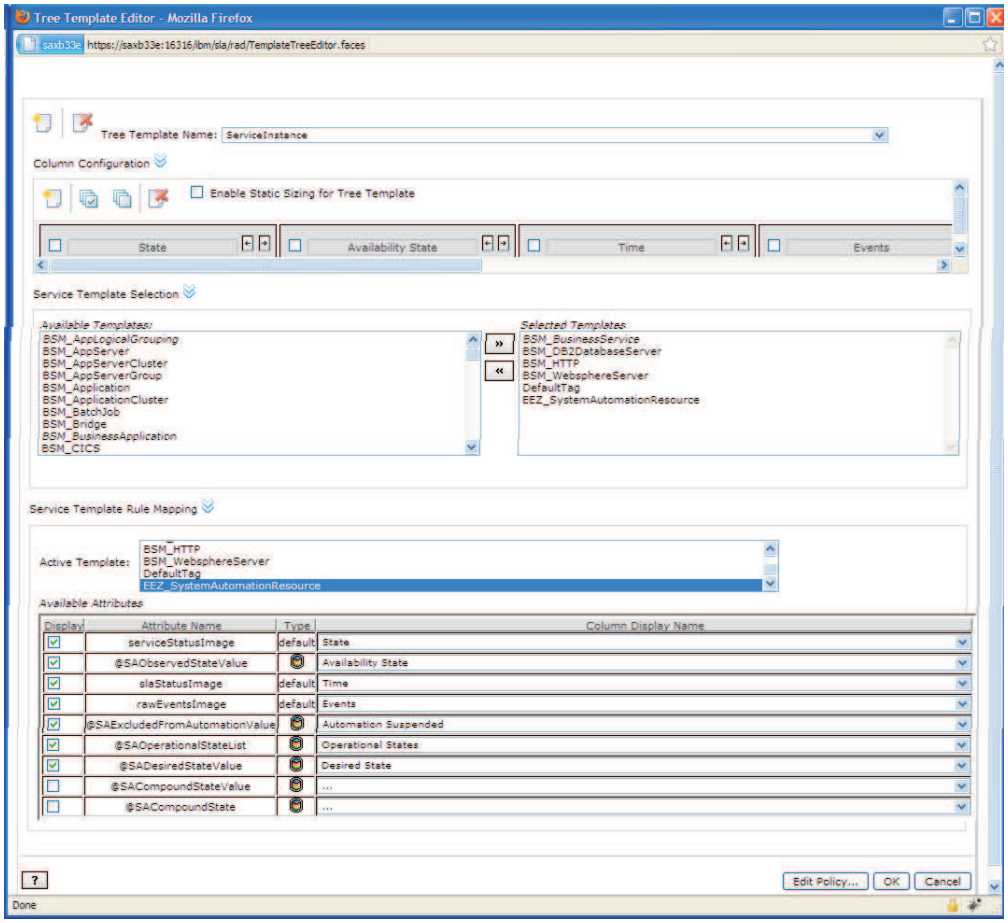

Figure 19. Editeur de modèle d'arborescence

Pour afficher l'arborescence de services mise à jour, actualisez le portlet de navigation des services. La nouvelle colonne affiche désormais la sortie de la règle d'état entrant que vous avez sélectionnée.

Remarque : Vous devez créer de nouveaux événements de modification de statut de ressource pour mettre à jour les informations d'état affichées dans TBSM. Les anciens événements ne sont pas traités à nouveau.

Utilisation de l'éditeur de règles TBSM :

Vous avez la possibilité de formater les valeurs de colonne dans l'éditeur de règles TBSM. Par exemple, vous pouvez afficher les valeurs d'état observé SA dans des couleurs différentes. Pour ce faire, procédez comme suit :

1. Cliquez sur le bouton **Editeur de modèle d'arborescence** dans la barre d'outils du portlet de navigation des services.
2. Choisissez le modèle d'arborescence à modifier dans la liste déroulante **Tree Template Name**.
3. Cliquez sur le bouton **Editer la règle...** pour ouvrir la règle affichant les valeurs de colonnes. La règle intitulée `GetTreeColumnValue` est ouverte dans l'éditeur de règles :

