Tivoli System Automation for Multiplatforms 4.1.0.7

インストールと構成のガイド

SA88-7249-05

お願い

本書および本書で紹介する製品を ご使用になる前に、135 ページの『特記事項』に記載されている情報をお読みください。

「*System Automation for Multiplatforms* インストールと構成のガイド」のこの版は、IBM Tivoli System Automation for Multiplatforms バージョン 4 リリース 1 モディフィケーション 0、 プログラム番号 5724-M00、および新しい版で明記されていない限り、以降のすべてのリリースおよびモディフィケーションに適用されます。

本書は、SA88-7249-04 の改訂版です。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典：
SC34-2699-05
Tivoli System Automation for Multiplatforms 4.1.0.6
Installation and Configuration Guide

発行：
日本アイ・ビー・エム株式会社

担当：
トランスレーション・サービス・センター

目次

図

表

本書について

本書では、IBM Tivoli System Automation for Multiplatforms (System Automation for Multiplatforms) が提供するポリシー・ベースの自動リカバリー機能を実装および使用する方法について説明します。

System Automation for Multiplatforms を使用すると、AIX® クラスター (IBM® System p 上)、Linux® クラスター (IBM System x、System z®、System i®、System p 上)、および Windows クラスター (IBM System x 上) 上のリソースの可用性が高くなります。

本書の対象読者

本ガイドは、System Automation for Multiplatforms の自動化機能およびフェイルオーバー機能を使用する必要があるシステム管理者およびオペレーターを対象としています。

詳細情報の参照先

Tivoli System Automation ライブラリーは、本書 (Tivoli System Automation for Multiplatforms について説明しています) を含め、以下の資料から構成されています。

- *System Automation for Multiplatforms* 管理者とユーザーのガイド (SA88-7250-01)
- *Tivoli System Automation for Multiplatforms* インストールと構成のガイド (SA88-7249-01)
- *Tivoli System Automation for Multiplatforms* リファレンス・ガイド (SA88-7251-01)
- *Tivoli System Automation for Multiplatforms* 高可用性ポリシー・ガイド *(SA88-7252-01)*

資料一式を、次のサイトからダウンロードできます。

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

Tivoli System Automation ライブラリーには、System Automation Application Manager について説明する以下の資料が用意されています (本書も含まれています)。

- *System Automation Application Manager Administrator's and User's Guide* (SC34-2701-00)
- *System Automation Application Manager Installation and Configuration Guide*、SC34-2702-00
- *System Automation Application Manager Reference and Problem Determination Guide*、SC34-2703-00

これらの資料は、以下のページからダウンロードすることができます。

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

IBM Tivoli System Automation ホーム・ページには、サポート・リンクおよび保守パッケージのダウンロードなど、役に立つ最新情報が記載されています。 IBM Tivoli System Automation のホーム・ページは 以下からアクセスできます。

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

表記規則

本書では、以下の強調表示の規則を使用しています。

表 *1.* 本書の強調表示の規則	
太字	コマンド、サブルーチン、キーワード、ファイル、構造体、ディレクトリー、およびシステムによって名前が事前に定義されているその他の項目を示します。また、ユーザーが選択するボタン、ラベル、およびアイコンなどのグラフィカル・オブジェクトも 示します。

表 1. 本書の強調表示の規則 (続き)	
イタリック	ユーザーが指定する実際の名前または値のパラメーターを示します。
モノスペース	具体的なデータ値の例、画面に表示されるものと同様のテキスト例、プログラマーが作成するものと同様のプログラム・コードの一部の例、システムからのメッセージ、または実際に入力する必要がある 情報を示します。

本資料では、リソース、リソース・グループ、同値、および関係を示すために シンボルを使用します。使用するシンボルは以下のとおりです。

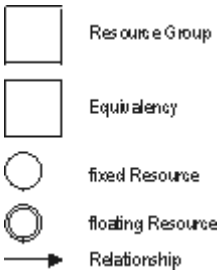


図 1. このガイドで使用するシンボル

ISO 9000

本製品の開発および製造において、ISO 9000 審査登録済みの品質システムが 使用されました。

RSCT 関連情報

以下の IBM Reliable Scalable Cluster Technology (RSCT) の資料は System Automation for Multiplatforms CD として入手できます。

- *RSCT* 管理ガイド
- *RSCT for AIX 5L:* テクニカル・リファレンス
- *RSCT for Multiplatforms:* テクニカル・リファレンス
- *RSCT* メッセージ
- *RSCT Diagnosis Guide*

RSCT について詳しくは、『IBM Cluster systems』を参照してください。

詳しくは、『Linux on IBM zSeries and S/390®: High Availability for z/VM® and Linux』IBM Redpaper を参照してください。

資料の入手方法

System Automation for Multiplatforms の資料は、以下の Web サイトでも入手可能です (リリース時点で有効)。

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

連絡先電子メール・アドレス

以下は英語のみの対応となります。電子メールでのご連絡を希望される場合は、eservdoc@de.ibm.com までコメントをお寄せください。

このリリースの新機能

System Automation for Multiplatforms バージョン 4.1.0 の新機能について概説します。

新規 samcc コマンドによるコマンド行での操作の向上

System Automation for Multiplatforms バージョン 4.1.0.2 には新規コマンド samcc が追加されました。このコマンドをコマンド行インターフェースでの操作コンソールとして使用できます。詳しくは、「」を参照してください。

追加プラットフォーム・サポート

System Automation for Multiplatforms バージョン 4.1.0.1 では以下の新規プラットフォームをサポートします。

- SUSE SLES 12 (64 ビット)
- Red Hat RHEL 7 (64 ビット)
- Ubuntu 14.04 (64 ビット): System x、Power Systems (リトル・エンディアンのみ)

System Automation for Multiplatforms バージョン 4.1.0.2 では以下の新規プラットフォームをサポートします。

- Red Hat RHEL 7.1 on Power Systems Little Endian (64 ビット)

System Automation for Multiplatforms バージョン 4.1.0.3 では以下の新規プラットフォームをサポートします。

- AIX 7.2

System Automation for Multiplatforms バージョン 4.1.0.4 では以下の新規プラットフォームをサポートします。

- Ubuntu 16.04 (64 ビット): System x、Power Systems (リトル・エンディアンのみ)。

詳しくは、「*System Automation for Multiplatforms* インストールと構成のガイド」を参照してください。

System Automation for Multiplatforms バージョン 4.1.0.5 では以下の新規プラットフォームをサポートします。

- SUSE SLES 15 (64 ビット)
- Ubuntu 18.04 (64 ビット): System x、Power Systems (リトル・エンディアンのみ)。

System Automation for Multiplatforms バージョン 4.1.0.5 では以下のサポートが追加されました。

- SAP Netweaver 7.5.3 ENSA2

System Automation for Multiplatforms バージョン 4.1.0.6 では以下の新規プラットフォームをサポートします。

- Red Hat RHEL 8 (64 ビット)
- Ubuntu 20.04 (64 ビット): System x, Power Systems (リトル・エンディアンのみ)

System Automation for Multiplatforms バージョン 4.1.0.6 では以下のサポートが追加されました。

- S/4HANA 1809 の SAP NetWeaver サポートの追加
- S/4HANA 1909 の SAP NetWeaver サポートの追加
- Oracle 19c のサポートの追加
- SAP HANA 2.0 SPS 04 リビジョン 046 のサポートの追加

System Automation for Multiplatforms バージョン 4.1.0.7 では次の新規プラットフォームがサポートされます。

- AIX 7.2 TL5

System Automation for Multiplatforms バージョン 4.1.0.7 では次のサポートが追加されました。

- S/4HANA 2020 の SAP NetWeaver サポートの追加
- SAP HANA 2.0 SPS 05 リビジョン 050 のサポートの追加

SAP の高可用性ポリシーの改善

SAP Central Services 高可用性ポリシーは、別個に課金される System Automation for Multiplatforms のオプション・フィーチャーとして使用可能です。この SAP Central Services 高可用性ポリシーが、SAP Netweaver テクノロジーに適応するようになりました。

ユーザーは、システム自動化ポリシーに干渉することなく、SAP ユーザー・インターフェースを使用して SAP Netweaver スタックの開始と停止を実行することができます。SAP Software Update Manager では、更新プロセス中にシステム自動化を使用不可にすることなく、Netweaver ソリューションを更新できます。

サポートされる SAP 構成オプションは、SAP Central Services のフェイルオーバーの Java、ABAP、および DUAL スタック・サポートです。また、以下の構成オプションもサポートされます。

- アプリケーション・サーバー (主要アプリケーション・サーバーと追加のアプリケーション・サーバーの代わりに再始動)
- SAProuter のフェイルオーバー
- SAP Web ディスパッチャーのフェイルオーバー
- データベースに対する依存関係サポートを行ってからの始動

System Automation for Multiplatforms バージョン 4.1.0.2 では以下のサポートが追加されました。

- SAP HANA System Replication フェイルオーバー

サポートされる SAP カーネルのバージョンは 7.20 以上です。

詳しくは、「*System Automation for Multiplatforms* 高可用性ポリシー・ガイド」を参照してください。

アプリケーション障害に関する情報の収集

samwhy プログラムは、System Automation で制御されているアプリケーションに関してアプリケーション障害の検出とその障害の分析ができるようになっている、使いやすい簡易ツールです。samwhy は、発生した事象についてオペレーターが把握するのを支援し、それに対する System Automation の対応の仕方について理由を明らかにするものです。

詳しくは、「*System Automation for Multiplatforms* リファレンス・ガイド」を参照してください。

エンドツーエンド自動化アダプターの高可用性の単純化

追加の自動化ポリシーおよび仮想 IP アドレスが不要になっています。

詳しくは、「System Automation for Multiplatforms インストールと構成のガイド」を参照してください。

非 root ユーザーでのエンドツーエンド自動化アダプターの実行

デフォルトでは、エンドツーエンド自動化アダプターは root ユーザーで実行されます。このリリースでは、非 root ユーザーで実行されるようにアダプターをセットアップすることもできるようになりました。

詳しくは、「System Automation for Multiplatforms インストールと構成のガイド」を参照してください。

第 1 章 計画

計画には、現行インフラストラクチャーの評価と、システムに必要な前提条件が備わっていることの確認が含まれます。

インストールの計画

ご使用の AIX および Linux 環境に System Automation for Multiplatforms をインストールする前に、正しい前提条件が備わっているようにする必要があります。

このタスクについて

パッケージ化

System Automation for Multiplatforms は、IBM® にメディア・パックとしてオーダーするか、IBM ソフトウェア配布ダウンロード・サイトからダウンロードすることができます。

製品 DVD

System Automation for Multiplatforms バージョン 4.1 製品 DVD の内容。

このタスクについて

以下のラベルの付いた個別の DVD に、各プラットフォームおよび対応するアーキテクチャーのスクリプトとソフトウェア・パッケージが含まれています。

- Tivoli System Automation for Multiplatforms 4.1 - Linux on System x、Linux on POWER®、および Linux on System z
- Tivoli System Automation for Multiplatforms 4.1 - AIX

System Automation for Multiplatforms をインストールするには、下表の右側の列に記載されているインストール・スクリプトを使用します。

表 2. 製品 *DVD* のバージョン

オペレーティング・システム	製品 DVD のラベル	インストール・スクリプト
Linux	Tivoli System Automation for Multiplatforms v4.1 - Linux on System x、Linux on POWER および Linux on System z	`SAM4100MPLinux/installSAM`
AIX	Tivoli System Automation for Multiplatforms v4.1 - AIX	`SAM4100MPAIX/installSAM`

電子配布

DVD による配布より電子配布の方が望ましい場合は、System Automation for Multiplatforms の購入後に、提供される URL を使用して該当するアーカイブ・ファイルを Web からダウンロードできます。

Linux

表 *3. Linux* プラットフォーム用のアーカイブ

アーカイブ名	説明
SA MP 4.1 Linux.tar	製品のインストールに使用するアーカイブです。 このアーカイブを解凍するためには、GNU tar 1.13 以降が必要です。**tar xf** コマンドを使用して、アーカイブを解凍してください。ファイルの解凍が完了すると、以下のディレクトリーにインストール・スクリプト installSAM が配置されます。SAM4100MPLinux

AIX

表 *4. AIX* プラットフォーム用のアーカイブ

アーカイブ名	説明
SA MP 4.1 AIX.tar	製品のインストールに使用するアーカイブです。 **tar xf** コマンドを使用して、アーカイブを解凍してください。ファイルの解凍が完了すると、以下のディレクトリーにインストール・スクリプト installSAM が配置されます。SAM4100MPAIX

前提条件

System Automation for Multiplatforms のソフトウェアおよびハードウェアの要件を満たしていることを確認します。

AIX システムでの前提条件

- System Automation for Multiplatforms をインストールするには、root 権限が必要です。
- 32 ビット・バージョンの Java 7、Java 7.1、または Java 8 (最小限で、以下に示す Service Refresh レベルのもの) が必要です。
  - Java 7.0 SR8: AIX パッケージ Java7.jre/Java7.sdk 7.0.0.145
  - Java 7.1 SR2: AIX パッケージ Java71.jre/Java71.sdk 7.1.0.25
  - Java 8.0 SR0: AIX パッケージ Java8.jre/Java8.sdk 8.0.0.507
  - System Automation for Multiplatforms フィックスパック・バージョン 4.1.0.6 では、Java 8 SR6 FP15: AIX パッケージ Java8.jre/Java8.sdk 8.0.6.15 がサポートされています。
- AIX 上の System Automation for Multiplatforms フィックスパック・バージョン 4.1.0.6 では、RSCT 3.2.5.2 がインストールされます。次の AIX TL レベルがサポートされるのは、このフィックスパックが適用されている場合のみです。
- AIX 7.1 TL 5
- AIX 7.2 TL 2
- AIX 7.2 TL 3
- AIX 7.2 TL 4

Linux システムでの前提条件

System Automation for Multiplatforms を Linux システムにインストールするには、以下の前提条件を満たす必要があります。

- RedHat v7.1 システムごとに以下のパッケージが必要です。
  - `perl-Sys-Syslog`
- RedHat v8 システムごとに以下のパッケージが必要です。
  - `perl-Net-Ping`
- System Automation for Multiplatforms をインストールするには root 権限が必要です。
- 64 ビット・カーネルが実行されている場合でも、System Automation for Multiplatforms をインストールする前に、いくつかの 32 ビット・ライブラリーをそれぞれの RedHat 6 システムにインストールする必要があります。 これらのライブラリーは、以下の RPM Package Manager パッケージに含まれています。
- `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 o db4-4.7.25`
- `libselinux-2.0.94 o pam-1.1.1`
- `compat-libstdc++-33-3.2.3`
- System Automation for Multiplatforms フィックスパック・バージョン 4.1.0.6 では、Java 8 SR6 FP15: Linux パッケージ Java8.jre/Java8.sdk 8.0.6.15 がサポートされています。

RSCT パッケージ

AIX への System Automation for Multiplatforms のインストール時に、System Automation for Multiplatforms に必要な RSCT パッケージのレベルがオペレーティング・システムに既にインストールされている RSCT パッケージのレベルに対して検査され、不足しているパッケージまたは上位の RSCT パッケージが必要に応じてインストールされます。ある環境では、上位レベルの特定の RSCT パッケージを手動でインストールする必要があります。例えば、RSCT 基本パッケージがインストールされておらず、インストールされている RSCT コア・パッケージのレベルが System Automation for Multiplatforms に付属の RSCT パッケージのレベルより高い場合は、RSCT 前提条件が満たされていないことが原因で、RSCT 基本パッケージのインストールが失敗する可能性があります。適切な RSCT ファイル・セットを AIX サービス・センターからダウンロードして インストールすることによって、インストールされているすべての RSCT パッケージが確実に同じレベルに なるようにする必要があります。

System Automation for Multiplatforms バージョン 4.1.0.0 には、RSCT レベル 3.1.5.3 (APAR IV52893) が含まれています。

System Automation for Multiplatforms バージョン 4.1.0.6 には、RSCT レベル 3.2.5.3 (Linux 64 ビット OS)、RSCT レベル 3.1.5.16 (Linux 32 ビット OS)、および RSCT レベル 3.2.5.2 (AIX OS) が含まれています。

KVM または VMWare などの仮想環境における要件

仮想マシンには時刻を追跡するための確実な方法がないことが多いため、タイム・スタンプ・カウンターを備えた CPU では同期の問題が発生しやすくなります。時刻同期の問題を回避するには、仮想環境で実行されるノードに対して適切な時刻同期 (NTP など) を構成します。

前提条件の検査

前提条件検査の実行方法を確認します。

このタスクについて

以下のステップを実行してください。

1. root または同等の権限でログインします。

2. インターネットから tar ファイルをダウンロードした場合は、次のようにしてファイルを解凍します。

```
tar -xvf <tar file>
```

   DVD で製品を入手した場合は、DVD をマウントし、DVD がマウントされているディレクトリーに移動します。
3. 以下のコマンドを入力します。
   - **Linux: cd SAM4100MPLinux**
   - **AIX: cd SAM4100MPAIX**

   サポートされるプラットフォームについては、5 ページの『サポートされるプラットフォーム』を参照してください。
4. 前提条件検査を開始するために、以下のコマンドを発行します。

```
./prereqSAM
```

   通常、**prereqSAM** コマンドに使用できるオプションは指定しません。このコマンドの詳細については、*Tivoli System Automation for Multiplatforms* リファレンス・ガイド を参照してください。
5. 検査が完了したら、欠落した前提条件についての情報がないかどうか、次のログ・ファイルを調べます。

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

   <#> タグは番号です。最も大きな番号が最新のログ・ファイルを示します。
6. ご使用のシステムが前提条件検査に合格しなかった場合は、問題を解決した後、インストールを開始します。

インストールの前提条件

このタスクについて

インストールを開始する前に、以下の要件を満たしておく必要があります。

- システムに System Automation for Multiplatforms をインストールするには、root 権限が必要です。
- SUSE OS プラットフォームを除くすべての OS プラットフォームに Korn シェルをインストールする必要があり、SUSE OS プラットフォームには MirBSD Korn シェル (mksh) をインストールする必要があります。
- ネイティブ RSCT コマンドを含む System Automation for Multiplatforms のコマンド行インターフェースを使用するには、Perl が必要です。コマンド行インターフェースは、オペレーティング・システムの一部として Linux または AIX システムにデフォルトでインストールされます。英語以外の言語で System Automation for Multiplatforms を使用している場合は、Perl の特別なバージョンが必要になることがあります。Perl 5.8.0 の既知の問題および Perl 5.8.0 による UTF-8 エンコード・ロケール の処理方法が原因で、一部の文字が正しく表示されないことがあります。Perl 5.8.0 がインストールされているシステムで UTF-8 エンコード・ロケールを使用している場合に、この問題が発生する可能性があります。Perl 5.8.0 より前のバージョンまたは 5.8.0 より後のバージョンを使用しているか、非 UTF-8 エンコード・ロケールを使用している場合は、この問題は発生しません。

  Linux ディストリビューションの Perl 5.8.0 バージョンをアップグレードする場合は、以下のステップを処理します。

  1. Perl 5.8.1 ソースをダウンロードします。
  2. **-xvf** を使用して、ファイルを任意のディレクトリーに解凍します。
  3. ダウンロードしたファイルに付属する説明を参照し、UTF-8 システムでコンパイルとインストールを実行します。
  4. System Automation for Multiplatforms が使用する Perl バージョンのディレクトリーを指し示すシンボリック・リンクを変更します。

変更前のリンク:

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

Perl の新しいバージョンがインストールされている変更後のディレクトリーのリンク:

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

- ディレクトリー /usr/sbin および /opt に 100 MB 以上のフリー・スペースがあり、ディレクトリー /var にも 100 MB 以上のフリー・スペースがあることを確認します。
- エンドツーエンド自動化アダプターを実行するよう構成されているノードでは、128MB 以上の RAM が使用可能である必要があります。
- AIX への System Automation for Multiplatforms のインストール時に、System Automation for Multiplatforms に必要な RSCT パッケージのレベルが、オペレーティング・システムに既にインストールされている RSCT パッケージのレベルに対して検査されます。不足しているパッケージまたは上位の RSCT パッケージが必要に応じてインストールされます。ある環境では、上位レベルの特定の RSCT パッケージを手動でインストールする必要があります。例えば、RSCT 基本パッケージがインストールされておらず、インストールされている RSCT コア・パッケージのレベルが System Automation for Multiplatforms に付属の RSCT パッケージのレベルより高い場合は、RSCT 前提条件が満たされていないことが原因で、RSCT 基本パッケージのインストールが失敗します。適切な RSCT ファイル・セットを AIX サービス・センターからダウンロードして インストールすることによって、インストールされているすべての RSCT パッケージが確実に同じレベルに なるようにする必要があります。
- その他のオペレーティング・システム固有の要件については、『Software Product Compatibility Reports』を参照してください。
- 2 バイト文字セット (DBCS) を使用する言語 では、Telnet ダイアログ・バッファーが、長いメッセージを正しく表示するのに十 分な大きさである必要があります。不足している場合は、Telnet ダイアログ・バッファーのサイズを大きくしてください。
- 一部の RHEL ディストリビューションでは、SELinux 環境がデフォルトでオンになっています。System Automation for Multiplatforms が正常に動作するように、SELinux 環境をオフにしてください。

サポートされるプラットフォーム

System Automation for Multiplatforms によってサポートされるプラットフォームについて説明します。

このタスクについて

System Automation for Multiplatforms は、以下の UNIX 環境をサポートします。

- Linux on System z
- Linux on System x
- Linux on Power®
- Ubuntu on System x[5]
- Ubuntu on Power[5]
- AIX

System Automation for Multiplatforms は、以下のマシンとシステムで稼働します。

- Linux を稼働しているすべての IBM Systems マシン。
- AIX を稼働している IBM System p マシン。

System Automation for Multiplatforms は、以下の環境で稼働します。

- IBM System x (Intel IA64 ベース・サーバーを除く) およびその他すべての 32 ビット Intel ベース・サーバー、AMD Opteron ベース・サーバー (64 ビット)、または Intel EM64T ベース・サーバー (64 ビット) 上の VMware。vMotion を使用したシステムの稼働中のマイグレーションはサポートされます (8 ページの『VMware vMotion のサポート』を参照)。

- IBM System x 上のすべてのサポート対象の Linux ディストリビューションでの RHEV-H バージョン 4.3、KVM ハイパーバイザー・バージョン 5.4 以上。システムの稼働中の移行はサポートされません。

サポートされるオペレーティング・システム・バージョンを次の表にリストします。

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

表 *5. System Automation for Multiplatforms* のサポートされる *UNIX* および *Linux* プラットフォーム

	IBM System x[1]	**IBM System z**	**Power Systems**	**Power Systems (リトル・エンディアン)**
SUSE SLES 12 (64 ビット)[4]	x	x		x
SUSE SLES 15 (64 ビット)[7]	x	x		x
Red Hat RHEL 7 (64 ビット)	x[4]	x[4]	x[4]	x [5]
Red Hat RHEL 8 (64 ビット)[8]	x	x		x
Ubuntu 18.04 LTS (64 ビット)[7]	x			x
Ubuntu 20.04 LTS (64 ビット)[8]	x			x
AIX 7.1.5	x[6]			
AIX 7.2.3	x[7]			
AIX 7.2.4	x[8]			
AIX 7.2.5	x[9]			

以下の注記のいずれかがさらに具体的な最小要件を示している場合を除き、上記のサポート対象の SUSE バージョンおよび Red Hat バージョンのすべての SP レベルもサポートされます。

注 :

1. System x とは、System x (Intel IA64 ベース・サーバーを除く) およびその他すべての 32 ビット Intel ベース・サーバー、または AMD Opteron ベース・サーバー (64 ビット)、または Intel EM64T ベース・サーバー (64 ビット) を意味します。
2. zSystems バージョン z15 と pSystems バージョン p9 がサポートされています。
3. このフィックスパックにバンドルされている RSCT パッケージでサポートされており (詳しくは、「前提条件」(ページ 2) を参照)、かつこのフィックスパックで認定されている SP レベルとの後方互換がある場合は、Linux の将来または新規のすべての SP レベル (SUSE および RHEL) がサポートされます。
4. プラットフォーム・サポートはフィックスパック 4.1.0.1 で導入されます。
5. プラットフォーム・サポートはフィックスパック 4.1.0.2 で導入されます。
6. プラットフォーム・サポートはフィックスパック 4.1.0.4 で導入されます。
7. プラットフォーム・サポートはフィックスパック 4.1.0.5 で導入されます。
8. プラットフォーム・サポートはフィックスパック 4.1.0.6 で導入されます。
9. プラットフォーム・サポートはフィックスパック 4.1.0.7 で導入されます。

詳しくは、37 ページの『新しいオペレーティング・システムへのインストール』 (ページ 34) を参照してください。

サポートされるネットワーク・インターフェース

このタスクについて

すべてのプラットフォームで、10 メガビット・イーサネット、高速イーサネット、およびギガビット・イーサネットがサポートされます。さらに、System z プラットフォームでは、ハイパーソケット、CTC、および VM Guest LAN も サポートされます。

ネットワーク・ファイル・システムのサポート

System Automation for Multiplatforms では、Linux on POWER、Linux on System x、Linux on System z、および AIX 上のネットワーク・ファイル・システムがサポートされます。

ネットワーク・ファイル・システムは獲得されません。ネットワーク・ファイル・システムを自動化するには、ユーザー定義の `IBM.AgFileSystem` リソースを使用します。

制約事項 :

- `IBM.AgFileSystem` クラスのネットワーク・ファイル・システムは、インポートするシステムの `root` ユーザーがファイル・システムに対して書き込み権限を持っている場合にのみ、正常に自動化およびモニターできます。
- ファイル・システムをカスケードした使用法は実行できません。

  System Automation for Multiplatforms を使用すると、エクスポートされたファイル・システムが、共用ディスク・メディアに常駐する `IBM.AgFileSystem` クラスのリソースとして自動化される、可用性の高い NFS サーバーを定義できます。NFS サーバー自身は、共用ディスク・メディアに対するアクセス権限を持つシステム上で移動する可能性のある `IBM.Application` クラスのリソースとして自動化されます。ただし、追加システムがネットワーク・ファイル・システムをインポートする場合は、インポートされるファイル・システムが、インポートするシステム上にユーザー定義の `IBM.AgFileSystem` リソースとして既に存在していてはなりません。存在する場合は、ファイル・システムのモニターは失敗し、リソースは OpState 3 (`FAILED OFFLINE`) の状態になります。

ライブ・パーティション・モビリティー・サポートの要件

このタスクについて

AIX レベル 6100-00-01 (またはそれ以上) がソースおよび宛先の POWER6® サーバーにインストールされている場合は、ライブ・パーティション・モビリティー機能を使用して、System Automation for Multiplatforms ノードとして実行されている LPAR をマイグレーションできます。System Automation for Multiplatforms クラスターの状態や操作には影響しません。クラスターは、標準 (デフォルト) のハートビート設定を使用するように構成されます。その場合、アプリケーション・サーバーでは、マイグレーション中に操作が短時間中断されるという影響を受けます。System Automation for Multiplatforms またはアプリケーション・サーバーを再始動する必要はありません。

ライブ・パーティション・モビリティー中の中断期間が原因で不要なクラスター・イベントが発生しないようにします。平均的な中断期間中に、ノードからのハートビートの受信ミスが多すぎる場合は、不要なクラスター・イベントが発生します。その場合、ライブ・パーティション・モビリティーの時間のハートビート設定を緩和してください。

LPAR の移動中に不要なクラスター・イベントが発生する機会を最小限に抑えるための別の方法は、ピア・ドメインを強制的に停止してから、`stoprpdomain -f` を使用して移動を開始することです。すなわち、クラスター・サービスによって管理されるアプリケーションを停止しません。 移動の完了後に、ピア・ドメインを再始動します。

制約事項 : ディスク・タイ・ブレーカーは、ライブ・パーティション・モビリティーの前提条件である仮想 SCSI ではサポートされません。

VMware vMotion のサポート

このタスクについて

vCenter Server によって管理される複数の ESX サーバーが存在する VMware vSphere セットアップでは、vMotion フィーチャーを使用して、System Automation for Multiplatforms ノードとして動作している稼働中のゲストをマイグレーションすることができます。System Automation for Multiplatforms クラスターが標準の (つまり、デフォルトの) ハートビート設定を使用するように構成されていれば、このマイグレーションによってクラスターの状態や操作が影響を受けることはありません。その場合、System Automation for Multiplatforms の制御下で実行されているアプリケーション・サーバーでは、マイグレーション中に操作が短時間中断されるという影響を受けます。System Automation for Multiplatforms もアプリケーション・サーバーも再始動の必要はありません。

vMotion 中の中断期間が原因で不要なクラスター・イベントが発生しないようにします。平均的な中断期間中に、ノードからのハートビートの受信ミスが多すぎる場合は、不要なクラスター・イベントが発生します。その場合、vMotion の時間のハートビート設定を緩和してください。

仮想ゲストの移動中に不要なクラスター・イベントが発生する可能性を最小限に抑えるための別の方法は、ピア・ドメインを強制的に停止してから、`stoprpdomain -f` を使用して移動を開始する方法です。この場合、クラスター・サービスによって管理されるアプリケーションは停止しません。移動の完了後に、ピア・ドメインを再始動します。

System Automation for Multiplatforms では、以下のゲスト・オペレーティング・システムを稼働しているバージョン 3.5 以上の ESX サーバーと ESXi サーバーに対して vMotion がサポートされます。

- RHEL 6 (x86-64 または x86-32)
- SLES 12 または 15 (x86-64)
- RHEL 7 または 8 (x86-64)
- Ubuntu 16.04、18.04、または 20.04 (x86-64)

制限: System Automation for Multiplatforms は、共有ストレージを使用するノードの vMotion はサポートしません。これは、共有実ストレージ・ボリューム (ディスク) または共有仮想ストレージ・ボリューム (ディスク) を vMotion がサポートしていないためです。

z/VM Single System Image および Live Guest Relocation のサポート

z/VM 6.2 では、マルチシステム・クラスター化テクノロジーである Single System Image (SSI) のサポートが導入されています。Single System Image を使用することで、最大で 4 つの z/VM イメージをクラスター化できます。SSI は、クラスター内のメンバー間でのリソース共有を容易にします。また、System z ゲストを停止することなく、System z ゲスト上のアクティブな Linux を別の z/VM システムに移動することもできます。この機能は Live Guest Relocation (LGR) と呼ばれており、Linux on System z ゲストに対してのみサポートされます。

z/VM SSI および LGR の概念や機能を理解するには、An Introduction to z/VM Single System Image (SSI) and Live Guest Relocation (LGR) (SG24-8006) を参照してください。

必要なレベルの z/VM がソース・システムと宛先システムにインストールされている場合は、z/VM の Live Guest Relocation 機能を使用して z/VM Linux ゲスト・システムを再配置できます。必要なレベルの System Automation for Multiplatforms が Linux ゲスト・システムにインストールされている場合は、標準 (デフォルト) のハートビート設定が構成されていれば、このゲスト・システムを再配置しても System Automation for Multiplatforms クラスターの状態や操作は影響を受けません。System Automation for Multiplatforms によって管理されるアプリケーションでは、再配置のプロセス中は操作が短時間中断されます。System Automation for Multiplatforms およびアプリケーションの再始動は不要です。

Live Guest Relocation 中の中断の期間が原因で不要なクラスター・イベントが発生しないことを検証してください。不要なクラスター・イベントは、Live Guest Relocation 中に中断されているノードから、構成されている数のハートビートが欠落している場合に発生します。平均的な中断期間が原因で欠落するハートビートが多すぎる可能性があることがテストで分かった場合、Live Guest Relocation の間のハートビート設定を緩和する必要があります。z/VM ゲスト・システムの再配置中に不要なクラスター・イベントが発生する可能性を極めて最小限に抑えるには、再配置を開始する前に、**stoprpdomain -f** を使用してピア・

ドメインを強制的に停止します。例えば、クラスター・サービスによって管理されるアプリケーションを停止することはありません。再配置が正常に完了した後に、**startrpdomain** コマンドを使用してピア・ドメインを再始動します。

要件

- System Automation for Multiplatforms バージョン 3.2.2.4 (またはそれ以上)
- z/VM バージョン 6.2

制限

ディスク上に予約を保持するゲストを再配置することはできないため、ECKD Disk タイ・ブレーカーおよび SCSI PR タイ・ブレーカーを Live Guest Relocation と共に使用することはできません。

インストールの準備

System Automation for Multiplatforms は、自動化する各クラスター・ノードにインストールする必要がある複数のパッケージに含まれています。パッケージのタイプと内容は System Automation for Multiplatforms のインストール先オペレーティング・システムによって異なります。

構成の開始

以下の初期構成を実行します。

- すべてのノードで、次のように System Automation for Multiplatforms の全ユーザーについて環境変数 CT_MANAGEMENT_SCOPE を 2 (ピア・ドメイン・スコープ) に設定およびエクスポートします。`export CT_MANAGEMENT_SCOPE=2`

  この変数を永続的に設定するには、プロファイル内に設定およびエクスポートしてください。

  SLES システムでは、以下の内容で `/etc/profile.d` にスクリプトを作成できます。

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

- `root` ユーザーの LANG 環境変数に、サポートされるいずれかのロケールが設定されていることを確認します。 この環境変数を設定するには、次のコマンドを使用します。

  ```
  export LANG=xx_XX
  ```

  xx_XX は、サポートされるいずれかの言語を示します。

サポートされる言語とロケールのリストについては、26 ページの『サポートされている言語およびロケール』を参照してください。

ノードの負荷

クラスター・サービスが正しく動作するために、System Automation for Multiplatforms では、そのサブシステムのいくつかがノード上で常に処理されていること、例えば、サブシステム間のハートビートおよび通信が行われていることを必要とします。これが可能でないと、短期間内にこれらのサブシステムが通信できないケースで、System Automation がクリティカル・リソース保護メソッドを起動する場合があります。この保護メカニズムにより、最終的には、この問題が発生しているノードが再始動されます。

不要なシステム再始動を回避するには、常時入出力およびスワップ負荷が 10% 未満になるようにする必要があります。

クリティカル・リソースの保護メソッドについて詳しくは、*Tivoli System Automation for Multiplatforms* 管理者とユーザーのガイドを参照してください。

クラスターのノード数

Linux
単一クラスターのノードの最大数は 32 です。

AIX
単一クラスターのノードの最大数は 130 です。

注 :

1. ソフトウェア・パッケージは、System Automation for Multiplatforms のインストール先のノードで使用可能である 必要があります。例えば、PC に DVD をマウントしてから FTP を使用してファイルをノードに転送したり、 あるいは、共用ネットワーク・ファイル・システム (NFS) を通じてパッケージをインストールしたりできます。
2. ソフトウェア・パッケージを確実に正しくインストールおよびアンインストールするために、System Automation for Multiplatforms スクリプトの **installSAM** および **uninstallSAM** を使用してください。これらのスクリプトにより、要件の検査、ライセンスのインストール、およびマイグレーション・タスクも実行されます。
3. System Automation が機能するためには、言語パッケージを除くすべてのパッケージが必要です。System Automation for Multiplatforms 4.1 から、製品全体をアンインストールせずに RSCT パッケージ `rsct.opt.storagerm` だけをアンインストールすることはできなくなりました。

新規プラットフォーム計画のサポート

フィックスパック 4.1.0.1 以降、System Automation for Multiplatforms では、32 ビット言語環境用および 64 ビット言語環境用の別個のインストール・パッケージを導入しています。

対応するパッケージは、後続するすべてのフィックスパック 4.1.0.x でも提供されます。どちらのパッケージも同じコードをベースにしています。

- 一方のパッケージ `4.1.0-TIV-SAMP-Linux-FPxxxx` には、複数の 32 ビット言語環境用の System Automation for Multiplatforms 製品ビルドが含まれています。Linux オペレーティング・システム RHEL 6 での System Automation for Multiplatforms で、これらの 32 ビット言語環境が必要となります。
- もう一方のパッケージ `4.1.0-TIV-SAMP-Linux64-FPxxxx` には、複数の 64 ビット言語環境用の System Automation for Multiplatforms 製品ビルドが含まれています。Linux オペレーティング・システム RHEL 7/8、SLES 12/15、および Ubuntu 16.04/18.04/20.04 での System Automation for Multiplatforms で、これらの 64 ビット言語環境が必要となります。

Linux オペレーティング・システム RHEL 6 では、後者のパッケージを使用することはできません。 System Automation for Multiplatforms 4.1.0.0 以下は、SLES 12/15、RHEL 7/8、および Ubuntu 16.04/18.04/20.04 ではサポートされていません。

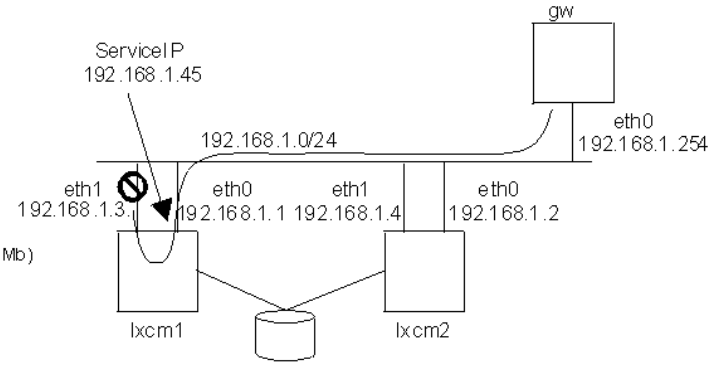
高可用ネットワーク・インフラストラクチャーの計画

複雑さを理解し、高可用ネットワークのセットアップを計画します。

次の図は、Linux 上のネットワーク・インフラストラクチャーを示します。

```
eth0  Link encap:Ethernet  HWaddr 00:00:00:00:00:00
      inet addr:192.168.1.1  Mask:255.255.255.0
      inet6 addr: fe80::200:ff:fe00:0/10 Scope:Link
      UP RUNNING NOARP MULTICAST  MTU:1492  Metric:1
      RX packets:1147264 errors:0 dropped:0 overruns:0 frame:0
      TX packets:1557235 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:100
      RX bytes:873548285 (833.0 Mb)  TX bytes:674939696 (643.6 Mb)
      Interrupt:2

eth1  Link encap:Ethernet  HWaddr 00:00:00:00:00:00
      inet addr:192.168.1.3  Mask:255.255.255.0
      inet6 addr: fe80::200:ff:fe00:0/10 Scope:Link
      UP RUNNING NOARP MULTICAST  MTU:1492  Metric:1
      RX packets:297057 errors:0 dropped:0 overruns:0 frame:0
      TX packets:289815 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:100
      RX bytes:30153527 (28.7 Mb)  TX bytes:38726923 (36.9 Mb)
      Interrupt:5
```



Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.1.0	*	255.255.255.0	U	0	0	0	eth1
192.168.1.0	*	255.255.255.0	U	0	0	0	eth0
default	192.168.1.254	0.0.0.0	UG	0	0	0	eth1

図 *2.* 高可用ネットワークを計画する際の問題

構成された各静的ネットワーク・デバイスは、ルーティング・テーブル内の項目で識別されます。ルーティング・アルゴリズムは、このテーブルから最初に一致する経路を選択します。この例では、ノード `lnxcm1` のデバイス `eth1` に障害が発生します。`eth1` はルーティング・テーブルの最初の項目であるため、別の機能ネットワーク・インターフェース (`eth0`) が存在しても、ノードはネットワークにパッケージを送信できません。

高可用ネットワークの計画を始める前に、以下のことを考慮にしてください。

1. 必要とする高可用ネットワークの種類は何か。
   - 同じノード上のあるインターフェースから別のインターフェースに `ServiceIP` を移動する必要があるか。
   - 必要なサブネット内に作動インターフェースを持つ別のノードに切り替えるのは適切であるか。
2. 追加の IP サブネットをインプリメントできるか、または既存のネットワーク・インフラストラクチャーを使用する必要があるか。
3. クラスター・ノードの有効範囲内でのみ作業するのか、または自動化クラスターの外側にある他のノードでネットワーク・サービスをインプリメントまたはデプロイできるか。
4. 所有しているネットワーク・ハードウェアは何か。

質問への回答に応じて、以下のセットアップのいずれかを選択して、独自の高可用ネットワーク計画を作成できます。

ストレージ・デバイスの計画

単一パス・ストレージ・デバイスの使用

単一パス・ストレージ・デバイスのサポートは、ご使用の稼働環境によって異なります。

AIX

次のように、単一パス・ストレージ・デバイスでは完全なサポートが提供されます。

- 取得された IBM.AgFileSystem リソースを自動化できます。

  IBM.AgFileSystem リソースは、タイプが jfs または jfs2 であり、取得されているストレージ・エンティティー (IBM.LogicalVolume、IBM.VolumeGroup、IBM.Disk クラスのストレージ・エンティティー) 上にある場合、取得されます。
- ユーザー定義の IBM.AgFileSystem リソースを自動化できます (例えば、ネットワーク・ファイル・システム)。
- SCSI-2 予約がサポートされます。

制限:

- ストライピングはありません
- ユーザー定義の IBM.AgFileSystem リソースは、ファイル・システムをホスティングするディスクが、クラスターのすべてのノード上で同じデバイス名を持つ場合にのみ自動化できます。

Linux on POWER および Linux on System x

次のように、制限されたサポートが提供されます。

- 取得された IBM.AgFileSystem リソースを自動化できます。

  タイプが ext2、ext3、または reiserfs のいずれかであり、それ自体が取得されているストレージ・エンティティー (IBM.LogicalVolume、IBM.Partition、IBM.VolumeGroup、IBM.Disk クラスのストレージ・エンティティー) 上に存在する場合、IBM.AgFileSystem リソースは取得されます。
- ユーザー定義の IBM.AgFileSystem リソースを自動化できます (例えば、ネットワーク・ファイル・システム)。

制限:

- SCSI 予約のサポートは制限されます。ディスク予約操作を実行して、SCSI 予約が使用可能かどうか検査します。
- ユーザー定義の IBM.AgFileSystem リソースは、ファイル・システムをホスティングするディスクが、クラスターのすべてのノード上で同じデバイス名を持つ場合にのみ自動化できます。

Linux on System z

pvcreate コマンドを使用して、md デバイス上に物理ボリュームが作成された場合、提供されたデバイス・マッパー・デバイスまたは md デバイスは、**IBM.Disk** リソースとして取得されます。

制限:

- ユーザー定義の IBM.AgFileSystem リソースや、取得された提供されたデバイス・マッパー・デバイスまたは md デバイス上にある IBM.AgFileSystem リソースのみを自動化できます。他のディスクでのリソース取得はサポートされません。他のディスク・リソースの取得が成功した場合でも、取得されたリソースは自動化できません。
- ユーザー定義の IBM.AgFileSystem リソースは、ファイル・システムをホスティングするディスクが、クラスターのすべてのノード上で同じデバイス名を持つ場合にのみ自動化できます。
- SCSI 予約はサポートされません。

マルチパス・ストレージ・デバイスの使用

ご使用の環境に応じて、マルチパス・ストレージ・デバイスにいくつかの制限がある場合があります。

AIX

次のように、SPIO および MPIO ストレージ・デバイスでは完全なサポートが使用できます。

- 取得された IBM.AgFileSystem リソースを自動化できます。

IBM.AgFileSystem リソースは、タイプが jfs または jfs2 であり、取得されているストレージ・エンティティー (IBM.LogicalVolume、IBM.VolumeGroup、IBM.Disk クラスのストレージ・エンティティー) 上にある場合、取得されます。

- ユーザー定義の IBM.AgFileSystem リソースを自動化できます (例えば、ネットワーク・ファイル・システム)。
- Redundant Disk Array Controller (RDAC) ドライバーを使用する SPIO および MPIO ストレージ・デバイスでは、SCSI-2 予約がサポートされます。

注 : このドライバーは、IBM TotalStorage DS4k ファミリー および DS6k ファミリーでのみ使用できます。

制限:

- ストライピングはありません
- ユーザー定義の IBM.AgFileSystem リソースは、ファイル・システムをホスティングするディスクが、クラスターのすべてのノード上で同じデバイス名を持つ場合にのみ自動化できます。

Linux on POWER および Linux on System x

単一パス I/O (SPIO) ストレージ・デバイス、Redundant Disk Array Controller (RDAC) デバイス・ドライバーを持ったマルチパス・ストレージ I/O (MPIO) デバイス、および md デバイスと提供されたデバイス・マッパー・デバイスでは、完全なサポートが使用できます。