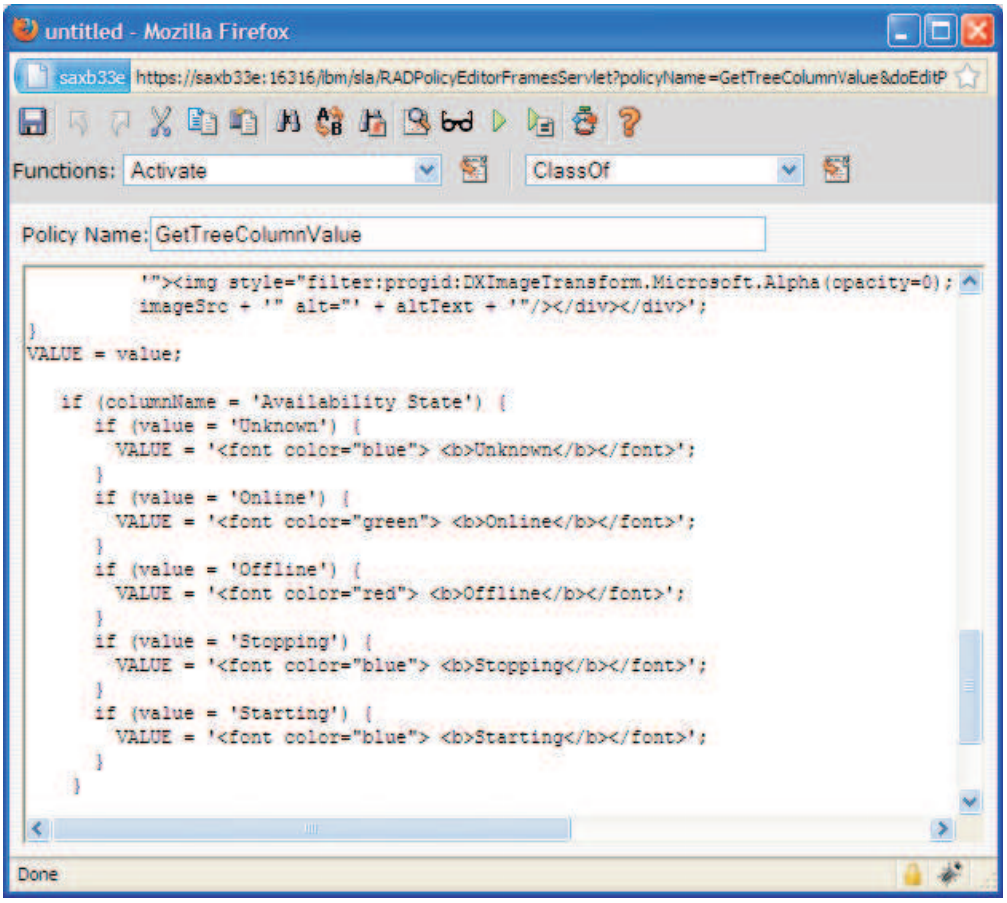

Figure 20. Editeur de modèle d'arborescence TBSM

4. Modifiez la règle. Le fragment de code ci-après illustre comment modifier la couleur des valeurs de sortie basées texte. Cet exemple suppose qu'une colonne nommée “Availability State” (Etat de disponibilité) a été définie et affiche la sortie de la règle `SAObservedState`. Le fragment de règle renvoie la valeur dans une couleur différente en fonction de l'état observé :

```
if (columnName = 'Availability State') {
      if (value = 'Unknown') {
        VALUE = '<font color="blue"> <b>Unknown</b></font>';
   }
   if (value = 'Online') {
        VALUE = '<font color="green"> <b>Online</b></font>';
   }
   if (value = 'Offline') {
        VALUE = '<font color="red"> <b>Offline</b></font>';
   }
   if (value = 'Stopping') {
        VALUE = '<font color="blue"> <b>Stopping</b></font>';
   }
   if (value = 'Starting') {
        VALUE = '<font color="blue"> <b>Starting</b></font>';
   }
```

5. Enregistrez la règle modifiée.

Chapitre 5. Sécurisation

La sécurisation de System Automation for Multiplatforms implique la configuration des connexions SSL (Secure Socket Layer) et la protection des environnements de cluster contre les accès non autorisés.

Vous pouvez configurer la sécurité non root pour l'interface de ligne de commande des systèmes System Automation for Multiplatforms sous AIX et Linux.

Sur les systèmes Linux et AIX, par défaut, l'utilisateur `root` est le seul à disposer des droits requis pour effectuer des tâches opérationnelles dans System Automation for Multiplatforms et pour modifier sa règle d'automatisation, tandis que tous les autres utilisateurs ne possèdent qu'un droit d'accès en lecture.

Gestion des autorisations pour les utilisateurs accédant au cluster

Le concept de sécurité de System Automation for Multiplatforms est basé sur le composant RMC de RSCT, qui implémente l'autorisation de sécurité à l'aide d'un fichier de liste de contrôle d'accès. En particulier, RMC utilise le fichier ACL sur un noeud particulier pour déterminer les autorisations dont un utilisateur doit disposer pour accéder à des classes de ressources et aux instances correspondantes. Dans la mesure où les gestionnaires de ressources de System Automation sont implémentés en interne sous forme d'application RMC, le même ensemble de règles de contrôle ACL doit être utilisé pour permettre aux utilisateurs non root de gérer (définir, annuler la définition ou modifier) les classes de ressources System Automation (`IBM.ResourceGroup`, `IBM.ManagedRelationship`, `IBM.Equivalency`, `IBM.ManagedResource`, `IBM.CHARMControl`, `IBM.Application` et `IBM.ServiceIP`) et de lancer et d'arrêter les groupes de ressources correspondants.

Pour des informations détaillées sur la configuration des fichiers ACL de RMC, reportez-vous aux sections suivantes du manuel IBM RSCT Administration Guide :

- “Managing user access to resources using RMC ACL files” au chapitre 4 ("Managing and monitoring resources using RMC and resource managers")
- “Configuring the global and local authorization identity mappings” au chapitre 7 ("Understanding and administering cluster security services")

Configuration des ID utilisateur non root pour l'interface de ligne de commande

Le support des autorisations de sécurité RSCT et RMC gère l'accès utilisateur en fonction des classes de ressources individuelles et des noeuds simples. Par exemple, l'accès utilisateur peut être limité à une classe de ressource RMC spécifique sur un noeud particulier dans le cluster. Ce paramètre de niveau d'autorisation, en revanche, est complexe et nécessite une compréhension claire de la nature individuelle de chaque classe de ressources RMC.