- 取得された IBM.AgFileSystem リソースを自動化できます。

  IBM.AgFileSystem リソースは、タイプが ext2、ext3、または reiserfs のいずれかであり、取得されているストレージ・エンティティー (IBM.LogicalVolume、IBM.Partition、IBM.VolumeGroup、IBM.Disk クラスのストレージ・エンティティー) 上にある場合、取得されます。
- ユーザー定義の IBM.AgFileSystem リソースを自動化できます (例えば、ネットワーク・ファイル・システム)。
- RDAC ドライバーから取得されたディスクでは、SCSI-2 予約がサポートされます。
- Linux RAID (提供された /dev/device mapper または md デバイス) がサポートされます。
- デバイス・マッパーの管理対象のディスクがサポートされます。

制限:

- LVM を使用せずに提供されたデバイス・マッパー・デバイス上または md デバイス上に作成されたファイル・システムは取得されません。それらのファイル・システムは、ユーザー定義の IBM.AgFileSystem リソースを使用する場合のみ自動化できます。
- **pvcreate** コマンドを使用して md デバイス上に物理ボリュームが作成された場合、提供されたデバイス・マッパー・デバイスまたは md デバイス自身は、IBM.Disk リソースとしてのみ取得されます。
- 非 RDAC ドライバーや、提供されたデバイス・マッパー・デバイスや md デバイス自身に対しては、SCSI-2 予約はサポートされません。
- ユーザー定義の IBM.AgFileSystem リソースは、ファイル・システムをホスティングするディスクが、クラスターのすべてのノード上で同じデバイス名を持つ場合にのみ自動化できます。
- EVMS はサポートされません。これには、EVMS によって作成または管理される Volume Groups/Logical Volumes が含まれているためです。
- SLES 12/15 および RHEL 7/8 の場合、IBM.Disk、IBM.VolumeGroup、 IBM.LogicalVolume、IBM.Partition、および IBM.AgFileSystem クラスのストレージ・エンティティーの獲得がサポートされます。提供されたデバイス・マッパー・デバイスまたは md デバイスの、上記のリストされた制限が満たされる場合は、ファイル・システムを自動化できます。

Linux on System z

pvcreate コマンドを使用して、提供されたブロック・デバイス上に物理ボリュームが作成された場合、提供されたデバイス・マッパー・デバイスまたは md デバイスは、IBM.Disk リソースとして取得されます。これは、 基礎のディスク・テクノロジーである ECKD または SCSI からは独立しています。

制限:

- ユーザー定義の IBM.AgFileSystems リソースや、取得された提供されたデバイス・マッパー・デバイスまたは md デバイス上にある IBM.AgFileSystems リソースのみを自動化できます。他のディスクでのリソース取得はサポートされません。他のディスク・リソースの取得が成功した場合でも、取得されたリソースは自動化できません。
- ユーザー定義の IBM.AgFileSystems リソースは、ファイル・システムをホスティングするディスクが、クラスターのすべてのノード上で同じデバイス名を持つ場合にのみ自動化できます。
- SCSI 予約はサポートされません。

ネットワーク・インターフェースの使用

クラスター内に、それぞれ 2 つのネットワーク・インターフェースを持つ 2 つのノードで高可用性構成をセットアップできます。

このセットアップを開始する前に、同一 IP サブネットに複数の静的構成ネットワーク・インターフェース を含めることはできない点に注意してください。IP アドレスごとに、カーネル・ルーティング・テーブルに項目が 作成されます。同一サブネットに 2 つのインターフェースがある場合は、同一サブネットに対して 2 つのルートがあります。最初の項目を作成したインターフェースで障害が発生すると、まだ通信が可能な別のインターフェースが存在する場合でも、このサブネットの通信は切断されます。

物理的に分離した 2 つのネットワーク、ノード間での ServiceIP の移動

以下のネットワーク・セットアップが適用されます。

表 6. ネットワーク・インターフェースを 持つ 2 ノード・クラスターのネットワーク・セットアップ

リソース	名前	デバイス	IP
クラスター・ノード	lnxcm1	eth0 eth1	9.152.172.1/24 192.168.1.1/24
クラスター・ノード	lnxcm2	eth0 eth1	9.152.172.2/24 192.168.1.2/24
ルーター	gw	eth0	9.152.172.254/24
ServiceIP	-	–	9.152.172.3/24

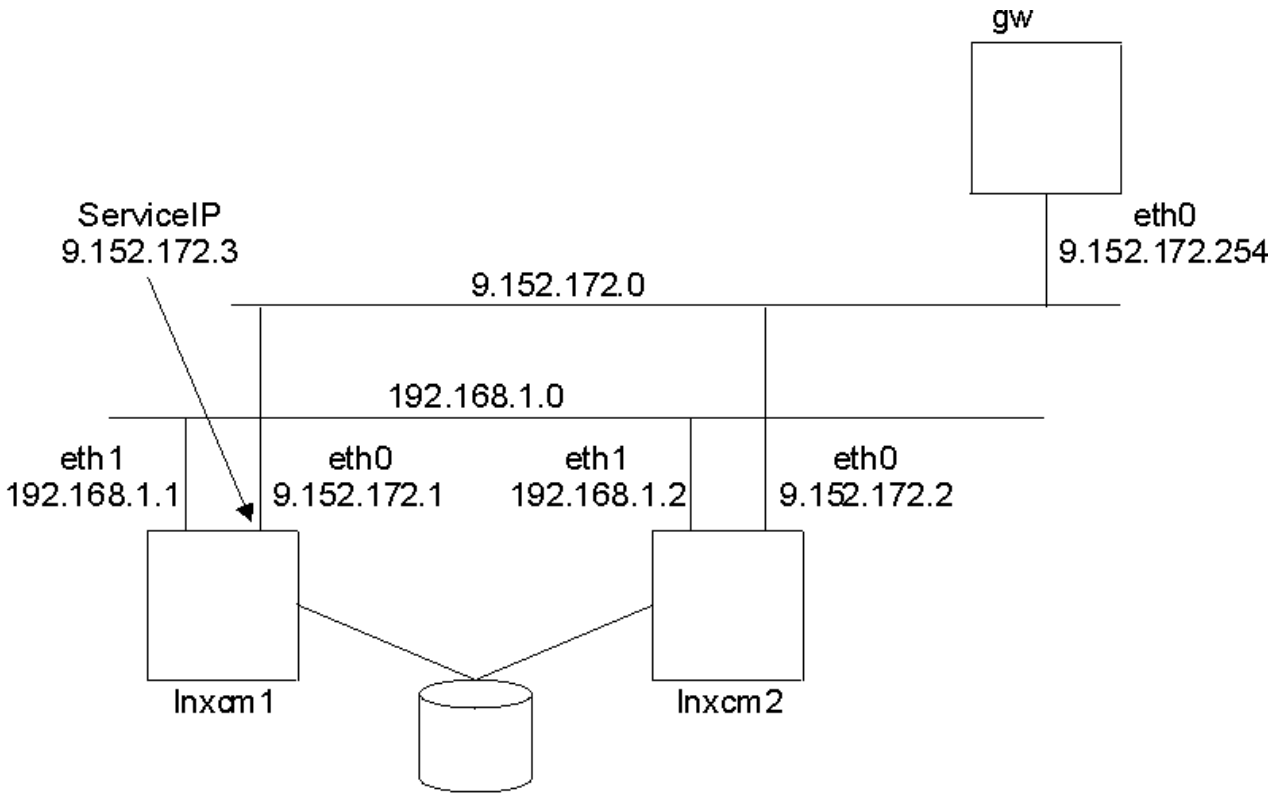


図 *3. 2* ノード、*2* インターフェース、物理的に分離した *2* つのネットワーク

クラスター通信のネットワークとして、192.168.1.0 と 9.152.172.0 があります。1 つのネットワーク・インターフェースで障害が発生した場合でも、クラスターは中断されません。

- ネットワーク 9.152.172.0 は高可用 IT サービスのネットワークを表します。
- ネットワーク 192.168.1.0 は、クラスター内部通信の信頼性を強化します。

ServiceIP のネットワークのみがゲートウェイに接続されるため、lnxcm1 のインター フェース eth0 で障害が発生すると、自動化により ServiceIP が別のノード lnxcm2 のインターフェース eth0 に移動します。2 つのネットワークが物理的に分離しているため、ServiceIP を同一ノード内の eth0 から eth1 に移動することはできません。

System Automation for Multiplatforms ポリシーの例は、19 ページの図 7 に示す例と同一です。

表 *7.* ネットワーク・インターフェース を持つ *2* ノード・セットアップの利点と欠点	
利点	**欠点**
セットアップが容易である。	ServiceIP はノード間のみを移動する。
クラスター通信に冗長性がある。	

1 物理ネットワーク内の 3 論理ネットワーク、ネットワーク・インターフェース間での ServiceIP の移動

クラスター内のノード間で ServiceIP を移動するのみでなく、1 つのノード内のインターフェース間で ServiceIP を移動するためには、別のネットワーク・セットアップが必要となります。

ノードのインターフェースごとに別個の論理ネットワークと、ServiceIP 用の追加のネットワークが必要です。既存のネットワーク (eth0 または eth1 のいずれか) を選択すると、ルーティングの問題が発生する可能性があります。すべてのインターフェースが同一物理ネットワークに接続していることを確認します。これにより、各インターフェースですべての論理ネットワークのアド レスを保持できます。

以下のネットワーク・セットアップが適用されます。

表 *8. 1* 物理ネットワーク内の *3* 論理ネットワークのネットワーク・セットアップ			
リソース	**名前**	**デバイス**	**IP**
クラスター・ノード	lnxcm1	eth0 eth1	192.168.1.1/24 192.168.2.1/24
クラスター・ノード	lnxcm2	eth0 eth1	192.168.1.2/24 192.168.2.2/24
ルーター	gw	eth0	9.152.172.254/24
ServiceIP	-	–	9.152.172.3/24

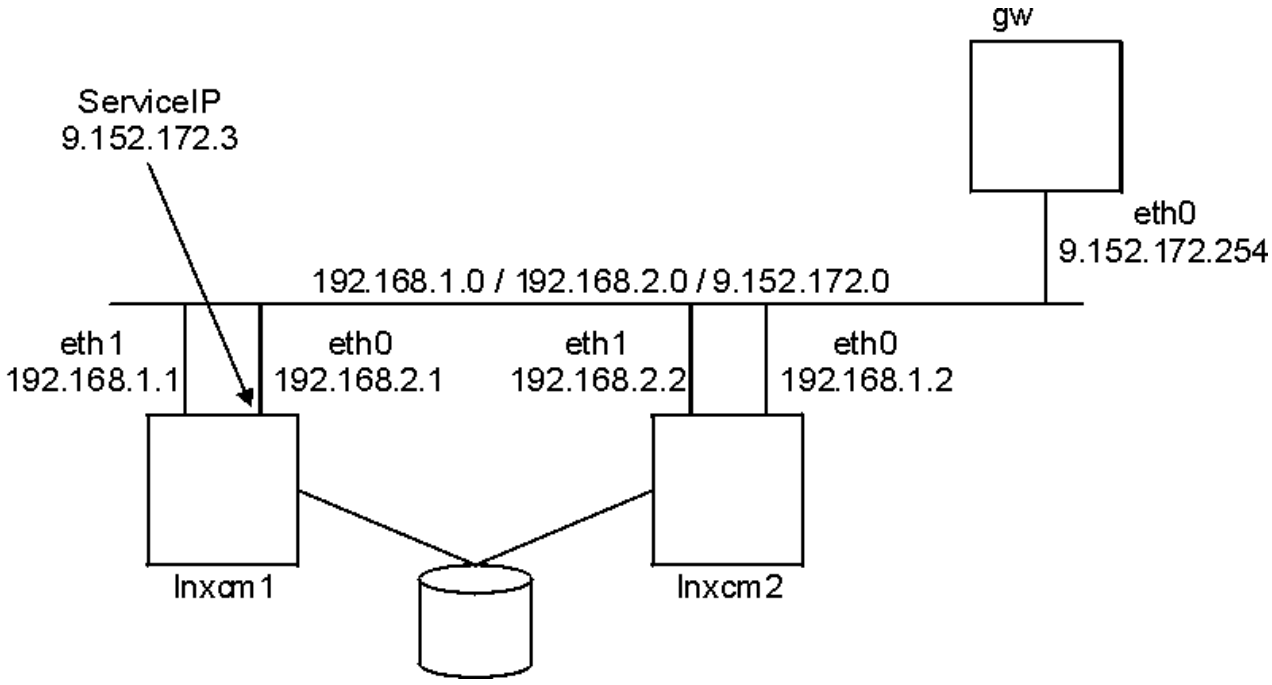


図 *4. 2* ノード、*2* インターフェース、*1* 物理ネットワーク

- ネットワーク 9.152.172.0 は高可用 IT サービスのネットワークを表します。
- ネットワーク 192.168.1.0 は 1 番目のクラスター内部通信ネットワークを表します。
- ネットワーク 192.168.2.0 は 2 番目のクラスター内部通信ネットワークを表します。

System Automation for Multiplatforms ポリシーの例:

```
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
```

表 *9. 1* 物理ネットワーク内の *3* 論理ネットワークのネットワーク・セットアップの利点と欠点	
利点	**欠点**
セットアップが容易である。	1 つの物理ネットワークに 3 つの論理ネットワークが存在する。

表 *9. 1* 物理ネットワーク内の *3* 論理ネットワークのネットワーク・セットアップの利点と欠点 *(*続き*)*	
利点	**欠点**
クラスター通信に冗長性がある。	1 つの物理メディアに 3 つのネットワークのトラフィック。
ServiceIP がインターフェースとノードの間を移動できる。	

物理的に分離した 2 つのネットワーク、動的ルーティングおよ び VIPA

このセットアップの詳細説明は、本書のスコープを超えています。 基本的に、ServiceIP はクラスター・ノードのカーネル内の仮想ネットワーク に割り当てられます。すべてのクラスター・ノードでの動的ルーティングとゲートウェイによ り、ServiceIP へのルートが確立されます。

以下のネットワーク・セットアップが適用されます。

表 *10.* 物理的に分離した *2* つのネットワークのネットワーク・セットアップ			
リソース	**名前**	**デバイス**	**IP**
クラスター・ノード	lnxcm1	eth0 eth1	9.152.170.1/24 9.152.171.1/24
クラスター・ノード	lnxcm2	eth0 eth1	9.152.170.2/24 9.152.171.2/24
ルーター	gw	eth0 eth1	9.152.170.254/24 9.152.171.254/24
ServiceIP	-	–	9.152.172.3/24

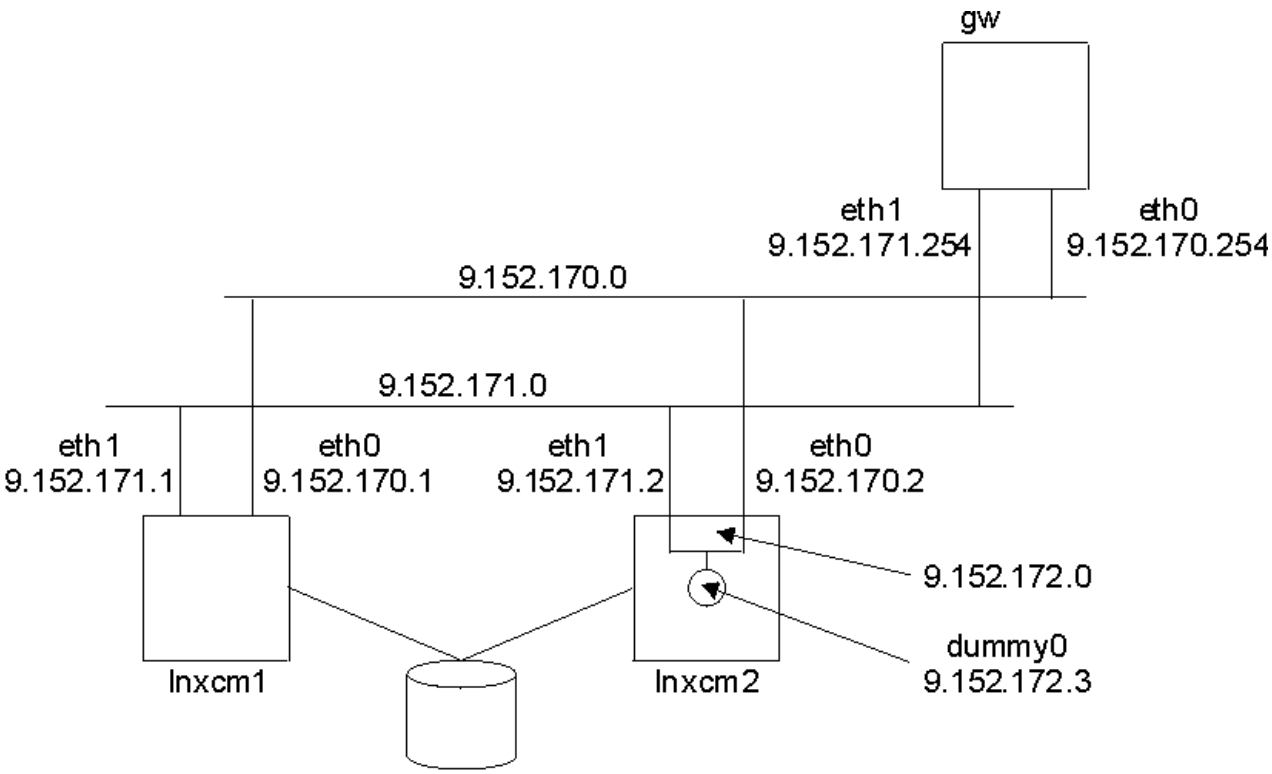


図 *5.* 物理的に分離した *2* つのネットワーク、動的ルーティングおよ び *VIPA*

表 11. 物理的に分離した 2 つのネットワークのネットワーク・セットアップ の利点と欠点	
利点	**欠点**
物理ネットワーク・デバイスに依存しない。	セットアップが複雑である。
ホスト (IP アドレス) への最適な経路を動的に検出するという概念。	動的ルーティングが必要である。
インターフェース間での ServiceIP の移動が不要である。	セットアップがクラスター・ノードに制限されない。ゲートウェイでも動的ルーティングをサポートする必要がある。

インターフェースの接合

1 つの論理ネットワーク・デバイスには、複数の物理ネットワーク・インターフェースが接合されます。オペレーティング・システムは、特殊な接合デバイス・ドライバーを使用して、この機能をサポートする必要があります。ご使用のシステムでインターフェースの接合を構成する方法については、オペレーティング・システムの資料を参照してください。必ず高可用性の接合を構成してください。また、ご使用のネットワーク・インターフェース・カードが、接合ドライバーが必要とするインターフェース障害検出メカニズムをサポートしていることを確認してください。

以下のネットワーク・セットアップが適用されます。

表 12. 接合された物理ネットワーク・インターフェース のネットワーク・セットアップ			
リソース	**名前**	**デバイス**	**IP**
クラスター・ノード	lnxcm1	eth0 eth1	9.152.172.1/24 9.152.172.1/24
クラスター・ノード	lnxcm2	eth0 eth1	9.152.172.2/24 9.152.172.2/24
ルーター	gw	eth0	9.152.172.254/24
ServiceIP	-	-	9.152.172.3/24

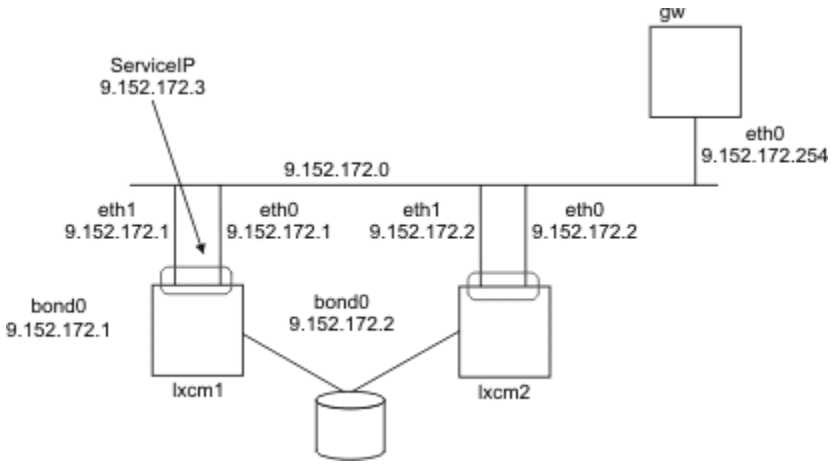


図 6. 1 つの論理ネットワーク・デバイスに接合された複数のネットワーク・インターフェース

表 *13.* 接合された物理ネットワーク・インターフェースのネットワーク・セットアップ の利点と欠点	
利点	**欠点**
セットアップが容易である。	オペレーティング・システムはインターフェースの接合をサポートする必要がある。
クラスター通信に冗長性がある。	ネットワーク・インターフェース・ハードウェアは、インターフェース障害検出をサポートする必要がある (例えば MII リンクのモニター)。
同じノード上のデバイス間での ServiceIP の移動が不要である。	

イーサネット・インターフェースの使用

クラスター内で、それぞれ別個にイーサネット・インターフェースがある 2 つのノードにより、高可用性構成をセットアップできます。

以下のネットワーク設定が指定されています。

表 *14.* イーサネット・インターフェースを 持つ *2* ノード・クラスターのネットワーク・セットアップ			
リソース	**名前**	**デバイス**	**IP**
クラスター・ノード	lnxcm1	eth0	9.152.172.1/24
クラスター・ノード	lnxcm2	eth0	9.152.172.2/24
ルーター	gw	eth0	9.152.172.254/24
ServiceIP	–	–	9.152.172.3/24

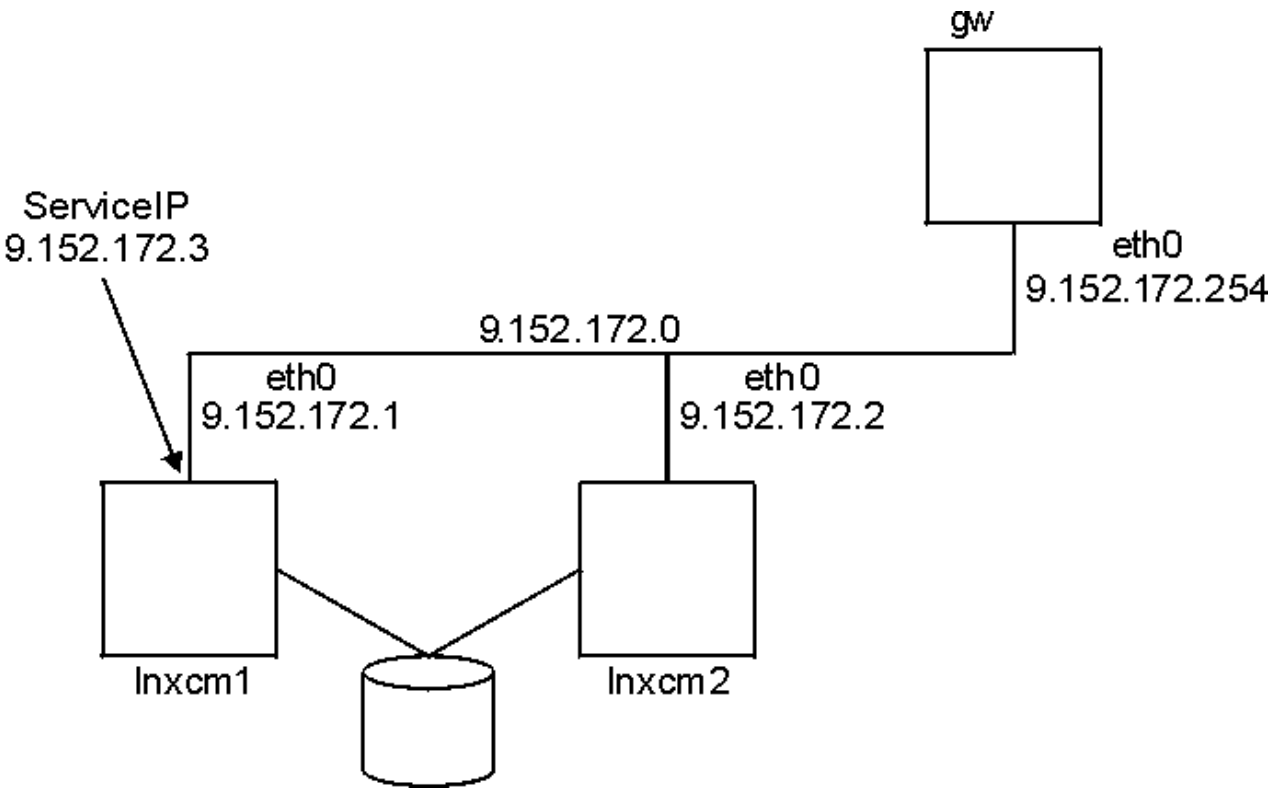


図 *7. 2* ノード、*1* インターフェース

このセットアップでは、クラスター通信と高可用 IT サービスの表示において、同一通信パス (9.152.172.0 ネットワーク) が使用されます。

自動化により、lnxcm1 インターフェース eth0 または lnxcm2 インターフェース eth0 のいずれかに ServiceIP を割り当てることができます。1 つのインターフェースで障害が発生すると、自動化は ServiceIP を別のノードに移動します。このように、稼働中のネットワーク・インターフェ ースでの ServiceIP 割り当てを必要とするポリシーの要求を満たします。

このセットアップでは、1 つのネットワーク・インターフェースで障害が発生すると、System Automation for Multiplatforms 管理者とユーザーのガイドで説明したすべての問題によりクラスター通信の中断につながります。20 ページの図 8 に示すように通信が中断した場合、タイ・ブレーカーは、 自動化を続行するノードを判別します。タイ・ブレーカーがノード lnxcm1 によって予約されている場合、ノード lnxcm1 で ServiceIP を割り当てるのには、どのオンライン・ネットワーク・インターフェースも使用できません。

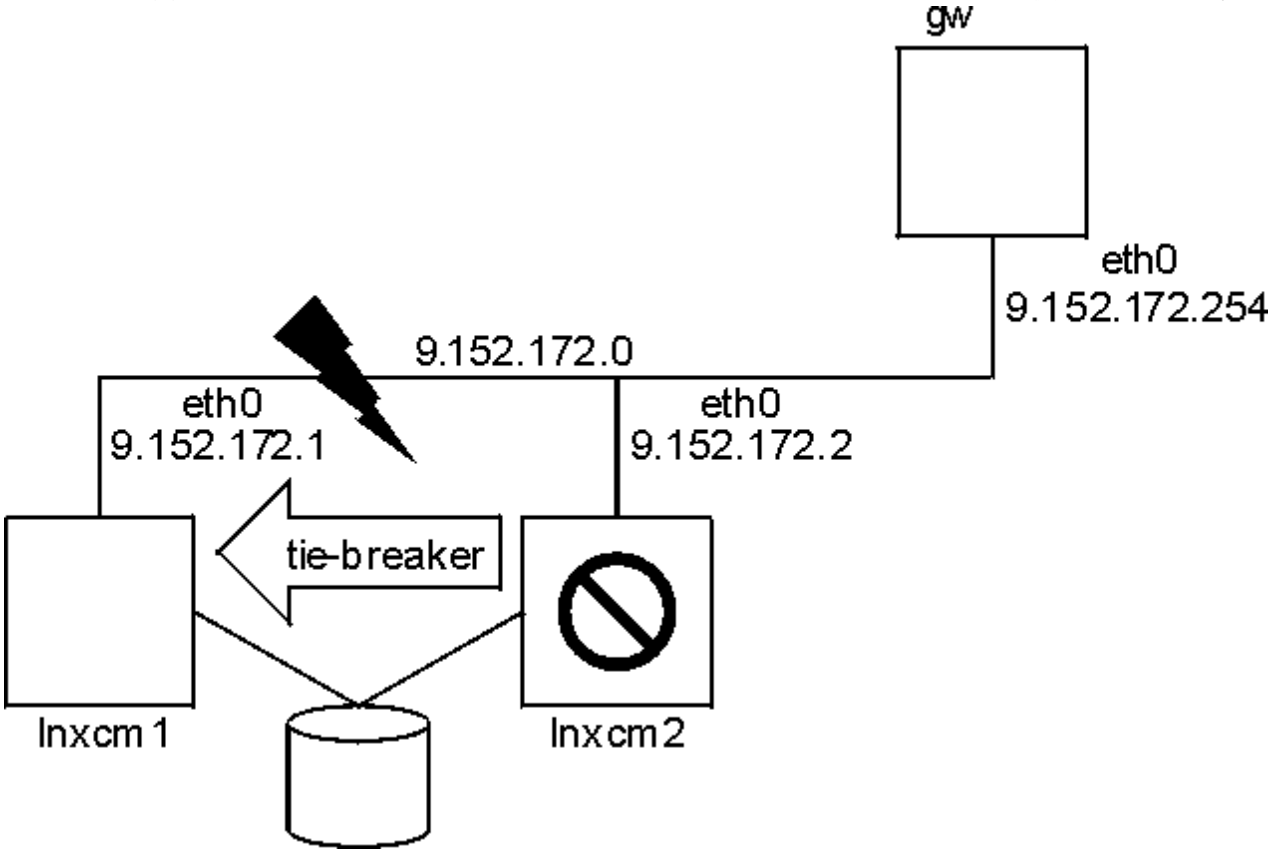


図 *8. 2* ノード、*1* インターフェース、インターフェースの障害

この例では、ネットワーク 9.152.172.0 は以下の 2 つの目的で使用されます。

1. 高可用 IT サービスのネットワークを表す。
2. 内部クラスター通信に使用する。

System Automation for Multiplatforms ポリシーの例:

```
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
```

表 *15.* イーサネット・インターフェース を持つ *2* ノード・クラスターの利点と欠点	
利点	**欠点**
セットアップが単純である。	各通信の問題が原因で、クラスターが分割される。

表 *15.* イーサネット・インターフェース を持つ *2* ノード・クラスターの利点と欠点 *(*続き*)*	
利点	**欠点**
必要なネットワーク・ハードウェアが少ない。	ServiceIP はノード間のみを移動する。

第 2 章 インストール

System Automation for Multiplatforms のインストールまたはアップグレードには、システムを準備することと、ご使用の環境に固有の一連のタスクを実行することが含まれます。

アップグレード

System Automation for Multiplatforms では、体験版からフル・バージョンへのアップグレード、または実行中のバージョンから最新のリリースへのアップグレードができます。

体験版からフル製品バージョンへのアップグレード

System Automation for Multiplatforms の体験版が既にインストールされていて、フル製品バージョンを購入したとします。その場合は、フル・ライセンス用のライセンス・ファイルを含む、別のインストール・メディアが配布されます。

このタスクについて

ライセンス・ファイルは、インストール・メディアの `license` サブディレクトリーにあります。ライセンスのアップグレードを実行するには、次のように入力します。

```
samlicm -i <license_file_name>
```

ライセンスを表示するには、以下を入力します。

```
samlicm -s
```

ライセンスのアップグレード後は、System Automation for Multiplatforms の更新が使用可能かどうかを調べて、更新をインストールしてください。

バージョン 4.1 より前のバージョンからのアップグレード

前のバージョンの製品からバージョン 4.1 にアップグレードできます。

このタスクについて

System Automation for Multiplatforms をバージョン 4.1 より前のバージョンからアップグレードする場合は、以下の説明に従ってください。

サイレント・アダプター構成
サイレント・モードで `cfgsamadapter` 構成ユーティリティーを使用して、エンドツーエンド自動化アダプター設定を構成する場合は、新規リリース・レベルで新規のサイレント入力プロパティー・ファイルを生成するようにしてください。オプション `-s` を使用して `cfgsamadapter` ユーティリティーを始動すると、自動化アダプター設定がサイレント・モードで構成されます。サイレント構成を実行する場合は、既存の入力プロパティー・ファイルを使用するのではなく、事前に新規入力プロパティー・ファイルを生成します。これを行うには、オプション `-s [ -g | -gr ]` を指定して `cfgsamadapter` ユーティリティーを開きます。

削除されたオペレーション・コンソール
オペレーション・コンソールとポリシー・エディターは、バージョン 4.1 に含まれていません。オペレーション・コンソールを使用して第 1 レベル・ドメインを操作したり、バージョン 3.2.2 までの System Automation for Multiplatforms に付属するポリシー・エディターを使用してポリシーを保守したりすることは可能です。

System Automation for Multiplatforms のインストール

ご使用の環境に System Automation for Multiplatforms をインストールすることも、製品の旧バージョンをアップグレードすることもできます。

このタスクについて

以降のトピックでは、AIX または Linux 環境で System Automation for Multiplatforms をインストールまたはアップグレードする方法について説明します。

初期インストール
System Automation for Multiplatforms の初期インストールを実行する場合は、24 ページの『インストールの実行』を参照してください。

既存のインストール
前のバージョンの System Automation for Multiplatforms が既にインストールされている場合は、新規バージョンの System Automation for Multiplatforms を インストールする前にいくつかのステップを実行する必要があります。製品の新規バージョンにマイグレーションする方法について詳しくは、27 ページの『システム自動化ドメインのマイグレーション』を参照してください。

インストールの実行

インストール・スクリプトを使用して System Automation for Multiplatforms をインストールします。

このタスクについて

インストール・スクリプトは、次のアクションを実行します。

- すべての前提条件が使用可能であり、かつ必要なレベルであることを確認するための、前提条件の完全な検査。ご使用のシステムがこの検査に合格しない場合、インストールは開始されません。インストールを再開する前に、欠落している前提条件を提供する必要があります。3 ページの『前提条件の検査』を参照してください。
- エンドツーエンド自動化アダプターを含め、System Automation for Multiplatforms をインストールします。

インストールを再開しなくても済むようにするには、インストールを開始する前に、前提条件検査を別途起動する必要があります。

IBM Reliable Scalable Cluster Technology (RSCT) ピア・ドメインが存在している場合は、スクリプトの実行に使用するノードがドメインでオフラインであることを確認します。オフラインでない場合は、インストールが取り消されます。

自動化アダプターを含めて、本製品をインストールします。

1. root または同等の権限でログインします。
2. インターネットから `.tar` ファイルをダウンロードした場合は、次のようにしてファイルを解凍します。

   ```
   tar -xvf <tar file>
   ```

   DVD で製品を入手した場合は、DVD をマウントし、DVD がマウントされているディレクトリーに移動します。
3. 以下のコマンドを入力します。
   - Linux: `cd SAM4100MPLinux`
   - AIX: `cd SAM4100MPAIX`
4. インストール・スクリプトを実行します。

   ```
   ./installSAM
   ```

   通常、**installSAM** コマンドに使用できるオプションを指定する必要はありません。デフォルト・インストールでは、サポートされるすべての言語用パッケージがインストールされます。すべての言語では

なく英語のみをインストールする場合は、--nonls オプションを指定できます。**installSAM** コマンドについて詳しくは、*Tivoli System Automation for Multiplatforms* リファレンス・ガイド を参照してください。

5. 表示されるご使用条件およびライセンス情報を読みます。Enter キーを使用すると 1 行ずつ、スペース・バーを使用すると 1 ページずつ先へスクロールできます。これは、UNIX の「more」オプションに類似しています。ライセンス情報ファイルの最後までスクロールし、ご使用条件に同意する場合は、「y」と入力します。その他の文字を入力すると、インストールが取り消されます。

   ライセンス・ファイルが見つからない場合も、インストールが取り消されます。

6. ご使用条件に同意した後、インストール・プログラムは前提条件を検査して、それらが使用可能であり、かつ必要なレベルであることを確認します。

   ご使用のシステムがこの検査に合格しない場合、インストールは開始されません。インストールを再開する前に、欠落している前提条件を提供する必要があります。

   前提条件検査の結果に関する情報は、ログ・ファイル /tmp/installSAM.<#>.log にあります。

   ご使用のシステムがこの検査に合格した場合、自動化アダプターを含めて本製品がインストールされます。

7. インストールに関する情報がないかどうか、次のログ・ファイルを調べます。

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

   ハッシュ記号 <#> は番号を示します。最も大きな番号は最新のログ・ファイルを示します。

   ログ・ファイル内のエントリーには、次のプレフィックスが付きます。

   prereqSAM
   前提条件検査時に書き込まれたエントリー。

   installSAM
   製品のインストール時に書き込まれたエントリー。

8. インストールされたパッケージを確認するには、 /tmp/installSAM.<#>.log を検査します。この <#> は、見つかったログ・リストのうち、最大の数です。

製品ライセンスのインストール

System Automation for Multiplatforms を実行する各システムに、有効な製品ライセンスをインストールする必要があります。

このタスクについて

ライセンスはインストール・メディアの「license」サブディレクトリーに あります。ライセンスのインストールは製品インストール時に実行されます。ライセンスが正常にインストールされなかった場合は、次のコマンドを発行してライセンスをインストールしてください。

```
samlicm –i license_file
```

ライセンスを表示するには、以下を発行します。

```
samlicm -s
```

このコマンドの詳細については、*Tivoli System Automation for Multiplatforms* リファレンス・ガイド を参照してください。

サポートされている言語およびロケール

System Automation for Multiplatforms を英語以外の言語で使用する場合は、サポートされる言語とロケールを確認してください。

このタスクについて

Linux

26 ページの表 16 に、Linux システム上の System Automation for Multiplatforms に翻訳されたメッセージを表示するためにサポートされている言語とロケールの組み合わせを示します。 新バージョンの Linux オペレーティング・システムでは、リストされているエンコード方式の一部はサポートされないことがあります。UTF-8 エンコードは常にサポートされます。

表 *16. Linux* システム上の *System Automation for Multiplatforms* でサポートされている言語およびロケール

言語	UTF-8	ISO-8859-1	EUC/GBK	Euro	GB18030/BIG5
ドイツ語	de_DE.UTF-8	de_DE、de_DE.ISO-8859-1		de_DE@euro	
スペイン語	es_ES.UTF-8	es_ES、es_ES.ISO-8859-1		es_ES@euro	
フランス語	fr_FR.UTF-8	fr_FR、fr_FR.ISO-8859-1		fr_FR@euro	
イタリア語	it_IT.UTF-8	it_IT、it_IT.ISO-8859-1		it_IT@euro	
日本語	ja_JP.UTF-8		ja_JP.eucJP		
韓国語	ko_KR.UTF-8		ko_KR.eucKR		
ブラジル・ポルトガル語	pt_BR.UTF-8	pt_BR			
中国語 (簡体字)	zh_CN.UTF-8		zh_CN.GBK、zh_CN.GB2312		zh_CN.GB18030
中国語 (繁体字)	zh_TW.UTF-8				zh_TW.Big5、zh_TW

AIX

以下の表に、AIX 上の System Automation for Multiplatforms に翻訳されたメッセージを表示するためにサポートされている言語とロケールの組み合わせを示します。

表 *17. AIX* システム上の *Tivoli System Automation* でサポートされている言語およびロケール

言語	UTF-8	ISO-8859-1	EUC/GBK	SJIS/GB18030/BIG5
ドイツ語	DE_DE	de_DE		
スペイン語	ES_ES	es_ES		
フランス語	FR_FR	fr_FR		
イタリア語	IT_IT	it_IT		
日本語	JA_JP		ja_JP	Ja_JP

表 17. AIX システム上の Tivoli System Automation でサポートされている言語およびロケール (続き)				
言語	**UTF-8**	**ISO-8859-1**	**EUC/GBK**	**SJIS/GB18030/ BIG5**
韓国語	KO_KR		ko_KR	
ブラジル・ポルトガル語	PT_BR	pt_BR		
中国語 (簡体字)	ZH_CN		ZH_CN	Zh_CN
中国語 (繁体字)	ZH_TW		zh_TW	Zh_TW

システム自動化ドメインのマイグレーション

旧バージョンが既にインストールされている場合に System Automation for Multiplatforms バージョン 4.1 にマイグレーションできます。

このタスクについて

1 つ以上のノードを新規レベルにマイグレーションする前に、以下の特性をよく理解しておくようにしてください。

- マイグレーション・プロセスは、アクティブ・クラスター内の任意のノードがより上位のコード・レベルに アップグレードされるときに開始されます。
- 上位コード・レベルへのアップグレードは常に可能です。下位移行はできません。
- マイグレーション・プロセスは、アクティブ・バージョン番号がインストール済みの 最上位のバージョン番号と同じになると完了します。それまでの間、異なるコード・レベルを 共存させることができます。
- バージョン 4.1 以降では、エンドツーエンド自動化アダプターの高可用性の実現に自動化ポリシーは必要なくなりました。詳しくは、30 ページの『高可用性エンドツーエンド自動化アダプターのマイグレーション』を参照してください。

ドメイン全体をマイグレーションする

マイグレーション中はドメインが使用不可になります。ダウン時間を最小限に抑えるために、実際の移行を開始する前に、前提条件検査を実行できます。

このタスクについて

詳しくは、3 ページの『前提条件の検査』を参照してください。

以下の手順に従って、ドメイン全体をマイグレーションします。

1. すべてのリソースがオフラインであることを確認してください。
   a. エンドツーエンド自動化アダプターが稼働しているかどうかを確認します。

   ```
   samadapter status
   ```

   稼働している場合は、自動化アダプターを停止します。

   ```
   samadapter stop
   ```

   b. NominalState を Offline に設定して、すべてのオンライン・リソース・グループを停止します。

   ```
   chrg -o Offline <resource-group-name>
   ```

2. ドメインがオンラインの場合は、ドメインを停止します。

   ```
   stoprpdomain <domain-name>
   ```

3. AIX では、クラスターが停止した後、インストールが始まる前に以下のコマンドを入力します。

```
# /usr/sbin/slibclean
```

4. 製品 DVD のインストール・ディレクトリーから、または抽出済み電子成果物から、すべてのノード対して ./installSAM スクリプトを実行します。installSAM スクリプトについて詳しくは、24 ページの『インストールの実行』を参照してください。
5. ドメインを開始します。

```
startrpdomain <domain-name>
```

6. lssrc –ls IBM.RecoveryRM コマンドを使用して、コード・レベルを 検査します (29 ページの『アクティブ・バージョン番号およびインストール・バージョン番号の検証 』の例を参照)。すべてのノードは、新たにインストールされた コード・レベルになっています。ただし、アクティブ・コード・レベルは以前のレベルです。
7. 新規バージョンをアクティブにするには、29 ページの『マイグレーションの完了』に進みます。

ノードごとのマイグレーション

ノードごとのマイグレーションは、 System Automation for Multiplatforms V2.3 以上からのマイグレーションでのみサポートされます。ドメインのノードを 1 つずつ移行すると、移行中も引き続き System Automation for Multiplatforms が使用可能であるという利点があります。

このタスクについて

ダウン時間を最小限に抑える方法については、3 ページの『前提条件の検査』を参照してください。

ノードごとのマイグレーションを以下のように実行します。

1. 自動化からノードを除外します。これにより、使用可能な状態を保持する必要のあるリソースが、 ピア・ドメイン内の別のノードに必ず移動されるようにします。

```
samctrl -u a <node>
```

注: このコマンドを実行すると、すべての移動操作が完了するまでかなりの時間がかかる可能性があります。

2. ドメイン内の他のノードからノードを停止し、停止されたことを検証します。

```
stoprpnode <node>; lsrpnode
```

3. ノードをアップグレードするには、製品 CD のインストール・ディレクトリーから、または抽出済み電子成果物から、スクリプト ./installSAM を実行します。installSAM スクリプトについて詳しくは、24 ページの『インストールの実行』を参照してください。
4. ノードを開始します。

```
startrpnode <node>
```

5. アップグレードしたノードを再度自動化に組み込みます。

```
samctrl -u d <node>
```

6. これにより、アップグレードしたノードを既存ドメインに結合できるようになりました。lssrc –ls IBM.RecoveryRM コマンド を使用して (29 ページの『アクティブ・バージョン番号およびインストール・バージョン番号の検証 』の例を参照)、製品のインストール済みバージョンおよびアクティブ・バージョンを表示します。新規コードの機能は、アクティブな System Automation for Multiplatforms のバージョン番号が、クラスター内にインストール されている System Automation for Multiplatforms の最上位のバージョン番号と等しくなるまでアクティブになりません。また、すべてのノードがアップグレードされるまで、これらの新規コードの機能を完全に使用することは できません。
7. クラスター内の他のノードに対し、ステップ 1 から 6 を繰り返します。
8. 新規バージョンをアクティブにするには、29 ページの『マイグレーションの完了』に進みます。