Par conséquent, vous devez créer des rôles pour un opérateur System Automation for Multiplatforms et un administrateur System Automation for Multiplatforms avec des paramètres généraux qui permettent aux utilisateurs non root de gérer toutes les classes de ressources à partir d'un noeud défini dans le cluster. Utilisez la procédure suivante pour créer ces deux rôles :

- sa_admin pour un administrateur
- sa_operator pour un opérateur

Pour créer les rôles, suivez cette procédure (notez que le droit root est requis). Dans cet exemple, on montre les commandes à utiliser dans un environnement Linux :

1. Créez les ID utilisateur autorisés à gérer System Automation for Multiplatforms sur tous les noeuds :

   ```
   # /usr/sbin/useradd ernie
   # /usr/sbin/useradd bert
   ```

2. Créez un groupe pour les ID utilisateur sur tous les noeuds :

   ```
   # /usr/sbin/groupadd sagroup
   ```

3. Ajoutez le groupe aux ID utilisateur sur tous les noeuds :

   ```
   # /usr/sbin/usermod –G sagroup ernie
   # /usr/sbin/usermod –G sagroup bert
   ```

   Remarque : Assurez-vous de définir la variable d'environnement ci-dessous pour tous les utilisateurs de System Automation for Multiplatforms sur tous les noeuds (portée de domaine homologue) :

   ```
   CT_MANAGEMENT_SCOPE=2
   ```

   Vous pouvez définir la variable de façon permanente si vous la définissez dans le profil utilisateur.

4. Modifiez la propriété du groupe du fichier /var/ct/IBM.RecoveryRM.log.

   Le fichier est utilisé pour suivre l'historique de System Automation for Multiplatforms. Toutes les commandes qui modifient les ressources du gestionnaire d'automatisation (IBM.RecoveryRM) sont consignées dans ce fichier.

   Par défaut, le fichier appartient au groupe d'utilisateurs root :

   ```
   -rw-r--r--  1 root root   204 Oct 4 22:00 /var/ct/IBM.RecoveryRM.log
   ```

   Remplacez le propriétaire du groupe par sagroup :

   ```
   /bin/chgrp sagroup /var/ct/IBM.RecoveryRM.log
   ```

   Remplacez le type de droit d'accès aux fichiers par 664 :

   ```
   # /bin/chmod 664 /var/ct/IBM.RecoveryRM.log
          -rw-rw-r-- 1 root sagroup 204 Oct 4 22:00 /var/ct/IBM.RecoveryRM.log
   ```

   Remarque : Si le fichier /var/ct/IBM.RecoveryRM.log n'existe pas après l'installation initiale de System Automation for Multiplatforms, vous pouvez créer un fichier fictif à l'aide de la commande /usr/bin/touch :

   ```
   # /usr/bin/touch /var/ct/IBM.RecoveryRM.log
   ```

5. Modifiez le fichier /var/ct/cfg/ctsec_map.global sur tous les noeuds.

   Vous devez ajouter les entrées ci-dessous pour les ID utilisateur ernie et bert au fichier de mappage d'identités d'autorisations globales RSCT (/var/ct/cfg/ctsec_map.global) sur tous les noeuds du cluster. Ajoutez les entrées nouvelles au-dessus de l'entrée pour l'utilisateur clusteruser :

   ```
   unix:ernie@<cluster>=sa_operator
   unix:ernie@<any_cluster>=sa_operator
   unix:bert@<cluster>=sa_admin
   unix:bert@<any_cluster>=sa_admin
   unix:bert@<iw>=sa_admin
   ..
   unix:*@*=clusteruser
   ```

   Le fichier est utilisé pour mapper un ID utilisateur local sur un noeud en ID utilisateur global dans le domaine System Automation for Multiplatforms.

Dans l'exemple, l'ID utilisateur local `ernie` est mappé vers l'ID utilisateur global `sa_operator` et l'ID utilisateur local `bert` est mappé vers l'ID utilisateur global `sa_admin`.

Vous pouvez autoriser d'autres ID utilisateur locaux pour System Automation for Multiplatforms en ajoutant des lignes dans ce fichier de mappage global (sur tous les noeuds) et en les mappant vers le rôle opérateur ou administrateur souhaité.

Remarque : Si le fichier `//var/ct/cfg/ctsec_map.global` n'existe pas sur un noeud, copiez le fichier par défaut `/usr/sbin/rsct/cfg/ctsec_map.global` dans le répertoire `/var/ct/cfg` et ajoutez les nouvelles entrées dans le fichier `/var/ct/cfg/ctsec_map.global`. Ne supprimez pas des entrées du fichier `/var/ct/cfg/ctsec_map.global`, qui se trouve dans le fichier par défaut que vous avez copié. Les fichiers `/var/ct/cfg/ctsec_map.global` doivent être identiques sur tous les noeuds du cluster. Ajoutez toujours de nouveaux ID pour les utilisateurs non root au-dessus des entrées pour l'utilisateur `clusteruser`.

6. Modifiez le fichier `/var/ct/cfg/ctrmc.acls` sur tous les noeuds. Vous devez ajouter les entrées ci-dessous pour les ID utilisateur globaux `sa_operator` et `sa_admin` au fichier de contrôle d'accès de RMC (`/var/ct/cfg/ctrmc.acls`), sur tous les noeuds dans le cluster, et mettre en commentaire la ligne qui commence par `LOCALHOST`. Par exemple :

```
# Le paragraphe ci-dessous contient les entrées par défaut
# de la liste de contrôle d'accès.
# Ces entrées sont ajoutées à chaque liste de contrôle
# d'accès définie pour une classe de ressource et
# sont examinées après chaque entrée
# définie explicitement pour une classe de ressources
# par les paragraphes de ce fichier,
# dont le paragraphe OTHER.

DEFAULT
 root@LOCALHOST       *    rw
 # LOCALHOST       *     r  // Notez vos commentaires sur cette ligne
 none:root   *  rw   // Fournissez un accès root à tous
 none:sa_admin   *  rw   // Ajoutez cette ligne pour saadmin
 none:sa_operator   *  rso   // Ajoutez cette ligne pour saoperator
```

7. Une fois que les modifications nécessaires sont terminées, exécutez la commande ci-dessous sur chaque noeud de cluster pour activer les modifications :

```
# /usr/bin/refresh -s ctrmc
```

8. Des modifications supplémentaires sont nécessaires pour utiliser les commandes **`sampolicy`** et **`*samadapter`** :

   a. Accédez aux fichiers de configuration :

```
# /bin/chgrp -R sagroup /opt/IBM/tsamp/sam/cfg
# /bin/chmod g+ws /opt/IBM/tsamp/sam/cfg
# /bin/chmod g+w /opt/IBM/tsamp/sam/cfg/*
```

   b. Accédez aux fichiers journaux :

```
# /bin/chgrp -R sagroup /var/ibm/tivoli/common/eez/logs
# /bin/chmod g+ws /var/ibm/tivoli/common/eez/logs
# /bin/chmod g+w /var/ibm/tivoli/common/eez/logs/*
```

   c. Accédez aux fichiers de configuration dans le répertoire `/etc`. S'il n'existe pas de répertoire `/etc/opt/IBM/tsamp/sam/cfg`, créez-le en utilisant

```
# /bin/mkdir -p /etc/opt/IBM/tsamp/sam/cfg.
```

   Ensuite, définissez les autorisations :

```
# /bin/chgrp -R sagroup /etc/opt/IBM/tsamp/sam/cfg
# /bin/chmod g+ws /etc/opt/IBM/tsamp/sam/cfg
# /bin/chmod g+w /etc/opt/IBM/tsamp/sam/cfg/*
```

9. Instructions particulières relatives au package `sam.policies` (facultatif) : Les règles prédéfinies pour différentes applications sont fournies dans le package d'installation `sam.policies` , qui peut être téléchargé à partir du site IBM Integrated Service Management Library.
10. Pour permettre à un utilisateur qui possède le rôle `sa_admin` de configurer ces règles prédéfinies, les autorisations et la propriété du répertoire `/usr/sbin/rsct/sapolicies` doivent être modifiées une fois que le package `sam.policies` est installé sur tous les noeuds :

```
# chmod –R 2775 /usr/sbin/rsct/sapolicies
# chgrp -R sagroup /usr/sbin/rsct/sapolicies
```

Lorsque ces opérations sont terminées, les utilisateurs locaux `ernie` et `bert` peuvent effectuer des tâches opérationnelles dans System Automation for Multiplatforms, comme l'émission de requêtes de lancement et d'arrêt sur des ressources, et l'utilisateur local `bert` peut effectuer les tâches d'administration d'System Automation for Multiplatforms, comme la définition et la modification des règles.

Modification des autorisations par défaut des utilisateurs non root utilisant RSCT niveau 2.5.4.0 ou supérieur

A partir de RSCT niveau 2.5.4.0 (AIX 6 et Linux), une modification empêche les utilisateurs non root d'exécuter des commandes permettent de lister les ressources. Les autorisations sont configurées automatiquement lorsqu'un domaine est créé.

Si vous migrez un domaine existant vers ce niveau de RSCT, les autorisations pour exécuter des commandes telles que `lssam` ou `lsrg -m` ne sont pas automatiquement configurées pour les utilisateurs autres que l'utilisateur root. Selon le niveau de RSCT, effectuez les actions permettant d'ajuster la configuration :

Le niveau de RSCT est égal ou supérieur à 2.5.5.2 (AIX 6 et Linux :
Créez un domaine pour ajuster la configuration de manière implicite. Ne démarrez pas le nouveau domaine. Vous pourrez le supprimer ultérieurement.

Sinon, ou si le niveau de RSCT est inférieur à 2.4.13.2 :
Utilisez les commandes suivantes pour ajuster la configuration sur tous les noeuds en tant qu'utilisateur root :

1. Modifiez le fichier `/usr/sbin/rsct/cfg/ctsec_map.global` et ajoutez-lui le contenu suivant s'il n'existe pas :

   ```
   unix:*@*=clusteruser
   ```

2. Créez un fichier `/tmp/addacl` et ajoutez-lui le contenu suivant :

   ```
   DEFAULT
      none:clusteruser * r
   ```

3. Ajustez le fichier `acl` à l'aide de la commande suivante :

   ```
   /usr/sbin/rsct/install/bin/chrmcacl -a < /tmp/addacl
   ```

4. Actualisez le sous-système `ctrmc` pour que les modifications deviennent effectives :

   ```
   refresh -s ctrmc
   ```

Les utilisateurs autres que l'utilisateur racine sont désormais en mesure d'utiliser des commandes telles que `lssam` ou `lsrg -m` comme avec les niveaux antérieurs de RSCT.