アクティブ・バージョン番号およびインストール・バージョン番号の検証

アップグレード後、新規機能はまだ アクティブになりません。前のコード・レベルと新規コード・レベルは、マイグレーションが完了するまで共存 できます。

このタスクについて

lssrc -ls IBM.RecoveryRM コマンドを使用すると、製品のアクティブ・バージョン番号 AVN およびインストール・バージョン番号 IVN が表示されます。IVN と AVN が同一の場合、マイグレーションは完了しています。出力:

```
Subsystem         : IBM.RecoveryRM
PID               : 31163
Cluster Name      : xdr43
Node Number       : 1
Daemon start time : 02/19/13 15:12:00

Daemon State:
   My Node Name         : lnxxdr43
   Master Node Name     : lnxxdr43 (node number = 1)
   Our IVN              : 4.1.0.0
   Our AVN              : 4.1.0.0
   Our CVN              : d4b7e876c (4b7e876c)
   Total Node Count     : 2
   Joined Member Count  : 2
   Config Quorum Count  : 2
   Startup Quorum Count : 1
   Operational Quorum State: HAS_QUORUM
   In Config Quorum     : TRUE
   In Config State      : TRUE
   Replace Config State : FALSE
```

図 9. アクティブ・バージョン番号およびインストール・バージョン番号の検証

新規バージョンをアクティブにするには、29 ページの『マイグレーションの完了』に進みます。

マイグレーションの完了

マイグレーションが正常に実行されたかどうかを確認します。

このタスクについて

以下の手順に従って、マイグレーションを確認し、完了します。

1. ドメインが開始されており、ドメイン内の全ノードがオンラインであることを確認します。
2. **lsrpdomain** コマンドを発行します。ピア・ドメイン内でアクティブな RSCT のバージョンとバージョン混合の状態が表示されます。

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

3. **lsrpnode** コマンドを発行します。ノードにインストールされている RSCT のバージョンが表示されます。すべてのノードがオンラインである必要があることに注意してください。

   ```
   Name   OpState RSCTVersion
   node01 Online  2.5.5.1
   node02 Online  2.5.5.1
   node03 Online  2.5.5.1
   ```

4. RSCT ピア・ドメインが混合バージョン・モードで実行されていて (`MixedVersions = Yes`)、すべてのノードが新規リリースにアップグレード済みである場合は、いずれかのノードで RSCT `CompleteMigration` アクションを実行して、アクティブ RSCT のバージョンを更新します。このアクションを実行する前に、「*IBM RSCT* 管理ガイド」を参照して、RSCT のマイグレーション準備手順を確認してください。

RSCTActiveVersion を更新するには、すべてのノードを必ずオンラインにします。いずれかのノードで、以下のコマンドを入力してください。

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

アクティブ RSCT バージョンが更新されたことを確認するには、**lsrpdomain** コマンドを再度入力します。

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

5. **samctrl -m** コマンドを実行します。新規機能がアクティブになり、マイグレーションが完了されます。コマンドについて詳しくは、「*System Automation for Multiplatforms* リファレンス・ガイド」を参照してください。
6. System Automation for Multiplatforms リリース 3.1 からのマイグレーションを実行した場合は、いずれかのノードで以下のコマンドを入力して、属性 OperationalFlags の値を調整する必要があります。

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

この属性の実際の値を表示するには、以下のコマンドを入力します。

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

すべてのノードについて System Automation for Multiplatforms の ActiveVersion と InstalledVersion の値が同じである場合、新規コードの機能はアクティブです。

高可用性エンドツーエンド自動化アダプターのマイグレーション

高可用性エンドツーエンド自動化アダプターをバージョン 4.1 にアップグレードする方法について説明します。

System Automation for Multiplatforms バージョン 4.1 から、エンドツーエンド自動化アダプターを高可用性に対応させるための自動化ポリシーが不要になっています。Windows ではバージョン 4.1 より前から既にこのインプリメンテーションが使用可能になっていましたが、それ以外のすべてのオペレーティング・システムでも使用可能になっています。

System Automation for Multiplatforms バージョン 3.2 以下

エンドツーエンド自動化アダプターが UNIX および Linux クラスターで動作した環境を 31 ページの図 10 に示します。

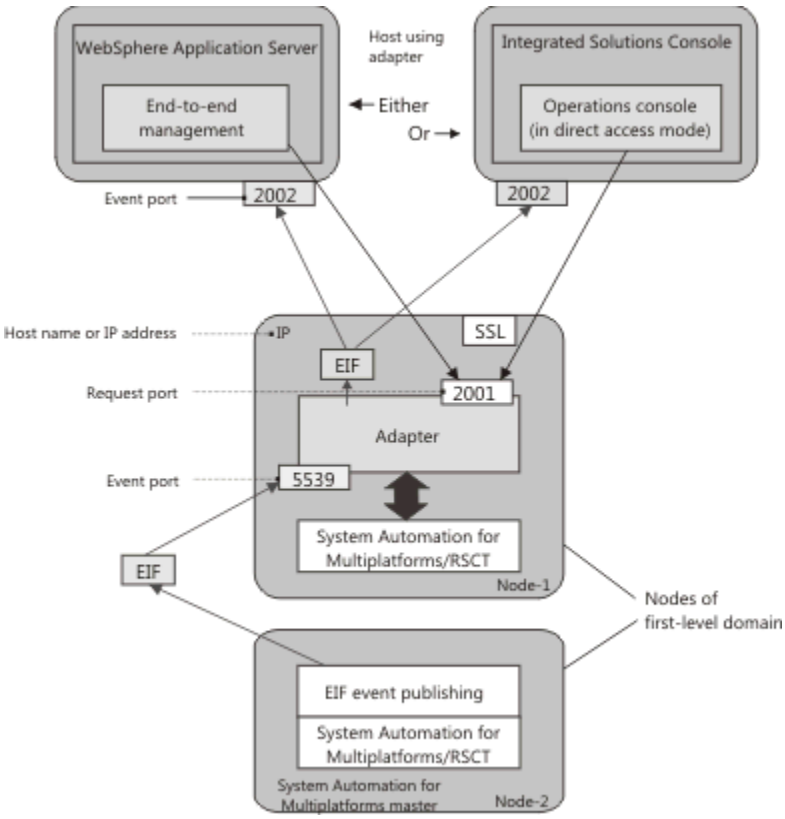


図 *10.* バージョン *4.1* より前の *UNIX* および *Linux* クラスターでのエンドツーエンド自動化アダプター環境

System Automation for Multiplatforms バージョン 4.1

アダプターがバージョン 4.1 以降で動作する環境を 31 ページの図 11 に示します。

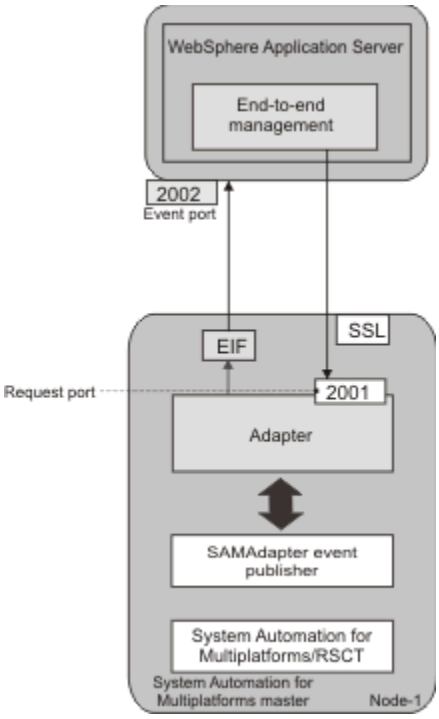


図 *11.* バージョン *4.1* で使用可能なエンドツーエンド自動化アダプター環境

バージョン 4.1 以降では、自動化アダプターが System Automation マスター・ノードに接続されます。クラスター・インフラストラクチャーにより、System Automation for Multiplatforms マスターとアダプターが常に使用可能であることが保証されます。アダプターを高可用性に対応させるための追加の自動化ポリシーは必要ありません。このシナリオでは、System Automation クリティカル・リソースである仮想 IP アドレスも追加で要求されることはありません。

エンドツーエンド自動化アダプターの高可用性インプリメンテーションが変更されたことで、28 ページの『ノードごとのマイグレーション』で説明するノードごとのクラスターのアップグレードを行う場合に、以下の影響が及びます。

マイグレーション処理中に古いインプリメンテーションがアクティブになります
マイグレーションがまだ完了していない場合は、クラスター内のノードごとに異なるバージョンのコードがアクティブな状態になっています。その間は、古い高可用性インプリメンテーションが引き続きアクティブです。新しいインプリメンテーションは、アクティブ・バージョンがバージョン 4.1.0.0 以降に設定され次第アクティブになります。詳しくは、29 ページの『マイグレーションの完了』を参照してください。

マイグレーション処理中も引き続き自動化ポリシーの構成が可能です
アダプターを高可用性に対応させるための自動化ポリシーは不要になっています。しかし、ノードごとのマイグレーションが完了していない場合は、古いインプリメンテーションも引き続きサポートされます。アダプター自動化ポリシー構成タスクは引き続きマイグレーション処理中に使用可能であり、サポートされます。これらの構成タスクに関する資料は削除されています。これらのタスクに関する説明を参照する必要がある場合は、本製品の旧バージョンの資料を参照してください。

注 : ノードごとのマイグレーション中に高可用性構成を変更する場合は、必ずオンラインのクラスター・ノードで構成ユーティリティーを実行してください。理由は、オフライン・ノードではアクティブ・バージョンの番号を判別できないためです。アクティブ・バージョンの番号がまだ 4.1.0.0 未満であっても、オフライン・クラスターやオフライン・ノードではアダプター高可用性構成の古いインプリメンテーションを使用できません。

バージョン 4.1 へのマイグレーションを完了する前に、ドメイン全体およびノードごとのマイグレーションのすべての自動化ポリシーを確認してください。自動化ポリシーには、エンドツーエンド自動化アダプターの高可用性に関連したリソースが含まれる可能性があります。以下のリソースをすべて削除してください。

- アダプター自動化の構成時に使用するリソース接頭部を確認してください。デフォルトの接頭部は `samadapter-` です。
- 名前がその接頭部で始まるすべての関係、リソース、およびリソース・グループを削除してください。
- `xml` 形式を使用してポリシーを定義する場合は、名前がその接頭部で始まるすべての関係、リソース、およびリソース・グループを `xml` ファイルから削除してください。

マイグレーションを完了した後で必要なアクション
クラスター・マイグレーションが開始しているのにアダプターが実行されている場合、アダプターは停止されて、マイグレーションが完了しても再始動されません。

アダプターを始動できるようになるのは、以下の手動マイグレーション手順を実行してからです。

1. 構成ユーティリティー `cfgsamadapter` を実行して、アダプター・ホスト名または IP アドレスを変更します。各クラスター・ノードのローカル・ホスト名をデフォルトとして選択するか、他と明確に区別できるホスト名または IP アドレスを指定します。
2. アダプター・ホストにデフォルトを選択した場合は、その構成をクラスター内の他のノードに複製します。そうしない場合は、ホスト名または IP アドレスを各クラスター・ノードに明示的に構成します。

これでアダプターを開始することができます。構成ダイアログを System Automation for Multiplatforms 管理者とユーザーのガイドで説明されているとおりに使用するか、`samadapter start` コマンドを使用します。

古いアダプター高可用性インプリメンテーションを引き続き使用します
まれに、新しいアダプター高可用性インプリメンテーションを使用できない場合があります。例えば、クラスターの使用可能ノードのサブセットのみでアダプターが実行されるように強制する場合です。

このシナリオは、以前の自動化ポリシーで可能です。 しかし、新しい方式ではアダプターを任意のクラスター・ノードで実行できます。

このような場合は、バージョン 4.1 を使用していると、アダプターを高可用性に対応させるための自動化ポリシーを引き続き使用するように強制することができます。新しい方式または古い方式のいずれかを使用してクラスターを既に実行している場合でも、他方の方式に切り替えることができます。以下のシナリオはサポートされています。

1. **バージョン 4.1 にマイグレーションするときに古いインプリメンテーションを引き続き使用します**

   バージョン 4.1 未満からバージョン 4.1 にクラスターをマイグレーションした場合は、新しいアダプター高可用性インプリメンテーションがアクティブになります。代わりに古いインプリメンテーションを使用する場合は、すべてのクラスター・ノード上でバージョン 4.1 に製品コードをアップグレードした後で、以下のステップを実行します。

   a. クラスター内の各ノード上で、構成プロパティー・ファイル /etc/opt/IBM/tsamp/sam/cfg/sam.adapter.properties を編集し、パラメーター use-adapter-ha-policy の値を false から true に変更します。

   b. **samctrl -m** コマンドを発行します。

2. **マイグレーションを完了した後の新しいアダプター高可用性インプリメンテーションへの切り替え**

   バージョン 4.1 未満からバージョン 4.1 にクラスターをマイグレーションし、上記のシナリオ 1 で説明されている手順を実行した場合は、古いアダプター高可用性インプリメンテーションが引き続き使用されます。その後、新しいアダプター高可用性インプリメンテーションに切り替える場合は、以下のステップを実行します。

   a. コマンド **stoprpdomain** を入力してドメインを停止します。

   b. クラスター内の各ノード上で、構成プロパティー・ファイル /etc/opt/IBM/tsamp/sam/cfg/sam.adapter.properties を編集し、パラメーター use-adapter-ha-policy の値を true から false に変更します。

   c. コマンド **startrpdomain** を入力してドメインを開始します。

3. **マイグレーションを完了した後の古いアダプター高可用性インプリメンテーションへの再切り替え**

   バージョン 4.1 未満からバージョン 4.1 へのクラスターのマイグレーションを完了し、上記のシナリオ 1 で説明されている手順を実行しなかった場合は、新しいアダプター高可用性インプリメンテーションが使用されます。これは、シナリオ 2 で説明されている手順を実行した場合も同じです。その後、古いアダプター高可用性インプリメンテーションに再度切り替える場合は、以下のステップを実行します。

   a. コマンド **samadapter stop** を入力してアダプターを停止します。

   b. クラスター内の各ノード上で、構成プロパティー・ファイル /etc/opt/IBM/tsamp/sam/cfg/sam.adapter.properties を編集し、パラメーター use-adapter-ha-policy の値を false から true に変更します。

   c. コマンド **cfgsamadapter** を入力して構成ユーティリティーを開始し、以下のタスクを実行します。

      i) 構成ダイアログのメインウィンドウで、「**構成**」をクリックします。

      ii)「**保存**」をクリックして、構成変更を保存します。これにより、いずれの場合でも、古いインプリメンテーションに必要な EEZ パブリッシャー・エントリーが構成プロパティー・ファイル /etc/Tivoli/tec/samPublisher.conf に追加されます。このタスクが必要になるのは、アダプターが新しいアダプター高可用性インプリメンテーションを使用するときに、パブリッシャー・エントリーがアダプターによって削除される可能性があるためです。

      iii) 構成ダイアログのメインウィンドウで、「**複製**」をクリックし、構成変更をクラスター内の他のノードに伝搬します。

      iv) 構成ダイアログのメインウィンドウで、「**定義**」をクリックして、アダプター高可用性ポリシーを再度アクティブにします。これは、System Automation for Multiplatforms によって **samctrl -m** コマンドの実行中に削除されています。

d. コマンド **samadapter start** を入力してアダプターを開始します。

4. **新しいバージョン 4.1.0.0 クラスターでの古いアダプター高可用性インプリメンテーションの使用**

   バージョン 4.1.0.0 の初期インストールを実行した場合は、新しいアダプター高可用性インプリメンテーションが使用されます。代わりに古いアダプター高可用性インプリメンテーションを使用する場合は、以下のステップを実行します。

   a. コマンド **samadapter stop** を入力してアダプターを停止します。

   b. クラスター内の各ノード上で、構成プロパティー・ファイル /etc/opt/IBM/tsamp/sam/cfg/sam.adapter.properties を編集し、パラメーター use-adapter-ha-policy の値を false から true に変更します。

   c. コマンド **cfgsamadapter** を入力して構成ユーティリティーを開始し、以下のタスクを実行します。

      i) 構成ダイアログのメインウィンドウで、「**構成**」をクリックします。

      ii)「**自動化**」タブで、アダプター高可用性ポリシーを構成します。

      iii)「**保存**」をクリックして、構成変更を保存します。

      iv) 構成ダイアログのメインウィンドウで、「**複製**」をクリックし、構成変更をクラスター内の他のノードに伝搬します。

      v) 構成ダイアログのメインウィンドウで、「**定義**」をクリックして、アダプター高可用性ポリシーをアクティブにします。

   d. コマンド **samadapter start** を入力してアダプターを開始します。

シナリオ 3 と 4 には、「**定義**」タスクと「**自動化**」タブについての記述があります。これらのタスクに対応する資料はバージョン 4.1 では削除されています。これらのタスクに関する説明を参照する必要がある場合は、本製品の旧バージョンの資料を参照してください。

ポストインストール

デバッグ・データを入手するため、システム・ロガーを構成する必要があります。

このタスクについて

AIX 上に System Automation for Multiplatforms をインストールしたら、以下のタスクを実行する必要があります。

AIX 上のシステム・ロガーの構成

システム・ロガーはデフォルトでは構成されません。メッセージは、エラー・ログに書き込まれます。

デバッグ・データを入手するため、ファイル /etc/syslog.conf にシステム・ロガーを構成する必要があります。 必要な変更を完了した後で、**refresh -s syslogd** コマンドを使用して syslogd をリサイクルする必要があります。ログ・ファイルのロケーションは /etc/syslog.conf に定義されています。

Linux の場合は追加の処置は不要です。

AIX 上で共用ボリューム・グループを拡張コンカレント対応にする

共用ボリューム・グループが拡張コンカレント対応でないと、ノードが破損したときにディスクがロックされ、リモート・ノードがこのディスクにアクセス できなくなります。この状態を避けるには、共用ボリューム・グループを拡張コンカレント対応にします。

このタスクについて

注 :

1. パッケージ bos.clvm.enh がシステムにインストールされていることを確認してください。

2. System Automation for Multiplatforms は、ポリシー内でクラス IBM.AgFileSystem または IBM.VolumeGroup のリソースを使用する際に、非コンカレント・モードで拡張コンカレント対応ボリューム・グループをサポートします。System Automation for Multiplatforms は、拡張コンカレント・ボリューム・グループのコンカレント・モードおよびそれに含まれるファイル・システムをポリシー内のリソースとしてサポートしません。拡張コンカレント・ボリューム・グループのサポートは、ポリシー・プロバイダーにより、 IBM.Application リソースを使用して拡張コンカレント・ボリューム・グループ上でファイル・システムを管理することで明示的に提供されます。

ボリューム・グループを拡張コンカレント対応にする前に、lsvg コマンドを使用 して、その共用ボリューム・グループに関する情報を表示してください。

```
# 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
```

SMIT を使用してボリューム・グループを拡張コンカレント対応にするには、以下を行います。

1. 以下のコマンドを入力します。

   ```
   # smitty vg
   ```

   以下のようなテキスト が表示されます。

   ```
         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. Enter を押します。

コマンド行から、ボリューム・グループを拡張コンカレント対応にするには、 以下を入力します。

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

ボリューム・グループを拡張コンカレント対応にした後は、lsvg コマンドを実行すると、以下の出力例のような情報が返されます。

```
# 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
```

ロールバック手順

記載されている手順に従って、インストール済み環境を前のリリースにロールバックします。

このタスクについて

System Automation for Multiplatforms を以前のリリースにロールバックするには、以下のステップを実行します。

1. 次のようにして自動化ポリシーを保存します。

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

2. すべてのリソース・グループをオフラインに変更します。あるいは、リソースに影響を与えないようにする場合は、次のようにしてドメインを停止します。

   ```
   stoprpdomain –f domain_name
   ```

3. RSCT レベルをロールバックする必要もある場合は、ドメインを削除します。 それ以外の場合は、ドメインをオフラインにします。
4. System Automation for Multiplatforms は、コマンド `./installSAM --forceAll` の実行によってロールバックできます。このコマンドにより、既にインストールされているバージョンに関係なく、`installSAM` が存在する System Automation for Multiplatforms および RSCT 成果物がインストールされます。
5. ドメインを削除した場合は、ドメインをもう一度作成します。それ以外の場合は、`startrpdomain -w domain_name` を入寮 k して、ドメインを開始します。
6. ドメインが再作成されたら、保存してあるポリシーを、 `sampolicy -a file.xml` を入力して再適用します。

アンインストール

System Automation for Multiplatforms は、示されている手順に従って AIX および Linux 環境から削除できます。

このタスクについて

アンインストール手順を開始する前に、以下のヒントを考慮してください。

- System Automation for Multiplatforms をアンインストールするには、ご使用のオペレーティング・システム向けに提供 される **uninstallSAM** スクリプトを使用します。例えば、インストール・ディレクトリーから **./uninstallSAM** を実行して、製品が正しくアンインストールされるようにします。
- アンインストールする前に、**sampolicy –s** コマンドを使用してご使用の構成を保存してください。System Automation for Multiplatforms 構成の保存方法について詳しくは、*Tivoli System Automation for Multiplatforms* 管理者とユーザーのガイドを参照してください。

  「*System Automation for Multiplatforms* リファレンス・ガイド」の **sampolicy** コマンドの説明。
- コマンド **uninstallSAM** により、ドメインについて定義したすべての構成情報は除去されます。したがって、新規バージョンにアップグレードするときには **uninstallSAM** を使用しないでください。

System Automation for Multiplatforms をアンインストールするには、以下のステップを実行してください。

1. ドメインがオフラインであることを確認します。
   - ドメインがオンラインかどうかを確認するには、以下のコマンドを実行します。

     ```
     lsrpdomain
     ```

- ドメインを停止し、以下のコマンドを実行します。

```
stoprpdomain <domain>
```

2. /opt/IBM/tsamp/sam/uninst/ ディレクトリーにある uninstallSAM スクリプトを使用して、製品をアンインストールします。

```
./uninstallSAM
```

通常、uninstallSAM コマンドに使用できるオプションを指定する必要はありません。コマンドについての詳しい説明は、 System Automation for Multiplatforms リファレンス・ガイドを参照してください。

CSM または GPFS が同じ Linux システム上にインストールされている場合、Redhat Package Manager は RSCT および SRC が System Automation for Multiplatforms と共にアンインストールされないようにします。CFM または GPFS でも RSCT およびシステム・リソース・コントローラー (SRC) のパッケージが使用されます。Redhat Package Manager のメッセージにこの状態が示されます。

3. アンインストールに関する情報がないかどうか、次のログ・ファイルを調べます。

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

ハッシュ記号 <#> は番号を示します。最も大きな番号は、最新のログ・ファイルを表します。

4. アンインストールされたパッケージを確認するには、 /tmp/uninstallSAM.<#>.log を検査します。この <#> は、見つかったログ・ファイルのうち、最も大きい番号です。

注: コマンド uninstallSAM は、/etc/opt/IBM/tsamp/sam に格納されているすべての設定も削除します。

新しいオペレーティング・システムへのインストール

フィックスパック 4.1.0.<f> (<f> は各フィックスパック番号) では、新しいオペレーティング・システムのサポートを導入することができます。

24 ページの『System Automation for Multiplatforms のインストール』 で説明した System Automation for Multiplatforms 4.1.0.0 のインストールを実行できるのは、このバージョン 4.1 リリース・レベルで当初からサポートされている一連のプラットフォームおよびオペレーティング・システム・バージョン上に限られます。ただし、後でフィックスパックを適用することにより、この他のプラットフォームまたはオペレーティング・システム・バージョンに対するサポートを追加することができます。以降の説明では、これを「新しいプラットフォームのサポート」と呼びます。既にサポートされているオペレーティング・システムにフィックスパックをインストールする場合は、インストール済み環境をアップグレードしてください。

新しいプラットフォームのサポートがどのフィックスパックで導入されるかを調べるには、5 ページの『サポートされるプラットフォーム』を参照してください。

フィックスパックで新しいオペレーティング・システムのサポートが導入される場合、このフィックスパックをイニシャル・インストールとして (アップグレード・インストールではなく) インストールする必要があります。このため、そのフィックスパックのインストールを開始する前に、4.1 のライセンス・ファイルを SAM410<f>MP<platform>/license ディレクトリーにコピーする必要があります。以下のステップを実行します。

1. 4.1 リリースの以下のいずれかの配布物に含まれている System Automation for Multiplatforms のライセンス・ファイルを入手します。

製品 DVD
1 ページの『製品 DVD』に記載されているいずれかの DVD を使用して、ライセンスを入手します。SAM4100MP<platform>/license ディレクトリーに、sam41.lic という名前のライセンス・ファイルがあります。

電子配布
2 ページの『電子配布』に記載されているいずれかのアーカイブ・ファイルを使用して、ライセンスを入手します。アーカイブ・ファイルを解凍します。展開したディレクトリー・ツリー内の

SAM4100MP<platform>/license ディレクトリーに、sam41.lic という名前のライセンス・ファイルがあります。

2. 39 ページの『プラットフォーム固有のアーカイブの使用法』の説明に従って、新しいオペレーティング・システムのサポートが含まれている 4.1.0.<f> フィックスパックのアーカイブ・ファイルを解凍します。展開したディレクトリー・ツリー内の SAM410<f>MP<platform>/license ディレクトリーは空です。
3. ステップ 1 で入手したライセンス・ファイルを、展開したフィックスパックのディレクトリー・ツリー内の SAM410<f>MP<platform>/license ディレクトリーにコピーします。
4. 24 ページの『インストールの実行』で説明されているように、System Automation for Multiplatforms のインストールを起動します。インストール・プログラムにより、新しいオペレーティング・システム上で製品のイニシャル・インストールが実行されます。

SLES 12 から SLES 15、または RHEL 6 から RHEL 7/8 へのマイグレーション

既存の System Automation for Multiplatforms クラスターとともに、SLES 12 から SLES 15、または RHEL 6 から RHEL 7/8、あるいは RHEL 7 から RHEL 8 にマイグレーションできます。

以下のステップを実行して、ご使用のクラスターをマイグレーションします。

1. sampolicy -s コマンドを使用して、ポリシーを保存します。リソースを停止して、ドメインを削除します。
2. ターゲット OS プラットフォーム SLES 15、RHEL 7、または RHEL 8 をすべてのクラスター・ノードにインストールします。
3. SLES 15 および RHEL 7/8 をサポートする System Automation for Multiplatforms パッケージ (4.1.0-TIV-SAMP-Linux64-FP000x) をインストールします。詳しくは、新しいオペレーティング・システムへのインストールを参照してください。
4. ドメインをもう一度作成し、ポリシー sampolicy -a をアクティブにします。

注 :

1. ノードごとのマイグレーション機能は、System Automation for Multiplatforms 製品のレベルのアップグレードを行うためにのみサポートされ、オペレーティング・システムのバージョンのアップグレードを行うためにはサポートされません。
2. SLES 12/15 や RHEL 6/7/8 のように、オペレーティング・システムのレベルが混在するドメインを使用することはサポートされていません。
3. 32 ビットと 64 ビットの言語環境は同じドメイン内で使用できません。

サービス・フィックスパックのインストール

サービスのインストールとは、System Automation for Multiplatforms のリリース 4.1 に修正サービス・フィックスパックを適用すること、またはリリース 4.1 からソフトウェア・リリース・レベルをアップグレードすることを意味します。このようなサービス・フィックスパックを製品フィックスパックと呼びます。

このタスクについて

製品フィックスパックは、次の形式で System Automation for Multiplatforms に使用可能です。

Linux
圧縮された .tar 形式のアーカイブ。

AIX
圧縮された .tar 形式のアーカイブ。

フィックスパックの入手

このタスクについて

詳しくは、System Automation for Multiplatforms 製品ページを参照してください。

製品フィックスパックのアーカイブは、System Automation for Multiplatforms サポート・ポータルからダウンロードできます。アーカイブを一時ディレクトリーにダウンロードします。通常、オペレーティング・システムごとに 1 つのアーカイブが使用可能です。製品フィックスパックのアーカイブに適用される命名規則について詳しくは、39 ページの『アーカイブの命名規則』を参照してください。

アーカイブの命名規則

アーカイブ名の構文について説明します。

このタスクについて

System Automation for Multiplatforms の製品フィックスパックのアーカイブには、次の構文が使用されています。

`4.1.0-TIV-SAMP-<platform>-FP<fix_pack_number>.<archive_type>` (System Automation for Multiplatforms 用のサービス・フィックスパックが含まれます)

説明:

<platform>
System Automation for Multiplatforms がインストールされているオペレーティング・システム。

<fix_pack_number>
フィックスパック番号。

<archive_type>
`tar.gz` または `tar.Z` のいずれか。

例:

AIX オペレーティング・システムに System Automation for Multiplatforms 4.1.0 用のフィックスパック 1 をインストールするのに使用される `tar.Z` アーカイブは、次のとおりです。

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

プラットフォーム固有のアーカイブの使用法

フィックスパックのダウンロードおよびインストールの方法について説明します。

このタスクについて

以下の表に、Linux および AIX オペレーティング・システムにサービスを適用するためのダウンロード可能なアーカイブ・ファイルをリストします。各アーカイブについては、「**説明**」列に示されている固有の指示に従ってください。

Linux

表 *18. Linux* オペレーティング・システム用のアーカイブ

アーカイブ名	説明
`4.1.0-TIV-SAMP-Linux-FP<fix_pack_number>.tar.gz`	`tar -zxf` コマンドを使用して、アーカイブを圧縮解除および解凍してください。アーカイブを解凍すると、インストール・スクリプト `installSAM` が `SAM41<maintenance_level>MPLinux/installSAM` に格納されます。

フィックスパック 4.1.0.1 以降では、さらなるオペレーティング・システム・バージョンのサポートが導入されています (詳しくは 5 ページの『サポートされるプラットフォーム』を参照)。それらのオペレーティング・システム・バージョンでは、32 ビット互換モードはサポートされなくなりました。次の表は、対応する 64 ビット・サービス成果物が含まれる System Automation for Multiplatforms アーカイブ・ファイルを示します。詳しくは、「37 ページの『新しいオペレーティング・システムへのインストール』」を参照してください。

表 *19. Linux 64* ビット・オペレーティング・システム用のアーカイブ	
アーカイブ名	**説明**
4.1.0-TIV-SAMP-Linux64-FP<fix_pack_number>.tar.gz	**tar -zxf** コマンドを使用して、アーカイブを圧縮解除および解凍してください。アーカイブを解凍すると、インストール・スクリプト `installSAM` が `SAM41<maintenance_level>MPLinux64/installSAM` に格納されます。

AIX

表 *20. AIX* オペレーティング・システム用のアーカイブ	
アーカイブ名	**説明**
4.1.0-TIV-SAMP-AIX-FP<fix_pack_number>.tar.Z	**uncompress** コマンドを使用して、アーカイブを圧縮解除してから、`tar -xf` コマンドを使用して、アーカイブを解凍してください。アーカイブを解凍すると、インストール・スクリプト `installSAM` が `SAM41<maintenance_level>MPAIX/installSAM` にあることが分かります。

System Automation for Multiplatforms 用のサービスのインストール

サービスをインストールすると、System Automation for Multiplatforms がリリース 4.1 からアップグレードされます。したがって、サービスを適用するには、事前にリリース 4.1 がインストールされている必要があります。

このタスクについて

始める前に

- 製品フィックスパックは常に累積されます。
- 製品フィックスパックをインストールするには、root 権限が必要です。
- System Automation for Multiplatforms サポート・サイトからアーカイブをダウンロードした (39 ページの『フィックスパックの入手』を参照) 場合、製品フィックスパックのアーカイブを一時ディレクトリーに解凍します。ご使用のオペレーティング・システム用のアーカイブ解凍方法については、39 ページの『プラットフォーム固有のアーカイブの使用法』を参照してください。
- サービス・フィックスパックをインストールする前に、システム構成をバックアップします。詳しくは、*Tivoli System Automation for Multiplatforms* 管理者とユーザーのガイドを参照してください。
- ダウン時間を最小限に抑えるために、インストールを開始する前に、前提条件検査を実行できます。詳しくは、3 ページの『前提条件の検査』を参照してください。

ピア・ドメイン内の各ノードで以下のステップを実行します。

1. サービスを予定しているノードでオンラインになっているリソースがあるかどうかを確認します。
   - リソースがオンラインになっており、今後もこのリソースを使用可能な状態で維持する必要がある場合は、このノードを自動化から除外します。

     ```
     samctrl -u a <node>
     ```

System Automation for Multiplatforms は、ノード上のリソースを停止し、可能な場合は、ピア・ドメイン内の異なるノードでそれらを再始動します。

- サービス中にリソースを使用可能な状態で維持する必要がない場合は、リソース・グループをオフラインにします。

2. ドメイン内の他のノードからノードを停止し、停止されたことを検証します。

```
stoprpnode <node>; lsrpnode
```

3. アーカイブを受信したら、解凍してください。ルート・ディレクトリー SAM41mfMP を持つディレクトリー構造が作成されます。ここで、mf は修正レベルとフィックス・レベルを表します。
4. installSAM スクリプトを使用してサービス・フィックスパックをインストールします。 このスクリプトについての詳細は、24 ページの『インストールの実行』を参照してください。
5. ノードを開始します。

```
startrpnode <node>
```

6. ステップ 2 でノードを除外した場合は、このノードを自動化に含めてください。

```
samctrl -u d <node>
```

7. リソース・グループをオンラインにする必要がある場合は、リソース・グル ープをオンラインにします。それ以外の場合は、ピア・ドメインの最後のノードにサービスが適用されるまで、このステップを延期します。
8. すべてのノードにサービスが適用されたら、29 ページの『マイグレーションの完了』で説明するステップを実行します。ドメイン全体で変更内容が有効になり、正しいバージョンが表示されます。

サービスのアンインストール

フィックスパックをアンインストールするには、製品全体をアンインストールする必要があります。

このタスクについて

System Automation for Multiplatforms をアンインストールするには、36 ページの『アンインストール』の説明に従います。

アンインストールが完了した後、System Automation for Multiplatforms および必要なサービス・レベル (フィックスパック・レベル) を再インストールすることができます。

Extended Disaster Recovery (xDR) フィーチャーのインストール

現在、ビジネスや企業は、重要なデータの復旧を、災害復旧ソリューションに 依存しています。この問題を解決するために、System Automation for Multiplatforms では GDPS/PPRC Multiplatform Resiliency on System z (xDR) をサポートしています。

このタスクについて

Geographically Dispersed Parallel Sysplex® (GDPS®) は、ご使用の z/OS® 環境と連携するよう大幅にカスタマイズされた、アプリケーションの可用性と災害復旧のためのソリューションです。これにより、災害および障害を単一制御点からリカバリーすることができ、データの整合性が保証されます。GDPS について詳しくは、IBM Redbooks からダウンロードできる、IBM Redbooks® 資料の『*GDPS Family - An Introduction to Concepts and Capabilities*』を参照してください。

System Automation for Multiplatforms は、System z で稼働する GDPS/PPRC for Linux システムを拡張します。これは、以下のプラットフォーム上で稼働するシステム用に調整された災害時回復ソリューションを備えています。

- zSeries (z/OS を含む)
- z/VM 下の Linux on System z

- LPAR で固有に稼働する Linux on System z

xDR のパッケージ化

xDR フィーチャーのコードは、System Automation for Multiplatforms 製品の一部として組み込まれます。このコードを有効にする個別のライセンスをインストールしない限り、対応する機能を使用することはできません。

このタスクについて

ライセンスは xDR フィーチャーの注文時に受け取れます。ライセンス・ファイルの名前は `sam41XDR.lic` です。

DVD
DVD「System Automation for Multiplatforms v4.1 – xDR for Linux on System z」から xDR フィーチャーをインストールします。ライセンス・ファイルは、ディレクトリー `SAM4100FeatXDR/license` にあります。

電子配布
xDR フィーチャーを電子配布経由で入手した場合、ライセンス・ファイルは電子配布ファイル `CIVG7ML.txt` にあります。このファイルはライセンス・ファイル自体と同一です。この電子配布ファイルを `sam41XDR.lic` に名前変更またはコピーしてください。

xDR 前提条件

xDR フィーチャーのライセンスをインストールするには、その前に System Automation for Multiplatforms 基本製品をインストールする 必要があります。

このタスクについて

xDR は Linux on System z でのみサポートされます。

xDR の場合は、以下の Linux ディストリビューションがサポートされます。

- z/VM® の下で実行されている xDR for Linux on System z には、次のいずれかのオペレーティング・システムが必要です。
  - SUSE SLES 12 (64 ビット)
  - SUSE SLES 15 (64 ビット)
  - Red Hat RHEL 6 (64 ビット)
  - Red Hat RHEL 7 (64 ビット)
  - Red Hat RHEL 8 (64 ビット)
- ECKD™ ディスクを使用して LPAR でネイティブに実行されている xDR for Linux on System z には、次のいずれかのオペレーティング・システムが必要です。
  - SUSE SLES 12
  - SUSE SLES 15

注 :

1. xDR 機能を使用する場合は、特定バージョンの z/VM、Linux on System z、GDPS、および System Automation for Multiplatforms をインストールする必要があります。 使用可能な機能および必要なバージョンについて詳しくは、GDPS の資料を参照してください。System Automation for Multiplatforms は、Linux on System z の xDR のみをサポートします。
2. xDR の命名規則では、クラスターおよびノードの名前は 32 文字を超えてはな りません。クラスター名およびノード名にピリオド (.) またはダッシュ (-) が含まれてはいけません。また、これらの名前が同一ではいけません。xDR の場合、クラスター名は大/小文字の区別がありません。xDR を使用する場合、System Automation for Multiplatforms は GDPS の資料の説明のようにカスタマイズする必要があります。

3. xDR および GDPS がサポートする言語は英語のみです。

xDR フィーチャー・ライセンスのインストール

samlicm コマンドを使用して、ライセンスをインストールします。

このタスクについて

ライセンス・ファイルは、System Automation for Multiplatforms がインストールされているシステムからアクセス可能である必要があります。 ファイル sam41XDR.lic を、**samlicm** を始動したときにアクセス可能な場所にコピーします。

以下のようにライセンスをインストールします。

```
samlicm -i  <license file location>/sam41XDR.lic
```

フィーチャー・ライセンスが正常にインストールされていることを以下のコマンドで確認します。

```
samlicm -s
```

xDR フィーチャーの名前が、コマンド出力の Product Annotation フィールドの値として表示されます。以下に例を示します。

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

samlicm コマンドについて詳しくは、「*System Automation for Multiplatforms* リファレンス・ガイド」を参照してください。

4.1 より前のバージョンからの xDR フィーチャーのアップグレード

バージョン 4.1 から、xDR フィーチャー・ライセンスは、異なるターゲット・ディレクトリーにインストールされます。

このタスクについて

xDR 機能を 4.1 より前のバージョンからアップグレードする場合は、以前にインストールされた xDR フィーチャー・ライセンスは削除されます。43 ページの『xDR フィーチャー・ライセンスのインストール』の説明に従って、機能ライセンスを再度インストールします。 製品コードのアップグレード元の System Automation for Multiplatforms バージョンのライセンス・ファイルを使用できます。あるいは、アップグレード先のバージョンのライセンス・ファイルを使用することもできます。

バージョン 4.1 から、z/VM® で実行されている xDR for Linux on System z® では、すべてのプロキシー・ノードのストレージが永久にロックされている状態のみがサポートされます。マスター・プロキシーのストレージをロックするオプションを備えたデュアル・ノード・プロキシー・クラスターを現在使用しているお客様は、スクリプト enableErpd を実行してマイグレーションする必要があります。その後、両プロキシー・ノードの boot.local または rc.local ファイルに LOCK コマンドを追加して、ストレージのロックを実行する必要があります。詳しくは、GDPS のマニュアルを参照してください。

xDR フィーチャーのアンインストール

このタスクについて

xDR フィーチャーに対して定義されている特定のアンインストール手順はありません。System Automation for Multiplatforms のアンインストール時に 暗黙でアンインストールされます。

SAP 高可用性ポリシーのインストール

SAP Central Services 高可用性ポリシー・フィーチャーは System Automation for Multiplatforms の一部として組み込まれていますが、別個のライセンスが必要です。

SAP 高可用性ポリシー・フィーチャーは System Automation for Multiplatforms の一部として組み込まれていますが、個別のライセンスが必要です。

SAP 高可用性ポリシー・フィーチャーをインストールする方法について詳しくは、「System Automation for Multiplatforms 高可用性ポリシー・ガイド」を参照してください。

第 3 章 構成

System Automation for Multiplatforms を正常にインストールした後は、必要となる System Automation for Multiplatforms コンポーネントおよび機能に応じた構成タスクを処理します。

注 : 自動化アダプター構成ダイアログを使用するには、X11 サーバーが必要です。構成ダイアログを実行するには、32 ビット・バージョン の X11 インストール・パッケージが必要です。一部の Linux オペレーティング・システムでは、それらのパッケージは配布メディアには含まれていますが、標準インストールには含まれていません。 32 ビット・バージョンの X11 インストール・パッケージがインストールされていることを確認してください。

自動化アダプターは、入力プロパティー・ファイルを使用してサイレント・モードで構成することもできます。 X11 サーバーが使用できない場合は、 サイレント構成が、このシステムでサポートされる唯一の方式です。 詳しくは、82 ページの『サイレント・モードでの構成』を参照してください。

システム自動化の動作の構成

System Automation for Multiplatforms は、製品の動作に影響を与える属性のセットを変更することにより、管理および制御できます。

例えば保守などの理由で、自動化機能の開始または停止、タイムアウト期間の定義、あるいは自動化からのノードの除外を行うことができます。

以下の属性を変更できます。

TimeOut
: System Automation for Multiplatforms によって 実行される開始制御操作のタイムアウト値を秒単位で指定します。タイムアウト期間が満了になった後、RetryCount の値を超えていない場合は操作が繰り返されます。

RetryCount
: 失敗やタイムアウトの場合に、制御操作を再試行できる回数。

Automation
: System Automation for Multiplatforms による自動化を使用可能に設定するか、使用不可に設定するためのフラグ。

ExcludedNodes
: System Automation for Multiplatforms が積極的にリソースを除外または停止する ノードのリスト。例えば、保守のために使用できます。

ResourceRestartTimeOut
: 障害になったノードにあったリソースを別のノードで 再始動するまで、System Automation for Multiplatforms が待機する時間間隔 (秒単位)。

TraceLevel
: 書き込まれるトレース項目の数を制御する場合は、トレース・レベルを使用できます。最大値 255 を指定すると詳細なトレースが行われ、値 0 を指定するとトレース項目のさまざまなクラスの書き込みが抑制されます。リソース数が多い自動化ポリシーの場合は、トレース・レベルを下げることをお勧めします。

属性の現行値は、**lssamctrl** コマンドを使用してリストできます。 属性は、**samctrl** コマンドを用いて変更されます。 詳しくは、「*IBM Tivoli System Automation for Multiplatforms* リファレンス」にある、これらのコマンドのリストと説明を参照してください。

TimeOut および RetryCount

`TimeOut` 属性は、常に `RetryCount` 属性とともに使用されます。

TimeOut
: リソース・マネージャーがある動作を完了するまでに System Automation for Multiplatforms が待機する時間を指定します。

RetryCount
制御操作が失敗した場合に、System Automation for Multiplatforms が `TimeOut` 期間内に行うことができる制御操作の試行回数を指定します。通常、最初の試行が失敗した場合は、2 回目以降の試行で成功する確率はかなり低くなります。

開始操作

System Automation for Multiplatforms がリソースに対して最初のリソース開始制御操作を送信した時点で、操作タイマーが開始されます。そのタイマーが開始された場合は、以下の 3 つの可能性があります。

1. タイムアウト期間内に、リソースが本来あるべき状態 (オンラインまたはオフライン) に なります。この場合、リソースは System Automation for Multiplatforms が要求する状態になるため、それ以上のアクションは起動されません。
2. タイムアウト期間内にリソースが開始制御操作を拒否します。その後に起こることは、拒否コードによって異なります。
   - 拒否コードにエラーがリカバリー可能であることが示されている場合、System Automation for Multiplatforms はそのリソースに対して開始制御操作を引き続き実行します。すべての制御操作の試行がカウントされます。RetryCount 値を超えると、System Automation for Multiplatforms はこれ以上の制御操作の実行を停止します。
   - エラーがリカバリー可能でない場合は、リソースが問題プログラム状態になります。これによってさらに自動化アクションが起動されるかどうかは、開始操作が実行されたリソースのタイプによって異なります。
     – 固定リソースが影響を受ける場合は、これ以上のアクションは起きません。
     – 制御操作が浮動リソースの構成要素に対して実行され、この構成要素が「オフライン」または「オフラインに失敗」状態である場合は、System Automation for Multiplatforms はリソースの別の構成要素に対して制御操作を実行しようとします。制御操作を拒否した構成要素は、この構成要素に対してリセット操作を実行するまで、リカバリー不能エラー状態のままになることに注意してください。
3. タイムアウト期間内に、リソースが本来あるべき状態 (オンライン) に到達 しません。この場合、System Automation for Multiplatforms はまず、リソースに対してリセット操作を実行し、リセット操作が受け入れられ、リソースがオフラインになるまで待機します。System Automation for Multiplatforms は次に、このリソースに対して別の開始制御操作を実行します。各制御操作の試行がカウントされ、RetryCount を超えるか、最大タイムアウト期間 (TimeOut * RetryCount) が満了するかのいずれかが先に達成された時点で、System Automation for Multiplatforms は制御操作の実行を停止します。

固定リソースまたは浮動リソースの構成要素について System Automation for Multiplatforms が制御操作の実行を停止した場合、このリソースの OpState は「オフラインに失敗」に設定されます。これは、このリソースが使用不可になっていること、および障害の原因を訂正するには手操作による介入が必要であることを示しています。問題が解決したら、リソースは RMC コマンド **resetrsrc** でリセットする必要があります。

しきい値はインプリメントされないため、リソースが本来あるべき状態になったときに、常に再試行カウンターがリセットされることに注意してください。 つまり、例えば、リソースが開始され、短期間オンラインのままになってから再度停止した場合、System Automation for Multiplatforms によってループになって再始動されます。

デフォルト値は以下のとおりです。

- TimeOut = 60
- RetryCount = 3

コマンド **samctrl -t Timeout** を使用して TimeOut 値を変更し、 コマンド **samctrl -r Retry_count** を使用して RetryCount 値を変更します。

`IBM.Application` クラスには、独自のタイムアウト値があります。クラス `IBM.Application` のリソースをグループに追加した場合、このリソースについては一般的な `TimeOut` 値は使用されません。このグループ・メンバーの `TimeOut` 値としては、`StartCommandTimeout` 属性または `MonitorCommandPeriod` 属性 (どちらも `IBM.Application` リソースの属性) のいずれか大きい方の値が使用されます。

停止操作

System Automation for Multiplatforms がリソースに対してリソース停止制御操作を最初に送った時点で、操作タイマーが開始されます。 そのタイマーが開始された後は、以下の 3 つの可能性があります。

1. リソースが、タイムアウト期間内に本来あるべき状態 (オフライン) に変わります。 これ以上のアクションは起きません。
2. リソースが、タイムアウト期間内に停止制御を拒否します。 その後に起こることは、拒否コードによって異なります。
   - エラーがリカバリー可能であることが示している場合、System Automation for Multiplatforms はそのリソースに対してもう一度停止制御操作を実行します。
   - エラーがリカバリー可能でない場合は、リソースは問題プログラム状態になります。 リソースを問題プログラム状態から戻すには、手操作による介入が必要です。
3. リソースが、タイムアウト期間内に本来あるべき状態 (オフライン) に到達しません。 この場合、System Automation for Multiplatforms は、まずリソースに対してリセット操作を実行し、リソースが本来あるべき状態 (オフライン) に到達するまで待ちます。

Automation

このフラグは、System Automation for Multiplatforms の自動化機能が使用可能になっているかどうかを示します。自動化が使用不可の場合、System Automation for Multiplatforms は制御操作の送信を停止します。リソースの 状態は変更されません。

デフォルト値は AUTO モードで、これは自動化がオンになっていることを意味します。

samctrl -M F を使用して自動化を使用可能に設定し、**samctrl -M T** を使用して自動化を使用不可に設定します。

ExcludedNodes

System Automation for Multiplatforms が、すべてのリソースを停止し、可能であれば、停止したリソースを別のノードに移動させるノードのリストです。

例えば node05、node06、node07、および node08 の 4 つのノードで稼働可能な浮動リソース A があるとします。このリソースは、リソース・グループ RG_A のメンバーです。このグループをオンラインにすると、このリソースは node05 で始動されます。node05 を除外ノードのリストに追加した場合、System Automation for Multiplatforms は node05 上でこのリソースを停止します。このリソースは、他のノードのうちの 1 つで再始動されます。

注意: ノードを除外し、グループの 1 つ以上の必須メンバーを他のノードで再始動できない場合、グループ全体が停止することがあります。

デフォルトでは、このリストは空です。これは、ピア・ドメイン内のすべてのノードが使用可能であることを意味します。

除外ノードのリストに 1 つ以上のノードを追加するには、**samctrl -u a** コマンドを使用します。このリストからノードを削除するには、**samctrl -u d** を使用します。リスト内のノードを置き換えるには、**samctrl -u r** を使用します。

ResourceRestartTimeout

ResourceRestartTimeout 値は、障害が発生した別のノード上にあるリソースを再始動するまで、System Automation for Multiplatforms が待機する時間 (秒数) を指定します。リソースが別のシステムに移動される前に、リソースまたは障害が発生したノードでクリーンアップを実行することができます。

デフォルト値は 5 秒です。

リソース再始動タイムアウト値の指定は、コマンド **samctrl -o** を使用して行います。

トレース・レベルの指定は、コマンド **samctrl -l** を使用して行うことができます。TraceLevel によって、書き込まれるトレース項目の数が決まります。デフォルト値は 127 です。 最大値 255 を指定すると詳

細なトレースが行われます。値を 0 に設定すると、トレース項目のさまざまなクラスの書き込みは行われません。リソース数が多い自動化ポリシーの場合は、トレース・レベルを下げることをお勧めします。

例

現行の System Automation for Multiplatforms の制御パラメーターをリストするには、 **lssamctrl** コマンドを使用します。

System Automation for Multiplatforms 制御情報:

```
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                      = {}
```

除外ノードのリストにノード node05 を追加するには、以下のコマンドを入力します。

```
samctrl -u a node05
```

RetryCount パラメーターを 5 に設定するには、以下のコマンドを入力します。

```
samctrl -r 5
```

タイ・ブレーカーの構成

偶数のノードを持つクラスター環境の場合は、タイ・ブレーカーを構成します。

System Automation for Multiplatforms では、自動化アクションを開始するには、ドメイン内のノードの半数以上がオンラインである必要があります。ドメインが偶数個のノードで構成されていると、ドメインのちょうど半分のノードがオンラインであるという状態が発生することがあります。この場合 System Automation では、タイ・ブレーカーを使用して、クォーラム状態 を判別します。これにより、自動化アクションを開始できる (**HAS_QUORUM**) のか、 それとも自動化アクションは不可 (**PENDING_QUORUM, NO_QUORUM**) なのかが決定されます。

IBM.TieBreaker リソース・クラスを使用して、ECKD または SCSI などの共有ディスク・タイ・ブレーカーを構成します。さらに、Operator および Fail の 2 つのタイ・ブレーカーが事前定義されています。Operator タイ・ブレーカーは、タイの発生時に不確定な結果を提供し、操作クォーラムを認可または否認することによるタイの解決は管理者に任せられます。タイが発生し、Fail タイプのタイ・ブレーカーがアクティブな場合は、タイ・ブレーカーを予約しようとする試行は常に否認されます。デフォルトのタイ・ブレーカー・タイプは Operator に設定されます。

タイ・ブレーカーの追加の実装は、タイ・ブレーカー・タイプ **EXEC** を使用して追加できます。System Automation for Multiplatforms は、追加のタイ・ブレーカー実装として、ネットワークと NFS タイ・ブレーカーを提供します。

使用可能なタイ・ブレーカー・タイプをリストするには、以下のように入力します。

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

出力:

```
Resource Class Persistent Attributes for: IBM.TieBreaker
        resource 1:
                 AvailableTypes ={["SCSI",""],["EXEC",""],["Operator",""],
["Fail",""]}
```

タイ・ブレーカー名をリストするには、以下のように入力します。

```
lsrsrc IBM.TieBreaker
```

出力:

```
Resource Persistent Attributes for: 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            = {}

resource 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"
```

リソース・クラス IBM.TieBreaker には複数のタイ・ブレーカー・リソースを定義できますが、クラスター内で同時にアクティブにできるのは 1 つのみです。クラスター内でアクティブなタイ・ブレーカーをリストするには、以下のコマンドを入力します。

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

出力:

```
Resource Class Persistent Attributes for: IBM.PeerNode
        resource 1:
          OpQuorumTieBreaker = "Operator"
```

アクティブなタイ・ブレーカーを設定するには、以下のように入力します。

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

タイ・ブレーカーが Operator である場合に操作クォーラムを認可または否認するには、以下のコマンドを入力します。

```
runact -c IBM.PeerDomain ResolveOpQuorumTie Ownership=1 (否認する場合 0)
```

注 : 競合状態を回避するために、続行しないサブクラスターでは Operator タイ・ブレーカーを否認する必要があります。その後、続行するサブクラスターに Operator タイ・ブレーカーを認可できます。

共有ディスク・タイ・ブレーカー

ノード数が偶数のクラスターにディスク・タイ・ブレーカーをセットアップします。タイ・ブレーカー・ディスクはすべてのクラスター ・ノード間で共用されます。

IBM.TieBreaker リソース・クラスを使用して、ディスクをタイ・ブレーカー・リソースとして使用することができます。サブドメインで、ノードの半数だけがオンラインである場合、System Automation for Multiplatforms は予約/解放機能を使用して、タイ・ブレーカー・ディスクを予約しようとします。予約が成功すると、 そのサブドメインがクォーラムを取得し、System Automation for Multiplatforms はリソースの自動化を 続行できます。別のノードがドメインに参加すると、ディスクの予約は解除されます。これにより、そのドメインの半数を超える数のノードがオンラインになります。

注 : タイ・ブレーカーを定義するとき、IBM.TieBreaker リソースには、ファイル・システムの保管用に使用されないディスクを指定するようにしてください。

以下の 3 つの例は、ECKD デバイス、SCSI デバイス、または DISK デバイスとともにタイ ・ブレーカーを使用する方法を示しています。タイ・ブレーカーをフォーマット設定したり、区画に分割したりする必要はありません。

2 ノード・クラスターの場合の ECKD タイ・ブレーカーのセットアップ

Linux on System z 上で ECKD タイ・ブレーカーをセットアップします。

ノードが z/VM の下で稼働している場合は、60 ページの『z/VM 環境内の ECKD タイ・ブレーカー』を参照して、 タイ・ブレーカーとして使用する ECKD DASD を定義することの構成上の詳細な意味を確認してください。

ECKD タイ・ブレーカー・タイプは、System z 上の Linux 固有のものです。ECKD タイ・ブレーカー・オブジェクトを作成す るには、DeviceInfo 永続リソース属性が ECKD デバイス番号を示すように設定する必要があります。このタイプのタイ・ブレーカーでは予約または解放メカニズムが使用されるた め、予約を維持するためにタイ・ブレーカーを定期的に再予約する必要があります。このため、このタイプのタイ・ブレーカーを作成するときには HeartbeatPeriod 永続リソース属性も指定することができます。HeartbeatPeriod 永続リソース属性は、予約要求を再入力する間隔を定義します。

以下のシステム情報を収集してください (Linux カーネル 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
```

Linux カーネル v2.6 では、**cat /proc/subchannels** コマンドの代わりに lscss コマンドを使用してください。タイ・ブレーカーを使用するには、以下のステップを実行します。

1. IBM.TieBreaker クラスで、タイ・ブレーカー・リソース・オブジェクトを作成します。DeviceInfo は、ECKD デバイス番号を示します。これは、/proc/dasd/devices ファイルから 入手できます。

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

```
node01:~ # lsrsrc IBM.TieBreaker
Resource Persistent Attributes for: 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. IBM.PeerNode クラスの OpQuorumTieBreaker 属性を、タイ・ブレーカー・リソース・オブジェクト の 1 つに変更します。

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

```
node01:~ # lsrsrc -c IBM.PeerNode
Resource Class Persistent Attributes for: IBM.PeerNode
resource 1:
        CommittedRSCTVersion  = ""
        ActiveVersionChanging = 0
        OpQuorumOverride      = 0
        CritRsrcProtMethod    = 1
        OpQuorumTieBreaker    = "myTieBreaker"
```

手動でのノードのリブート

2 ノード・クラスターの 1 つのノードをリブートする場合、リブートするノードが速くリブートされる場合があります。リブートによってタイ・ブレーカー方式が妨害され、残りのノードの不必要なリブートが発生する場合があります。クラスターに属するノードを手動でリブートする必要がある場合は、**reboot -nf** でなくコマンド **halt -nf** を使用してください。

手動でのディスク予約の解除

タイ・ブレーカーを予約しているノードがダウンしており、リブートできない場合は、その予約を解除し、正常なノードで予約を引き継ぐために、手動で正常なノードにアクセスする必要があります。

- タイ・ブレーカー・ディスクを正常なノードに接続したままにすることができます (この間、このノードがリブートされなかった場合):

```
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
```

- タイ・ブレーカー・ディスクを「boxed」状態にすることができます (このノードがリブートされ、タイ・ブレーカー・ディスクを認識できなくなった場合):

```
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
```

タイ・ブレーカー・ディスクの予約を解除するには、コマンド /usr/sbin/rsct/bin/tb_break を入力します。

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

これで、タイ・ブレーカー・ディスクは正常なノードに予約されます。

注 : tb_brk コマンドを初めて実行したときに機能しない場合は、もう一度実行してください。

2 ノード・クラスターの場合の SCSI タイ・ブレーカーのセットアップ

Linux on System x または Linux on POWER 上で SCSI タイ・ブレーカーをセットアップします。

この SCSI タイ・ブレーカー・タイプは、Linux on System x 、および Linux on POWER に特有のタイプです。SCSI タイ・ブレーカー・オブジェクトを作成する場合、DeviceInfo 持続リソース属性を使用して SCSI 装置を指定する必要があります。クラスター内のノードによって SCSI 構成が異なる場合は、NodeInfo 永 続リソース属性を使用してこれらの差異を反映することもできます。このタイプのタイ・ブレーカーでは予約/解放メカニズムが使用されるた め、予約を維持するためにタイ・ブレーカーを定期的に再予約する必要があります。このタイプのタイ・ブ レーカーを作成する場合は、HeartbeatPeriod 永続リソース属性を指定することもできます。HeartbeatPeriod 永続リソース属性は、予約要 求の再発行間隔を定義します。

Linux 上の SCSI デバイスは、HOST、CHAN、ID および LUN 属性の 4 つの整数値により識別できます。

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

通常、これらのパラメーターは各クラスター・ノードで同一です。例えば、node1 と node2 で、各パラメーターが HOST=0、CHAN=0、ID=4、LUN=0 になります。

この場合、タイ・ブレーカー・オブジェクトを作成するには、次のコマンドを使用します。

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

ターゲット・デバイスが同一であっても、4 つの値がノードによって異なることもあります。その場合、DeviceInfo フィールドに加えて、NodeInfo フィールドを使用します。

コマンド出力に示されている 4 つの整数 値を使用します。

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

sdf というディスクでは、SCSI ID 属性の値は HOST=2、CHAN=2、ID=4、LUN=0 です。例えば、SCSI デバイスが 、node1 および node2 という名前の 2 つのノードに接続されており、SCSI ID が 以下の値であるとします。

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

以下のように DeviceInfo を使用して共通の属性値を指定し、NodeInfo を使用してノードに特有の属性値を指定することで、タイ・ブレーカー・オブジェクトを作成します。

```
# 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 は、DeviceInfo および NodeInfo の 2 つの文字列を、DeviceInfo を先、NodeInfo を後の順にマージして処理します。例えば node1 の場合、マージされた文字列は以下のようになります。

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

この文字列が解析されます。

また、重複キーワードを使用でき、最後のキーワードが使用されます。したがって、同じコマンドを以下のようにして指定できます。

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

ほとんどの場合、多くのノードの SCSI ID は同じであるため、この簡略化は役立ちます。

手動でのディスク予約の解除

タイ・ブレーカーを予約しているノードがダウンしており、リブートできない場合は、SCSI タイ・ブレーカー・ディスクを解放するために、手動で正常なノードにアクセスする必要があります。ディスクを解放するには、**tb_break [-f] HOST CHAN ID LUN** コマンドを実行します。例えば、次のようなコマンドを入力します。

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

2 ノード・クラスターの場合の AIX DISK タイ・ブレーカーのセットアップ

AIX システム上で AIX DISK タイ・ブレーカーをセットアップします。

DISK タイ・ブレーカー・タイプは、AIX 固有のものです。DISK タイ・ブレーカー・オブジェクトを作成する には、DeviceInfo 永続リソース属性が AIX デバイス名を示すように設定する必要があります。AIX デバイス名は、ピア・ドメインのすべてのノードが共用する SCSI 物理 ディスクまたは SCSI 型物理ディスクを指定する必要があります。

ファイバー・チャネル、iSCSI、および Serial Storage Architecture を介して接続されている物理ディスクが DISK タイ・ブレーカーとして機能します。IDE ハード・ディスクは SCSI プロトコル をサポートしていないため、DISK タイ・ブレーカーとしては機能しません。また、論理ボリュームも DISK タイ・ブレーカーとしては機能しません。このタイプのタイ・ブレーカーでは予約または解放メカニズムが使用されるため、予約を維持するためにタイ・ブレーカーを定期的に再予約する必要があります。このため、このタイプのタイ・ブレーカーを作成するときには HeartbeatPeriod 永続リソース属性も指定することができます。HeartbeatPeriod 永続リソース属性は、予約要求を再入力する間隔を定義します。

システム内のすべての既知の物理ボリュームとその物理ディスク名をリストするには、次のコマンドを入力します。

```
lspv
```

出力は以下のようになります。

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

ディスクが SCSI ディスクまたは SCSI 型ディスクであることを確認するには、**lsdev** コマンドを使用します。このディスクが、DISK タイ・ブレーカーに適した候補となります。以下に例を示します。

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

出力は以下のようになります。

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

ディスクがタイ・ブレーカー・ディスクとして機能するには、そのディスクがピア・ドメインのすべてのノードによって共用されることが必要です。**lspv** コマンドで戻された物理ボリューム ID を調べて、このディスクがノード間で共用されているかどうかを確認します。上記の **lspv** コマンドの出力では、2 列目に物理ボリューム ID がリストされています。また、hdisk1 のボリューム ID は 000069683404ed54 です。AIX では、システムに接続されたすべてのディスクが記憶されるため、**lspv** コマンドでリストされたディスクが現在は接続されていないことがあります。このようなディスクが別のシステムに移動されている場合は、ディスクが既に元のシステムに接続されていないにもかかわらず、共用されているように示されることがあります。

IBM.TieBreaker リソースが保管されるディスクを、ファイル・システムの保管用に使用しないようにしてください。クラスターの各ノードが複数のディスクを共用している場合、タイ・ブレーカー・ディスクであるディスクと、アプリケーション・データ用に使用されるディスクの判別が難しいことがあります。**lsdev** コマンドの出力には、ディスクに関連付けられてい る SCSI アドレスが示されます。(前述の **lsdev** コマンド出力では、3 列目に SCSI アドレスがリス トされています。hdisk0 の SCSI アドレスは 10-60-00-0,0 です。) ディスクのインストール前にディ スクのアドレスがわかっている場合、正しいディスクを識別するときにこの情報が役に立ちます。

デバイス名を確認した後、次のように **mkrsrc** コマンドを使用して、タイ・ブレーカー・オブジェクトを定義します。

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

SCSI 予約機能の確認

タイ・ブレーカーは SCSI-2 の予約に依拠しますが、この予約は、ストレージとドライバー・セットアップのすべての組み合わせでサポートされるとは限りません。セットアップで SCSI-2 の予約がサポートされることを確認するために、RSCT には **disk_reserve** ユーティリティーが付属しています。このユーティリティーは、絶対パス /usr/sbin/rsct/bin/disk_reserve で開始する必要があります。

タイ・ブレーカーが正しく機能するのは、タイ・ブレーカー・ディスクをいずれかのノードから予約でき、ロックを解除できる場合、およびディスクが他のノードによってロックされている間はノードから予約できない場合です。

使用方法:

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

-h - このヘルプ・テキストを表示

-v - 詳細

-f - ブレークの後に予約 (-l または -b オプションの場合)

-d sdisk_name - 操作するディスク (例えば、/dev/sdb)

-l - ロック (予約)

-u - ロックを解除 (解放)

-b - ブレーク

-g sg_device_name 、例えば、/dev/sg1

例:

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

手動でのディスク予約の解除

タイ・ブレーカーを予約しているノードがダウンしており、リブートできない場合は、SCSI タイ・ブレーカー・ディスクを解放するために、手動で正常なノードにアクセスする必要があります。ディスクを解放するには、**tb_break** コマンドを使用します。例えば、次のように入力します。

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

以下に、タイ・ブレーカー・ディスクとして機能するための基準を満たしていないディスクの例を示します。例えば次のように、**lspath** コマンドを入力します。

```
lspath -l hdisk2
lspath: 0514-538 Cannot perform the requested function because the
                 specified device does not support multiple paths.
```

出力例:

```
#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
```

この出力例は、ディスクが SCSI-2 の予約をサポートしないため、タイ・ブレーカーとして使用できないことを示しています。

ディスク・タイ・ブレーカーの SCSI 永続予約

AIX および Linux for System x 上では、ディスク・タイ・ブレーカーで SCSI 永続予約を使用するように構成することができます。System Automation for Multiplatforms バージョン 3.2.1.3 以降では、この機能が拡張され、Linux for System z も対象になります。

AIX の SCSI-3 タイ・ブレーカー

デフォルトでは、AIX 上の DISK タイプのタイ・ブレーカーは SCSI-2 の予約/解放に依存しますが、この予約/解放機能が SCSI ディスク・ストレージとドライバーのセットアップのすべての組み合わせでサポートされるわけではありません。一般に、SAN ボリューム・コントローラーなどのストレージ仮想化ソリューションでは SCSI-2 予約はサポートされません。これらの環境では、SCSI-2 予約/解放コマンドを SCSI-3 永続予約コマンドに変換するように、AIX オペレーティング・システムを構成することができます。

AIX 上で SCSI-2 予約/解放から SCSI-3 永続予約への変換を構成するには、次のコマンドを使用します。

```
chdev -l <pv_name> -a PR_key_value=0x<unique_key> -a reserve_policy=PR_exclusive
```

<pv_name>
タイ・ブレークに使用する AIX システム上の物理ボリュームの名前。

<unique_key>
クラスター内の各ノードに固有の任意の数字キー。

このコマンドをドメインの各リモート・ピア・システム上で実行し、それぞれのシステムに別々の固有キーを指定します。DISK タイ・ブレーカーに使用する SCSI ディスクでこの方式がサポートされるかどうかを調べるには、次のコマンドを実行します。

```
lsattr -El <pv_name>
```

属性 PR_key_value と reserve_policy を探します。これらの属性が、前の段落の説明に従って調整できない場合は、『Host Attachment for SDDPCM on AIX』で、欠落しているデバイス・ドライバーがないか確認してください。

zBX 環境内にある POWER ブレード上のディスクは、仮想 SCSI ディスク・ドライブとしてのみ定義できます。これらのディスクを、SCSI-2 予約/解放または SCSI-3 永続予約をサポートするように構成することはできません。したがって、これらのディスクは、ディスク・タイ・ブレーカーには使用できません。

Linux on System x 上の SCSIPR タイ・ブレーカー

System Automation for Multiplatforms バージョン 3.2.1.2 では、Linux on System x に特有の SCSIPR タイプのタイ・ブレーカーが導入されました。これは、RHEL 7、RHEL 8、SLES 12、および SLES 15 でサポートされます。

SCSIPR タイ・ブレーカーは、タイ・ブレーク・メカニズムとして、SCSI ディスク・ストレージ・デバイス上で SCSI-3 永続的な予約を使用します。ピア・ドメインが 2 つのサブドメインに分割され、それぞれのサブドメインに定義済みのノードがちょうど半数ずつ含まれているタイ状態の場合、共有 SCSI ディスク・ストレージ・デバイスの排他的な永続予約を取得できるサブドメインが、操作クォーラムを取得します。

前提条件

SCSIPR タイ・ブレーカーで使用される SCSI ディスク・ストレージ・デバイスは、予約タイプが「Write Exclusive Registrants Only」に設定された SCSI-3 永続予約プロトコルをサポートする必要があります。ピア・ドメイン内のすべてのシステムがこのデバイスを共用する必要があり、すべてのシステムが SCSI-3 永続予約プロトコルを使用して、このデバイスを予約可能であることが必要です。

SCISPR タイ・ブレーカーは sg_persist ユーティリティーを使用します。このユーティリティーがピア・ドメインのすべてのシステムに既にインストールされているかどうかを確認するには、次のコマンドを使用します。

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

sg_persist ユーティリティーがまだインストールされていない場合は、以下の Linux パッケージの中から該当するものをインストールする必要があります。

- RHEL 7、RHEL 8、SLES 12、および SLES 15: sg3_utils*.rpm

定義

SCSIPR タイプのタイ・ブレーカーを作成する場合は、DeviceInfo 永続リソース属性を使用して、タイ・ブレーカーによって使用される SCSI ディスク・ストレージ・デバイスを指定します。ピア・ドメイン・システム間で SCSI 構成が異なる場合は、NodeInfo 永続リソース属性を使用して、これらの差異を反映します。

SCSIPR タイ・ブレーカーでは、予約または解放メカニズムが使用されるため、予約を維持するためにタイ・ブレーカーを定期的に再予約する必要があります。このため、このタイプのタイ・ブレーカーを作成するときには、HeartbeatPeriod 永続リソース属性を指定します。HeartbeatPeriod 永続リソース属性は、予約を再試行する間隔を定義します。

注: タイ・ブレーカー・リソースを定義するときには、ファイル・システムの保管用に使用されないディスクに、IBM.Tiebreaker リソースを保管するようにしてください。

DeviceInfo 永続リソース属性で以下のオプションのいずれかを使用して、タイ・ブレーカーによって使用される SCSI ディスク・ストレージ・デバイスを特定します。

- DEVICE=<generic or disk device name>
- HOST=<h> CHAN=<c> ID=<i> LUN=<I>
- WWID=<wwid as displayed by the system>
- RDAC.WWN=<wwn as displayed by the system when using LSI RDAC multi-path driver>

例:

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

検証

以下のステップをすべてのリモート・ピア・システムで実行して、選択した SCSI ディスク・ストレージ・デバイスに対して SCSIPR タイ・ブレーカーがすべてのシステムで正しくサポートされているかどうかを検証します。

- 次に示すように **tb_break** コマンドを使用して、ディスク装置を予約します。

```
/usr/sbin/rsct/bin/tb_break -l -t SCSIPR <DeviceInfo device specification for this system>
```

  このコマンドで、ディスク装置を正常に予約できる必要があります。

- 次に示すように、他のすべてのピア・ドメイン・システムで **tb_break** コマンドを使用して、同じディスク装置の予約を試行します。

```
/usr/sbin/rsct/bin/tb_break -l -t SCSIPR <DeviceInfo device specification for this system>
```

  このコマンドによるディスク装置の予約は失敗する必要があります。なぜなら、ディスク装置は最初のシステムによって既に排他的に予約されているからです。

- 次に示すように **tb_break** コマンドを使用して、ディスク装置を解放します。

```
/usr/sbin/rsct/bin/tb_break -u -t SCSIPR <DeviceInfo device specification for this system>
```

  このコマンドで、ディスク装置を正常に解放できる必要があります。

予約が維持されているかどうかの確認:

SCSI ディスク・ストレージ・デバイスで予約が維持されているかどうかを確認するには、次のコマンドを使用します。

```
sg_persist --read-reservation <generic or disk device name>
```

例: 予約が維持されていない場合:

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

例: 予約が維持されている場合:

```
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
```

ディスク装置を予約すると、各リモート・ピア・システムはそれぞれの RSCT ノード ID を予約キーとして使用します。**/usr/sbin/rsct/bin/lsnodeid** コマンドを使用すると、リモート・ピア・システムの RSCT ノード ID を表示できます。SCSI ディスク・ストレージ・デバイスが SCSIPR タイ・ブレーカーによって予約されている場合、予約を維持しているシステムを判別することができます。現在の予約キーを調べて、それをすべてのリモート・ピア・システムの RSCT ノード ID と比較します。

予約のブレーク:

リモート・ピア・システムが現在 SCSI ディスク・ストレージ・デバイスで予約を維持している場合、別のリモート・ピア・システムからこの予約をブレークすることができます。既存の予約を強制的にブレークし、新しい予約を獲得するには、次のコマンドを使用します。

```
/usr/sbin/rsct/bin/tb_break -f -t SCSIPR <DeviceInfo device specification for this system>
```

Linux on System z 上の SCSIPR タイ・ブレーカー

System Automation for Multiplatforms バージョン 3.2.1.3 では、Linux on System z で使用するための SCSIPR タイプのタイ・ブレーカーが導入されました。これは、SLES 12 および SLES 15 上でサポートされます。

SCSIPR タイ・ブレーカーは、タイ・ブレーク・メカニズムとして、SCSI ディスク・ストレージ・デバイス上で SCSI-3 永続的な予約を使用します。ピア・ドメインが 2 つのサブドメインに分割され、それぞれのサブドメインに定義済みのノードがちょうど半数ずつ含まれているタイ状態の場合、共有 SCSI ディスク・ストレージ・デバイスの排他的な永続予約を取得できるサブドメインが、操作クォーラムを取得します。

前提条件

SCSIPR タイ・ブレーカーで使用される SCSI ディスク・ストレージ・デバイスは、予約タイプが「Write Exclusive Registrants Only」に設定された SCSI-3 永続予約プロトコルをサポートする必要があります。ピア・ドメイン内のすべてのシステムがこのデバイスを共用する必要があり、すべてのシステムが SCSI-3 永続予約プロトコルを使用して、このデバイスを予約可能であることが必要です。SCISPR タイ・ブレーカーは sg_persist ユーティリティーを使用します。このユーティリティーがピア・ドメインのすべてのシステムに既にインストールされているかどうかを確認するには、次のコマンドを使用します。

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

sg_persist ユーティリティーがまだインストールされていない場合は、以下の Linux パッケージの中から該当するものをインストールする必要があります。

- RHEL 7、RHEL 8、SLES 12、および SLES 15: sg3_utils*.rpm

タイ・ブレーカーとして機能するディスクでは、N ポート ID 仮想化を有効にしておく必要があります。有効にしない場合、それぞれの予約は、zSeries の物理的なボックスである CEC の単一の論理区画のためではなく、CEC 全体のために行われます。zSeries での N ポート ID 仮想化について詳しくは、以下を参照してください。

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

定義

SCSIPR タイプのタイ・ブレーカーを作成する場合は、DeviceInfo 永続リソース属性を使用して、タイ・ブレーカーによって使用される SCSI ディスク・ストレージ・デバイスを指定します。ピア・ドメイン・システム間で SCSI 構成が異なる場合は、NodeInfo 永続リソース属性を使用して、これらの差異を反映します。

SCSIPR タイ・ブレーカーでは、予約または解放メカニズムが使用されるため、予約を維持するためにタイ・ブレーカーを定期的に再予約する必要があります。このため、このタイプのタイ・ブレーカーを作成するときには、HeartbeatPeriod 永続リソース属性を指定します。HeartbeatPeriod 永続リソース属性は、予約を再試行する間隔を定義します。

注 : タイ・ブレーカー・リソースを定義するときには、ファイル・システムの保管用に使用されないディスクに、IBM.Tiebreaker リソースを保管するようにしてください。

DeviceInfo 永続リソース属性で以下のオプションのいずれかを使用して、タイ・ブレーカーによって使用される SCSI ディスク・ストレージ・デバイスを特定します。

- DEVICE=<generic or disk device name>
- HOST=<h> CHAN=<c> ID=<i> LUN=<l>
- WWID=<wwid as displayed by the system>
- RDAC.WWN=<wwn as displayed by the system when using LSI RDAC multi-path driver>

例:

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

検証

以下のステップをすべてのリモート・ピア・システムで実行して、選択した SCSI ディスク・ストレージ・デバイスに対して SCSIPR タイ・ブレーカーがすべてのシステムで正しくサポートされているかどうかを検証します。

- 次に示すように tb_break コマンドを使用して、ディスク装置を予約します。

```
/usr/sbin/rsct/bin/tb_break -l -t SCSIPR <DeviceInfo device specification for this system>
```

このコマンドで、ディスク装置を正常に予約できる必要があります。

- 次に示すように、他のすべてのピア・ドメイン・システムで tb_break コマンドを使用して、同じディスク装置の予約を試行します。

```
/usr/sbin/rsct/bin/tb_break -l -t SCSIPR <DeviceInfo device specification for this system>
```

このコマンドによるディスク装置の予約は失敗する必要があります。なぜなら、ディスク装置は最初のシステムによって既に排他的に予約されているからです。

- 次に示すように tb_break コマンドを使用して、ディスク装置を解放します。

```
/usr/sbin/rsct/bin/tb_break -u -t SCSIPR <DeviceInfo device specification for this system>
```

このコマンドで、ディスク装置を正常に解放できる必要があります。

予約が維持されているかどうかの確認:

SCSI ディスク・ストレージ・デバイスで予約が維持されているかどうかを確認するには、次のコマンドを使用します。

```
sg_persist --read-reservation <generic or disk device name>
```

例: 予約が維持されていない場合:

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

例: 予約が維持されている場合:

```
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
```

ディスク装置を予約すると、各リモート・ピア・システムはそれぞれの RSCT ノード ID を予約キーとして使用します。**/usr/sbin/rsct/bin/lsnodeid** コマンドを使用すると、リモート・ピア・システムの RSCT ノード ID を表示できます。SCSI ディスク・ストレージ・デバイスが SCSIPR タイ・ブレーカーによって予約されている場合、予約キーを調べることによって、予約を維持しているシステムを判別できます。この予約キーを、すべてのリモート・ピア・システムの RSCT ノード ID と比較します。

予約のブレーク:

リモート・ピア・システムが SCSI ディスク・ストレージ・デバイスで予約を維持している場合、 別のリモート・ピア・システムからこの予約をブレークすることができます。既存の予約を強制的にブレークし、新しい予約を獲得するには、次のコマンドを使用します。

```
/usr/sbin/rsct/bin/tb_break -f -t SCSIPR <DeviceInfo device specification for this system>
```

z/VM 環境内の ECKD タイ・ブレーカー

Linux on System z® では、ECKD™ DASD をタイ・ブレーカー・リソースとして使用できます。

ECKD タイ・ブレーカーは、予約/解放機能を使用します。このため、追加の構成ステップが必要になる場合があります。予約されている ECKD DASD は、z/VM® からアクセスできません。したがって、z/VM では、他のシステムによって予約されているそのようなデバイスを接続することも、オンラインに変更することもできません。この状態に対処するには、一連の構成アクションが必要です。該当する必要事項について、以降の各セクションで説明します。

単一の *z/VM* システムで稼働するドメインに関する *ECKD DASD* の要件

システム自動化ドメインのすべてのノードが同じ z/VM システムのゲストである場合は、以下の定義が ECKD DASD のために必要です。

- フル・パック・ミニディスクを定義します。
- ミニディスク・キャッシュを使用する場合は、その値を `off` に設定します。
- ECKD DASD を z/VM システム内の両方のゲスト間で共用します。

2 つの *z/VM* システムにまたがるドメインに関する *ECKD DASD* の要件

システム自動化ドメインのノードが 2 つの別の z/VM システムのゲストである場合は、以下の定義が ECKD DASD のために必要です。

- タイ・ブレーカー・ディスクを、ユーザー・プロファイルの MiniDisk ステートメントに DEVNO ディスクとして定義する必要があります (ミニディスクなし、フル・パック・ミニディスクなし、専用 DASD および接続 DASD なし)。
- ECKD ディスク (DEVNO) を両方のノードで共有します。
- ECKD DASD は、z/VM の IPL の実行時に接続されるシステムであってはいけません。

Linux ゲストにログオンすると、次のデバイス接続が表示されます。仮想デバイス (この例では 291) と実アドレス (この例では 4a82) が示されています。この例では、コマンド `cp set shared on 4a82` を 使用して、このデバイスを共有デバイスにしています。このデバイスを、両サイドで共用する必要があります。

```
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
```

いずれかの z/VM システムがシャットダウンされている場合、ECKD DASD は、もう一方の z/VM システムの存続している Linux ゲストによって予約されます。存続しているサイドでは、以下の出力が表示されます。

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

z/VM システムの再始動後に DASD 4A82 は依然としてオフラインであり、もう一方の システムによって引き続き予約されているためオンラインに設定できません。代わりに、タイムアウト (20 分から 30 分) が発生します。

タイ・ブレーカー DASD なしで、再始動された z/VM 上の Linux を開始することをお勧めします。Linux を開始するのに DASD は不要であるため、これは成功します。Linux の開始後に、システム自動化が Linux ゲスト上で自動的に開始され、その後 Linux が自動的にシステム自動化ドメインに再度加わります。 ECKD DASD の予約が解除されます。タイ・ブレーカー・ディスクのデバイス (この例では 4a82) をオンに変更することが可能になります。新しく IPL が実行されたシステムで、**share** コマンドをコミットし、タイ・ブレーカー・ディスクの仮想アドレス (この例では 291) をリンクします。再始動された Linux 上で、コマンド **chccwdev -e 291** を入力します。このコマンドが完了すると、すべてのものが稼働します。存続している Linux でのこれ以上の対話は不要です。

必要なコマンドは CP コマンドのみです。したがって、VMCP を使用してそれらのコマンドを処理するスクリプトを作成すれば、障害のある Linux の修復を自動化できます。

この例の場合は、次のようなコマンドを含むスクリプトになります。

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

System Automation は、新しく定義された DASD を自動的に認識します。

ネットワーク・タイ・ブレーカー

ネットワーク・タイ・ブレーカーは、ディスクおよびオペレーター・ベースのタイ・ブレーカーの代替手段を提供します。ネットワーク・タイ・ブレーカーは、外部 IP (ネットワーク・インスタンス) を使用して、タイ状態を解決します。

ネットワーク・タイ・ブレーカーを使用するのが最適なシチュエーションの例は、以下のとおりです。

- ディスク・タイ・ブレーカーとして使用される共有ディスクが使用できない場合。
- クラスターの外部にあるインスタンスと通信する機能が最も優先される場合。

例: Web サーバーの主要な機能は、クラスターの外部のクライアントに Web ページを配信することです。このサービスを高可用にするため、タイ・ブレーカーは、クラスターの外部のインスタンスと通信できないノードへのアクセス権は付与してはなりません。

ネットワーク・タイ・ブレーカーは、すべてのノードが同じ IP サブ・ネット内にあるドメインのみに使用してください。ノードを異なる IP サブ・ネット内に置くと、両方のノードがネットワーク・タイ・ブレーカーに ping する可能性が高くなり、この間、それらのノードは互いに通信できなくなります。さらに、デフォルトのゲートウェイ IP アドレスがネットワーク・インフラストラクチャーによって仮想化されている場合、そのアドレスを使用することはできません。ドメイン内の各ノードから単一パスによってのみ到達できる IP アドレスを選択してください。

デフォルトの設定では、ネットワーク・タイ・ブレーカーは、ネットワーク・タイ・ブレーカー IP アドレスに対する ping を 2 回試行します。仮想化された環境や、ネットワーク接続が低速であるかまたは信頼性が低い環境では、このデフォルトの ping の回数では少なすぎる場合があります。このような環境では、ネットワーク・タイ・ブレーカーが実行する ping の回数を最大で 9 回まで増やすことができます。これにより、タイ・ブレーカーの予約操作が正しい結果になるようにすることができます。

ネットワーク・タイ・ブレーカー要件

ネットワーク・タイ・ブレーカー機能を確保するには、外部 IP インスタンスには、高可用クラスター内のすべてのノードから到達可能でなければなりません。外部 IP インスタンスも ICMP エコー要求 (ping) に応答できる必要があります。クラスターのノードと外部 IP インスタンス間の ICMP トラフィックをブロックするファイアウォール・ルールを導入した場合、ネットワーク・タイ・ブレーカーは機能しません。このシチュエーションでは、クラスター・ノードはそれらのピア (クラスター分割) と通信することができず、一方でサブクラスターは 2 つとも外部の IP インスタンスに到達できる状態です。通常、IP は、 サブクラスターが 2 つとも外部ゲートウェイに到達できる場合、それらがピアとも通信できるようにします。ファイアウォールの設定などのために、このルールを適用できない場合は、ネットワーク・タイ・ブレーカーを使用できません。

以下の表に、ネットワーク・タイ・ブレーカーとディスク・タイ・ブレーカーの利点と欠点をまとめます。

表 *21.* ネットワーク・ベースのタイ・ブレーカーとディスク・ベースのタイ・ブレーカーの比較

ネットワーク・ベースのタイ・ブレーカー	**ディスク・ベースのタイ・ブレーカー**
• +: ハードウェアに依存しない。 • +: 通信の可用性を評価する。	• +: 最も安全なタイ・ブレーカーである。ハードウェアは、1 つのインスタンス (ノード) のみがタイ・ブレーカーを取得できるようにする。

表 21. ネットワーク・ベースのタイ・ブレーカーとディスク・ベースのタイ・ブレーカーの比較 (続き)

ネットワーク・ベースのタイ・ブレーカー	ディスク・ベースのタイ・ブレーカー
• -: クラスター分割の発生時に外部 IP インスタンスが使用できない場合、どのサブクラスターもクォーラムを取得できない。 • -: タイ状態になるが複数のノードが通信できるエラー状態が発生することがある。この場合、両方のサブクラスターがタイ・ブレーカーを取得できる。	• -: 通信が途絶えた場合、このタイ・ブレーカーは、クラスターの外部のインスタンスと通信できないノードにアクセス権を付与する場合がある。

ネットワーク・タイ・ブレーカーのセットアップ

ネットワーク・タイ・ブレーカーを EXEC タイプの IBM.TieBreaker リソースとして定義します。EXEC タイ・ブレーカーについて詳しくは、RSCT の資料を参照してください。ネットワーク・タイ・ブレーカーの実行可能ファイルである samtb_net と samtb_net6 は、/usr/sbin/rsct/bin ディレクトリーにあります。現在のインプリメンテーションでは、RSCT EXEC タイ・ブレーカーの作成時に、以下のオプションを key=value のペアとして指定する必要があります。

Address=<IP address>
タイ状態を解決するために使用される外部 IP インスタンスのアドレス。IPv6 ネットワーク内では、アドレスを IPv6 形式で指定します。DNS 名は使用しないでください。通信に問題が発生した場合、DNS が正しく機能しないことがあります (通常これはクラスター分割時に発生します)。Address は必須オプションであり、デフォルト値はありません。

Log=<1/0>
ネットワーク・タイ・ブレーカーがシステム・ログ機能 (syslog) にログを記録するようにする場合は、1 を指定します。それ以外の場合は、0 を指定します。

Count=<number>
クォーラムを要求するために送信される ICMP エコー要求の数。最初の要求が応答を取得すると、以降の要求は送信されません。デフォルト値は 2 です。許可される値の範囲は、1 から 9 です。仮想環境や、ネットワーク接続が低速であるかまたは信頼性が低い環境の場合は、Count の値を大きくしてください。