Limites de la configuration de la sécurité non root

La liste ci-dessous résume les limites de la configuration de la sécurité non root :

- Un utilisateur classique ne peut pas afficher le contenu du fichier de trace du gestionnaire de ressources RMC (par exemple, la trace du démon `IBM.RecoveryRMd`).

  Tous les démons de gestionnaire de ressources RMC utilisent l'utilitaire de bibliothèque de cadre RMC pour créer des fichiers de trace et des images centrales dans le répertoire `/var/ct/<cluster>`. Dans la mesure où ces gestionnaires de ressources ne peuvent être lancés que par un super utilisateur (ID utilisateur `root`) par le biais de la commande **`/usr/bin/startsrc`**, les fichiers qui sont créés appartiennent à l'ID utilisateur `root`.

  Aucun utilisateur non root ne peut collecter des informations de débogage et de trace en utilisant la commande **`/usr/sbin/rsct/bin/ctsnap`**.

  Pour permettre à des utilisateurs non root de collecter des traces ou des données de débogage `ctsnap`, ou les deux, un mécanisme comme «sudo» doit être implémenté pour ces utilisateurs et ces commandes.
- Les commandes suivantes ne peuvent être lancées qu'avec les droits `root` car elles utilisent la consignation Tivoli, qui ne fonctionne que si les fichiers journaux sont gérés avec les droits `root` :
  - La commande **`sampolicy`**.
  - La commande **`samadapter`** pour démarrer l'adaptateur d'automatisation de bout en bout.
  - La commande **`samlicm`** pour installer ou mettre à niveau la licence.
- La granularité des objets de la liste de contrôle d'accès est basée sur les classes de ressources et non sur les ressources. Cela signifie qu'un utilisateur régulier a l'autorisation de modifier les ressources d'une classe de ressources ou non, mais il n'est pas possible d'accorder ou de refuser des autorisations sur la base d'une ressource. Par exemple, un administrateur de base de données ne peut pas disposer d'une autorisation uniquement pour les ressources de base de données.
- Le rôle «sa_operator» peut modifier les ressources en modifiant les valeurs d'attribut pour les ressources. Cela résulte de l'autorisation «s», qui est nécessaire pour émettre des demandes System Automation for Multiplatforms. Sans l'autorisation «s», les utilisateurs qui possèdent ce rôle ne peuvent pas effectuer de tâche utile. Avec l'autorisation «s», ils peuvent modifier et définir des attributs.

Le tableau ci-dessous indique le rôle ou le droit requis pour effectuer les tâches System Automation for Multiplatforms classiques.

Tableau 34. Autorisations et rôles pour effectuer des tâches System Automation for Multiplatforms

Tâche	Droits	Rôles	Autorisations
Installation du produit et de la licence d'utilisation du produit	root	Administrateur système	Installation et mise à niveau de System Automation for Multiplatforms et de la licence du produit.

Tableau 34. Autorisations et rôles pour effectuer des tâches System Automation for Multiplatforms (suite)

Tâche	Droits	Rôles	Autorisations
Gestion des clusters	root/sa_admin	Administrateur système/ Administrateur System Automation for Multiplatforms	Définition, lancement, arrêt et surveillance des clusters et des gestionnaires de ressources RMC individuelles
Définition de ressource et définition de règle System Automation for Multiplatforms	root/sa_admin	Administrateur système/ Administrateur System Automation for Multiplatforms	Définition, suppression, modification des ressources et configuration des règles d'automatisation
Opération d'automatisation	root/sa_admin/ sa_operator	Administrateur système/ Administrateur et opérateur System Automation for Multiplatforms	Emission de demandes en ligne et hors ligne, réinitialisation et surveillances des groupes de ressources et des ressources individuelles
Collecte de données de trace et de débogage pour la détermination des problèmes	root	Administrateur système	Accès à tous les fichiers (journaux) de trace du système et des applications (voir la liste des limitations)
Configuration de la sécurité	root	Administrateur système	Définition, modification et suppression de la configuration de la sécurité décrite dans cette section.
Configuration de l'adaptateur	root/sa_admin	Administrateur système/ Administrateur System Automation for Multiplatforms	Définition, modification et suppression de la configuration de l'automatisation de bout en bout.

Sécurisation de la connexion à l'adaptateur d'automatisation de bout en bout via SSL

Configurez SSL (Secure Socket Layer) dans votre environnement pour les communications entre le serveur d'automatisation de bout en bout System Automation Application Manager et l'adaptateur d'automatisation de bout en bout de System Automation for Multiplatforms.

Cette rubrique décrit la méthode de sécurisation de la connexion entre le serveur System Automation Application Manager et l'adaptateur d'automatisation de bout

en bout. La connexion entre le serveur System Automation Application Manager et l'adaptateur d'automatisation constitue une communication bidirectionnelle dont toutes les demandes et actions sont sécurisées au moyen d'un chiffrement SSL. L'envoi d'événements EIF de l'adaptateur d'automatisation vers le serveur System Automation Application Manager n'est pas sécurisé. Pour plus d'informations sur la sécurisation de cette connexion, voir *IBM Tivoli System Automation Application Manager - Guide d'installation et de configuration*.

Génération d'un fichier de clés et d'un magasin de certificats à l'aide de clés publiques et privées SSL

Générez les fichiers suivants :

- **Magasin de certificats** : Contient les clés publiques du gestionnaire d'application et des adaptateurs FLA.
- **Fichier de clés du gestionnaire d'application** : Contient la clé privée du gestionnaire d'application.
- **Fichier de clés d'adaptateur** : Générez un fichier de clés par adaptateur. Ce fichier contient la clé privée d'un adaptateur FLA.

La figure 21, à la page 138 donne un aperçu des composants, fichiers et étapes permettant de générer les fichiers. Dans ce qui suit, le terme *console d'opérations* fait référence à la console d'opérations System Automation Application Manager.

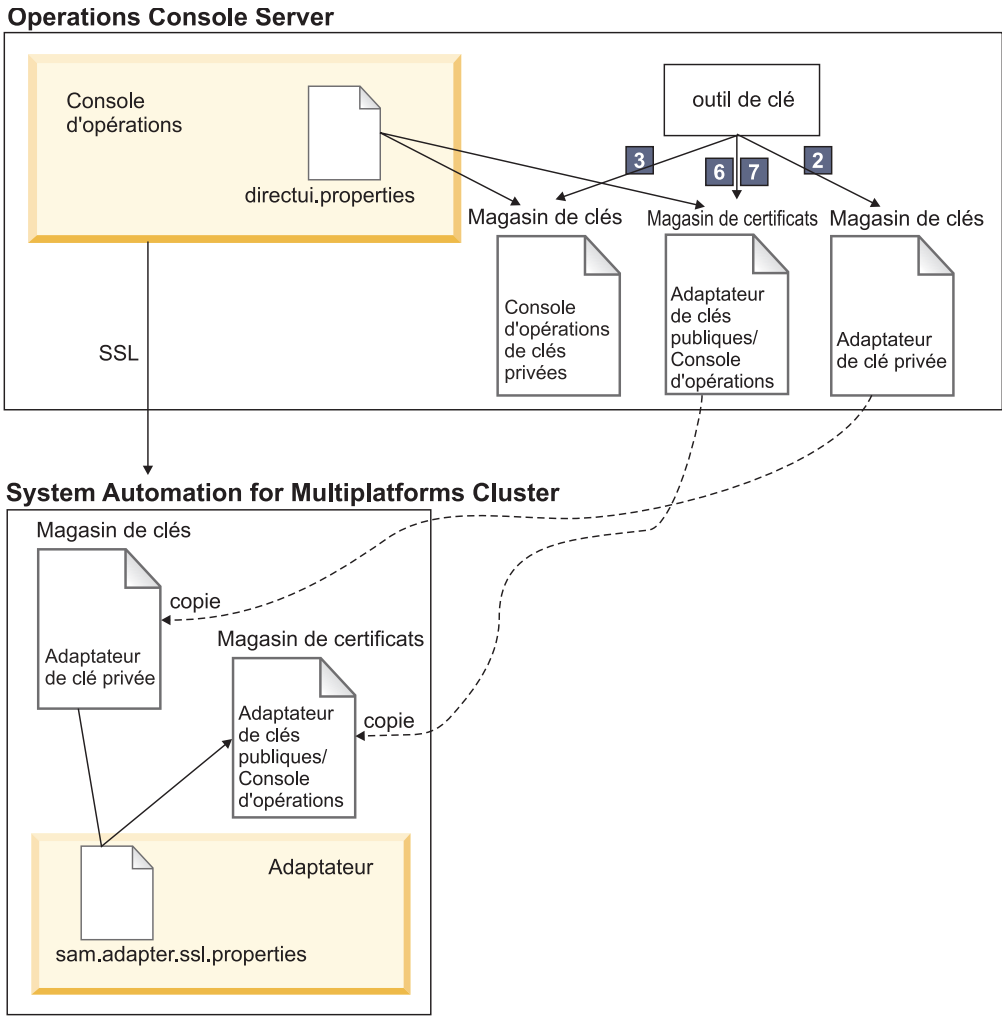

Figure 21. Génération du fichier de clés et du magasin de certificats à l'aide de SSL

Générez le fichier de clés et le magasin de certificats en effectuant les étapes ci-dessous. Les clés arrivent à expiration au bout de 25 ans, la validité par défaut étant paramétrée sur 9125. Veillez à ce que la phrase passe comporte au moins 6 caractères. Les numéros des étapes correspondent à ceux de la figure 21. Les valeurs utilisées sont des exemples ou des valeurs par défaut.