IP のバージョンに応じて、タイ・ブレーカーの定義時に、異なるネットワーク・タイ・ブレーカー実行可能ファイルを使用する必要があります。

以下のコマンドでは、IPv4 アドレス用のネットワーク・タイ・ブレーカーが新規作成されます。

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

以下のコマンドでは、IPv6 アドレス用のネットワーク・タイ・ブレーカーが新規作成されます。

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

ネットワーク・タイ・ブレーカーを活動化するには、以下のように入力します。

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

ネットワーク・タイ・ブレーカーの定義を操作するには、**chrsrc** コマンドを使用します。例えば、ping 回数の値を増やす場合は、以下のコマンドを入力します。

```
chrsrc -c IBM.PeerNode OpQuorumTieBreaker="Operator"
chrsrc -s "Name = 'your_tiebreaker_name'" IBM.TieBreaker ¥
DeviceInfo="PATHNAME=/usr/sbin/rsct/bin/samtb_net Address=<network-tb-ip> ¥
Count=<new-value-for-Count> Log=1"
chrsrc -c IBM.PeerNode OpQuorumTieBreaker="your_tiebreaker_name"
```

タイ・ブレーカー定義を削除するには、**rmrsrc** コマンドを使用します。

ネットワーク・タイ・ブレーカーの予約動作

ノードがタイ・ブレーカーを予約すると、そのタイ・ブレーカーは使用不可になり、他のノードによって予約できなくなります。このアプローチは、ネットワーク・タイ・ブレーカーには適していません。そのため、タイ・ブレーカー・ネットワークの予約動作は、以下のように異なります。

予約の試行に失敗後は、そのノードがクラスターに再結合するまで、他の予約を行うことはできません。ファイルは /var/ct/ に書き込まれます。これは、予約が失敗したことを示します。このファイルが存在する場合、タイ・ブレーカーの予約コマンドは常に失敗します。 クォーラムを監視し、ノードがドメインに再結合された場合はブロック・ファイルを削除する、追加のプロセスが fork されます。

以下のサンプル・ファイルは、外部 IP インスタンス 123.456.789.1 への失敗したタイ・ブレーカー予約操作の結果として、ネットワーク・タイ・ブレーカーにより作成されました。これには、失敗した予約操作のタイム・スタンプが含まれます。

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

ネットワーク・タイ・ブレーカー用のタイ・ブレーカー・リソースの構成

このトピックでは、ネットワーク・タイ・ブレーカーの定義時に考慮する必要があるタイ・ブレーカーの構成オプションについて説明します。

PostReserveWaitTime=30
: PostReserveWaitTime は、タイ・ブレーカーの予約が成功した時点から、クォーラムが付与される時点までの遅延時間を定義します。ネットワーク・タイ・ブレーカーを予約するノードでは、PostReserveWaitTime が経過するまで操作可能クォーラムを取得しません。十分な停止時間を与えるために、値として 30 秒を指定します。これは、他のノードがオフラインであることを検出し、通信を直ちに復元するためにノードが必要とする時間です。このケースでは、 両方のノードがネットワーク・タイ・ブレーカーを予約できます。待機時間が長いことで、ノード間の通信も再度確立されることになり、両方のノードがクォーラムを取得してリソースを並行で開始する可能性が最小化されます。

HeartbeatPeriod=30
: 予約の成功の後、ConfigRM はタイ・ブレーカーのハートビート操作の定期的な呼び出しを開始します。クラスターの分割中にシステムの負荷を低く保つには、タイ・ブレーカー・ハートビート間の時間を増加させるか、または HeartbeatPeriod を「0」に設定してハートビートをオフにしてください。

ネットワーク・タイ・ブレーカーのシステム・ログをレビューする

以下に、2 ノード・クラスター (ノード n1 およびノード n2) において、ネットワーク・タイ・ブレーカーでエラーが発生した場合のシステム・ログの内容を例として示します。

64 ページの図 12 で、2 ノード・クラスター (ノード n1 およびノード n2) のシステム・ログを確認できます。エラーのシナリオでは、両方のノード上で実行中のクリティカル・リソースはないことが前提です。ネットワークの問題により、ピア間のすべての使用可能な通信パスを切断します。しかし、1 つのピア (n2) は、そのゲートウェイ (123.456.789.1) にまだ通信することができます。しばらく経った後、通信は再確立され、両方のノードをクラスターに結合できます。

図 *12. 2* ノード・クラスターのシステム・ログ

NFS タイ・ブレーカー

NFS タイ・ブレーカーは、NFS v4 サーバー上に格納された予約ファイルに基づいて、タイ状態を解決します。NFS サーバーは、複数の System Automation for Multiplatforms クラスターで使用することができます。複数の NFS タイ・ブレーカー用に同じサーバーを使用する場合は、タイ・ブレーカーごとに、一意の名前を持つ予約ファイルが必要です。

クラスターの分割時には、どの時点においても複数のノードがクォーラムまたは保留中のクォーラムを保持することはできません。クォーラムを獲得したノードに後になって障害が起こった場合、自動的に他のノードがチャレンジャー/ディフェンダー・プロトコルに基づいてクォーラムを獲得しようとします。

NFS サーバーは、NFS v4 の実行をサポートする任意のシステム上に配置することができます。System Automation for Multiplatforms のタイ・ブレーカー用に、最新の NFS v4.1 または pNFS 標準に準拠した NFS サーバーを使用する場合は、NFS サーバーの複製機能およびフェイルオーバー機能を必ず無効にしてください。NFS サーバーは、System Automation for Multiplatforms のタイ・ブレーカー用としてのみ使用してください。

すべての System Automation for Multiplatforms クラスター・ノード上に、NFS v4 クライアント・ライブラリーをインストールする必要があります。

NFS タイ・ブレーカーを使用するシナリオの例として、3 つのサイトのセットアップを挙げます。2 つのサイトは 1 組の 2 ノード・クラスターをホストし、タイ・ブレーカーは 3 番目のサイト上にあるものとします。ディスク・タイ・ブレーカーでは、SAN のセットアップ (必ずしも 3 つのサイトすべてにまたがっている必要はない) が必要であるため、ディスク・タイ・ブレーカーは使用できません。また、ネットワーク・トポロジーに関する想定ができません。3 番目のサイト上のネットワーク・デバイスを、ネットワーク・タイ・ブレーカーの宛先アドレスとして選択することはできません。このケースでは、3 番目のサイトを使用して、タイ・ブレーカーとして使用される NFS v4 サーバーをホストすることができます。

クラスター分割の発生時に NFS クォーラム・サーバーがダウンしているか、または NFS クォーラム・サーバーにアクセスできない場合、クラスター・ノードはクォーラムを取得できません。このシチュエーションは、ディスク・デバイスに障害が発生したり、ディスク・デバイスに到達できないと、ノードがクォーラムを取得できないディスク・タイ・ブレーカーの場合と同様になります。NFS クォーラム・サーバーが永続的に稼働し、確実に機能するようにしてください。

System Automation は、NFS ファイル・システムをいくつかの段階でクラスター・ノードにマウントします。ただし、定期的ではありません。

Initialize

`Initialize` 操作時に、マウントが確立されます (NFS タイ・ブレーカーがアクティブ・タイ・ブレーカーとして設定されている場合)。ドメインまたはノードの開始時に同じことが発生します。これが失敗すると、ノードがドメインを結合できなくなる可能性があります。

Reserve
Reserve 操作時に、予約ファイルへのアクセスが行われる前に、NFS マウントが検査され、必要に応じて (再) 確立されます。

Terminate
Terminate 操作時に、NFS ファイル・システムがアンマウントされます (NFS タイ・ブレーカーがもはやアクティブ・タイ・ブレーカーではない場合、またはドメイン/ノードが停止している場合)。

System Automation for Multiplatforms は、NFS ファイル・システムをいくつかの段階でクラスター・ノードにマウントします。ただし、定期的ではありません。

- まず、Initialize 操作時、またはドメイン/ノードの開始時に、マウントが確立されます (NFS タイ・ブレーカーが active tie breaker として設定されている場合)。マウントが失敗すると、ノードがドメインを結合できなくなる可能性があります。
- Reserve 操作時に、reserve file へのアクセスが行われる前に、NFS マウントが検査され、必要に応じて (再) 確立されます。

Terminate 操作時に、NFS ファイル・システムがアンマウントされます (NFS タイ・ブレーカーがもはやアクティブ・タイ・ブレーカーではない場合、またはドメイン/ノードが停止している場合)。

注 : クラスター分割の発生時には、予約ファイルの存在が極めて重要になります。予約ファイルを削除すると、クラスター内の両方のノードにクォーラムが与えられる可能性があります。予約ファイルと予約ファイルを使用するクラスターとを直接関連付けることができる命名スキーマを、これらのファイルに使用してください。例えば、 NFS_reserve_file_SAP_HA_sapnode1_sapnode2_DO_NOT_REMOVE という名前は、このファイルの目的、クラスターの名前、およびこの予約ファイルを使用するノードの名前を明確に示しています。このファイルが削除された場合は、デフォルトの Operator タイ・ブレーカーをアクティブにして、ファイルを再作成した後、NFS タイ・ブレーカーをもう一度アクティブにしてください。
Operator タイ・ブレーカーについて詳しくは、48 ページの『タイ・ブレーカーの構成』を参照してください。

Linux 上での NFS サーバーの使用可能化

Linux 上で System Automation for Multiplatforms を稼働している場合に、NFS v4 サポートを有効にする方法について説明します。

以下の手順で NFS v4 サポートを有効にします。

1. クォーラム・サーバーのファイル・システムの /etc/exports に、以下の行を追加します。

   ```
   </your/quorumServerDir> *(fsid=0,rw,sync,no_root_squash)
   ```

   ディレクトリー名 </your/quorumserverDir> は、例として示しています。任意のディレクトリー名を使用することができます。fsid=0 を使用して、1 つのパスだけがエクスポートされるようにしてください。
2. <quorum_server_directory> ディレクトリーを作成し、その許可ビット・マスクを a+rwxt に設定します。
3. rpc_pipefs および nfsd ファイル・システムを自動的にマウントするために、/etc/fstab に以下の行を追加する必要がある場合もあります。

   a. rpc_pipefs /var/lib/nfs/rpc_pipefs rpc_pipefs defaults 0 0

   b. nfsd /proc/fs/nfsd nfsd defaults 0 0
4. /etc ディレクトリー内の config ファイルの変更を適用するために、サーバーの再始動が必要な場合があります。詳しくは、 Linux ディストリビューションの資料を参照してください。
5. /var/lib/nfs/v4recovery/ および /var/lib/nfs/ rpc_pipefs/ の各ディレクトリーが作成されたことを確認します。使用するディストリビューションによっては、modprobe nfs コマンドを実行して、NFS カーネル・モジュールをロードする必要がある場合があります。
6. 使用しているディストリビューションに応じた方法で、デーモンを開始します。例えば、rpc.idmapd デーモンを開始するには、/etc/init.d/idmapd start または service idmapd start と入力する必要があります。以下のデーモンを開始する必要があります。

a. rpc.idmapd
b. rpc.gssd
c. rpc.nfsd

7. exportfs –r コマンドを実行して、エクスポート・リストをリフレッシュします。
8. rpc.nfsd および rpc.idmapd デーモンが稼働していることを確認します。
   a. rpc.nfsd: コマンド ps –ef | grep nfsd を使用して、nfsd という名前のプロセスが稼働していることを確認します。
   b. rpc.idmapd: コマンド ps –ef | grep rpc.idmapd を使用します。
   c. コマンド rpcinfo –p を使用して、登録されているすべての RPC プログラムのバージョンを確認します。

NFS タイ・ブレーカーを実行している System Automation for Multiplatforms ノード上でマッピング・デーモン rpc.idmapd を実行するには、このデーモン用の NFS v4 ID が必要です。idmapd デーモンの開始方法については、ディストリビューションの資料を参照してください。

System Automation for Multiplatforms ノードが NFS サーバーに正しくアクセスできることを確認するには、以下のコマンドを入力します。

```
mount –t nfs4 <nfs_server_name>:/<quorum_directory_name>/<local_directory>
```

このマウント・コマンドが正常に実行された場合、およびマウントされた NFS v4 ディレクトリーでファイルの作成が可能な場合は、インストールが正常に検証されたことになります。

マウント操作が正常に行われない場合は、オペレーティング・システムの資料を参照して、インストールを修復してください。

詳しくは、 Linux ディストリビューションの資料を参照してください。

AIX 上での NFS サーバーの使用可能化

AIX 上で System Automation for Multiplatforms を稼働している場合に、NFS v4 サポートを有効にする方法について説明します。

NFS サーバーで、NFS v4 に関連するデーモンが開始されていることを確認します。

1. lssrc –g nfs コマンドを使用して、ご使用のサーバーで NFS v4 に関連するデーモンが開始されていることを確認します。
2. NFS サーバーがまだ始動していない場合は、以下のコマンドを実行して NFS サーバーを始動します。
   a. mknfs
   b. chnfsdom <your_nfs_domain_name>
   c. startsrc –s nfsrgyd
3. <quorum_server> ディレクトリーを作成し、その許可ビット・マスクを a+rwxt に設定します。
4. mknfsexp –v 4 –d <quorum_server> [-h <host>] コマンドを使用して、そのディレクトリーを NFS v4 クライアントにエクスポートします。
5. セキュリティー上の理由から、このディレクトリーのマウントが許可されるホストのリストを制限することができます。 –h オプションを指定することで、ホストのリストを、NFS サーバーを使用するすべての System Automation for Multiplatforms ノードに限定します。

mknfs コマンドを実行して、NFS クライアント上で必要な NFS 関連のデーモンを開始し、構成します。使用される NFS サーバーが Linux 上で稼働する場合は、NFS タイ・ブレーカーが初期化された後、システム・ログに以下のエラー・メッセージが示される場合があります。

```
vmount: operation not permited
```

Linux 上の NFS サーバーは、NFS クライアント用のポートが予約済みポートであるかどうかを調べます。エラー・メッセージが示される場合は、NFS タイ・ブレーカーが稼働するすべての AIX システム上で、以下のコマンドを実行します。

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

System Automation for Multiplatforms ノードが NFS サーバーに正しくアクセスできることを確認するには、以下のコマンドを入力します。

```
mount –o vers=4 <nfs_server_name>:/<quorum_directory_name>/<local_directory>
```

このマウント・コマンドが正常に実行された場合、およびマウントされた NFS v4 ディレクトリーでファイルの作成が可能な場合は、インストールが正常に検証されたことになります。

マウント操作が正常に行われない場合は、オペレーティング・システムの資料を参照して、インストールを修復してください。

NFS タイ・ブレーカーの構成

ネットワーク・タイ・ブレーカーを EXEC タイプの IBM.TieBreaker リソースとして定義します。

NFS タイ・ブレーカーの実行可能ファイルである samtb_nfs は、/usr/sbin/rsct/bin ディレクトリーにあります。現在のインプリメンテーションでは、RSCT exec タイ・ブレーカーの作成時に、以下のオプションを key=value のペアとして指定する必要があります。

nfsQuorumServer
使用される NFS v4 サーバーのホスト名。このオプションは必須です。

localQuorumDirectory
NFS タイ・ブレーカーが System Automation for Multiplatforms ノード上で使用するディレクトリー。このディレクトリーが存在しない場合は、自動的に作成されます。このオプションが指定されていない場合は、デフォルトのディレクトリー /var/ct/nfsTieBreaker/ が使用されます。

remoteQuorumDirectory
nfsQuorumServer によってエクスポートされ、System Automation for Multiplatforms の NFS タイ・ブレーカーが使用するディレクトリー。このオプションが指定されていない場合は、デフォルトである / が使用されます。

nfsOptions
mount コマンドに使用されるオプション。68 ページの『デフォルトの NFS マウント・オプション』に記載されているデフォルトのオプションを使用してください。

すべての「=」文字を「::」に置き換え、すべての「,」文字を「..」に置き換える必要があります。例えば、vers::4..fg..soft..retry::1..timeo::10 と指定すると、vers=4,fg,soft,retry=1,timeo=10 に変換された後、このマウント・オプションがオペレーティング・システムの mount コマンドに渡されます。

nfsOptions を指定しない場合、デフォルトのマウント・オプションは次のようになります。

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

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

reserveFileName
タイ・ブレーカーに関連する情報を格納するために、NFS タイ・ブレーカーによって nfsQuorumServer の remoteQuorumDirectory 内に作成されるファイルの名前。このオプションは必須です。

複数のクラスターが NFS タイ・ブレーカー用に同じ NFS v4 サーバーを使用している場合は、すべてのクラスターが別個の reserveFileName を使用するようにしてください。2 つのクラスターが同じ予約ファイルを使用していると、クラスター分割の発生時に 1 つのサブクラスターが不必要にクォーラムを失う可能性があります。予約ファイル名が一意であるようにするために、クラスター名と、クラスターのノード名のうちの少なくともいくつかの名前を利用する命名スキーマを検討することができます。

Log
syslog へのログ情報の書き込みを使用可能または使用不可にするために使用されます。

- Log=0: ログ情報は収集されません。
- Log=1: 重要な情報が syslog に書き込まれます。
- Log=2: トレースおよびデバッグ・レベルの情報が生成されます。

デフォルト値は 1 です。

HeartbeatPeriod
予約の成功の後、ConfigRM はタイ・ブレーカーのハートビート操作の定期的な呼び出しを開始します。NFS タイ・ブレーカーでは、15 より大きい値を指定してください。

PostReserveWaitTime
PostReserveWaitTime は、タイ・ブレーカーの予約の成功と 時間クォーラムの付与の間の遅延を定義します。タイ・ブレーカーを予約するノードでは、PostReserveWaitTime が経過するまで操作可能クォーラムを取得しません。NFS タイ・ブレーカーでは、PostReserveWaitTime は 15 に設定する必要があります。

NFS サーバー my.nfs.server.com 上で、localQuorumDirectory /my/quorumServer とログ・レベル 2 を使用し、その他のオプションではデフォルト値を使用して、NFS タイ・ブレーカー myNFSTiebreaker を作成するには、以下のコマンドを使用できます。

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

NFS タイ・ブレーカーを使用可能にすると、検証ロジックが実行され、NFS サーバーが予期したとおりに動作するようになります。

以下のセットアップ・エラーは、検証ロジックでは検出できません。

- HeartbeatPeriod が 15 より小さい場合。
- 使用される NFS v4 サーバーに対して reserveFileName が一意でない場合。
- PostReserveWaitTime が 15 でない場合。

EXEC タイ・ブレーカーについて詳しくは、RSCT の資料を参照してください。

デフォルトの *NFS* マウント・オプション

以下のマウント・オプションが使用されます。

rw
マウントされるディレクトリーが読み取りおよび書き込み可能であることを指定します。

soft
NFS サーバーに到達できない場合、エラーを返します。

intr
割り込みシグナルを許可します。

noac
ファイル属性はキャッシュされません。クライアントの書き込み要求が同期するように強制します。

fg
マウント・コマンドを実行し、マウント・コマンドが正常に実行されなかった場合は失敗します。

retry=0
マウント・コマンドが失敗した場合、システムは即座に停止します。

この他のマウント・オプションを使用するときは、いずれの場合も NFS タイ・ブレーカーが機能することを保証できません。

NFS タイ・ブレーカー操作のタイムアウト保護

EXEC タイ・ブレーカー操作が以下の理由で停止しないようにすることが重要です。

- タイ・ブレーカー操作の実行中に **lsrsrc**、**lsrpnode**、および **lssam** のような RSCT ベースの操作がブロックされる。
- 稼働中のクリティカル・リソースが存在するノード上で予約操作が停止した場合に、そのノードは PENDING_QUORUM 状態のままであるが、別のノードが HAS_QUORUM 状態に到達できる可能性がある。その結果、1 つのクリティカル・リソースがクラスター内の複数のノード上で同時にオンラインになる。

NFS タイ・ブレーカーには、2 つのプロセスが定義されています。1 つはワーカー・プロセスで、もう 1 つは、タイマーをアクティブにし、ワーカーがタイムアウト期間内に終了しなかった場合、ワーカーを停止するプロセスです。

- samtb_nfs_worker は、実際のタイ・ブレーカー操作を実行します。
- samtb_nfs は、タイマーを初期化した後、fork されたスレッドから samtb_nfs_worker を実行します。samtb_nfs_worker がタイムアウト期間内に終了した場合、 samtb_nfs は samtb_nfs_worker の戻りコードで終了します。samtb_nfs_worker がタイムアウト期間内に終了しなかった場合、アラーム・ハンドラーが、samtb_nfs_worker が停止されるようにして、syslog にエラー・メッセージを書き込み、-1 (FAILED) で終了します。

次のタイムアウト値が使用されます:

予約操作
クラスターの分割後 13 秒。

検証操作
タイ・ブレーカーの定義時に 60 秒。

初期化操作
クラスターの初期化時のノードのリブート後 20 秒。

その他のすべての操作
15 秒。

クラウド・タイ・ブレーカー

クラウド・タイ・ブレーカー・ソリューションは、Amazon Web Services (S3) に保管されている予約済みコンテナーのタイ状態を解決します。クラウド・タイ・ブレーカーは、2 ノード・クラスター、および AWS ストレージ・タイプのコンテナーのみをサポートします。

クラウド・タイ・ブレーカーのセットアップ

クラウド・タイ・ブレーカー・ソリューションは、Amazon Web Services (S3) に保管されている予約済みコンテナーのタイ状態を解決します。クラウド・タイ・ブレーカーは、2 ノード・クラスター、および AWS ストレージ・タイプのコンテナーのみをサポートします。

クラウド・タイ・ブレーカーは、オフサイトのクラウド・ストレージを使用してタイ・ブレーカー状態を保持することにより、スプリット・ブレーン状態を回避できる、クラウドであるため使用が容易である、ネットワークは仮想化に適している、などのいくつかの利点を実現します。

クラウド・タイ・ブレーカーは、クラウド・ストレージにアクセスするために使用されるアクセス・キーと秘密鍵のペアによって指定されます。クラウド・タイ・ブレーカー・サービスは、クラスター内の各ノードからアクセス可能である必要があります。

クラウド・タイ・ブレーカー・ストレージ・サービスは、複数のコンテナーおよびこれらのコンテナー内に含まれる複数のオブジェクトから成り立っています。

コンテナー名前空間はストレージ・サービスのすべてのユーザーによって共有されるため、コンテナー名は固有である必要があります。既存のコンテナーが削除されるまで、そのコンテナーの名前を別のコンテナーに割り当てることはできません。コンテナーには、ノードからクラウドへの接続を認証するために使用されるアクセス・コントロール・リストがあります。クラウド・サービス内でのコンテナーの固有性という特性があるため、2 ノード・クラスターの 1 つのノードのみがタイ・ブレーカー・デバイスを獲得できるようになります。これにより、スプリット・ブレーン状態の発生の可能性が回避されます。

これは、Amazon Web Services (S3) 内の共有ストレージへのアクセスを持つ、クラスター内に 2 つのノード (nodeha01 と nodeha02) があるクラウド・タイ・ブレーカー・セットアップを表します。各ノードがストレージ上にコンテナーを作成し、コンテナー内にタイ・ブレーカー・オブジェクトを作成できるように、両方のノードがクラウドに対する読み取り/書き込み権限を持ちます。スプリット・ブレーン状態が発生した場合は、コンテナーの所有権を持つノードが QUORUM の機能も取得し、そのノードがクラスター内で処理を続行します。

クラウド・タイ・ブレーカーの構成

まず、クラウド・タイ・ブレーカーを EXEC タイプの IBM.TieBreaker リソースとして定義します。EXEC タイ・ブレーカーについて詳しくは、RSCT の資料を参照してください。タイ・ブレーカー・セットアップ・ファイル samtb_cld は、/usr/sbin/rsct/bin ディレクトリーにあります。セットアップ・ファイル内のスクリプトは、リモート・ロケーションである Amazon Web Services (S3) にコンテナーを作成します。このスクリプトは、コンテナーを削除し、コンテナーの所有権を保守するためにも役立ちます。コンテナーを所有するノードは、クォーラムを持ち、スプリット・ブレーン状態のときにクラスターのアクティブ・メンバーとして機能します。

クラウド・タイ・ブレーカーをセットアップするには、以下の手順を実行します。

1. 70 ページの『AWS アカウントの作成』
2. 70 ページの『AWS からのアクセス・キーと秘密鍵の取り出し』
3. 71 ページの『クラウドへのクラスター・タイ・ブレーカーのセットアップ』

AWS アカウントの作成

2 つのクラウド・ストレージ・アカウントを作成します。アカウントには、コンテナーを作成および削除する権限が必要です。Amazon web services (AWS) Simple Storage Service (S3) に登録できます。

AWS S3 上にクラウド・ストレージ・アカウントを作成するには、以下のステップを実行します。

1. 以下のリンクをクリックします。
   Amazon web services (AWS) Simple Storage Service (S3)
   ブラウザーが AWS ホーム・ページにリダイレクトされます。
2. 「AWS アカウントの作成」ボタンをクリックします。
3. 表示されるフォームに、アカウントを作成するための個人の詳細情報を入力します。「続行」ボタンをクリックします。
4. Payment Gateway の詳細を入力します。
   Payment Gateway の詳細が検証された後で、アカウントがアクティブになります。

AWS からのアクセス・キーと秘密鍵の取り出し

各ノードは、それぞれ別個の AWS アカウントを使用して、共有クラウド・ストレージにアクセスします。クラウド・ストレージ・サービスの Web サイトから両方のアカウントのアクセス・キーと秘密鍵を取得します。各マシン上にアクセス・キー情報を配置します。

AWS からアクセス・キーと秘密鍵を取り出すには、以下のステップを実行します。

1. AWS コンソールにログインします。
2. ホーム・ページで、自分のアカウント名をクリックし、「My Security Credentials (セキュリティ認証情報)」をクリックします。
3. 「Create New Access Key」ボタンをクリックします。ボタンをクリックすると、ブラウザーからアクセス・キーと秘密鍵をダウンロードするように求めるプロンプトが出されます。
4. アクセス・キーと秘密鍵をダウンロードし、保存します。秘密鍵には Node1.secret、アクセス・キーには Node1.access という名前を付けます。
5. 同様に、もう 1 つのアカウントのアクセス・キーと秘密鍵をダウンロードし、保存します。秘密鍵には Node2.secret、アクセス・キーには Node2.access という名前を付けます。

キーの配置

各アカウントには、アクセス・キーと秘密鍵のペアが関連付けられています。タイ・ブレーカーがセットアップされるノード内にキーのペアを配置する必要があります。アクセス・キーと秘密鍵は、2 つのノードのそれぞれのルートからアクセス可能なファイル内に配置する必要があります。

以下の例は、ファイルの命名形式を示しています。ファイルの名前は、そのファイルの内容をそのまま直接的に表しています。

2 ノード・クラスターでは、ファイルは以下のように命名されます。

表 *22. 2* ノード・クラスターでのファイルの名前

通し番号	**2 ノード・クラスターでのファイルの名前**
1	/var/ct/cfg/Hostname_of_Node1.access
2	/var/ct/cfg/Hostname_of_Node1.secret
3	/var/ct/cfg/Hostname_of_Node2.access
4	/var/ct/cfg/ Hostname_of_Node2.secret

クラスター内の 2 つのノードのそれぞれに 4 つのファイルがすべて存在していること、およびそれらがルートから読み取り可能であることを確認してください。

環境の検証

各ノード上に Perl およびアクセス・キーと秘密鍵がインストールされている場合は、クラウド・タイ・ブレーカー構成を検証できます。root 権限を使用して最初のノードで以下のコマンドを実行します。

```
/usr/sbin/rsct/bin/samtb_cld
```

エラーがある場合は、前提条件が欠落していることを示しています。すべてのエラーを訂正し、上記の検証コマンドを再実行します。検証がエラーなしで実行されるまで、先に進まないでください。

同様に、もう 1 つのノードを検証します。

クラウドへのクラスター・タイ・ブレーカーのセットアップ

クラスター内の 2 つのノードのそれぞれで、クラウド・タイ・ブレーカー・リソースを検証し、リソースが正しく構成されていることを確認したら、root 権限を使用していずれかのノードで以下の一連の 3 つのコマンドを実行します。

注 : これらのコマンドは、クラスターのいずれかのノードで 1 回のみ実行してください。

以下のコマンドを実行します。

```
export CT_MANAGEMENT_SCOPE=2
```

root 権限を使用して以下のコマンドを実行して、タイ・ブレーカー・リソースを作成し、オブジェクトに CloudTB1 という名前を付けます。

```
mkrsrc IBM.TieBreaker Type=EXEC Name=CloudTB1 DeviceInfo=PATHNAME=/usr/sbin/
rsct/bin/samtb_cld
```

以下のコマンドを実行して、現在のクラスターのアクティブ・タイ・ブレーカーを設定します。このコマンドは、CloudTB1 という名前の新しく作成されたタイ・ブレーカー・オブジェクトをアクティブ・タイ・ブレーカーとして設定します。

```
chrsrc -c IBM.PeerNode OpQuorumTieBreaker=CloudTB1
```

3 つのコマンドがエラーなしで実行されたことを確認します。上記のコマンドを実行すると、2 ノード・クラスターに「クラウド」タイプのタイ・ブレーカーが設定されます。以下のコマンドを実行して、タイ・ブレーカー・セットアップを検証します。

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

出力は以下の画面のようになります。

```
Resource Class Persistent Attributes for IBM.PeerNode
resource 1:
        OpQuorumTieBreaker = "CloudTB1"
```

この出力は、新しく作成されたタイ・ブレーカー CloudTB1 がクラスター内のアクティブ・タイ・ブレーカーであることを示しています。

問題判別と分析

以下に、2 ノード・クラスターにおいて、クラウド・タイ・ブレーカーでエラーが発生した場合のシステム・ログの内容 (nodeha01 からのログ) を例として示します。

クラウド・タイ・ブレーカーは、以下のラベルが付加された定義済みのネイティブ SYSLOG 機能項目にログを記録します。
1 samtb_cld

例えば、SYSLOG 機能がこのマシン内のファイル /var/log/messages にデータを保管している場合は、以下のコマンドを実行すると、クラウド・タイ・ブレーカーによって記録されたすべてのログ項目を表示できます。

```
cat /var/log/messages | grep samtb_cld
```

最も重要な項目は、クォーラムが成立したことを示す項目です。具体的には、クラウド・タイ・ブレーカーがクォーラム・デバイスを獲得できる場合は、SYSLOG に以下の画面のようなメッセージが表示されます。

```
   Feb 19 15:59:03 nodeha01 samtb_cld[7203]:
   *****INFO: tryReserve: returning 0
   Feb 19 15:59:03 nodeha01 samtb_cld[7203]:
   *****INFO: op=reserve rc=0 log=1
   Feb 19 15:59:03 nodeha01 samtb_cld[7203]:
   *****INFO: Exiting samtb_cld main code returning 0
   Feb 19 15:59:03 nodeha01 ConfigRM[5642]: (Recorded using
   libct_ffdc.a cv 2):::Error ID: :::Reference ID:  :::Template ID:
     0:::Details File:  :::Location:RSCT,PeerDomain.C,1.99.22.61,18346
     :::CONFIGRM_HASQUORUM_ST The operational quorum state
   of the active peer domain has changed to HAS_QUORUM.
   In this state, cluster resources may be recovered and
   controlled as needed by management applications
```

操作クォーラムの無効化

操作クォーラムを成立させるための十分なノードがない場合は、操作クォーラムの状況を無効にします。

クラスターからノードを削除するには、**rmrpnode** コマンドを開始するために、クラスター内の少なくとも 1 つのノードがオンラインでなければなりません。このコマンドを実行するためには、操作クォーラムが必要です。操作クォーラムを成立させるための十分なノードがない場合、クォーラムを再度確立するためにクラスターのサイズを調整することはできません。

何らかの理由で操作クォーラム機能を非アクティブにする必要がある場合、永続属性 OpQuorumOverride を 1 に設定する必要があります。

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

この場合、操作可能クォーラムの状況は常に HAS_QUORUM であり、リソース保護は以後保証されません。

エンドツーエンド自動化アダプターの構成

System Automation for Multiplatforms ドメインを System Automation Application Manager エンドツーエンド自動化環境に統合する場合は、自動化アダプターを構成する必要があります。

System Automation for Multiplatforms ドメインを System Automation Application Manager エンドツーエンド自動化環境に統合する場合は、以下の条件が適用されます。

- System Automation for Multiplatforms のオブジェクト名。System Automation for Multiplatforms のオブジェクト名 (例えば、グループ名、リソース名、説明など) は、次の文字を含んではいけません。
  - " : 二重引用符
  - ' : 単一引用符
  - ; : セミコロン
  - $: ドル記号
  - / : スラッシュ
- System Automation for Multiplatforms ドメイン名は、同じエンドツーエンド自動化マネージャーに接続する自動化ドメインのスコープ内で固有である必要があります。

エンドツーエンド自動化アダプターが動作する環境およびエンドツーエンド自動化アダプターのために構成する必要がある内容を 73 ページの図 13 に示します。

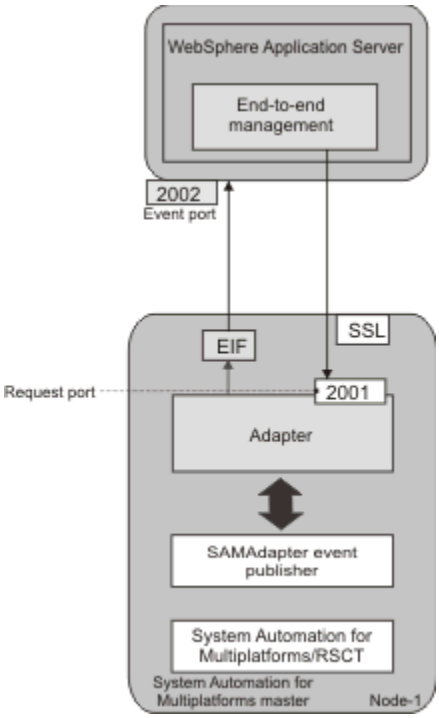


図 *13. System Automation for Multiplatforms* クラスターでのエンドツーエンド自動化アダプター環境の概要

System Automation for Multiplatforms ドメインを System Automation Application Manager エンドツーエンド自動化環境に統合するには、System Automation Application Manager 製品をインストールする必要があります。エンドツーエンド自動化管理について詳しくは、「*System Automation for Multiplatforms* 管理者とユーザーのガイド」を参照してください。

エンドツーエンド自動化アダプター構成ダイアログの開始

cfgsamadapter コマンドを使用して、構成ダイアログを開始します。

このタスクについて

注 :

1. cfgsamadapter ユーティリティーは X Window システム・アプリケーションであり、X Window システム・サーバー機能のあるワークステーションから使用する必要があります。構成ダイアログを実行するには、X11 インストール・パッケージが必要です。一部のオペレーティング・システムでは、それらのパッケージは配布メディアには含まれていますが、標準インストールには含まれていません。
   - 32 ビット・バージョンの System Automation for Multiplatforms がインストールされている AIX および Linux オペレーティング・システムに 32 ビット・バージョンの X11 インストール・パッケージをインストールします。
   - 64 ビット・バージョンの System Automation for Multiplatforms がインストールされている Ubuntu および Linux オペレーティング・システムに 64 ビット・バージョンの X11 インストール・パッケージをインストールします。
2. AIX システムでは、エンドツーエンド自動化アダプター・インストール済み環境が次の要件を満たす 必要があります。アダプター構成の「**複製**」タスクを完了可能に するためには、**SSL/SSH** パッケージがインストールされており、**sshd** サブシステムが稼働している必要があります。
3. エンドツーエンド自動化アダプターは、入力プロパティー・ファイルを使用してサイレント・モードで構成することもできます。X11 サーバーが使用できない場合は、サイレント構成が、このシステムでサポートされる唯一の方式です。 詳しくは、82 ページの『サイレント・モードでの構成』を参照してください。
4. 構成ダイアログを使用するには、ユーザー ID root を使用してシステムにログオンするか、ディレクトリー /etc/opt/IBM/tsamp/sam/cfg および /etc/Tivoli への書き込みアクセス権限を 持っている必要があります。

cfgsamadapter コマンドを入力して、Tivoli System Automation アダプター構成ダイアログを開始します。ダイアログのメインウィンドウが表示されます。

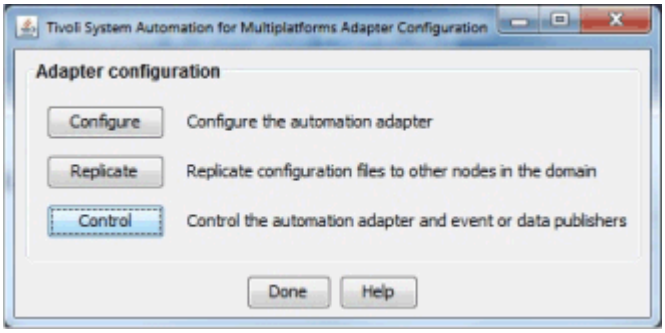


図 *14.* エンドツーエンド自動化アダプター構成ダイアログのメインウィンドウ

構成タスク:

1. エンドツーエンド自動化アダプターを構成する (75 ページの『自動化アダプター 設定の構成』 ページを参照)
2. 他のノードにエンドツーエンド自動化アダプター構成ファイルを複製する (81 ページの『エンドツーエンド自動化アダプターの構成ファイルの複製』 ページを参照)
3. 自動化アダプター、イベント・パブリッシャー、およびデータ・パブリッシャーを制御する。エンドツーエンド自動化アダプター、Tivoli Netcool/OMNIbus イベント・パブリッシャー、またはレポート・データ・パブリッシャーを開始または停止します。アダプターおよびパブリッシャーについて詳しくは、System Automation for Multiplatforms 管理者とユーザーのガイドを参照してください。

自動化アダプター 設定の構成

構成ダイアログのメインウィンドウで、「**構成**」をクリックします。以降のセクションで説明する、複数の構成タブが表示されます。

このタスクについて

「アダプター」タブ

「**アダプター**」タブを使用して、アダプター・ホストを構成します。

「**アダプター**」タブのフィールドおよびコントロール

ホスト名または IP アドレス
アダプターが稼働しているノードのホスト名。ローカル・ホスト名がデフォルト値として使用されます。ローカル・ホスト名とは異なる値を使用する場合は、「**ローカル・ホスト名の使用**」チェック・ボックスをクリアして、入力フィールドを編集可能にしてください。例えば、別のネットワークを使用する場合などです。

構成ファイルの複製への影響: ローカル・ホスト名を使用する場合、「**複製**」機能により、それぞれのローカル・ホスト名が各リモート複製ターゲット・ノードで使用されるようになります。異なるホスト名または IP アドレスを指定すると、「**複製**」機能により、この値がクラスター内の他のノードに複製されます。この場合、同じ値をすべてのノードで使用しないようにするには、各ノード上で個別にアダプター・ホストを構成します。詳しくは、81 ページの『エンドツーエンド自動化アダプターの構成ファイルの複製』を参照してください。

要求ポート番号
アダプターがエンドツーエンド自動化管理ホストからの要求を listen するポートの番号 を指定します。デフォルトのポートは 2001 です。

ポリシー・プールのロケーション
XML ポリシー・ファイルを含むディレクトリーの修飾パス名を 指定します。System Automation Application Manager を使用して System Automation for Multiplatforms 自動化ポリシーをアクティブにする場合、ポリシー・プールが必要です。クラスター内のすべてのノードに、ポリシー・プール・ディレクトリーを定義し、 作成します。このパラメーターはオプションです。

アダプターの実行時の動作を 指定するには、「**拡張**」をクリックします。

アダプター停止遅延
時間を秒単位で定義します。アダプターがドメイン退出イベントを適切に配信できるようにするために、アダプターの停止はこの時間内で遅延されます。デフォルト値は 5 です。低速なシステムでは、この値を大きくできます。この値の範囲は 3 から 60 秒までです。

リモート接続アクティビティーの間隔
エンドツーエンド自動化管理ホストからの接続がない場合に、アダプターを停止させるまでの猶予時間を秒単位で定義します。このホストは、定期的にアダプターに接続して、アダプターが引き続き稼働しているかどうかを確認します。デフォルト値は 360 です。 間隔に 0 以外の値を指定する場合は、チェック間隔の倍数を指定する必要があります。

値に 0 を設定した場合は、アダプターは停止することなく 稼働し続けます。

初期接続再試行間隔
時間を分単位で定義します。アダプターは、この時間内にエンドツーエンド自動化管理ホストに接続しようとします。この試行は、成功するか、指定の時間が経過するまで続けられます。デフォルト値は 0 です。これは、アダプターがエンドツーエンド自動化管理ホストへの接続を無期限に試行することを意味します。

EIF イベント・キャッシュを使用可能にする
イベント・キャッシュをアクティブ化するには、このチェック・ボックスを選択します。

EIF イベント再接続試行間隔
時間を秒単位で定義します。接続が中断されると、アダプターは、エンドツーエンド自動化管理ホストへの接続の再確立を試行するまで待機します。デフォルト値は 30 です。

「アダプター使用ホスト」タブ

「アダプター使用ホスト」タブを使用して、アダプターが接続されているエンドツーエンド自動化マネージャー・ホストを構成します。

「アダプター使用ホスト」タブのフィールド

ホスト名または IP アドレス
エンドツーエンド自動化マネージャーが稼働するホストの名前または IP アドレス。

代替ホスト
このフィールドの値はオプションです。System Automation Application Manager について 2 つの異なるサイトを使用して災害時回復セットアップを構成した場合は、エンドツーエンド自動化マネージャーはいずれのサイトでも実行できます。このようなセットアップをサポートするには、2 番目のサイトのホスト名または IP アドレスも指定してください。これにより、Application Manager のサイト切り替え時に、アダプターがイベント送信先のターゲットを新規のアクティブなエンドツーエンド自動化マネージャー・インスタンスにシームレスに切り替えるようになります。

イベント・ポート番号
エンドツーエンド自動化マネージャーが自動化アダプターからのイベントを listen するポート。ここに指定するポート番号は、エンドツーエンド自動化マネージャーのドメインを構成するときにイベント・ポート番号として指定するポート番号と一致している必要があります。デフォルトのポートは 2002 です。

注 : エンドツーエンド自動化アダプターとエンドツーエンド自動化管理ホストの間の通信で IPv6 を使用する場合は、以下の制限が適用されます。

アダプターからアダプター使用ホストへの 通信の場合*:*

1. エンドツーエンド自動化管理ホストの構成に IPv6 ホスト名が指定されている場合、DNS サーバーは IPv6 レコードのみを返すよう構成されている必要があります。
2. IPv4 と IPv6 のレコードを返すよう DNS サーバーが構成されている場合 は、IPv4 アドレスのみが使用されます。IPv6 を使用するには、エンドツーエンド自動化管理ホストの構成にあるホスト名ではなく、IPv6 アドレスを明示的に指定してください。

エンドツーエンド自動化管理ホストからアダプターへの通信の場合*:*

1. アダプター・ホストの構成に IPv6 ホスト名が指定されている場合、DNS サーバーは IPv6 レコードのみを返すよう構成されている必要があります。
2. IPv4 と IPv6 のレコードを返すよう DNS サーバーが構成されている場合 は、IPv4 アドレスのみが使用されます。IPv6 を使用するには、アダプター・ホストの構成にあるホスト名ではなく、IPv6 アドレスを明示的に指定してください。

コマンド `host -n -a <ipv6_hostname>` を使用して DNS ルックアップ・レコードを検査してください。

レポート・タブ

「レポート」タブを使用して、System Automation Application Manager データベースにレポート・データを収集するための設定を構成します。

レポート・データベースを構成した後で、レポート・データ・パブリッシャーを開始する必要があります。

注 :

1. レポート生成などのレポート機能は、 バージョン 3.2.2 までは System Automation Application Manager 製品の一部として提供されています。
2. System Automation Application Manager をエンドツーエンド自動化管理ホストからアンインストールする前にレポート機能を無効にしてください。

   System Automation Application Manager のローカル・データベース・インストールは、アンインストール中に除去されます。この場合、レポート・データ・パブリッシャーを停止してください。

レポート・データ・パブリッシャーの開始または停止については、*System Automation for Multiplatforms* 管理者とユーザーのガイドを参照するか、次のコマンドを使用してください。

```
samctrl -e JDBC or samctrl -d JDBC
```

System Automation Application Manager の DB2® データベースにレポート・データを収集する場合は、「**レポート・データ収集を使用可能に設定**」チェック・ボックスを選択してください。それ以外の場合は、このチェック・ボックスを選択解除してください。このタブの入力フィールドが無効になります。

「**レポート**」タブのフィールド:

DB2 サーバー名または IP アドレス
レポート・データのデータベースをホストする DB2 サーバーのホスト名または IP アドレス。レポート生成などの実際のレポート機能は、System Automation Application Manager 製品の一部として 提供されています。DB2 サーバーは、System Automation Application Manager の DB2 データベースが配置されているシステムと同じシステムでなければなりません。

この値を省略した場合は、「**アダプター使用ホスト**」タブで、System Automation Application Manager ホストに指定する値がデフォルトとして使用されます。System Automation Application Manager データベースとしてリモート DB2 を使用している場合は、このリモート DB2 システムのホスト名または IP アドレスを指定してください。

注 : DB2 サーバーが z/OS 上で稼働している場合、ファイル `db2jcc_license_cisuz.jar` がご使用の System Automation for Multiplatforms クラスターの各ノードで使用可能であることを確認してください。このファイルには、z/OS でないシステムから z/OS 上の DB2 に接続するライセンスが含まれます。

このファイルは、System Automation Application Manager に使用される WebSphere Application Server のディレクトリーにあります。以下のディレクトリー・ツリーでこのファイルを検索してください。

```
<WAS_INSTALL_ROOT>/deploytool/itp/plugins
```

このファイルをご使用の System Automation for Multiplatforms クラスターの各ノード上のディレクトリー `/opt/IBM/tsamp/sam/lib` にコピーします。DB2 の使用許諾契約があることを確認してください。

代替 DB2 サーバー
このフィールドの値はオプションです。System Automation Application Manager について 2 つの異なるサイトを使用して災害時回復セットアップを構成した場合は、エンドツーエンド自動化マネージャーはいずれのサイトでも実行できます。このようなセットアップをサポートするには、このフィールドに 2 番目のサイトの System Automation Application Manager のホスト名または IP アドレスを指定してください。Application Manager のサイト切り替え時に、アダプターはレポート・データ収集のターゲットを新規のアクティブなエンドツーエンド自動化マネージャー・インスタンスに自動的に切り替えます。以下のすべての設定値は、両方の DB2 サーバーに使用されます。データベースがエンドツーエンド自動化マネージャーと同じシステム上にある場合は、アダプターを使用する代替 System Automation Application Manager ホストに使用したのと同じ値を指定してください。

System Automation Application Manager データベースにリモート DB2 を使用する場合、このフィールドは空のままにしておきます。

注 : 代替 DB2 サーバーを指定する場合は、DB2 自動クライアント・リルート機能を構成する必要があります。これで、レポート機能は DB2 HADR プライマリー・インスタンスにレポート・データを常に送信できるようになります。この機能のセットアップ方法の説明については、DB2 の資料を参照してください。

例:

DB2 HADR が 2 つのホスト `lnxcm5x` および `lnxcm6x` 上でデータベース `eautodb` に対してセットアップされています。DB2 ポートはどちらのホストでも 50000 です。2 つのホストに対して自動クライアント・リルートを構成するには、以下のコマンドを実行します。

- lnxcm5x の場合:

```
db2 update alternate server for database eautodb using host name
lnxcm6x port 50001
```

- lnxcm6x の場合:

```
db2 update alternate server for database eautodb using host name
lnxcm5x port 50001
```

DB2 データベース名
レポート・データが格納される System Automation Application Manager の DB2 データベースの名前。

DB2 スキーマ名
レポート・データが格納されるデータベース表に使用されるスキーマの名前。 このパラメーターの値は、System Automation Application Manager の DB2 データベースが z/OS システム上にある場合にのみ変更してください。DB2 インストール済み環境にあるデータベース表を一意的に識別するようにスキーマ名を制御することが必要な場合があります。

DB2 ポート
レポート・データが格納される System Automation Application Manager の DB2 データベースにアクセスする際に使用されるポートの番号。デフォルトのポートは 50001 です。

ユーザー ID
レポート・データが格納される System Automation Application Manager の DB2 データベースにアクセスする際に使用されるユーザー ID。

パスワード
レポート・データが格納される System Automation Application Manager の DB2 データベースにアクセスする際に使用されるパスワード。

パスワードを変更するには、「**変更**」を クリックします。

注 : DB2 データベースのパスワードが変更された場合は、構成したパスワードを必ず更新してください。構成したパスワードが DB2 データベースのパスワードと一致しない場合、イベントはデータベースに書き込まれません。

「イベント・パブリッシュ」タブ

「**イベント・パブリッシュ**」タブを使用して、EIF イベントを Tivoli Netcool/Omnibus にパブリッシュするための設定を構成します。

「**イベント・パブリッシュ**」タブ上のコントロールおよびフィールド:

OMNIbus イベント・パブリッシュ

OMNIbus EIF イベント・パブリッシュを使用可能にする
OMNIbus Probe for Tivoli EIF が稼働しているホストに EIF イベントを送信する場合は、このチェック・ボックスを選択します。チェック・ボックスを選択しない場合、このタブにある他のすべてのフィールドは使用不可になります。EIF イベント・パブリッシュを使用可能または使用不可にする場合は、対応するイベント・パブリッシャーを開始または停止するようにしてください。EIF イベント・パブリッシャーの開始または停止については、*System Automation for Multiplatforms* 管理者とユーザーのガイドを参照するか、次のコマンドを使用してください。

```
samctrl -e TEC or samctrl -d TECs
```

注 : 互換性のために、Tivoli Enterprise Console サーバーおよびポートを代わりに構成することもできます。

イベント・サーバー

ホスト名または IP アドレス
OMNIbus Probe for Tivoli EIF が稼働中のホストのホスト名または IP アドレス。値は、コンマで区切って、最大 8 個まで指定できます。1 番目の位置は 1 次イベント・サーバーで、それ以降は 1 次サーバーがダウンした時に使用する 2 次サーバーを順番に指定します。

ポート番号 (Port number)
EIF イベントを listen するために OMNIbus Probe for Tivoli EIF で使用されるポート番号。ポート・マッピングを使用する場合は、ポート番号として `0` を指定できます。

イベント・フィルター

パブリッシュする EIF イベントの発行元:

関係の構成変更
関係の追加、削除、および変更により発生したすべての EIF イベントをイベント・サーバーに送信する場合は、このチェック・ボックスを選択します。それ以外の場合、関係の構成変更イベントはフィルターによって除外されます。

リソースの構成変更
リソースの追加、削除、および変更により発生したすべての EIF イベントをイベント・サーバーに送信する場合は、このチェック・ボックスを選択します。それ以外の場合、リソースの構成変更イベントはフィルターによって除外されます。

要求の追加および削除
要求の追加および削除により発生した EIF イベントをイベント・サーバーに送信する場合は、このチェック・ボックスを選択します。それ以外の場合、要求の追加および削除のイベントはフィルターによって除外されます。

リソース状況変更
リソースの状況変更に関連する EIF イベントをイベント・サーバーに送信する場合は、このチェック・ボックスを選択します。それ以外の場合、リソースの状況変更イベントはすべてフィルターによって除外されます。パブリッシュする状況の変更イベントを定義するには、重大度に応じてラジオ・ボタンのいずれか 1 つを選択します。

追加のフィルターの定義:

このタブで使用可能または使用不可に設定できるイベント・フィルターは、System Automation for Multiplatforms に組み込まれている事前定義フィルターです。追加のフィルターを定義する場合は、対応する次の構成プロパティー・ファイルを手動で変更します。

```
/etc/Tivoli/TECPublisher.conf
```

事前定義フィルターを編集する場合は、フィルターを追加し、事前定義フィルターを使用不可にします。構成変更が `cfgsamadapter` 構成ユーティリティーによって適用された場合、追加したすべてのフィルターは保持されます。

「セキュリティー」タブ

「**セキュリティー**」タブを使用して、アダプター使用ホストとエンドツーエンド管理ホストとの間のインターフェース用のセキュリティーを構成します。

自動化アダプターと、アダプターを使用するホストとの間の通信用に Secure Socket layer (SSL) プロトコルを使用する場合は、「**SSL を使用可能にする**」を選択します。チェック・マークを付けた場合は、以下の入力フィールドに入力する必要があります。

「セキュリティー」タブのコントロールおよびフィールド

トラストストア
SSL に使用するトラストストア・ファイルの名前。ファイル名はピリオド文字を複数含むことがあります。「**参照**」をクリックしてファイルを選択します。

鍵ストア
SSL に使用する鍵ストア・ファイルの名前。ファイル名はピリオド文字を複数含むことがあります。「**参照**」をクリックしてファイルを選択します。

鍵ストアのパスワード
鍵ストア・ファイルのパスワード。パスワードを変更するには、「**変更**」を クリックします。

注 : トラストストアが鍵ストアと異なるファイルに格納されている場合は、それらのファイルのパスワードが同一である必要があります。

証明書の別名
サーバーが使用する証明書の別名。

ユーザー認証の施行
Pluggable Access Module (PAM) を使用してユーザーの認証を使用可能にするには、「ユーザー認証の施行」チェック・ボックスを選択します。

System Automation Application Manager を使用して、System Automation for Multiplatforms XML ポリシーも保持する場合は、「**ユーザー認証の施行**」を使用可能にする必要があります。

PAM サービス
アダプターが稼働しているオペレーティング・システムに基づいて、ユーザー検証のために行う検査を決定する Pluggable Access Module サービスの名前。

- SUSE Linux 配布版の場合は、ディレクトリー `/etc/pam.d` にあるファイル
- RedHat Linux 配布版の場合は、ファイル `/etc/pam.conf` にある項目
- AIX の場合は、ファイル `/etc/pam.conf` にある項目

「ロガー」タブ

「ロガー」タブを使用して、ロギング、トレース、および First Failure Data Capture の設定を指定します。設定は永続的または一時的に変更できます。

構成ファイルに現在設定されている値が常に「ロガー」タブに表示されます。

「ロガー」タブでは、次の操作を実行できます。

設定の永続的変更
以下のステップを実行します。

1. タブで必要な変更を行います。
2. 「**保管**」をクリックします。

結果: 構成ファイル内の設定が更新されます。 アダプターを再始動し、変更を有効にします。

設定の一時的変更
アダプターが稼働していることを確認してから以下のステップを実行します。

1. タブで必要な変更を行います。
2. 「**適用**」をクリックします。

結果: 新規設定は即時に有効になります。設定は構成ファイルに保管されません。アダプターが稼働していない場合は、エラー・メッセージを受け取ります。

永続的設定への復帰
設定を一時的に変更した場合、またはアダプターで現在アクティブな設定が不確かな場合に、構成ファイルに定義されている永続的設定に復帰するには、以下のステップを実行します。

1. 構成ダイアログを呼び出し、「ロガー」タブを開きます。構成ファイルに現在設定されている値が「ロガー」タブに表示されます。
2. 「**適用**」をクリック、設定をアクティブにします。

結果: 設定は即時に有効になります。アダプターが稼働していない場合は、エラー・メッセージを受け取ります。

「**ロガー**」タブのコントロールおよびフィールド

ログ/トレース・ファイルの最大サイズ
ログ・ファイルの最大ディスク使用量 (KB 単位)。この限度に達すると、別のログ・ファイルが作成されます。 ログ・ファイルの最大数は 2 個です。つまり、両方のファイルがいっぱいになった後は、古い方のファイルが上書きされます。 デフォルトの最大ファイル・サイズは 1024 KB です。

メッセージ・ロギング・レベル
ログに記録するメッセージの重大度に応じて、「**メッセージ・ロギング・レベル**」を選択します。

トレース・ロギング・レベル
ログに記録する問題の重大度に応じて、「**トレース・ロギング・レベル**」を選択します。

First Failure Data Capture (FFDC) 記録レベル
FFDC データを収集する問題の重大度に応じて、FFDC 記録レベルを選択します。

First Failure Data Capture (FFDC) 最大ディスク・スペース
FFDC トレース・ディレクトリーに書き込まれる、FFDC トレースで使用する最大ディスク・スペースをバイト単位で指定します。デフォルトのスペースは 10485760 バイト (10 MB) です。

First Failure Data Capture (FFDC) スペース超過ポリシー
以下のいずれかのオプションを選択します。

無視
警告を出しますが、FFDC ディスク・スペース制限は施行しません。

自動削除
FFDC ディスク・スペース制限を施行するため、FFDC ファイルを自動的に削除します。 これは、スペース超過ポリシーのデフォルト値です。

サスペンド
ディスク・スペースを手動で解放するまで、以降の FFDC アクションを一時停止します。

First Failure Data Capture (FFDC) メッセージ ID フィルター・モード
以下のいずれかのオプションを選択します。

パススルー
メッセージ ID リストに指定されているメッセージがあるすべてのログ・イベントがフィルターを通過し、FFDC データが書き込まれます。 これがデフォルトのフィルター・モードです。

ブロック
メッセージ ID リストに指定されているメッセージがあるすべてのログ・イベントがブロックされます。

First Failure Data Capture (FFDC) メッセージ ID リスト
フィルター・モードに応じて FFDC データの書き込み対象のログ・イベントを制御するメッセージ ID です。メッセージ ID の比較では大/小文字が区別されます。メッセージ ID ごとに改行する必要があります。 ワイルドカード文字 (例えば、*E はすべてのエラー・メッセージを意味する) を使用できます。

構成の保管

アダプター構成ファイルの変更を保存するには、構成ウィンドウの「**保存**」をクリックします。

このタスクについて

項目が欠落しているか、値が範囲外である (ポート番号など) 場合、エラー・メッセージが表示されます。正常終了後、「構成更新状況」ウィンドウが表示され、構成ファイルおよびその更新状況のリストが示されます。アダプターを再始動して、変更を有効にします。

エンドツーエンド自動化アダプターの構成ファイルの複製

ドメイン内の他のノードへのエンドツーエンド自動化アダプターの構成ファイルの複製

このタスクについて

構成ダイアログのメインウィンドウで「**複製**」をクリックします (74 ページの『エンドツーエンド自動化アダプター構成ダイアログの開始』 を参照)。「**構成ファイルの複製**」ウィンドウが表示されます。

自動化アダプター構成ファイルを RSCT ピア・ドメインの残りのノードに配布 (複製) します。

1. 複製する構成ファイルを選択するか、「**すべて選択**」をクリックしてリスト内のすべての構成ファイルを選択します。
   - (1) 選択したファイルの中にファイル `sam.adapter.ssl.properties` があり、かつ (2) アダプター構成の「**セキュリティー**」タブで構成した SSL トラストストア・ファイルと鍵ストア・ファイルが複

製ソース・ノードに存在する場合は、そのトラストストア・ファイルと鍵ストア・ファイルが複製されます。

- 複製ソース・ノードにファイルが配置されているディレクトリーが、すべてのターゲット・ノードでも存在していることを確認します。

2. 複製ターゲット・ノードのリストの下にある「**すべて選択**」をクリックして、すべてのノードでアダプター構成が同一となるようにします。
3. ファイルの複製先であるターゲット・ノードのユーザー ID およびパスワードを入力します。
4. 「**複製**」をクリックして、複製を開始します。

複製にはしばらく時間がかかる場合があります。ファイルを複製している間は、「**複製**」ボタンがインデントおよびグレイアウトされます。 複製が完了すると、各構成ファイルの複製状況が表示されます。

エンドツーエンド自動化アダプターの高可用性の実現

Tivoli System Automation クラスターが複数のノードで構成されている場合は、エンドツーエンド自動化アダプターを可用性が高いままにする必要があります。

このタスクについて

System Automation Application Manager オペレーション・コンソールへの通信は、クラスター内のノードの停止中や保守中も活動状態のままです。

73 ページの『エンドツーエンド自動化アダプターの構成』 に示されているように、自動化アダプターは System Automation マスター・ノードに接続されています。クラスター・インフラストラクチャーにより、マスター・ノードは常に使用可能になるため、アダプターも暗黙的にマスター・ノード上で常に使用可能になります。System Automation for Multiplatforms バージョン 4.1.0.0 以降では、アダプターの高可用性を実現するための自動化ポリシー構成は必要ありません。

サイレント・モードでの構成

エンドツーエンド自動化アダプターの構成にはサイレント構成を使用できます。

サイレント・モードの構成ツールでは、構成ダイアログを開始することなく、エンドツーエンド自動化アダプターを構成できます。この場合、X Window セッションを有効にする必要はありません。

関連するプロパティー・ファイル内の構成パラメーター値を編集することにより、エンドツーエンド自動化アダプターを構成します。サイレント構成モードを使用する場合、X Window セッションを有効にする必要はありません。

構成の更新を処理する前に、まず構成ツールを始動して、サイレント・モードの入力プロパティー・ファイルを生成する必要があります。詳しくは、73 ページの『エンドツーエンド自動化アダプターの構成』を参照してください。

サイレント・モードでの作業

サイレント構成モードでの主な作業について説明します。

構成ツールをサイレント・モードで使用するには、構成するコンポーネントごとに以下の手順を実行してください。

1. サイレント・モードの入力プロパティー・ファイルを生成するか見つけます。83 ページの『サイレント・モードの入力プロパティー・ファイル』を参照してください。
2. ファイル内のパラメーター値を編集します。84 ページの『入力プロパティー・ファイルの編集』を参照してください。
3. 構成ツールをサイレント・モードで開始して、ターゲット構成ファイルを更新します。83 ページの『サイレント構成の開始』を参照してください。
4. 構成ツールが正常に完了しなかった場合は、報告されたすべてのエラーに対処し (85 ページの『サイレント・モードでの出力』を参照)、構成ツールを再度開始します。

一部の作業では、サイレント構成がサポートされていません。構成ダイアログを使用しない場合は、それらの作業を手動で行う必要があります。詳しくは、83 ページの『手動で実行する構成タスク』を参照してください。

手動で実行する構成タスク

ランチパッド・ウィンドウにある対応するプッシュ・ボタンをクリックすることにより、ダイアログ・モードで起動されるいくつかの構成タスクは、サイレント構成モードではサポートされていません。

構成ダイアログを使用しない場合は、以下のタスクを手動で実行する必要があります。

1. **構成ファイルを複製する**

   System Automation for Multiplatforms ドメインが複数のノードで構成されている場合は、エンドツーエンド自動化アダプター構成ファイルを、System Automation for Multiplatforms ドメイン内の他のノードに手動で複製する必要があります。構成ファイルを複製するには、ドメイン内の各ノードで同一内容の入力プロパティー・ファイルを使用して、サイレント・モードで構成ツールを実行します。
2. **自動化アダプターおよびパブリッシャーを制御する**
   - コマンド `samadapter {start|stop}` を使用して、エンドツーエンド自動化アダプターを開始または停止します。
   - コマンド `samctrl {-e|-d} TEC` を使用して、Tivoli Netcool/OMNIbus イベント・パブリッシャーを開始または停止します。
   - コマンド `samctrl {-e|-d} JDBC` を使用して、レポート・データ・パブリッシャーを開始または停止します。

サイレント構成の開始

コマンド **cfgsamadapter -s** を使用して、サイレント構成を開始します。

エンドツーエンド自動化アダプターのサイレント構成を開始する:

- システム自動化アダプター構成ツールをサイレント・モードで使用するには、ディレクトリー `/etc/opt/IBM/tsamp/sam/cfg` および `/etc/Tivoli` への書き込みアクセス権限を持っている必要があります。
- コマンド `cfgsamadapter -s` を入力してください。

`cfgsamadapter` コマンドについて詳しくは、*Tivoli System Automation for Multiplatforms* リファレンスを参照してください。

サイレント・モードの入力プロパティー・ファイル

現在構成されている値から、サイレント・モードの入力プロパティー・ファイルを生成します。このファイルを使用して、構成設定をサイレント・モードで変更します。

サイレント・モードの入力プロパティー・ファイルを、対応するターゲット構成ファイルに現在定義されている値から生成します。利点は次のとおりです。

- インストールの直後から、カスタマイズを開始するまでの間に、プロパティー・ファイルを生成できます。
- 構成ダイアログを使用し、サイレント・モードでカスタマイズする場合に、最新の入力ファイルを生成してからサイレント・モードで変更を適用できます。
- サイレント・モードの入力プロパティー・ファイルを誤って削除した場合に容易に回復できます。

サイレント・モードの入力プロパティー・ファイルを生成するには、サイレント構成の開始時に、以下のいずれかのオプションを使用します。

-g
存在していない場合にのみ入力プロパティー・ファイルを生成します。

-gr
入力プロパティー・ファイルを生成し、存在している場合は置換します。

-l *location*
サイレント構成用の入力プロパティー・ファイルは、*location* で指定したディレクトリーにあります。-l を省略した場合は、入力プロパティー・ファイルは、デフォルト・ディレクトリーの /etc/opt/IBM/tsamp/sam/cfg にあります。

表 *23.* 生成される入力プロパティー・ファイル

構成コマンド	**サイレント入力プロパティー・ファイル**
cfgsamadapter -s -g | -gr	/etc/opt/IBM/tsamp/sam/cfg/silent.samadapter.properties
cfgsamadapter -s -g | -gr -l *location*	*location*/silent.samadapter.properties

サイレント・モードで構成設定を更新すると、サイレント・プロパティー・ファイルが更新タスクの入力として使用されます。構成ユーティリティーに /etc/opt/IBM/tsamp/sam/cfg ディレクトリー以外の場所から入力ファイルを取得させるには、**-l** *location* オプションを使用します。

入力プロパティー・ファイルの編集

構成をサイレント・モードで変更するために、入力プロパティー・ファイルの値を変更します。

コンポーネントごとに生成される入力プロパティー・ファイルは、構成パラメーターのキーワードと値の対を含んでいます。モード間の切り替えをできるだけ容易にし、またプロパティー・ファイルを編集するときのエラーをできるだけ排除するために、サイレント・モード・プロパティー・ファイルで使用されている構造、用語、および表現は、構成ダイアログでの構造、用語、および表現と同一になっています。

構成ダイアログでのタブの名前 (「**アダプター**」など) またはボタンの名前 (「**拡張...**」など) は、プロパティー・ファイル内で ID として使用されます。次に例を示します。

```
# ============================================================================
# ... アダプター
⋮
# ============================================================================
# ... 拡張
```

構成ダイアログの各フィールド名、「**要求ポート番号**」などは、プロパティー・ファイルに含められます。当該フィールドの簡単な説明やキーワードが組み込まれます。以下に例を示します。

```
#     ----------------------------------------------------------------------
#     ... 要求ポート番号
#         Port of the automation adapter to receive requests from the host using
#         the adapter
adapter-request-port=2001
#
```

プロパティー・ファイルを編集するには、変更する値に関連するキーワードを見つけて、値を上書きします。

必要なキーワードの値にブランクを設定したり、そのキーワードをコメント化したりした場合は、ターゲット構成ファイルに定義されている値が変更されないままになります。

注 :

1. 1 つのキーワードを複数回指定した場合は、ファイル内の最後のオカレンスの値が使用されます。
2. 各値は、単一行で指定する必要があります。

サイレント・モードでの出力

サイレント・モードで構成ツールによって生成された出力を検査します。

構成ツールをサイレント・モードで開始した場合の出力は、構成ダイアログによって表示される出力とほぼ一致します。下記の出力タイプが生成される可能性があります。

更新なし
There are no configuration updates to be saved. 全ターゲット構成ファイル内のすべてのパラメーターが、指定したサイレント入力パラメーターと既に一致している。 サイレント入力パラメーターの検査時にエラーが検出されなかった。追加情報がある場合や、警告状態が検出される場合は、その情報および警告が報告されます。 警告が報告される場合、構成ツールは戻りコード「0」ではなく「1」を出します。サイレント構成を開始するときに (例えばシェル・スクリプト内で) この動作を監視する必要があるかもしれません。

正常終了
1 つ以上のターゲット構成ファイルが更新され、すべての構成ファイルおよびそれらの更新状況がリストされます。サイレント入力パラメーターの検査時にエラーは検出されません。追加情報がある場合や、警告状態が検出される場合は、その情報および警告が報告されます。 警告が報告される場合、構成ツールは戻りコード「0」ではなく「1」を出します。サイレント構成を開始するときに (例えばシェル・スクリプト内で) この動作を監視する必要があるかもしれません。

非正常終了
いずれのターゲット構成ファイルも更新されていません。サイレント入力パラメーターの検査時に検出されたエラーがすべて報告されます。戻りコード「2」が返されると、構成ツールは終了します。

サイレント入力プロパティー・ファイルの生成
ターゲット構成ファイルの値が、入力ファイルの生成に使用されています。いずれのターゲット構成ファイルも更新されていません。

回復不能エラー
エラーが報告された理由を示すエラー・メッセージ。「2」より大きい戻りコードが返されると、構成ツールは終了します。

ネットワーク・インターフェース障害の検出

単一ノードまたは 2 ノード・クラスターを実行している場合は、ネットワーク・インターフェースの障害を検出するには追加の構成が必要です。

クラスター・ソフトウェアは、定期的にクラスターの各ネットワーク・インターフェースへの接続を試みます。2 ノード・クラスターの一方のノード上でインターフェースに接続しようとして失敗すると、もう一方のノード上の対応するインターフェースにもオフラインのフラグが立てられます。オフラインのフラグが立てられるのは、そのピアから応答を受け取らなくなるためです。

この動作を回避するには、クラスター・ソフトウェアを、クラスター外のネットワーク・インスタンスに接続するよう構成する必要があります。インターフェースが存在するサブネットのデフォルト・ゲートウェイを使用できます。

各ノードで、次のファイルを作成します。

```
/var/ct/cfg/netmon.cf
```

このファイルの各行には、外部ネットワーク・インスタンスのシステム名または IP アドレスが含まれます。IP アドレスは、小数点付き 10 進数のフォーマットで指定することができます。

`netmon.cf` ファイルの例:

```
#This is default gateway for all interfaces in the subnet 192.168.1.0
192.168.1.1

# This is default gateway for all interfaces in the subnet 192.168.2.0
gw.de.ibm.com
```

Power Systems での仮想化イーサネットの使用

ネットワーク・アダプターの状態に関する判断は、ローカル・アダプターで何らかのネットワーク・トラフィックが見られるかどうかに基づいて行われます。例えば、ローカルまたはリモートのアダプターが故障しているかどうかなどです。ネットワーク・トラフィック は、インターフェースのインバウンド・バイト数に反映されます。

仮想入出力 (VIO) が関係している場合、このテストは、信頼できなくなります。これは、 インバウンド・トラフィックが VIO サーバーからのものなのかクライアントからのものなのかを区別できないためです。LPAR は、仮想アダプターと実際のアダプターを区別できません。この問題に対処するために、netmon ライブラリーでは、 ローカル・ネットワーク・アダプターごとに 32 個までのターゲットをサポートします。このいずれかのターゲットに対する ping が可能であれば、ローカル・アダプターは稼働しているとみなされます。ターゲットは、netmon.cf ファイルに !REQD キーワード を使用して指定できます。

```
!REQD <owner><target>
```

- !REQD: ストリング値。先行スペースなし。常に行の先頭に配置します。
- <owner>: インターフェースを指定します。<owner> は、アダプターをモニターし、<owner> の下の行に定義されているいずれかのターゲットに対する ping が可能であるかどうかに基づいた状況を判別します。<owner> は、ホスト名、IP アドレス、 またはインターフェース名で指定できます。ホスト名または IP アドレスを指定する場合は、開始名または IP アドレスを参照する値である必要があります。サービス別名は許可されません。ホスト名を指定する場合は、IP アドレス に解決可能なものでなければなりません。そうでない場合、その行は無視されます。!ALL キーワードは、すべてのアダプターを指定します。
- <target>: <owner> の ping 先の IP アドレス またはホスト名です。netmon.cf 項目として使用できるためには、 ホスト名のターゲットは、IP アドレスに解決できる必要があります。

z/VM で稼働する Linux on System z 上での実行

netmon.cf ファイルを作成することに加えて、z/VM 環境の Linux on System z 上で System Automation for Multiplatforms を実行する場合は、すべての通信グループのブロードキャストをオフにします。RSCT ハートビート機構は、ネットワーク・インターフェース・アダプターが使用不可の場合は特に、ブロードキャスト ping を時々実行します。この機能の目的は、このブロードキャスト ping を送信するネットワーク・インターフェース・アダプターがまだ操作可能かどうかを調べることです。他のシステムがこのブロードキャスト ping に応答するかどうかを検査します。 netmon.cf ファイルが正しくセットアップされていれば、この機能は必要ありません。その場合、使用可能かどうかを検査するべき既知のネットワーク・インターフェース・アダプターが他にもあります。スタンドアロン・システム上のブロードキャスト ping はパフォーマンス問題を引き起こしませんが、システムを z/VM 環境で実行している場合、ブロードキャスト ping はパフォーマンスに否定的影響を与えます。このようなパフォーマンスへの影響が発生するのは、z/VM の下、および同じネットワーク・セグメント (同じ IP ネットワークとネットマスク) 内で実行されている他のすべてのシステムが、このブロードキャスト ping 要求に応答するためです。この結果、活動停止中で現在ページアウトされている VM ゲスト・システムでさえ、この ping に応答するためにのみ z/VM にロードされます。そのため、z/VM の下で実行しているゲスト・システムの数によっては、z/VM システム全体のパフォーマンスが低下する可能性があります。

パフォーマンスに対する否定的影響を防ぐためには、セットアップを次のように変更します。

- クラスターのすべての通信グループを取得する。

  ```
  # lscomg
  ```

- すべての通信グループに対してブロードキャストをオフにする。

  ```
  # chcomg -x b <communication group> ...
  ```

  以下に例を示します。

  ```
  chcomg -x b CG1
  ```

- 再び **lscomg** コマンドを使用して、ブロードキャストがオフになっていることを検査する。

ディスク・ハートビートの使用可能化

ディスク・ハートビートを使用可能にして、クラスター環境内のデータ保全性を確保できます。

ディスク・ハートビートでは、ネットワーク障害とノード障害を区別することができるため、ディスク・ハートビートを使用すると、クラスター分割が発生する可能性を減らすことができます。

ネットワーク障害は、87 ページの図 15 に示すように、ノード間および 1 つのノードから共有ディスクへのネットワーク接続が失敗した場合に発生します。

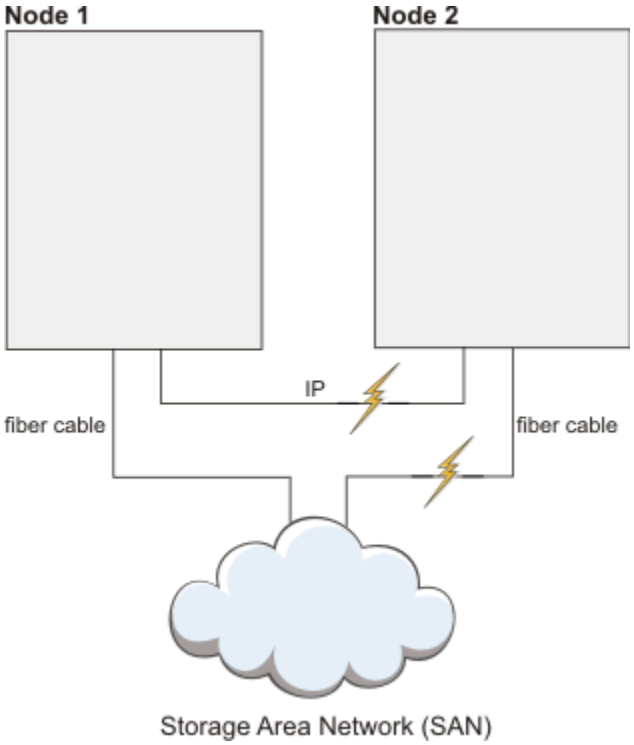


図 *15. 2* つのノードと共有ディスクの場合のネットワーク障害

88 ページの図 16 に示すように、1 つのノードがこれ以上到達できない場合にノード障害が発生します。

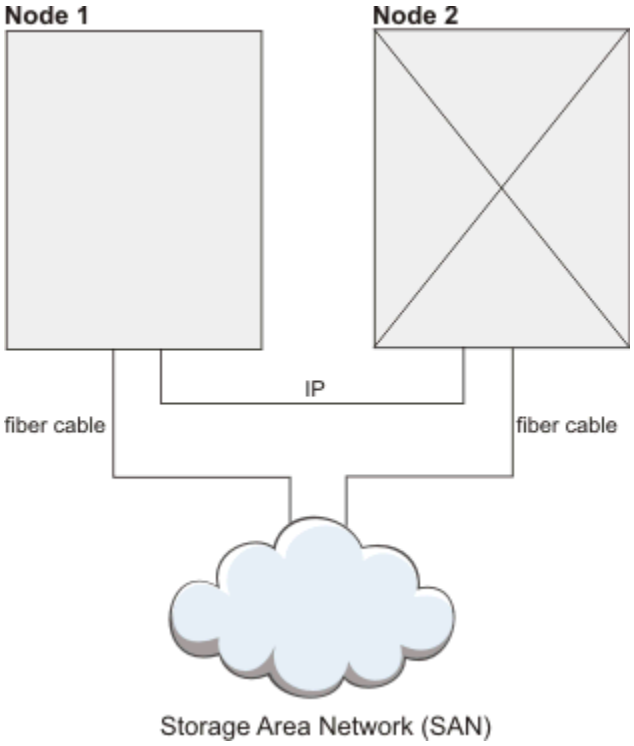


図 *16. 2* つのノードと共有ディスクの場合のノード障害

クラスター分割を回避できる場合、クリティカル・リソースの保護は必要ありません。システムをリブートする必要はありません。データ保全性の問題も回避されます。

クラスター分割が発生した場合、ハートビートを発信しているディスクにアクセスできなくなった ノードは、重要データにもアクセスできなくなります。クリティカル・リソースの保護は、データの破壊を防ぐのに役立ちます。ディスク・ハートビートは、ディスクにアクセスできないノードがデータを変更できないため、クリティカル・リソース保護ルールの緩和を許可します。

注 :

1. ディスク・ハートビート機能は、ピア・ドメインが既にオンラインである場合に限って使用可能にすることができます。
2. ディスク・ハートビート機能は、2 つのノード間にのみ定義できます。3 個以上のノードの場合は、各ペアを個別に接続する必要があります。

適切な物理ボリューム、論理ボリューム、または Linux 上のマルチパス・デバイスを見つけます。このボリューム上のデータが消去されます。次のコマンドを使用して、ハートビート・インターフェース・リソースを作成します。

```
CT_MANAGEMENT_SCOPE=2
mkrsrc IBM.HeartbeatInterface attributes [Force=0|1]
```

属性

名前
36 文字までの任意の名前。

DeviceInfo
有効なディスク ID またはボリューム ID:

- /dev/hdisk: ロー・ディスク
- LVID: 論理ボリューム
- MPATH: マルチパス・デバイス
- PVID: 物理ボリューム

CommGroup
IBM.CommunicationGroup にあるインスタンスの名前。Force パラメーターが 1 の場合に作成されます。

NodeNameList
このハートビート・インターフェースのノード・ペアであり、例えば、{'node1','node2'} です。

MediaType
2 (ディスク)

ハートビート・リングごとに通信グループが 1 つ作成されます。これは、 標準的なネットワーク・ベースのハートビート機能でも同じです。通信グループは、 ハートビート・デバイスと一緒に作成されます。 通信グループは、ネットワーク・ベースのグループ同様に調整 できます。ディスク・ハートビート機能では、PingGracePeriodMilliSec は変更できません。

セットアップしたディスク・ハートビートを確認するには、以下のタスクを実行します。

- システム・セットアップの構成で、ディスク・ハートビート機能に使用されるディスクがピア・ノードによって予約されていないことを確認します。
- ディスク・ハートビート機能は、以下のコマンドを使用してテストできます。

```
dhb_read -p <device-name> -t    # run it on a sender side
dhb_read -p <device-name> -r      # run it on a receiving side
```

  総合的な検証のためには、送信側ノードと受信側ノードを交換して、これらのコマンドを再実行してください。テストが動作しない場合は、ディスク予約のためサポートされていない可能性があるか、あるいはシステム・セットアップまたは構成の互換性がありません。
- ノード間で以下のシステム・コールが正しく動作することを確認します。

```
open("<dev>", O_RDWR|O_DIRECT), pread() and pwrite();
```

クリティカル・リソースの保護 (Dead-Man-Switch)

高可用性環境で Dead-Man-Switch (DMS) を使用可能にします。

高可用性環境においては、多くて 1 つのクリティカル・リソースのインスタンスが実行されていることが重要です。クリティカル・リソースの代表的な例として、共有ディスクに対する書き込み権限があります。一度に複数のノードに書き込み権限が与えられると、ファイル・システム構造が完全に破壊されます。

RSCT ConfigRM のクォーラム・アルゴリズムは、このシナリオの発生を防ぎます (ConfigRM、HATS、および HAGS にそれぞれの計算を実行するための十分なシステム・リソースが与えられた場合)。プロセスの長時間の停止やデッドロックなどの理由から、クリティカル・リソースの処理のために、これらの RSCT インフラストラクチャー・コンポーネントに依存できなくなった場合に、DMS が効力を発揮します。DMS には、一定の期間内に定期的にアクセスする必要があります。アクセスに失敗すると、オペレーティング・システム・カーネルが即時システム・リスタートをトリガーして、クリティカル・リソースが 2 度開始されないようにします。

Linux システムでは、この機能は reboot と halt システム・コール、および softdog モジュールを使用して実装されます。AIX では、この目的のために、デバイス・ドライバー haDMS が使用されます。

作動クォーラムの値

クォーラムを失ったサブクラスター上でクリティカル・リソースがアクティブな場合、ConfigRM がシステムを停止させる方法を決定します。各ノード上で CritRsctProtMethod 属性を使用して、6 つの異なる保護方法を構成することができます。

以下の表に、CritRsctProtMethod 属性の各値がどのシステム終了方法を表すかを示します。

表 24. 作動クォーラムの保護方式		
意味	**値**	
オペレーティング・システムをハード・リセットし、再始動する (デフォルト)	1	
オペレーティング・システムを停止する	2	
オペレーティング・システムを同期あり (sync) でハード・リセットし、再始動する	3	
同期あり (sync) で停止する	4	
保護なし。システムは作動を続行する	5	
RSCT サブシステムを終了して再始動する	6	

IPv6 サポートの使用可能化

IPv6 と System Automation を組み合わせて使用するには、IPv4 および IPv6 用にオペレーティング・システムをセットアップする必要があります。通常の RSCT クラスター操作では、IPv4 接続を使用しますが、IBM.ServiceIP リソースは IPv6 アドレスを使用するように定義できます。

このタスクについて

RSCT および System Automation for Multiplatforms で IPv6 サポートを使用可能にするには、次のコマンドを実行します。

```
chrsrc -c IBM.NetworkInterface IPv6Support=1
```

chrsrc コマンドによって、IPv6 対応インターフェース用の IBM.NetworkInterface リソースも作成されます。これで、物理インターフェースごとに、IPv4 用に 1 つと IPv6 用に 1 つ の 2 つの IBM.NetworkInterface リソースが存在するようになりました。IPv6 アドレスを使用する IBM.ServiceIP リソースの作成方法の例は、System Automation for Multiplatforms 管理者とユーザーのガイドを参照してください。 IPv6 で使用する Netprefix という新規 IBM.ServiceIP クラス属性が定義されています。

非 root ユーザー・アカウントでの自動化アダプターのセットアップ

デフォルトでは、System Automation for Multiplatforms のエンドツーエンド自動化アダプターは、root ユーザーで実行されます。非 root ユーザーで実行されるようにアダプターをセットアップする方法について説明します。

非 root ユーザーでアダプターをセットアップする前に、root ユーザー・アカウントを使用してアダプターの構成とセットアップを行う必要があります。

- システム自動化ドメインを作成して開始する。
- cfgsamadapter ユーティリティーを使用してアダプターを構成する。
- System Automation Application Manager との SSL 接続を構成する (オプション)。
- System Automation Application Manager オペレーション・コンソールを使用してアダプターの機能を確認する。

上記のステップをあらかじめ処理しておくと、アダプターの非 root セットアップのステップは 1 回処理するだけで済みます。

アダプターの非 root セットアップは、以下のステップから構成されます。

1. オペレーティング・システム固有のセキュリティーの準備処理を実行します (アダプターの専用ユーザーや専用グループの作成など)。手動で処理する必要がある、対応するアクションの説明については、91 ページの『特定のオペレーティング・システム用のセキュリティーのセットアップ』を参照してください。
2. デフォルト・インストールで作成された特定のファイルとディレクトリーのグループ所有権とアクセス権を変更します。アダプター・ユーザーに対して適切な System Automation と RSCT のアクセス権を設定します。このステップに関連するアクションは、スクリプト `setupAdapterNonRoot.sh` を使用して、自動的に実行されます。このスクリプトによって処理されるすべてのアクションについては、92 ページの『非 root ユーザー・アダプター・セットアップ・スクリプトの実行』のトピックを参照してください。

特定のオペレーティング・システム用のセキュリティーのセットアップ

スクリプト `setupAdapterNonRoot.sh` を起動する前に必要な、オペレーティング・システム固有のセキュリティーの準備について説明します。すべてのクラスター・ノードで、このセクションで説明しているアクションを実行します。

ユーザーおよびグループ・アカウントの作成

各クラスター・ノードで同じグループおよびユーザー・アカウントを作成する必要があります。これらは、スクリプト `setupAdapterNonRoot.sh` への入力パラメーターとして渡されます。

アダプター・ユーザー・アカウントの 1 次グループとなるグループを作成します。以下のセクションでは、グループ名 `sagroup` を使用します。他の任意の名前でも有効です。`sagroup` は、System Automation for Multiplatforms のいくつかのファイルおよびディレクトリーのグループ所有権を変更することで、アダプター・ユーザー・アカウントにアクセス権限を付与する場合に使用されます。System Automation for Multiplatforms バージョン 4.1.0.4 以上では、新しいオプション「**--manage-group**」を使用すると、スクリプト「setupAdapterNonRoot.sh」によってもグループを作成できます。

グループ ID `sagroup` をユーザーの 1 次グループとして使用してアダプターを実行するためのユーザー・アカウントを作成します。以下のセクションでは、ユーザー名 `samadapt` を使用します。`samadapt` ユーザー・アカウントは、ログイン・シェルで使用することを意図しないテクニカル・ユーザー・アカウントにすることができます。この場合、パスワードは不要です。ユーザーのホーム・ディレクトリーが存在し、正しいアクセス権限が設定されているようにしてください。

`samadapt` ユーザーは、System Automation for Multiplatforms 管理者またはオペレーターのいずれかにすることができます。適切な権限をセットアップするために、123 ページの『第 5 章 保護』に示されている指示に従う必要があります。

オペレーターの場合は、ロール `sa_operator` を割り当てます。管理者の場合は、ロール `sa_admin` を割り当てます。`sa_operator` ロールを使用した場合、アダプターはリソースおよびリソース・グループを開始および停止できます。`sa_admin` ロールを使用した場合、さらにポリシーのアクティブ化および非アクティブ化を行うことができます。

注 : システム自動化の管理および操作のために追加の非 root ユーザーを使用可能にする場合は、123 ページの『第 5 章 保護』を参照してください。それらのユーザーにもグループ `sagroup` を使用します。

ユーザー認証が使用可能になっている場合の構成ステップ

自動化アダプターの構成で Pluggable Authentication Modules (PAM) を使用したユーザー認証が使用可能になっている場合は、追加の構成ステップを実行する必要があります。

Linux 固有 (SLES)

`samadapt` ユーザー・アカウントをシャドー・グループ ID に追加して、ユーザーおよびその暗号化パスワードを保持するファイル `/etc/shadow` を `samadapt` が読み取ることができるようにする必要があります。ファイル `/etc/shadow` の所有権は `root:shadow` であり、標準許可ビット設定は 640 です。非 root ユーザー・アカウントからの PAM (Pluggable Access Module) ユーザー認証を可能にするには、`/etc/shadow` にアクセスできる必要があります。System Automation Application Manager 自動

化エンジンまたはオペレーション・コンソールから System Automation for Multiplatforms ドメインにアクセスする際にユーザー資格情報を検証するために PAM が使用される場合に、これが発生します。

AIX 固有

samadapt ユーザー・アカウントを security グループ ID に追加して、samadapt が PAM 機能を使用してディレクトリー /etc/security にアクセスできるようにする必要があります。これは、System Automation Application Manager 自動化エンジンまたはオペレーション・コンソールから System Automation for Multiplatforms ドメインにアクセスする際にユーザー資格情報を検証するために必要です。さらに、ファイル /etc/security/password の ACL 設定を変更する必要があります。