1. **Définissez les variables :**

```
# java keytool from the operations console install directory
OC_INSTALL_DIR=/opt/IBM/tsamp/eez/jre/bin/keytool
# Operations console config file directory
OC_CONFIG_DIR=/opt/IBM/tsamp/eez/ewas/AppServer/profiles/AppSrv01/Tivoli/EEZ
# Les clés arrivent à expiration au bout de 25 ans
KEY_VALIDITY_DAYS=9125
# phrase passe comportant au moins 6 caractères
PASSPHRASE=passphrase
```

2. **Créez le fichier de clés (avec des clés publiques et privées) utilisé pour l'adaptateur d'automatisation :**

```
${JAVA_KEYTOOL} -genkey -keyalg RSA -validity ${KEY_VALIDITY_DAYS} \
          -alias samadapter -keypass ${PASSPHRASE} -storepass ${PASSPHRASE} \
          -dname "cn=SAAM Adapter, ou=Tivoli System Automation, o=IBM, c=US" \
          -keystore ${OC_CONFIG_DIR}/ssl/sam.ssl.adapter.keystore.jks
```

3. **Créez le fichier de clés avec des clés publiques et privées pour la console d'opérations :**

```
{JAVA_KEYTOOL} -genkey -keyalg RSA -validity ${KEY_VALIDITY_DAYS} \
          -alias samoperationsconsole -keypass ${PASSPHRASE} -storepass ${PASSPHRASE} \
          -dname "cn=SAAM Server, ou=Tivoli System Automation, o=IBM, c=US" \
          -keystore "${OC_CONFIG_DIR}/ssl/sam.ssl.operationsconsole.keystore.jks"
```

4. **Exportez le fichier de certificats (avec clé publique) utilisé pour l'adaptateur d'automatisation :**

```
${JAVA_KEYTOOL} -export -alias samadapter \
          -file ${OC_CONFIG_DIR}/ssl/samadapter.cer -storepass ${PASSPHRASE} \
          -keystore "${OC_CONFIG_DIR}/ssl/sam.ssl.adapter.keystore.jks"
```

5. **Exportez le fichier de certificats (avec clé publique) utilisé pour la console d'opérations :**

```
${JAVA_KEYTOOL} -export -alias eezoperationsconsole \
          -file "${OC_CONFIG_DIR}/ssl/eezoperationsconsole.cer" -storepass ${PASSPHRASE} \
          -keystore "${OC_CONFIG_DIR}/ssl/sam.ssl.operationsconsole.keystore.jks"
```

6. **Créez un fichier de clés certifiées et importez le certificat (avec clé publique) utilisé pour l'adaptateur d'automatisation :**

```
${JAVA_KEYTOOL} -import -noprompt -alias samadapter \
          -file "${OC_CONFIG_DIR}/ssl/samadapter.cer" -storepass ${PASSPHRASE} \
          -keystore "${OC_CONFIG_DIR}/ssl/sam.ssl.authorizedkeys.truststore.jks"
```

7. **Créez un fichier de clés certifiées et importez le certificat (avec clé publique) utilisé pour la console d'opérations :**

```
{JAVA_KEYTOOL} -import -noprompt -alias samoperationsconsole \
          -file "${OC_CONFIG_DIR}/ssl/samoperationsconsole.cer" -storepass ${PASSPHRASE} \
          -keystore "${OC_CONFIG_DIR}/ssl/sam.ssl.authorizedkeys.truststore.jks"
```

8. **Supprimez le fichier de certificats utilisé pour l'adaptateur d'automatisation. Ce fichier n'est plus requis pendant la phase d'exécution :**

```
rm ${OC_CONFIG_DIR}/ssl/samadapter.cer
```

9. **Supprimez le fichier de certificats utilisé pour la console d'opérations. Ce fichier n'est plus requis pendant la phase d'exécution :**

```
rm ${OC_CONFIG_DIR}/ssl/samoperationsconsole.cer
```

Activation de la sécurité SSL dans les configurations de l'adaptateur d'automatisation

Effectuez les opérations suivantes pour activer la sécurité SSL dans les configurations de l'adaptateur d'automatisation.

1. **Copiez le fichier de clés certifiées dans tous les noeuds du cluster IBM Tivoli System Automation for Multiplatforms :**

```
scp ${OC_CONFIG_DIR}/ssl/sam.ssl.authorizedkeys.truststore.jks \
    root@<nom_de_noeud_adaptateur>:/etc/opt/IBM/tsamp/eez/cfg/ssl/sam.ssl.authorizedkeys.truststore.jks
```

2. **Copiez le fichier de clés certifiées dans tous les noeuds du cluster IBM Tivoli System Automation for Multiplatforms :**

```
cp ${OC_CONFIG_DIR}/ssl/sam.ssl.adapter.keystore.jks \
    root@<nom_de_noeud_adaptateur>:/etc/opt/IBM/tsamp/sam/cfg/ssl/sam.ssl.adapter.keystore.jks
```

3. **Démarrez l'utilitaire de configuration.**

   Entrez la commande `cfgsamadapter`.

4. **Entrez les paramètres :**

   Dans la fenêtre principale de la boîte de dialogue de configuration, cliquez sur **Configurer**. Renseignez les paramètres suivants dans l'onglet **Sécurité** décrit à la rubrique «Onglet Sécurité», à la page 85. Les valeurs ci-dessous sont des exemples.

   - Fichier de clés certifiées : `/etc/opt/IBM/tsamp/sam/cfg/ssl/sam.ssl.authorizedkeys.truststore.jks`

- Fichier de clés : `/etc/opt/IBM/tsamp/sam/cfg/ssl/sam.ssl.adapter.keystore.jks`
- Mot de passe du fichier de clés : `passphrase`
- Alias de certificat : `samadapter`

Cliquez sur **Enregistrer** pour enregistrer les modifications de la configuration.