AIX では、ファイル /etc/security/passwd にユーザー・アカウントおよびその暗号化パスワードが含まれています。ファイル /etc/security/passwd の所有権は root:security であり、標準許可ビット設定は 600 です。この設定により、samadapt ユーザー・アカウントからのアクセスは、このユーザー・アカウントがセキュリティー・グループのメンバーであっても拒否されます。ファイルの ACL を変更することで、所有権および許可ビットを変更せずに、アクセス権限を付与できます。

ACL を変更するには、acledit または aclget/aclput ユーティリティーを使用します。 出力例を以下に示します。

```
*
* ACL_type   AIXC
*
attributes:
base permissions
    owner(root):  rw-
    group(security):  ---
    others:  ---
extended permissions
    enabled                      <== enable extended permissions
    permit   r--     u:samadapt  <== permit read access to samadapt
```

これらの変更を、前に適用されたその他の変更とマージします。

samadapter ユーザー・アカウントを System Automation Application Manager が使用できるようにする

自動化アダプターのユーザー認証が使用可能になっていて、System Automation Application Manager から System Automation for Multiplatforms クラスターへのアクセスに samadapt ユーザー・アカウントを使用する場合は、このユーザー ID のパスワードを設定する必要があります。その資格情報を指定すると、cfgeezdm 構成ユーティリティーで第 1 レベル自動化ドメインにアクセスできます。あるいは、資格情報を使用して、System Automation Application Manager オペレーション・コンソールからドメインにアクセスすることができます。

非 root ユーザー・アダプター・セットアップ・スクリプトの実行

非 root アダプター・セットアップの残りのアクションを行うために、スクリプト setupAdapterNonRoot.sh を実行します。

このスクリプトは、ディレクトリー /opt/IBM/tsamp/sam/bin にあります。スクリプトを実行する前に、以下の条件を満たしている必要があります。

- 4.1 より低いバージョンからバージョン 4.1 に System Automation for Multiplatforms をアップグレードした場合、クラスター内のすべてのノードが新しいバージョンにアップグレードされていること。クラスターのマイグレーションが完了していること。コマンド samctrl –m が正常に実行されていること。
- アダプターが停止している。
- System Automation for Multiplatforms バージョン 4.1.0.3 以下の場合、91 ページの『特定のオペレーティング・システム用のセキュリティーのセットアップ』に説明されている手動ステップが正常に完了していることを確認すること。
- システム自動化クラスターが定義されていること。ただし、クラスターを停止する必要はありません。セットアップ・ステップは、クラスター操作に干渉しません。

すべてのクラスター・ノードでスクリプト setupAdapterNonRoot.sh を実行します。

このスクリプトには、インストールされている製品バージョンに基づいて異なるバージョンがあり、必要とする前提条件と機能が異なります。次の使用情報とサンプル出力は、System Automation for Multiplatforms 4.1.0.0 からバージョン 4.1.0.3 までに含まれているスクリプトに該当します。

```
名前
setupAdapterNonRoot.sh  - 非 root ユーザー・アカウントを使用して実行されるように
エンドツーエンド自動化アダプターを構成します。

概要
      setupAdapterNonRoot.sh [-x] userName [groupName]

説明
      非 root ユーザー・アカウントを使用して実行されるようにエンドツーエンド自動化アダプターを
構成するためのスクリプト。
      このアダプターは、RSCT セキュリティー定義の他にグループ所有権および権限を調整します。

オプション
      -x  sa_admin 役割に対する ACL 権限を設定します。Optional, if omitted, the default is to set ACL
          permissions for the sa_operator role.

パラメーター
      userName  - アダプターを実行する必要があるユーザー・アカウント名。
      groupName - アダプター・ユーザー・アカウントの 1 次グループ名。

終了コード
    0 すべての構成が正常に完了しました (all configurations completed successfully)
    1 少なくとも 1 つの構成タスクが失敗しました (at least one configuration task failed) - 出力で詳細を確認してくだ
さい。
    2 前提条件を満たしていません (prerequisites not satisfied) - 出力で詳細を確認してください。
```

root 権限を持つユーザーとしてスクリプトを実行します。

前提条件の検査
クラスターが存在するかどうか、自動化アダプターが停止しているかどうか、およびユーザー・アカウントが存在するかどうかが検査されます。指定したグループがユーザー・アカウントの 1 次グループかどうかも検査されます。

グループの所有権とアクセス権の変更
いくつかのファイルとディレクトリーは、最初は root ユーザーのみがアクセスできるように作成されるため、それらの所有権とアクセス権を変更する必要があります。詳しくは、95 ページの『グループの所有権とアクセス権の変更』を参照してください。

注 : スクリプトは、ファイル `/etc/ibm/tivoli/common/cfg/log.properties` を所有するグループを変更します。 このファイルは、他の Tivoli 製品でも使用されることがあります。これらの製品のいずれかが非 root ユーザー・アカウントでも実行される場合、それらの製品で `log.properties` ファイルが引き続き読み取り可能であることを確認してください。

適切な System Automation と RSCT のアクセス権の設定
非 root ユーザー・アカウント `samadapt` が RSCT Resource Management Control (RMC) を使用できるようにするために、`/var/ct/cfg/ctrmc.acls` ファイルを使用してアクセス権を付与する必要があります。詳しくは、96 ページの『適切な System Automation と RSCT のアクセス権の設定』を参照してください。

自動化アダプター構成の調整
非 root のユーザーとグループが、アダプターの構成プロパティーに追加されます。詳しくは、97 ページの『自動化アダプター構成の調整』を参照してください。

出力例:

```
root@p6sa13 /opt/IBM/tsamp/sam/bin# ./setupAdapterNonRoot.sh -x samadapt
-------------------------------------------------------------------------------
Checking userid samadapt.
Group not set as parameter. Retrieving the primary group for user samadapt.
-------------------------------------------------------------------------------
Checking group sagroup for userid samadapt.
User account samadapt and group sagroup verified successfully. Continuing...
-------------------------------------------------------------------------------
Checking whether a Peer Domain exists  ...
Peer domain exists. Continuing ...
-------------------------------------------------------------------------------
```

```
Checking whether adapter exists and is offline ...
samadapter is not running.
Adapter exists and is offline. Continuing ...
--------------------------------------------------------------------------------
Checking for a previous non-root adapter setup ...
--------------------------------------------------------------------------------
Change various permissions. Press enter to continue ...

PolicyPool is /etc/opt/IBM/tsamp/sam/policyPool
Tivoli Common Directory is /var/ibm/tivoli/common
KeyStore not set.
TrustStore not set.
--------------------------------------------------------------------------------
Replacing the DEFAULT stanza in file /var/ct/cfg/ctrmc.acls. Press enter to continue ...

Adding the following entires to the DEFAULT Stanza of /var/ct/cfg/ctrmc.acls
DEFAULT
   samadapt@0xc3d084925f78e253   *   rw
--------------------------------------------------------------------------------
The command 'refresh -s ctrmc' will now be issued. Press enter to continue ...

0513-095 The request for subsystem refresh was completed successfully.
--------------------------------------------------------------------------------
Adapting the file sam.adapter.properties
 Press enter to continue ...

Replacing lines in property file
--------------------------------------------------------------------------------
All configurations have been completed successfully.
Run this script, including user account and group preparations on all nodes of the cluster.
If this was the last node of the cluster where you ran the script, you may now start the adapter.
```

次の使用情報とサンプル出力は、System Automation for Multiplatforms バージョン 4.1.0.4 以上に含まれているスクリプトに該当します。

```
Synopsis:
   setupAdapterNonRoot.sh [-h] [--local] [--manage-group]
                          [-x|--sa-admin][-g|--group <groupName>]
                    userName

 説明
  非 root ユーザー・アカウントを使用して実行されるようにエンドツーエンド自動化アダプターを
構成するためのスクリプト。
  このアダプターは、RSCT セキュリティー定義の他にグループ所有権および権限を調整します。

パラメーター
  userName - the name of the user account that is used to start the adapter.

終了コード
  0 すべての構成が正常に完了しました (all configurations completed successfully)
  1 at least one configuration task failed
  2 prerequisites not satisfied

Options:
  -h               Print this help.
  -g or --group <groupName> The name of the primary group for the specified user account. (default:
group name = sagroup)
  --local             Run script only on local node. Optional, if omitted, the default is to perform
changes on all cluster nodes.
  --manage-group         Create local UNIX group (if group does not exist) and add specified user to
this group.
                            Set group as primary group for the user. If omitted, the default is to not
make any changes to group and user.
  -x or –sa-admin        Set ACL permissions for the sa_admin role.Optional, if omitted, the default is
to set ACL permissions for the sa_operator role.
```

root 権限を持つユーザーとしてスクリプトを実行します。

前提条件の検査

クラスターが存在するかどうか、自動化アダプターが停止しているかどうか、およびユーザー・アカウントが存在するかどうかが検査されます。指定したグループがユーザー・アカウントの 1 次グループかどうかも検査されます。

グループの所有権とアクセス権の変更
いくつかのファイルとディレクトリーは、最初は root ユーザーのみがアクセスできるように作成されるため、それらの所有権とアクセス権を変更する必要があります。詳しくは、95 ページの『グループの所有権とアクセス権の変更』を参照してください。

注 : スクリプトは、ファイル /etc/ibm/tivoli/common/cfg/log.properties を所有するグループを変更します。 このファイルは、他の Tivoli 製品でも使用されることがあります。これらの製品のいずれかが非 root ユーザー・アカウントでも実行される場合、それらの製品で log.properties ファイルが引き続き読み取り可能であることを確認してください。

適切な System Automation と RSCT のアクセス権の設定
非 root ユーザー・アカウント samadapt が RSCT Resource Management Control (RMC) を使用できるようにするために、/var/ct/cfg/ctrmc.acls ファイルを使用してアクセス権を付与する必要があります。詳しくは、96 ページの『適切な System Automation と RSCT のアクセス権の設定』を参照してください。

自動化アダプター構成の調整
非 root のユーザーとグループが、アダプターの構成プロパティーに追加されます。詳しくは、97 ページの『自動化アダプター構成の調整』を参照してください。

```
Usage Examples
  1) Configure SA MP adapter to run with non-root user "saoperator" and group "sagroup"
      ("sagroup" already exists).
     Prerequisites:
     - User "saoperator" and group "sagroup" exist.
     - "sagroup" is the primary group for user "saoperator"

     Setup adapter non-root:
     # setupAdapterNonRoot.sh -g sagroup saoperator
     Result:
     - Configured SA MP adapter non-root user "saoperator" on all cluster nodes

  2) Configure SA MP adapter to run with non-root user "saoperator" and group "sagroup"
      ("sagroup" does not exist).
     Prerequisites:
     - User "saoperator" exists.
     Setup adapter non-root:
     # setupAdapterNonRoot.sh --manage-group -g sagroup saoperator
     Result:
     - Group "sagroup" is created on all cluster nodes
     - User "saoperator" is added to group "sagroup" on all cluster nodes
     - "sagroup" is set as primary group for user "saoperator" on all cluster nodes
     - Configured SA MP adapter non-root user "saoperator" on all cluster nodes
  3) Remove SA MP adapter non-root user configuration
     Prerequisites:
     - SA MP adapter non-root user is configured
     Remove adapter non-root setup
     AIX:
     # setupAdapterNonRoot.sh -g system root
     Linux:
     # setupAdapterNonRoot.sh -g root root
     Result:
     - SA MP adapter non-root user configuration is removed on all cluster nodes
```

グループの所有権とアクセス権の変更

スクリプト setupAdapterNonRoot.sh は、グループ sagroup を使用して、System Automation for Multiplatforms のファイルおよびディレクトリーのグループ所有権に各種変更を適用します。ユーザー ID を所有しているファイルは変更されません。必要に応じて、アクセス権限もグループ・レベルで変更されます。

ファイル・システムに対して行われる変更は、以下のとおりです。

- アダプターがキャッシュ・ディレクトリー /var/opt/IBM/tsamp を読み取り/書き込みできるようにします。
- ファイル /etc/ibm/tivoli/common/cfg/log.properties のアクセス権および所有権を変更します。 これには、アダプターによって使用される Tivoli 共通ディレクトリーのロケーションが含まれています。

- Tivoli 共通ディレクトリーへの読み取り/書き込み/操作権限を付与します。ディレクトリー名は、ファイル /etc/ibm/tivoli/common/cfg/log.properties に保管されています。 デフォルトのディレクトリーは /var/ibm/tivoli/common です。
- ディレクトリー /etc/opt/IBM/tsamp/sam/cfg および /etc/Tivoli/tec でのアダプターの構成ファイルの読み取りを許可します。
- アダプター・ポリシー・プールへのアクセス権限を付与します。ロケーションは、cfgsamadapter ツールを使用して構成できます。デフォルトのディレクトリーは、/etc/opt/IBM/tsamp/sam/policyPool です。
- /opt/IBM/tsamp/sam/bin と /usr/sbin/rsct/bin 内のアダプター・バイナリー・ファイル、および /opt/IBM/tsamp/sam/lib 内の関連 JAR ファイルのグループを変更します。

詳しくは、setupAdapterNonRoot.sh スクリプト・ソースを参照してください。

適切な System Automation と RSCT のアクセス権の設定

非 root ユーザー・アカウント samadapt が RSCT Resource Management Control (RMC) を実行できるようにするために、スクリプト setupAdapterNonRoot.sh は、/var/ct/cfg/ctrmc.acls ファイルを使用してアクセス権を付与します。System Automation バージョン 4.1.0.4 以上でこのスクリプトを使用すると、ファイル /var/ct/cfg/ctsec_map.global も調整されます。

RSCT セキュリティーについて詳しくは、RSCT テクニカル・リファレンス・マニュアルを参照してください。このマニュアルは、システム自動化配布物とともにパッケージされています。

ctrmc.acls は、RSCT リソース・クラスのアクセス権限を記述した各種ブロック (スタンザ) で構成されています。また、DEFAULT スタンザの内容は、他のすべてのスタンザに追加されます。このスタンザは、ctrmc.acls 内に独自のスタンザを持たない RSCT リソース・クラスのデフォルトとして使用されます。アダプター非 root ユーザー・アカウントに対して RSCT リソース・クラスへのアクセス権限を付与するには、DEFAULT スタンザを変更します。

以下の Linux SLES の例は、ctrmc DEFAULT スタンザに追加された項目を示しています。

```
DEFAULT
root@LOCALHOST                  * rw
LOCALHOST                       * r
none:clusteruser                * r // added by preprpnode
none:root                       * rw // added by preprpnode
```

新しい項目のタイプは userid@RSCT-nodeid です。

userid
アダプターを実行するために作成した非 root ユーザー・アカウント。

RSCT-nodeid
各クラスター・ノード上の /var/ct/cfg/ct_node_id ファイルに含まれている RSCT nodeid。

各クラスター・ノードの項目は、既存の具体性の低い項目より優先されるように、DEFAULT スタンザの先頭に追加されます。

AIX オペレーティング・システムの DEFAULT スタンザが、Linux の例よりもはるかに大きいことがあります。ただし、行う変更はまったく同じです。

ローカル・システムのユーザーを RSCT ユーザーにマップするために、ファイル ctsec_map.global が使用されます。その内容は次のとおりです。

```
unix:root@<iw>=root
unix:root@<cluster>=root
unix:*@<cluster>=clusteruser
unix:root@<any_cluster>=any_root
hba2:root@<iw>=root
hba2:root@<cluster>=root
hba2:root@<any_cluster>=any_root
```

ctrmc.acls (および該当する場合は ctsec_map.global も) の変更後に、このファイルを再度読み取るように RSCT RMC をトリガーします。これを行うには、以下のコマンドを実行します。

```
refresh -s ctrmc
```

スクリプト setupAdapterNonRoot.sh の実行後に、正しい変更が行われているか、ctrmc.acls (および該当する場合は ctsec_map.global も) の内容を確認します。

自動化アダプター構成の調整

アダプターは開始時に、非 root ユーザーおよびグループを認識している必要があります。

そのため、スクリプト setupAdapterNonRoot.sh は、アダプター構成プロパティー・ファイル /etc/opt/IBM/tsamp/sam/cfg/sam.adapter.properties に以下のパラメーターが含まれていることを確認します。

```
non-root-user=samadapt
non-root-group=sagroup
```

サービスおよび保守

フィックスパックをインストールした場合、またはノードをクラスターに追加した場合は、アダプターの非 root セットアップを適用するステップを部分的に繰り返す必要があります。

シナリオおよび繰り返す必要があるステップを以下に示します。

フィックスパックのインストール
System Automation for Multiplatforms フィックスパックをインストールすると、/opt/IBM/tsamp/sam ディレクトリー内のファイルおよび対応するグループ所有権とアクセス権が置き換えられることがあります。

ノードでフィックスパックをインストールした直後に、各ノードでスクリプト setupAdapterNonRoot.sh を再度実行します。初期起動と同じ入力パラメーターをスクリプトに対して指定します。

新規ノードの追加
preprpnode および addrpnode コマンドを使用して、ノードをクラスターに追加します。

ノードをクラスターに追加した後に、新しいノードで、91 ページの『特定のオペレーティング・システム用のセキュリティーのセットアップ』に記載されているステップを実行します。クラスターのすべてのノード (古いノードと新しいノード) で、92 ページの『非 root ユーザー・アダプター・セットアップ・スクリプトの実行』の説明に従って、スクリプト setupAdapterNonRoot.sh を実行します。以前のクラスター・ノードでの初期起動と同じ入力パラメーターをスクリプトに対して指定します。

非 root アダプター・ユーザー ID の変更

非 root アダプター・セットアップに使用されるユーザー ID を変更する場合は、既存のセットアップを削除します。その後、新規ユーザーのセットアップを定義できます。

既存のセットアップを削除するには、次のパラメーターを指定してスクリプト setupAdapterNonRoot.sh を実行します。System Automation for Multiplatforms バージョン 4.1.0.0 から 4.1.0.3 の場合、次のコマンドを使用します。

```
setupAdapterNonRoot.sh -x root
```

次に、必要な新規ユーザー ID およびグループを使用してスクリプトを再度実行します。

System Automation for Multiplatforms バージョン 4.1.0.4 以上の場合、次のコマンドを使用します。

```
AIX:
setupAdapterNonRoot.sh -g system root
Linux:
setupAdapterNonRoot.sh -g root root
```

次に、必要な新規ユーザー ID およびグループを使用してスクリプトを再度実行します。

非 root アダプター・セットアップの削除

非 root アダプター・セットアップを削除するには、すべてのアクセス権および許可を root にリセットします。

以下のパラメーターを指定してスクリプト setupAdapterNonRoot.sh を実行します。

System Automation for Multiplatforms バージョン 4.1.0.0 から 4.1.0.3 の場合、次のコマンドを使用します。

```
AIX:
setupAdapterNonRoot.sh -x root system
Linux:
setupAdapterNonRoot.sh -x root root
```

System Automation for Multiplatforms バージョン 4.1.0.4 以上の場合、次のコマンドを使用します。

```
AIX:
setupAdapterNonRoot.sh -g system root
Linux:
setupAdapterNonRoot.sh -g root root
```

制限

制限は、System Automation for Multiplatforms ポリシー・プール内の XML ポリシーにアクセスするときに起こり得る問題に関連しています。クラスター内の他のノードに構成ファイルを複製するときに、制限される可能性があります。

非 root ユーザー・アカウントで読み取ることができないアクティブ・ポリシーを使用したアダプターの開始

ポリシーが XML ポリシー・ファイルからロードされている場合、いずれかのクラスター・ノードでコマンド・シェルから lssamctrl コマンドを入力すると、このファイルの名前とロケーションを表示できます。sampolicy -a コマンドは任意のロケーションのポリシー・ファイルを使用できるため、ポリシー・ファイルのロケーションは、ポリシー・プールであるとは限りません。

```
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 = Disabled
TraceLevel = 31
ActivePolicy = [/etc/opt/IBM/tsamp/sam/policyPool/nonRootAdapter-testuser-2.xml,20130415143902+0200,0]
CleanupList = {}
PublisherList = {}
```

この XML ポリシーファイルは存在するが、非 root ユーザー・アカウントで読み取ることができない場合があります。その場合、アダプターはそのノードで正常に開始できず、System Automation Application Manager への接続が確立されません。

解決方法: XML ポリシー・ファイルのアクセス権を変更するか、ファイルをポリシー・プールに移動してください。

ポリシー・プールからの System Automation for Multiplatforms ポリシーの読み取りおよびアクティブ化。samadapt がオペレーター・ロールを備えている場合、これは実行できません。

System Automation Application Manager オペレーション・コンソールから新規または変更された自動化ポリシーをアクティブにするには、samadapt ユーザー ID は、ポリシー・プール内の対応する XML ファイルを読み取るためのアクセス権を持っていなければなりません。所有権または許可ビット設定が適切ではない XML ポリシーは、オペレーション・コンソールの「ポリシーの選択」ダイアログに表示されません。

解決方法: 非 root セットアップ・ステップは、既存の XML ポリシー・ファイルの所有権およびアクセス権を調整します。後で (例えば、`sampolicy -s` コマンドを使用してポリシーを保存することで) ポリシー・プールに保管される XML ポリシー・ファイルには、適切なアクセス権を必ず設定してください。

構成ファイルの複製

`cfgsamadapter` ユーティリティーの「**複製**」機能を使用して、構成ファイルをクラスター内の他のノードに複製します。 複製されたファイルの一部には、root ユーザー ID のためにのみ書き込み権限が設定されます。そのため、root ユーザー ID を使用している場合しか「**複製**」機能を実行することができません。

解決方法: 複製の完了直後に、複製ターゲット・ノードで `setupAdapterNonRoot.sh` スクリプトを実行します。初期起動と同じ入力パラメーターをスクリプトに対して指定します。「**複製**」機能を使用する代わりに、`cfgsamadapter` を実行して、各クラスター・ノードで同じ構成変更を明示的に実行します。

第 4 章 統合

System Automation for Multiplatforms は、他の Tivoli アプリケーションと統合することにより、包括的なソリューションを提供します。Tivoli アプリケーションとご使用の環境を統合するには、既存のインフラストラクチャーに適合させるための特定の構成タスクが必要です。

以下の統合に必要な構成について説明します。

- System Automation for Multiplatforms イベントを IBM Tivoli Enterprise Console® (TEC) に転送する。
- System Automation for Multiplatforms イベントを IBM Tivoli® Netcool/OMNIbus に転送する。
- System Automation for Multiplatforms リソースとイベントからの情報で TBSM ビューを強化する。

イベント・コンソール

System Automation for Multiplatforms は、EIF イベントを Tivoli Enterprise Console (TEC) または Tivoli Netcool/OMNIbus (OMNIbus) のいずれかに送信します。TEC と OMNIbus は、着信イベントを処理するために中央サーバーを使用する、ルール・ベースのイベント管理アプリケーションです。

これらは、以下のさまざまなソースからアラームとイベントを収集します。

- Tivoli アプリケーション
- Tivoli パートナー・アプリケーション
- カスタマー・アプリケーション
- ネットワーク管理プラットフォーム
- リレーショナル・データベース・システム

IBM Tivoli System Automation for Multiplatforms では、以下の場合はイベントが生成され、TEC または OMNIbus イベント・コンソールに転送されます。

- IBM Tivoli System Automation for Multiplatforms の構成または自動化リソースの状態が変わった場合。
- 問題が発生した場合。

System Automation イベントを Tivoli Business Service Manager (TBSM) で使用するには、イベントを OMNIbus に転送する必要があります。

IBM Tivoli System Automation for Multiplatforms は、以下のイベントのタイプを生成できます。

表 *25. System Automation Application Manager* イベント・クラス・タイプ

イベント・クラス/アラート・グループ	**説明**
SystemAutomation_Resource_Status_Change	自動化リソースの状況が変更されました。
SystemAutomation_Resource_Configuration_Change	新規の自動化リソースが追加されたか、既存のリソースが削除または変更されました。
SystemAutomation_Relationship_Configuration_Change	新規の関係が追加されたか、既存の関係が削除または変更されました。
SystemAutomation_Domain_Status_Change	ドメインの状況が変更されました。例: • ドメインの自動化マネージャーまたは自動化アダプターが開始または停止した。 • 新規の自動化ポリシーがアクティブになった。
SystemAutomation_Request_Configuration_Change	新規の要求が自動化リソースに対して発行されたか、既存の要求が取り消されました。

以下のトピックでは、イベントを TEC または OMNIbus に転送できるように IBM Tivoli System Automation for Multiplatforms とイベント・コンソールをセットアップする方法について説明します。

- IBM Tivoli System Automation for Multiplatforms で使用するよう OMNIbus をセットアップ: 102 ページの『Tivoli Netcool/OMNIbus』
- IBM Tivoli System Automation for Multiplatforms で使用するよう TEC をセットアップ: 110 ページの『Tivoli Enterprise Console』

任意のイベント・コンソールを準備したら、110 ページの『イベント生成の使用可能化』に説明されているようにイベント生成を有効にする必要があります。

Tivoli Netcool/OMNIbus

このセクションのトピックでは、System Automation イベントを OMNIbus イベント・コンソールに転送するよう IBM Tivoli Netcool/OMNIbus をセットアップする方法について説明します。 この OMNIbus のセットアップは、IBM Tivoli System Automation for Multiplatforms を Tivoli Business Service Manager と統合する場合の前提条件でもあります。

前提条件

System Automation for Multiplatforms は、通信に Tivoli Event Integration Facility (EIF) イベントを使用するため、以下のコンポーネントが必要です。

- IBM Tivoli Netcool/OMNIbus (OMNIbus)
- OMNIbus Probes Library for Nonnative Base
- OMNIbus Probe for Tivoli EIF (EIF Probe)。このプローブは、System Automation から送信された EIF イベントを受信して、ObjectServer に転送できます。

以下のバージョン以上が必要です。

- OMNIbus Probe for Tivoli EIF V.9.0
- IBM Tivoli Netcool/OMNIbus 7.2.1

注 : IBM Tivoli Netcool/OMNIbus V7.2.1 を実行している場合は、暫定修正 3 (7.2.1.5-IF0003) をインストールしてください。IBM Tivoli Netcool/OMNIbus V7.3 以降を実行している場合は、追加のフィックスパックは不要です。

IBM Tivoli Netcool/OMNIbus Knowledge Center で入手可能な資料に従って、これらのコンポーネントをインストールし、セットアップします。

環境変数

$NCHOME
パッケージがインストールされている Netcool® ホーム・ディレクトリーを参照します。Linux でのデフォルトのディレクトリーは `/opt/IBM/tivoli/netcool` です。

$OMNIHOME
`$OMNIHOME` 変数は、引き続き `$OMNIHOME` 環境変数を使用するスクリプト、サード・パーティーのアプリケーション、およびプローブのレガシー・サポートを提供するために使用されます。`$OMNIHOME` は `$NCHOME/omnibus` を参照します。

OMNIbus データベースのイベント・フィールド

OMNIbus `alerts.status` 表は、System Automation for Multiplatforms に固有の情報を保持するために、以下の新規の列で拡張されます。これらの列は、イベントの処理時に System Automation for Multiplatforms に固有の OMNIbus ルール・ファイルで入力されます。

表 *26.* リソース状況変更イベントで使用される *System Automation for Multiplatforms* 状況属性 *(alerts.status)*		
属性名	**Type**	**説明**
SADesiredState	varchar(16)	自動化リソースの自動化目標を反映した本来あるべき状態。可能な値を次に示します。 • オンライン • オフライン • NoChange これは、オペレーターがリソースの自動化目標を変更できないことを意味します。
SAObservedState	varchar(16)	自動化リソースの現在の監視状態。可能な値を次に示します。 • Unknown • オンライン • オフライン • Starting • Stopping • NotApplicable **注 :** TEC イベントでの `c_status_observed` に対応します。
SAOperationalState	varchar(255)	リソースの現行状態に関する詳細情報を提供する動作状態値のリスト。可能な値のリストについては、`SystemAutomation.baroc` ファイルを参照してください。 **注 :** TEC イベントでの `c_status_operational` に対応します。
SACompoundState	varchar(16)	リソースが要求どおりに動作しているか、またはエラーが発生しているかどうかを示す複合状態。可能な値を次に示します。 • OK • Warning • Error • Fatal **注 :** TEC イベントでの `c_status_compound` に対応します。

表 *27.* リソース、ドメイン、イベント *ID (alerts.status)*		
SADomainName	varchar(64)	自動化ドメインの名前。リソースを識別するリソース・キーの部分。 **注 :** TEC イベントでの `sa_domain_name` に対応します。

表 *27.* リソース、ドメイン、イベント *ID (alerts.status)* (続き)		

SAResourceName	varchar(255)	リソースの名前。これは、リソース・クラス (およびオプションのリソース・ノード) と連結されたリソース名自体で構成される複合リソース名です。名前部分と区切り文字の順序は、送信側の System Automation 製品によって異なります。
		SA MP および SA AM の場合:
		`<class_name>:<resource_name>:<node_name>`
		SA z/OS の場合:
		`<resource_name>:<class_name>:<node_name>`
		注 : <node_name> は、存在する場合のみ設定されます。System Automation Application Manager リソース参照の場合は、ノード名には、参照先の第 1 レベルの自動化ドメインの名前が含まれています。TEC イベントでの `sa_resource_name` に対応します。

SAEventReason	varchar(255)	イベント理由。TEC イベントでは、1 つのイベントに複数のイベント理由を指定できます。イベント理由の例は以下のとおりです。 • StatusCommonObservedChanged • ConfigurationDeleted • PreferredMemberChanged **注 :** TEC イベントでの `sa_event_reason` に対応します。
SAReferencedResource	varchar(255)	System Automation Application Manager エンドツーエンド・リソース参照の場合は、これには参照先リソース・キーが含まれています。

表 *28.* リソース状況変更イベントで使用されるその他の属性 *(alerts.status)*		
SAExludedFromAutomation	varchar(16)	リソースが自動化から除外される (例えば、自動化がサスペンドされている) かどうかを示すフラグ。リソース状況変更イベントで使用されます。 可能な値を次に示します。 • NotExcluded • Excluded **注 :** TEC イベントでの `sa_flag_excluded` に対応します。
SADesiredRole	varchar(16)	本来あるべき役割。本来あるべきストレージ複製方向を示す複製参照に使用されます (SA AM のみ)。 リソース状況変更イベントで使用されます。 **注 :** TEC イベントでの `sa_role_desired` に対応します。
SAObservedRole	varchar(16)	監視された役割。監視されたストレージ複製方向を示す複製参照に使用されます (SA AM のみ)。 リソース状況変更イベントで使用されます。 **注 :** TEC イベントでの `sa_role_observed` に対応します。

表 29. ドメイン状況変更イベント (alerts.status)		
SADomainState	varchar(16)	自動化ドメインの状況。可能な値は以下のとおりです。 • オンライン • オフライン • Unknown **注:** TEC イベントでの sa_domain_state に対応します。
SACommunicationState	varchar(32)	ドメインが System Automation Application Manager に接続されている場合は、この状態は、ドメインの接続と可用性の状態を反映します。可能な値を次に示します。 • OK • AsyncTimeout • AsyncMissedEvent • SyncFailed • SyncFailedAndAsyncMissedEvent • SyncFailedAndAsyncTimeout • DomainHasLeft **注:** TEC イベントでの sa_communication_state に対応します。

System Automation イベントの新規フィールドに加えて、イベントの処理中に System Automation イベントのルール・ファイルで以下の既存フィールドが設定されます。

表 30. System Automation イベントの既存ルール・ファイル・フィールド	
属性名	**説明**
Manager	アラームを収集して ObjectServer に転送したプローブの記述名。 SA イベントの値は tivoli_eif on <host name> です。
Agent	イベントを生成したマネージャーの記述名。 System Automation for Multiplatforms イベントの値は SystemAutomation です。
Node	イベントの発生元のホスト名を識別します。
AlertGroup	System Automation によって発行されたイベントのタイプを識別します。可能なイベント・クラスのリストについては、101 ページの表 25 を参照してください。
AlertKey	イベントをトリガーしたリソースを示す記述キー。リソース・イベントの場合は、System Automation ソース・トークン形式のリソース・キー (例えば、EEZResourceKey,DN={DB2Cluster},NN={},RN={db2rs},RC={IBM.Application}) が含まれています。ドメイン・イベントの場合は、System Automation ソース・トークン形式のドメイン名 (例えば、EEZDomain,DN={Db2Cluster}) が含まれています。

表 *30. System Automation* イベントの既存ルール・ファイル・フィールド *(*続き*)*	
属性名	**説明**
Severity	イベントの重大度レベルを示します。リソース・イベントの場合は、リソースの複合状態によって重大度レベルが決まります。イベント・リストのイベントの色は、重大度値によって制御されます。 • 0: クリア • 1: 不確定 • 2: 警告 • 3: マイナー • 4: メジャー • 5: クリティカル 106 ページの『複合状態から重大度へのマッピング』を参照してください。
Summary	イベントを説明するテキスト要約。
Service	このイベントの影響を受けるサービスの名前。 フィールド SAResourceName に対応します。
Identifier	問題の原因を一意的に識別し、ObjectServer 非重複化を制御する ID。ObjectServer は、非重複化を使用して、同じソースから生成されるイベント情報がイベント・リストで複製されないようにします。反復イベントは、「ID」属性を使用して識別され、ObjectServer でデータの量を削減するために単一のイベントとして格納されます。System Automation イベントの場合は、「ID」フィールドは「`AlertKey + ":" + AlertGroup`」に設定されます。 そのため、イベント・コンソールには、同じリソースの最後のイベントと AlertGroup が常に表示されます。
Class	System Automation イベントの固有のクラス。 値は 87725 (Tivoli System Automation) です。
ExtendedAttr	`alerts.status` 表に専用の列が存在しない、System Automation に固有の追加の内部属性の名前と値のペアを保持します。

OMNIbus の `alerts.status` 表に格納されるこれらの属性に加えて、追加情報が `alerts.details` 表に書き込まれます。例えば、ドメイン・イベントの場合は、ドメインに対応する自動化製品の製品名とバージョンは、`alerts.details` 表に格納されます。

複合状態から重大度へのマッピング

すべてのリソース状態変更イベントなど、SACompoundState 値が含まれているイベントでは、以下のマッピング表が使用されます。

表 *31.* 複合状態から *OMNIbus* 重大度へのマッピング	
SACompoundState	**OMNIbus の「重大度」フィールド**
Fatal	5 (クリティカル)
Error	4 (メジャー)
Warning	3 (マイナー)
OK	1 (不確定)

要求イベントやドメイン・イベントなど、SACompoundState 値を含まないその他のイベントでは、EIF の重大度フィールドは、OMNIbus の重大度を判別するために使用されます。

表 32. *EIF* から *OMNIbus* 重大度へのマッピング	
EIF の重大度	**OMNIbus の「重大度」フィールド**
60 (致命的)	5 (クリティカル)
50 (クリティカル)	5 (クリティカル)
40 (マイナー)	4 (メジャー)
30 (警告)	3 (マイナー)
20 (無害)	2 (警告)
Else	1 (不確定)

注 : 元の EIF イベントの EIF 重大度値は、イベントの ExtendedAttr フィールドにあります。

System Automation イベントを処理するよう OMNIbus を構成

OMNIbus の構成には、OMNIbus データベースの更新およびルール・ファイルの使用可能化が含まれます。

OMNIbus データベースの更新

OMNIbus ObjectServer データベースには、イベント・リストによって表示および選択されるすべてのフィールドが入っている alerts.status 表が含まれています。

このタスクについて

System Automation for Multiplatforms イベントでは、102 ページの『OMNIbus データベースのイベント・フィールド』で説明されている追加の列を alerts.status 表に作成する必要があります。

sa_db_update.sql ファイルによって、alert.status 表に新規の列が作成されます。Tivoli System Automation からのイベントに使用されるイベント・クラスも作成されます。System Automation for Multiplatforms はそのイベントにイベント・クラス 87725 を使用します。このクラスは、コンテキスト起動ツールなどのツールを特定のタイプのイベントに関連付けるために使用されます。

OMNIbus サーバーで以下のコマンドを入力します。

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
```

プロンプトが出されたら、パスワードを入力します。

ファイル sa_db_update.sql は、System Automation for Multiplatforms 製品 DVD のディレクトリー / integration にあります。

注 : イベント・クラス 87725 は、OMNIbus バージョン 7.3.1 以降で事前定義されます。OMNIbus バージョン 7.3.1 を使用して sa_db_update.sql スクリプトを実行すると、以下のエラー・メッセージが表示されます。

```
ERROR=Attempt to insert duplicate row on line 2 of statement 'insert into
alerts.conversions values ( 'Class87725','Class',87725,'Tivoli System
Automation' );...'
```

このエラー・メッセージは無視できます。

SA に固有の列とイベント・クラスが正常に OMNIbus に追加されたことを確認します。

1. nco_config コマンドを使用して「Netcool/OMNIbus 管理者」ウィンドウを開きます。
2. 「Netcool/OMNIbus 管理者」ウィンドウで、「**システム**」メニュー・ボタンを選択します。

3.「**データベース**」をクリックします。「データベース」ペインが開きます。
4. **alerts.status** 表を選択します。 alerts.status 表ペインが開きます。
5. 次の列がリストされていることを確認してください。
    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.「Netcool/OMNIbus 管理者」ウィンドウで、「**ビジュアル**」メニュー・ボタンを選択します。
7.「**クラス**」をクリックします。「クラス」ペインが開きます。
8. ID が「**87725**」で、ラベル「**Tivoli System Automation**」が付いたクラスが表にリストされていることを確認します。

ルール・ファイルの使用可能化

OMNIbus ルール・ファイルは、プローブがアラートを作成するためにイベント・データを処理する方法を定義します。ルール・ファイルによって、問題の原因を一意的に識別する ID もアラートごとに作成されます。

このタスクについて

Tivoli EIF のプローブは、tivoli_eif.rules という名前の標準のルール・ファイルを使用します。System Automation for Multiplatforms には、System Automation に固有のルール・ファイルである tivoli_eif_sa.rules が付属しています。 このファイルは、include ステートメントを使用してデフォルトの tivoli_eif.rules 内に含める必要があります。ルール・ファイル tivoli_eif_sa.rules は、Tivoli EIF のプローブが受信した EIF イベントのイベント・フィールド source に System Automation という値が含まれている場合に、そのイベントを処理します。

デフォルトの tivoli_eif.rules ファイルは、Tivoli EIF のプローブがインストールされているシステムの以下のディレクトリーにあります。

```
Windows: %OMNIHOME%¥probes¥<os_dir>¥tivoli_eif.rules
UNIX: $OMNIHOME/probes/<os_dir>/tivoli_eif.rules
```

tivoli_eif_sa.rules ファイルを使用可能にするには、以下の手順を実行します。

1. System Automation for Multiplatforms 製品 CD の /integration ディレクトリーにあるファイル tivoli_eif_sa.rules を、OMNIbus Probe for Tivoli EIF がインストールされているシステムにコピーします。ターゲット・ディレクトリーとして、tivoli_eif.rules ファイルがあるディレクトリーを選択します。
2. 付属のルール・ファイル tivoli_eif_sa.rules を使用可能にします。 Tivoli EIF のプローブで使用する tivoli_eif.rules ファイルを編集して、tivoli_eif_sa.rules ファイルの include ステートメントを追加します。

tivoli_eif.rules の内容は、ご使用の OMNIbus インストール済み環境のタイプによって異なります。

a. スタンドアロンの OMNIbus インストール済み環境を使用している場合:

テキスト・エディターで tivoli_eif.rules ファイルを開き、switch($source) ブロックの後に include ステートメントを追加します。

```
:
else
{
        switch($source)
        {
                case "dummy case statement": ### This will prevent syntax errors in case
                             no includes are added below.