5. Dans l'écran principal de la boîte de dialogue de configuration, cliquez sur **Répliquer**. Répliquez les fichiers de configuration sur les autres noeuds du cluster IBM Tivoli System Automation for Multiplatforms, y compris la configuration SSL.
6. Redémarrez l'adaptateur d'automatisation à l'aide de la commande `samadapter`, utilisée pour le contrôle de l'adaptateur d'automatisation. Cela permet d'activer la configuration SSL.
7. Redémarrez le serveur System Automation Application Manager pour activer la configuration SSL.

   Exécutez les commandes suivantes pour démarrer ou arrêter manuellement le serveur System Automation Application Manager :

   Démarrage
   `/opt/IBM/WebSphere/AppServer/bin/startServer.sh server1`

   Arrêt `/opt/IBM/WebSphere/AppServer/bin/stopServer.sh server1`

   Remarque : L'ID et le mot de passe administrateur WebSphere Application Server sont obligatoires pour pouvoir arrêter le serveur System Automation Application Manager.

Utilisation d'IBM Support Assistant

IBM Support Assistant est une application autonome gratuite que vous pouvez installer sur n'importe quel poste de travail. IBM Support Assistant permet de gagner du temps lors des recherches de ressources relatives aux produits, au support et à la formation et permet de recueillir des informations d'assistance lorsque vous devez ouvrir un PMR (problem management record) ou ETR (Electronic Tracking Record), que vous pouvez ensuite utiliser pour suivre le problème.

L'application peut être enrichie en installant les modules de plug-in spécifiques au produit pour les produits IBM utilisés. Le plug-in spécifique au produit pour Tivoli System Automation for Multiplatforms offre les ressources suivantes :

- Liens de support
- Liens éducatifs
- Possibilité de soumettre des rapports de gestion d'incident
- Fonction de collecte de traces

Installation d'IBM Support Assistant et du plug-in Tivoli System Automation for Multiplatforms

Pour installer IBM Support Assistant V4.1, procédez comme suit :

- Accédez au site Web IBM Support Assistant :
  `www.ibm.com/software/support/isa/`
- Téléchargez le module d'installation correspondant à votre plateforme. Vous devrez vous connecter avec un ID utilisateur IBM et un mot de passe (par exemple, un ID utilisateur MySupport ou developerWorks). Si vous ne possédez pas d'ID utilisateur IBM, vous pouvez exécuter la procédure d'enregistrement gratuite en vue d'en obtenir un.
- Décompressez le module d'installation dans un répertoire temporaire.
- Suivez les instructions indiquées dans le *guide d'installation et de résolution des incidents*, accompagnant le module d'installation, pour installer l'application IBM Support Assistant.

Pour installer le plug-in de Tivoli System Automation for Multiplatforms, procédez comme suit :

1. Démarrez l'application IBM Support Assistant. IBM Support Assistant est une application Web qui s'affiche dans le navigateur Web configuré par défaut par le système.
2. Cliquez sur l'onglet **Updater** dans l'application IBM Support Assistant.
3. Cliquez sur l'onglet **New Products and Tools**. Les modules de plug-in sont présentés par famille de produits.
4. Sélectionnez **Tivoli > Tivoli Tivoli System Automation for Multiplatforms**.
5. Sélectionnez les fonctions à installer, puis cliquez sur **Installer**. Veuillez consulter les informations sur la licence et les instructions d'utilisation.
6. Redémarrez IBM Support Assistant.

Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services dans ce pays.

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans certains autres pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations
IBM Canada Ltd.
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7
Canada

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Corporation
Mail Station P300
2455 South Road
Poughkeepsie New York 12601-5400
U.S.A.

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions de l'ICA, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit à l'adresse suivante :

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japon

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales. LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut modifier sans préavis les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

Si vous visualisez ces informations en ligne, il se peut que les photographies et illustrations en couleur n'apparaissent pas à l'écran.

Marques

- IBM, le logo IBM, ibm.com, AIX, DB2, developerWorks, HACMP, NetView, Tivoli, Tivoli Enterprise, Tivoli Enterprise Console, WebSphere et z/OS sont des marques d'International Business Machines Corporation aux Etats-Unis et/ou dans certains autres pays. IBM Redbooks et le logo IBM Redbooks sont des marques d'IBM.
- Adobe, Acrobat, Portable Document Format (PDF) et PostScript sont des marques d'Adobe Systems Incorporated aux Etats-Unis et/ou dans certains autres pays.
- Microsoft, Windows et le logo Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.
- Java ainsi que tous les logos et toutes les marques incluant Java sont des marques de Sun Microsystems, Inc. aux Etats-Unis et/ou dans certains autres pays.
- Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

- Red Hat et l'ensemble des marques associées à Red Hat sont des marques de Red Hat, Inc., aux Etats-Unis et/ou dans certains autres pays.
- UNIX est une marque enregistrée de The Open Group aux Etats-Unis et/ou dans certains autres pays.
- Les autres noms de sociétés, de produits et de services peuvent appartenir à des tiers.

Index

N

O

P

Q

R

S

T

U

V

Z

Numéro de programme : 5724-M00

SC11-7498-04