                        include "tivoli_eif_tpc.rules"
                        include "tivoli_eif_tsm.rules"

                        # Uncomment the following line when using TADDM integration
                        # This rules file is available in OMNIbus 7.3 and newer only
                        # include "tivoli_eif_taddm.rules"

                default:
                        # Comment out the following line when not receiving events from TEC
                        include "tivoli_eif_default.rules"
        }
        include "tivoli_eif_sa.rules"
}
```

b. Tivoli Business Service Manager (TBSM) と統合していて、TBSM とともにパッケージされた OMNIbus バージョンを使用する場合:

テキスト・エディターで tivoli_eif.rules ファイルを開き、事前定義のルール・ファイルが含まれているブロックに include ステートメントを追加します。行 # Include customer rules which would override any previous rules. を検索して、この行の前に tivoli_eif_sa.rules の include ステートメントを追加します。

```
:
:
    ###
    ### Handle TEC Events
    ###
    include "tec_event.rules"

    ###
    ### Handle Z Events
    ###
    # include "zos_event.rules"

    ###
    ### Handle Z user defined events.
    ###
    # include "zos_event_user_defined.rules"

    ###
    ### Handle Z identity assignement.
    ###
    # include "zos_identity.rules"

    ###
    ### Handle EE( Event Enablement) events.
    ###
    # include "tivoli_eif_ee.rules"

   include "tivoli_eif_sa.rules"

    # Include customer rules which would override any previous rules.
    # include "customer_override.rules"
:
:
```

3. EIF probe を停止します。

- Windows の場合: 「**コントロール パネル**」>「**管理ツール**」>「**サービス**」を選択します。サービスのリストで、「**EIF probe**」をダブルクリックして、「**停止**」をクリックします。
- UNIX の場合: コマンド行に以下のコマンドを入力します。

```
$OMNIHOME/bin/nco_pa_stop -process <probe_name>
```

4. EIF probe を再度開始します。
   - Windows の場合: サービスのリストで、「**OMNIbus EIF Probe**」をダブルクリックしてから、「**開始**」をクリックします。
   - UNIX の場合: コマンド行に以下のコマンドを入力します。

```
$OMNIHOME/bin/nco_pa_start -process <probe_name>
```

注 :

1. OMNIbus サーバーとともに提供される構文検査ツール nco_p_syntax を使用して、ルール・ファイルに対する変更をテストできます。ルート・ルール・ファイル tivoli_eif.rules を使用します。インクルード・ファイルが自動的に検査されます。

   例:

```
$OMNIHOME/probes/nco_p_syntax -rulesfile $OMNIHOME/probes/linux2x86/tivoli_eif.rules
```

2. イベントを失うことなく、プローブにルール・ファイルを強制的に再度読み取らせるには、以下のコマンドを入力します。

```
kill -HUP <pid>
```

   pid はプローブ・プロセス ID です。pid を判別するには、nco_pa_status コマンドを使用します。

Tivoli Enterprise Console

Tivoli Enterprise Console® を構成して、システム自動化イベントを TEC に転送できます。

System Automation イベントを処理するよう TEC を構成

イベントの構造およびプロパティーを定義するには、プログラミング言語 Basic Recorder of Objects in C (BAROC) を使用します。これらの定義は、.baroc という 拡張子のファイルに保管されます。System Automation イベントの baroc ファイルは SystemAutomation.baroc と呼ばれ、インストール後にディレクトリー /usr/sbin/rsct/samples/tec/SystemAutomation.baroc に入れられます。System Automation for Multiplatforms で使用するよう TEC を準備するには、TEC サーバーで、TEC baroc ファイル SystemAutomation.baroc をインポート、コンパイル、ロード、およびアクティブ化します。詳細については、「IBM Tivoli Enterprise Console Rule Builder's Guide」(GC32–0669) を参照してください。

イベント生成の使用可能化

イベントを TEC または OMNIbus に送信するには、System Automation for Multiplatforms でイベント転送を使用可能にします。

このタスクについて

TEC パブリッシャーを使用可能にすることで、EIF イベントの生成と転送機能をアクティブにして構成します。以下のステップを実行します。

1. cfgsamadapter 構成ユーティリティーを使用して、イベント・パブリッシュを構成します。イベント・パブリッシュの構成方法に関する詳細については、「78 ページの『「イベント・パブリッシュ」タブ』」を参照してください。
2. System Automation for Multiplatforms クラスター内の各ノードでパブリッシャーを使用可能にします。デフォルトでは、パブリッシャーが使用不可です。パブリッシャーを使用可能にするには、構成ダイア

ログを使用する (*System Automation for Multiplatforms* 管理者とユーザーのガイドを参照) か、`samctrl` コマンドを使用します (111 ページの『コマンド行インターフェースの使用によるパブリッシャーの使用可能化』 を参照)。

3. デフォルトのシステム・ロケールを使用しない場合は、TEC イベント・メッセージ用に新規言語ロケールを設定します。

コマンド行インターフェースの使用によるパブリッシャーの使用可能化

System Automation for Multiplatforms コマンド行インターフェース (CLI) または `cfgsamadapter` 構成ダイアログを使用して、パブリッシャーを制御できます。

このタスクについて

このセクションでは、CLI を使用してパブリッシャーを制御する方法を説明します。`cfgsamadapter` 構成ダイアログを使用する場合は、*System Automation for Multiplatforms* 管理者とユーザーのガイドを参照してください。

パブリッシャー機能はデフォルトで使用不可になっています。パブリッシャーの状況を照会するには、以下のコマンドを実行します。

```
node1:/usr/sbin/rsct/samples/tec # lssamctrl
```

以下の Tivoli System Automation 制御情報が表示されます。

```
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        = {}
```

TEC パブリッシャーを使用可能にするには、任意のノードで以下のコマンドを発行します。

```
node1:/usr/sbin/rsct/samples/tec # samctrl -e TEC
```

TEC パブリッシャーを使用不可にするには、任意のノードで以下のコマンドを発行します。

```
node1:/usr/sbin/rsct/samples/tec # samctrl -d TEC
```

定義済みのすべてのパブリッシャーを使用可能にするには、任意のノードで以下のコマンドを実行します。

```
node1:/usr/sbin/rsct/samples/tec # samctrl -e P
```

定義済みのすべてのパブリッシャーを使用不可にするには、任意のノードで以下のコマンドを実行します。

```
node1:/usr/sbin/rsct/samples/tec # samctrl -d P
```

TEC または OMNIbus イベント・メッセージのための新規言語ロケールの設定

このタスクについて

TEC または OMNIbus イベント・メッセージは、System Automation for Multiplatforms マスターが稼働しているノードのデフォルト・システム・ロケールの言語で常に表示されます。

注 : ユーザーがデフォルトのシステム・ロケール以外のロケールを指定したシェルでリソース (mkrg、mkrsrc) を作成した場合、または、端末プログラムがシェル・ロケールで定義されている文字セット以外の文字セット変換を使用する場合、TEC または OMNIbus イベント・メッセージのリソース名が破損すること

があります。この問題を解決するために、 システム・ロケールとシェル・ロケールの設定は同一である必要があり、これに応じて端末プログラムの文字変換が設定される必要があります。シェル・ロケールを変更する場合で、古いシェル・ロケール設定でリソースが既に作成されている場合は、すべてのリソースを削除し、新規のシェル・ロケールを使用して再作成する必要があります。

ユーザーがデフォルトのシステム・ロケールを別のシェル設定に調整する場合は、この変更をクラスターのすべてのノード上で実行する必要があります。これを行うには、以下を実行してください。

1. **stoprpdomain** コマンドを使用して、クラスターを停止します。
2. デフォルトのシステム・ロケールが含まれるファイルを編集し、該当する値を設定して、ファイルを保管します。

   SUSE Linux

   ファイル: /etc/sysconfig/language

   キーワード: RC_LANG="<NewLocale>"

   <NewLocale> はご使用のロケール設定に置き換えます。

   ROOT_USES_LANG="yes"

   RC_LC_ で始まるすべてのキーワードを空ストリング "" に設定する必要があります (例えば、RC_LC_ALL= "")。

   /etc/SUSEconfig を実行して、変更をご使用のシステムに適用します。 yast2 sysconfig システム構成ツールを使用して、変更を適用する こともできます。

   RedHat Linux

   ファイル: /etc/sysconfig/i18n

   キーワード: LANG="<NewLocale>"

   <NewLocale> はご使用のロケール設定に置き換えます。

   AIX

   ファイル: /etc/environment

   キーワード: LANG="<NewLocale>"

   <NewLocale> はご使用のロケール設定に置き換えます。
3. システムをリブートします。
4. クラスター内のすべてのノードで、このステップを繰り返します。
5. **startrpdomain** コマンドを使用して、クラスターを始動します。

Tivoli Business Service Manager (TBSM)

TBSM は、ビジネス要件に沿ってアラートに効果的に応答し、オプションでサービス・レベル・アグリーメント (SLA) を満たすために必要なリアルタイム情報を送信します。

TBSM ツールを使用すると、IBM Tivoli Netcool®/OMNIbus™ アラート、またはオプションで SQL データ・ソースのデータと統合するサービス・モデルを構築できます。

TBSM データ・サーバーは、サービス・モデルに対して構成された着信状況ルールとの突き合わせのために、IBM Netcool/OMNIbus ObjectServer イベントまたは SQL データを分析します。一致するデータによってサービス状況が変更された場合は、それに応じて TBSM サービス・モデルの状況も変更されます。サービス状況が変わると、TBSM は、対応するサービス・イベントを ObjectServer に返送します。

Discovery Library Toolkit では、ディスカバリー・ライブラリー・アダプター (DLA) の資料または IBM Tivoli Application Dependency Discovery Manager からのデータを使用して、TBSM サービス・オブジェクトを作成できます。

TBSM コンソールには、サービス・モデル内でサービスとビジネス要件を論理的にリンクできる、Tivoli Integrated Portal (TIP) で実行されるグラフィカル・ユーザー・インターフェース (GUI) が用意されています。 サービス・モデルは、特定の時点における企業のパフォーマンス、または特定の期間にわたる企業のパフォーマンスのビューをオペレーターに提供します。

以下のピクチャーは、TBSM の基本アーキテクチャーを示します。

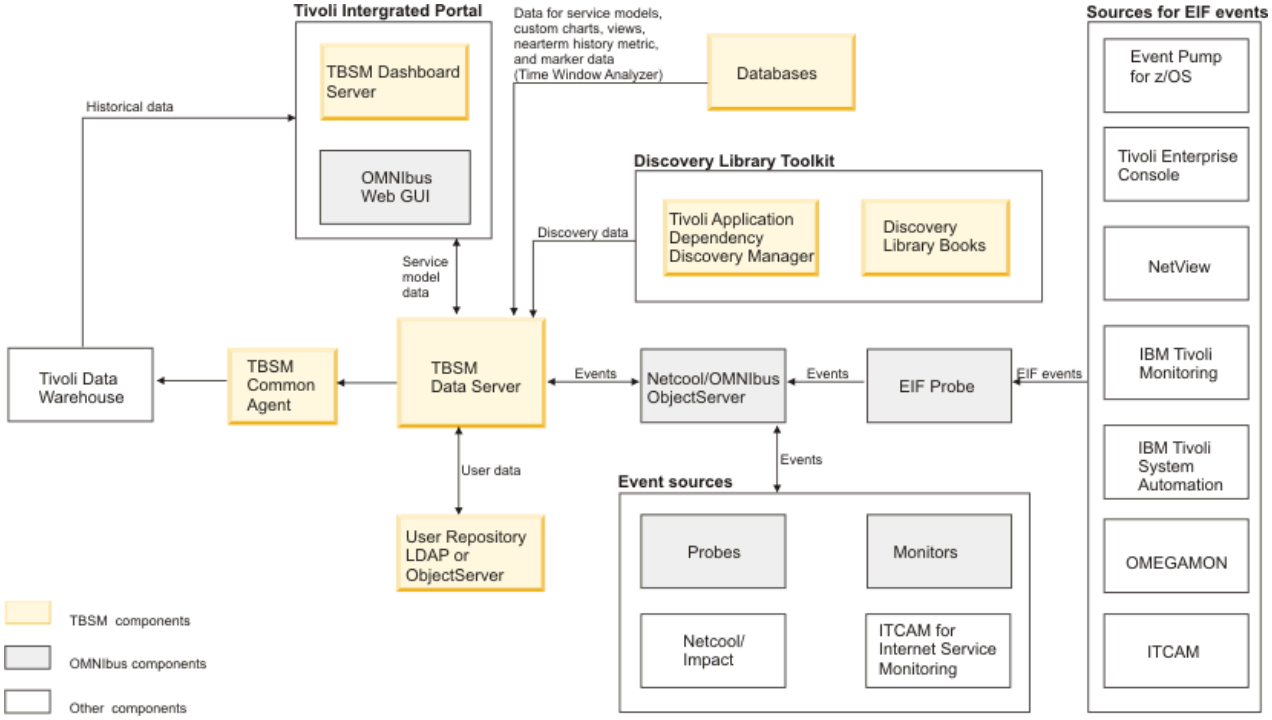


図 *17. TBSM* の基本アーキテクチャー

メイン・コンポーネント

Tivoli Integrated Portal

Tivoli Integrated Portal では、共通のポータルを使用して、Tivoli 製品間の対話とデータの安全な引き渡しを行うことができます。あるアプリケーションから別のアプリケーションの起動、および同じダッシュボード・ビュー内からの起動を行って、管理対象エンタープライズのさまざまな局面を調査できます。

Tivoli Netcool/OMNIbus

TBSM は、Tivoli Netcool/OMNIbus ObjectServer で着信イベントをモニターします。ObjectServer は、プローブ、モニター、および IBM Tivoli Monitoring などのその他のアプリケーションからイベントを収集します。着信イベントで受信したデータに応答するサービス・モデルを作成するには、TBSM を使用します。例えば、着信イベント・データに応じて、サービスの状況を変更したり、潜在的な SLA 違反のトラッキングを開始したりすることができます。

Tivoli Netcool/Webtop (OMNIbus Web GUI)

Netcool/Webtop は Netcool/OMNIbus のブラウザー・コンソールであり、TBSM は、Netcool/Webtop コンポーネントを使用して、サービス・モデルに関連するイベントを表示します。TBSM のアクティブ・イベント・リスト (AEL) およびサービス詳細ポートレットは Netcool/Webtop コンポーネントであり、TBSM の一部としてインストールされます。 Tivoli Integrated Portal には、Netcool/Webtop コンポーネントも組み込まれています。

TBSM ダッシュボード・サーバー

TBSM ダッシュボード・サーバーは TBSM コンソールの表示を管理し、TBSM データ・サーバーと通信して、接続されている TBSM コンソールを介してサービス・モデルの作成と視覚化をサポートします。コンソール・ユーザーがサービス・モデルの部分を表示すると、ダッシュボード・サーバーは、データ・サーバーからサービスの状況を獲得して保守します。

TBSM データ・サーバー
TBSM データ・サーバーは、ObjectServer と外部データベースで、TBSM コンソールで構成した、または radshell コマンド行ツールを使用して構成したサービスの状況に影響を与えるデータをモニターします。サーバーは、外部データにルールを適用することでこれらのサービスの状況を計算します。サービス・モデルとルールは TBSM データベースに格納されます。

System Automation for Multiplatforms の統合

ビジネス・アプリケーションは通常、さまざまなミドルウェア・コンポーネントで構成され、多階層であり、異機種混合プラットフォームで実行されます。Tivoli Business Service Manager (TBSM) は、多階層アプリケーションに関する正常性情報を提供します。 また、TBSM は、多数のソースから取得した情報に基づいてサービス・レベル・アグリーメント (SLA) をモニターします。ビジネス・アプリケーション・ランドスケープに関連するすべてのイベントの収集には Netcool/OMNIbus が使用され、TBSM は、これらのイベントを使用して、ビジネス・アプリケーションの状況を判別します。

System Automation for Multiplatforms は、ビジネス・アプリケーション・ランドスケープにおける開始依存関係または停止依存関係を自動化し、障害状態に対し共通する操作の自動的な復旧を提供し、集約された可用性状況を取得します。System Automation for Multiplatforms と System Automation for z/OS は、ビジネス・アプリケーションの個々のコンポーネント (例えば、重要なデータベース) の可用性を高めます。

TBSM サービス・ビューを System Automation イベントからのデータで強化することにより、System Automation for Multiplatforms を TBSM との統合に使用できます。System Automation for Multiplatforms は、状態を System Automation から TBSM サービス・インスタンスにマップする方法に関する事前構成済みのルールが含まれる TBSM サービス・テンプレートを送信します。

前提条件

開始する前に、以下の製品をインストールして構成し、インストール済み環境をテストします。

- System Automation for Multiplatforms イベントについて OMNIbus へのイベント転送を構成し、使用可能にします。詳しくは、107 ページの『System Automation イベントを処理するよう OMNIbus を構成』および 110 ページの『イベント生成の使用可能化』を参照してください。
- Tivoli Business Service Manager (TBSM) V4.2.1 以降
- TBSM 用の Netcool OMNIbus ObjectServer スキーマを更新します。
  - 既存の OMNIbus サーバーがある場合は、スキーマ・ファイル `tbsm_db_update.sql` と `ClearServiceDeps.auto` をインポートします。
  - OMNIbus が TBSM とともにインストールされている場合は、TBSM インストーラーによって必要なスキーマ更新が実行されます。

TBSM に固有の製品情報は、Tivoli Business Service Manager にあります。製品のインストールについて詳しくは、Tivoli Business Service Manager Knowledge Center を参照してください。

TBSM の構成

このタスクについて

TBSM でサービスを定義して構成するためのプロセスを単純化するために、共通の動作を行うサービス・インスタンスについて、サービス・テンプレートを定義できます。各サービスとその依存関係を個別に定義するのではなく、1 つのテンプレートを 1 つのタイプのサービスについて作成してから、適切なサービスに割り当てることができます。

サービス・インスタンスは、テンプレートを割り当てられる実際のサービスを表します。テンプレートは、サービスが着信データや、その他のサービスの状況に対し、どのように応答するかを定義します。同じタイプのサービスを共通テンプレートに割り当てる必要があります。これによって、同じテンプレート・ルールを使用して、複数のサービスの状況を評価できます。

テンプレートをサービスに割り当てる場合は、サービスをテンプレートでタグ付けします。テンプレートによって、サービス・タイプに関する同じルールを複数回作成する必要がなくなります。

TBSM のサービス・テンプレート

System Automation for Multiplatforms には、TBSM サービス・ツリーに表示される System Automation リソースに使用される TBSM サービス・テンプレートが用意されています。

このタスクについて

サービス・テンプレートには、EEZ_SystemAutomationResource という名前が付いています。これは、以下のものを提供します。

- SACompoundState という名前の着信状況ルール。これは、System Automation for Multiplatforms リソースから取得した状態変更イベントを使用して、サービスの全体的な状態を判別します。
- テキスト・ベースの着信状況ルール。これは、System Automation の監視状態とリソースのその他の System Automation に固有の状態をエクスポートして、TBSM ビューで使用できるようにします。 テキスト・ベースの着信状況ルールの使用方法について詳しくは、118 ページの『System Automation から情報を追加するために TBSM ビューをカスタマイズ』を参照してください。

EEZ_SystemAutomationResource サービス・テンプレートには、サービスの全体的な状態を判別する、SACompoundState という名前の着信状況ルールが含まれています。サービス・テンプレートが特定のサービス・インスタンスに割り当てられている場合、System Automation for Multiplatforms から取得したリソース状態変更イベントは、サービスの全体的な状態に影響を与えます。イベントの AlertKey がサービス・インスタンスの ID として定義されている AlertKey と一致する場合は、イベントはサービス・インスタンスに関連付けられます。

TBSM では、全体的な状態として「不良」、「限界」、および「良好」の 3 つを使用できます。 以下のマッピングは、System Automation からのリソース状態変更イベントをサービス・インスタンスの全体的な TBSM 状態にマップするために、SACompoundState ルールで定義されます。

表 *33. System Automation* のリソース状態変更イベント から *TBSM* 状態へのマッピング

イベントの重大度	**TBSM の状態**
5 (クリティカル)	不良 (赤)
4 (メジャー)	不良 (赤)
3 (マイナー)	限界 (黄色)
1 (不確定)	良好 (緑)

リソースの複合状態からイベントの重大度への 1 対 1 のマッピングが存在するため、System Automation の複合状態によって TBSM の状態が直接決定されます。複合状態からイベントの重大度へのマッピングに関する詳細については、106 ページの『複合状態から重大度へのマッピング』を参照してください。

TBSM での System Automation サービス・テンプレートの定義

このタスクについて

TBSM で System Automation イベントを使用するには、EEZ_SystemAutomationResource テンプレートが必要です。次のようにして、EEZ_SystemAutomationResource テンプレートを TBSM にインポートしてください。

1. System Automation for Multiplatforms 製品 CD の /integration ディレクトリーから、TBSM データ・サーバーがインストールされている一時ディレクトリーにファイル EEZ_SystemAutomationResource.radsh をコピーします。
2. TBSM データ・サーバー・システムでコマンド・プロンプトを開きます。 EEZ_SystemAutomationResource.radsh をコピーしたディレクトリーに変更して、以下のコマンドを発行します。

- **UNIX:**

```
cat EEZ_SystemAutomationResource.radsh  |
$TBSM_HOME/bin/rad_radshell
```

- **Windows:**

```
type EEZ_SystemAutomationResource.radsh |
%TBSM_HOME%¥bin¥rad_radshell
```

これにより、System Automation for Multiplatforms によって提供されるサービス・テンプレートが TBSM で定義されます。

Netcool/OMNIbus でのトリガーの定義

このタスクについて

OMNIbus ObjectServer では、リソースの新規の状態変更イベントによって、前のイベントが置き換えられます (イベントの非重複化)。

デフォルトでは、TBSM は、「**重大度**」フィールドの値が変更された場合のみ、重複排除されたイベントを処理します。そのような場合は、TBSM は非重複化イベントを処理し、サービス状況を更新します。状況変更はリソースで発生する可能性があり、これによって EEZ_SystemAutomationResource サービス・テンプレートに含まれているテキスト・ベースの着信状況ルールで使用される状況フィールドが更新されます。 ただし、リソースの複合状態は変更されないため、重大度値は変更されません。TBSM がこれらの場合もサービスを更新するように、OMNIbus でトリガーを定義します。

sa_db_tbsm_update.sql ファイルは、OMNIbus で update_tbsm_service_on_sa_events という名前のトリガーを定義するために使用されます。このトリガーによって、重大度値が変更されていない場合でも、テキスト・ベースの着信状況ルールで使用される状態の 1 つが変更されたときに、TBSM がイベントを再処理するようになります。EEZ_SystemAutomationResource サービス・テンプレートに含まれているテキスト・ベースの着信状況ルールを使用する場合は常に、このトリガー定義を作成します。

トリガーを定義するには、OMNIbus サーバーで以下のコマンドを入力します。

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
```

プロンプトが出されたら、ユーザー ID とパスワードを入力します。

sa_db_tbsm_update.sql は System Automation for Multiplatforms に含まれており、製品 DVD のディレクトリー /integration にあります。

System Automation リソースと TBSM の統合

このタスクについて

System Automation リソースを TBSM サービス・ツリーに追加するには、TBSM でサービス・インスタンスを手動で作成してから、System Automation サービス・テンプレートを割り当てる必要があります。これについては 117 ページの『サービス・インスタンスへのサービス・テンプレートの割り当て』で説明します。この作業は、TBSM サービス・ツリーに既に存在するサービス・インスタンスを System Automation イベントからの情報で強化する場合も行います。

注 : System Automation Application Manager も使用している場合は、System Automation Application Manager によって管理されるリソースのサービス・インスタンスを自動的に作成するために、ディスカバリー・ライブラリー・アダプターを活用できます。

サービス・インスタンスへのサービス・テンプレートの割り当て

サービス・テンプレートは、サービス・インスタンスに適用できるルールで構成されます。テンプレートは、複数のインスタンスに使用できます。EEZ_SystemAutomationResource テンプレートをサービスに割り当てる場合は、サービスをテンプレートでタグ付けできます。

このタスクについて

以下のように進めます。

1. EEZ_SystemAutomationResource テンプレートを使用してサービスをタグ付けして、これらのサービスで定義済みの着信状況ルールを使用できるようにします。
   a. **サービス・ナビゲーション**・ポートレットで、System Automation 固有のサービス・テンプレート EEZ_SystemAutomationResource を割り当てる「**サービス名**」を選択します。
   b.「**サービス・エディター**」で「**サービスの編集**」タブを選択して、サービスを編集します。
   c.「**テンプレート**」タブを選択します。以下の 2 つのリストを表示できます。
      - **使用可能なテンプレート**: 選択したサービス・インスタンスに割り当てる許可を持つテンプレートがすべて表示されます。
      - **選択されたテンプレート**: サービスに割り当てられたテンプレートがすべて表示されます。
   d. System Automation テンプレートをサービスに割り当てるには、「**使用可能なテンプレート**」リストから EEZ_SystemAutomationResource テンプレートを選択します。テンプレートを「**選択されたテンプレート**」リストに移動するには、矢印ボタン **>>** をクリックします。
2. このサービスの「**識別フィールド**」値を構成します。TBSM は、「識別フィールド」を使用して、着信イベントをサービス・インスタンスにマップします。
   a.「**サービスの編集**」タブを選択します。
   b. EEZ_SystemAutomationResource テンプレートで定義したルールを指定する「**識別フィールド**」タブと、選択したサービス・インスタンスにイベントをマップするために必要な ID フィールド値を選択します。 EEZ_SystemAutomationResource テンプレートに含まれているルールでは、AlertKey イベント属性が ID として使用されます。デフォルトでは、各 ID フィールドの値は、「**サービス名**」フィールドに入力した値です。
   c. 選択したサービスに対応する正しい AlertKey 属性値を入力します。AlertKey には、CDM SourceToken 形式の固有の System Automation リソース・キーが含まれている必要があります。構造は次のように定義されます。

```
EEZResourceKey,DN={DomainName},NN={NodeName},
RN={ResourceName},RC={ResourceClass}
```

   リソースのいずれかのイベントを開いて、入力エラーを回避するために AlertKey 値をイベントからコピーして貼り付けることを検討できます。有効な AlertKey 値の例:

   Resource
   構成要素リソースまたは固定リソース。これは、lssam では IBM.Application:db2-rs:saxb32c と表示されます。

   AlertKey:

```
EEZResourceKey,DN={DB2Cluster},NN={saxb32c},RN={db2- rs},
RC={IBM.Application}
```

   移動グループ
   浮動リソース。ドメイン DB2Cluster は、lssam では IBM.Application:db2-rs と表示されます。

   AlertKey:

```
EEZResourceKey,DN={DB2Cluster},NN={},RN={db2- rs},
RC={IBM.Application}
```

リソース・グループ
ドメインは DB2Cluster であり、これは lssam では IBM.ResourceGroup:DB2 と表示されます。

AlertKey:

```
EEZResourceKey,DN={DB2Cluster},NN={},RN={DB2},
RC={IBM.ResourceGroup}
```

d.「**保存**」をクリックして、変更内容を適用します。

指定された AlertKey と一致するサービスについて新規の System Automation for Multiplatforms 状態変更イベントを受信するたびに、TBSM は、着信状況ルールを処理して、場合によってはイベントの重大度に基づいてサービスの全体的な状態を変更するようになります。

System Automation から情報を追加するために TBSM ビューをカスタマイズ

このタスクについて

EEZ_SystemAutomationResource サービス・テンプレートには、リソースの System Automation 監視状態やその他の System Automation 固有の状態を取得するテキスト・ベースの着信状況ルールが含まれています。この情報は、System Automation for Multiplatforms から取得した情報でサービス・インスタンスを強化するために TBSM ビューで使用できます。

以下のテキスト・ベースの着信状況ルールが使用可能です。

表 *34. TBSM* のテキスト・ベースの着信状況ルール

ルール名	**説明**
SAObservedStateValue	リソース状況変更イベントからフィールド SAObservedState を取得します。 可能な値を次に示します。 • Unknown • オンライン • オフライン • Starting • Stopping • NotApplicable
SADesiredStateValue	リソース状況変更イベントからフィールド SADesiredState を取得します。 可能な値を次に示します。 • オンライン • オフライン • NoChange (例えば、オペレーターがリソースの自動化目標を変更できない場合)
SAOperationalStateValue	リソース状況変更イベントからフィールド SAOperationalStateValue を取得します。リソースの現行状態に関する詳細情報を提供する「動作状態」値のリスト。可能な値のリストについては、SystemAutomation.baroc ファイルを参照してください。

表 *34. TBSM* のテキスト・ベースの着信状況ルール *(続き)*	
ルール名	**説明**
SACompoundStateValue	リソース状況変更イベントからフィールド SACompoundStateValue を取得します。リソースが要求どおりに動作しているか、またはエラーが発生しているかどうかを示す複合状態。可能な値を次に示します。 • OK • Warning • Error • Fatal
SAExcludedFromAutomationValue	リソース状況変更イベントからフィールド SAExcludedFromAutomationValue を取得します。リソースが自動化から除外される (例えば、自動化がサスペンドされている) かどうかを示すフラグ。 可能な値を次に示します。 • NotExcluded • Excluded

追加の System Automation 情報の列を TBSM サービス・ツリーに追加

このタスクについて

以下の場所で、TBSM に表示されるカスタム・ツリーの列を変更できます。

- **サービス・ナビゲーション**・ポートレット
- **サービス・ツリー**・ポートレット

デフォルトの**サービス・ナビゲーション**・ポートレットには以下の 3 つの列があります。

- **状態**
- **時刻**
- **イベント**

「**ツリー・テンプレート・エディター**」を使用して、ツリー列の変更、削除、および追加を行うことができます。「**ツリー・テンプレート・エディター**」は、**サービス・ナビゲーション**・ポートレットの「**サービス**」ツールバーから使用可能です。新規のツリー・テンプレートを**サービス・ナビゲーション**・ポートレットに追加できます。カスタム列ごとに、「**ツリー・テンプレート・エディター**」を使用して、列に表示するルール・データを指定します。

列の追加:

この機能は、EEZ_SystemAutomationResource テンプレートによって定義された、提供されるテキスト・ベースの着信状況ルールの列を追加するために使用できます。例えば、EEZ_SystemAutomationResource テンプレートが割り当てられているサービス・インスタンスごとに System Automation から取得した現行の監視状態を表示する列を定義できます以下のステップを実行します。

1. サービス・ナビゲーション・ポートレットのツールバーで「**ツリー・テンプレート・エディター**」ボタンをクリックします。
2. 変更するツリー・テンプレートを「**ツリー・テンプレート名**」ドロップダウン・リストで選択します。
3. 「列構成」セクションで「**新規ツリー列の追加**」ボタンをクリックします。
4. 使用する名前 (例えば、「Availability State」) を新規列のブランク・フィールドに入力します。

5. 必要に応じて列の位置と幅を調整します。
6. 「**サービス・テンプレートの選択**」セクションで、EEZ_SystemAutomationResource テンプレートを選択します。
7. 「**サービス・テンプレート・ルール・マッピング**」の「アクティブ・テンプレート」リストで EEZ_SystemAutomationResource テンプレートを選択します。
8. サービス・ツリー列に表示するルールごとに、「**表示**」チェック・ボックスを選択して、ドロップダウン・ボックスから列を選択して、出力値を表示します。この例では、属性 @SAObservedStateValue の「**表示**」チェック・ボックスを選択して、その行のドロップダウン・ボックスから「**Availability State**」列を選択します。
9. 「**OK**」をクリックして、ツリー・テンプレートに対する変更を保存します。

以下の図は、ツリー・テンプレート・エディターの画面取りを示しています。System Automation の監視状態を示す新規の列「**Availability State**」が追加されています。

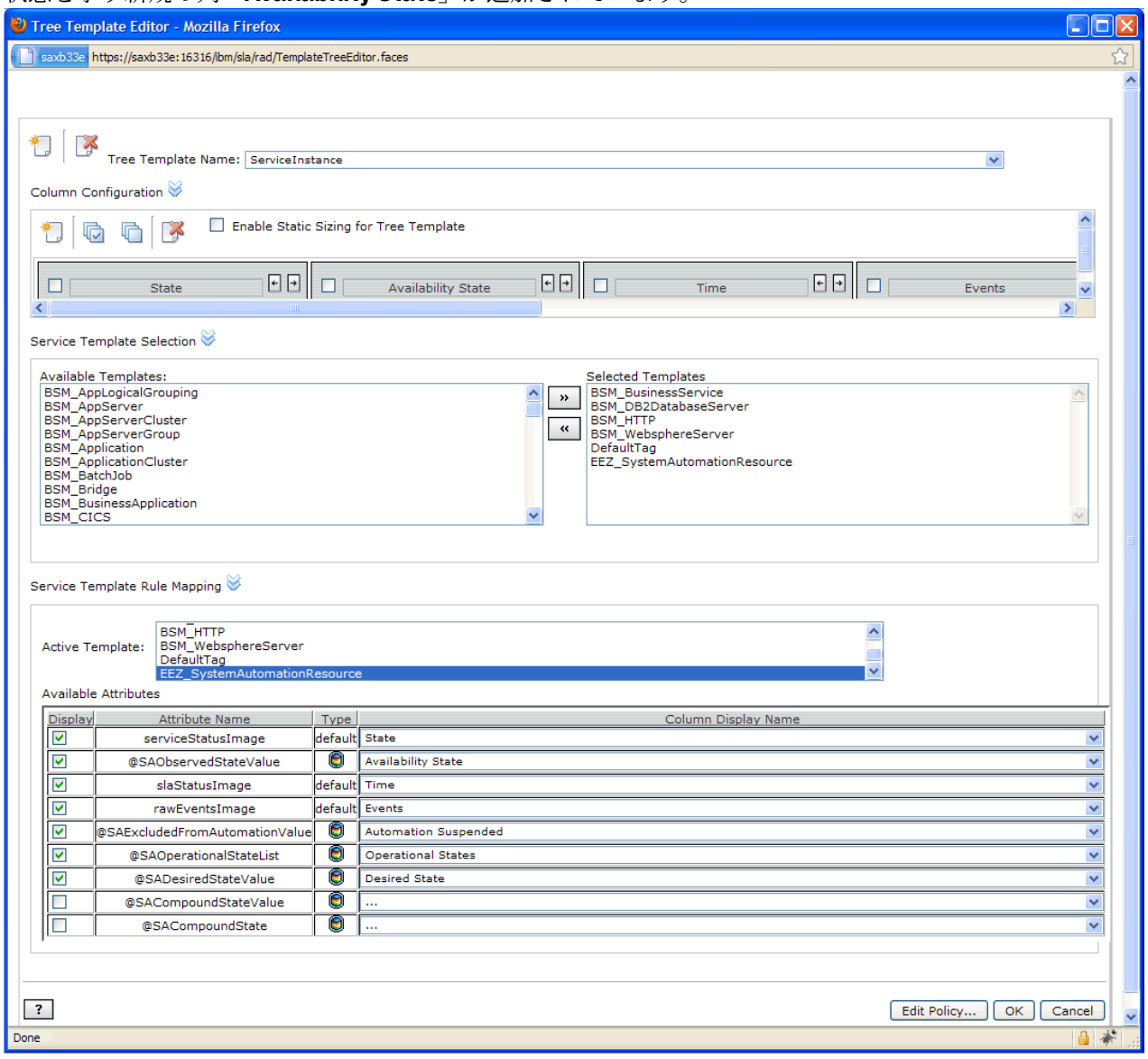


図 *18.* ツリー・テンプレート・エディター

更新したサービス・ツリーを表示するには、サービス・ナビゲーション・ポートレットを最新表示します。新規列には、選択した着信状況ルールの出力が表示されるようになります。

注 : TBSM に表示される状態情報を更新するには、新規のリソース状況変更イベントを作成する必要があります。古いイベントは再度処理されません。

TBSM ポリシー・エディターの使用:

オプションで、TBSM ポリシー・エディターを使用して、列値をフォーマット設定できます。例えば、SA の「監視状態」値を別の色で表示します。以下のように進めます。

1. サービス・ナビゲーション・ポートレットのツールバーで「**ツリー・テンプレート・エディター**」ボタンをクリックします。
2. 変更するツリー・テンプレートを「**ツリー・テンプレート名**」ドロップダウン・リストで選択します。
3. 列値を表示するポリシーを開くには、「**ポリシーの編集...**」ボタンをクリックします。
   `GetTreeColumnValue` という名前のポリシーがポリシー・エディターで開きます。

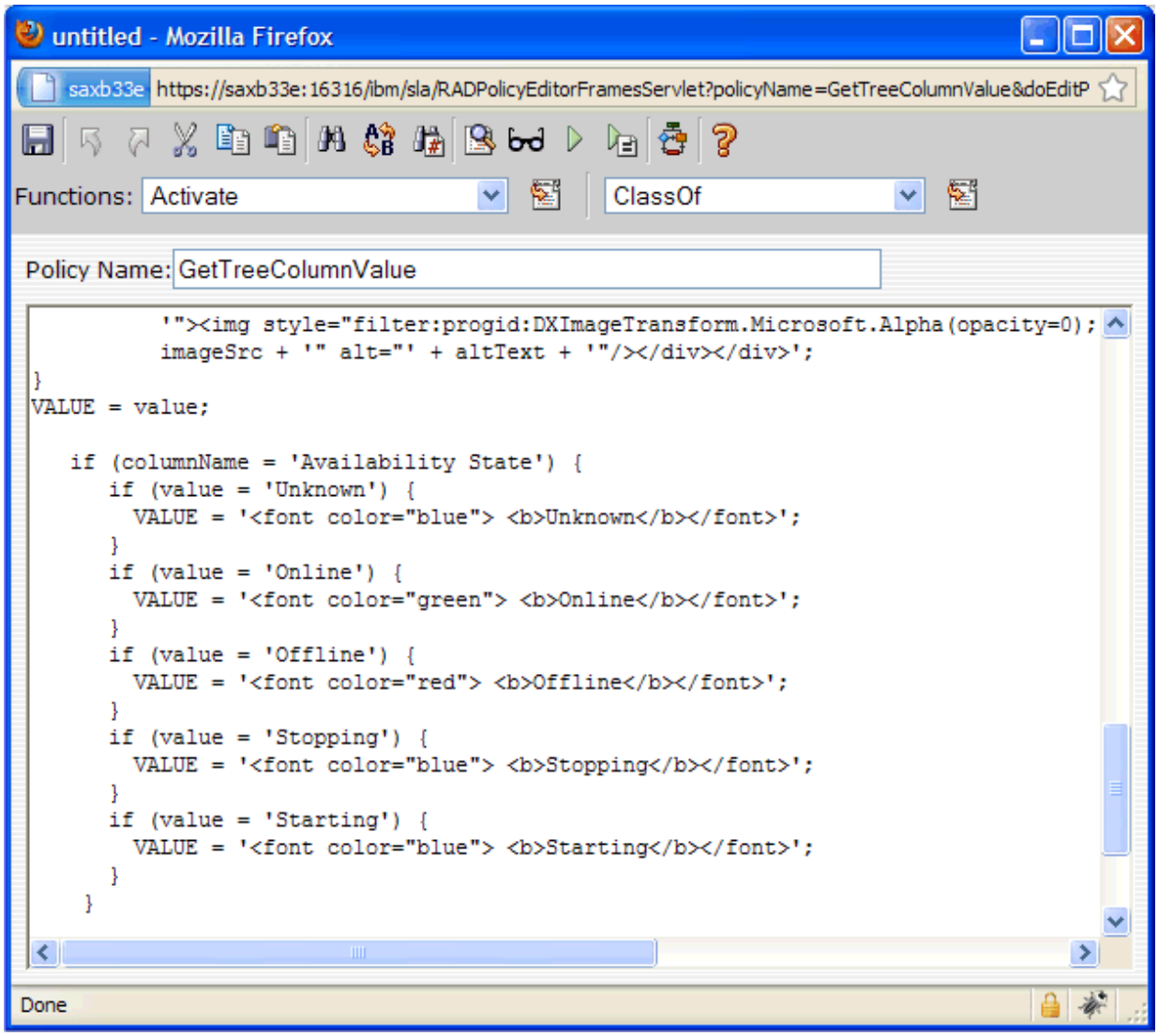


図 *19. TBSM* ツリー・テンプレート・エディター

4. ポリシーを変更します。以下のコード・スニペットは、テキスト・ベースの出力値の色を変更する方法の例です。この例では、`SAObservedState Rule` の出力を表示する「Availability State」という名前の列が定義されていることが想定されています。 監視状態の値によっては、ポリシー・スニペットは値を別の色で戻します。

```
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. 変更したポリシーを保存します。

第 5 章 保護

System Automation for Multiplatforms 環境の保護には、Secure Socket Layer (SSL) 接続の構成と、無許可アクセスからのクラスター環境の保護が含まれます。

AIX および Linux システムで、System Automation for Multiplatforms のコマンド行インターフェースの非 root セキュリティーをセットアップできます。

Linux および AIX システム上で、System Automation for Multiplatforms で操作可能タスクを実行して System Automation for Multiplatforms の自動化ポリシーを変更するのに必要な権限をデフォルトとして持つのは、ユーザー `root` のみです。その他のすべてのユーザーが持つのは読み取りアクセス権限のみです。

クラスターにアクセスするユーザーの許可の管理

System Automation for Multiplatforms のセキュリティーの概念は、アクセス・コントロール・リスト (ACL) ファイルを使用してセキュリティー許可をインプリメントする、RSCT コンポーネント RMC に基づいています。特に、RMC は特定ノードで ACL ファイルを使用して、ユーザーがリソース・クラスおよびそのリソース・インスタンスにアクセスするために必要なアクセス権を判別します。System Automation リソース・マネージャーは RMC アプリケーションとして内部的に実装されるため、非 root ユーザーが System Automation に関連するリソース・クラス (`IBM.ResourceGroup`、`IBM.ManagedRelationship`、`IBM.Equivalency`、`IBM.ManagedResource`、`IBM.CHARMControl`、`IBM.Application`、`IBM.ServiceIP`) を管理 (定義、定義解除、または変更) し、対応するリソース・グループを開始および停止できるようにするために、同じ ACL 制御ルール・セットを使用する必要があります。

RMC ACL ファイルのセットアップ方法の詳細については、「IBM RSCT Administration Guide」の以下のセクションを参照してください。

- 第 4 章 (『Managing and monitoring resources using RMC and resource managers』) の『Managing user access to resources using RMC ACL files』
- 第 7 章 (『Understanding and administering cluster security services』) の『Configuring the global and local authorization identity mappings』

コマンド行インターフェースの場合の非 root ユーザー ID のセットアップ

RSCT および RMC セキュリティー許可サポートは、個々のリソース・クラスおよび単一のノードに基づいてユーザー・アクセスを管理します。例えば、ユーザー・アクセスをクラスター内の特定のノードの特定の RMC リソース・クラスに限定することができます。このレベルの許可設定は複雑で、それぞれ個々の RMC リソース・クラスの性質を明確に理解する必要があります。

したがって、System Automation for Multiplatforms のオペレーターおよび System Automation for Multiplatforms の管理者の役割を、クラスター内に定義されたすべてのノードから非ルート・ユーザーがすべてのリソース・クラスを管理できる一般的な設定で作成する必要があります。以下の手順を使用して、次の 2 つの役割を作成します。

- 管理者用の `sa_admin`
- オペレーター用の `sa_operator`

役割は、次のセクションで詳細に説明されています。http://www.ibm.com/support/knowledgecenter/en/SSRM2X_4.1.0/com.ibm.samp.doc_4.1/sampugbug_limit_non-root.html

System Automation for Multiplatforms バージョン 4.1.0.4 以上には、非 root ユーザーのセットアップを実行するためのスクリプト samnonrootuse が用意されています。このスクリプトは既存のユーザーを必要とし、「sa_admin」または「sa_operator」としてユーザーを定義するために、ファイルのアクセス権と ACL ファイルを調整します。

インストールされている System Automation バージョンが 4.1.0.4 より低い場合は、以下に説明する手動セットアップを実行する必要があります。

役割の作成には、以下のステップを実行します (root 権限が必要なことに注意してください)。この例では、Linux 環境で実行する必要があるコマンドを示します。

1. すべてのノード上の System Automation for Multiplatforms を管理する際に許可する、ユーザー ID を作成します。

```
# /usr/sbin/useradd ernie
# /usr/sbin/useradd bert
```

2. すべてのノードにユーザー ID のグループを作成します。

```
# /usr/sbin/groupadd sagroup
```

3. すべてのノードにユーザー ID のグループを追加します。

```
# /usr/sbin/usermod –G sagroup ernie
# /usr/sbin/usermod –G sagroup bert
```

注 : すべてのノードの System Automation for Multiplatforms のすべてのユーザーに、以下の環境変数を必ず設定します (ピア・ドメイン・スコープ)。

```
CT_MANAGEMENT_SCOPE=2
```

これをユーザー・プロファイルに設定すると、変数を永続的に設定できます。

4. ファイル /var/ct/IBM.RecoveryRM.log のグループの所有権を変更します。

ファイルは、System Automation for Multiplatforms ヒストリーを追跡するのに使用されます。 自動化マネージャー (IBM.RecoveryRM) のリソースを変更するコマンドは、すべてこのファイルに記録されます。

デフォルトでは、ファイルはユーザー・グループ root によって所有されます。

```
-rw-r--r--  1 root root   204 Oct 4 22:00 /var/ct/IBM.RecoveryRM.log
```

次のようにして、グループ所有権を sagroup に変更します。

```
/bin/chgrp sagroup /var/ct/IBM.RecoveryRM.log
```

次のようにして、ファイル許可を 664 に変更します。

```
# /bin/chmod 664 /var/ct/IBM.RecoveryRM.log
       -rw-rw-r-- 1 root sagroup 204 Oct 4 22:00 /var/ct/IBM.RecoveryRM.log
```

注 : System Automation for Multiplatforms の初期インストール後にファイル /var/ct/IBM.RecoveryRM.log が存在しない場合は、/usr/bin/touch コマンドを実行してダミー・ファイルを作成できます。

```
# /usr/bin/touch /var/ct/IBM.RecoveryRM.log
```

5. すべてのノードで、ファイル /var/ct/cfg/ctsec_map.global を変更します。

クラスター内のすべてのノード上の RSCT グローバル許可 ID マッピング・ファイル (/var/ct/cfg/ctsec_map.global) に、ユーザー ID ernie および bert の以下の項目を追加する必要があります。ユーザー clusteruser の項目の上に、以下のように新しい項目を追加します。

```
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
```

このファイルは、ノード上のローカル・ユーザー ID を、System Automation for Multiplatforms ドメイン内のグローバル・ユーザー ID にマップする際に使用されます。 この例では、ローカル・ユーザー ID ernie はグローバル・ユーザー ID sa_operator にマップされ、ローカル・ユーザー ID bert はグローバル・ユーザー ID sa_admin にマップされます。

すべてのノード上でこのグローバル・マップ・ファイルに行を追加し、ローカル・ユーザー ID を必要な役割 (オペレーターまたは管理者) にマップすることによって、System Automation for Multiplatforms のローカル・ユーザー ID を追加で許可することができます。

注: ノード上にファイル //var/ct/cfg/ctsec_map.global が存在しない場合は、デフォルトのファイル /usr/sbin/rsct/cfg/ctsec_map.global をディレクトリー /var/ct/cfg にコピーして、新しい項目を ファイル /var/ct/cfg/ctsec_map.global に追加します。コピーしたデフォルト・ファイルにあるファイル /var/ct/cfg/ctsec_map.global から、項目を削除しないでください。 クラスター内のすべてのノード上の /var/ct/cfg/ctsec_map.global ファイルが同一でなければなりません。必ずユーザー clusteruser の項目の上に、非 root ユーザーの新しい ID を追加してください。

6. すべてのノードのファイル /var/ct/cfg/ctrmc.acls を変更します。 グローバル・ユーザー ID sa_operator および sa_admin の次の項目を、クラスター内のすべてのノードの RMC ACL ファイル (/var/ct/cfg/ctrmc.acls) に追加し、例えば次のように、LOCALHOST で始まる行を削除する必要があります。

```
   The following stanza contains default ACL entries.
   # These entries are appended
   # to each ACL defined for a resource class and
   # are examined after any entries
   # explicitly defined for a resource class
   # by the stanzas in this file,
   # including the OTHER stanza.
   DEFAULT
   root@LOCALHOST *      rw
   none:root * rw // give root access to all
   none:sa_admin * rw // append this row for saadmin
   none:sa_operator * rso // append this row for saoperator
```

7. 必要な変更が完了したら、クラスター内のすべてのノードで次のコマンドを実行して、変更をアクティブにします。

```
# /usr/bin/refresh -s ctrmc
```

8. **sampolicy** および ***samadapter** コマンドの使用に必要な追加の変更:

   a. 構成ファイルへのアクセス:

   ```
   # /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. ログ・ファイルへのアクセス:

   ```
   # /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. /etc ディレクトリー内の構成ファイルへのアクセス。 ディレクトリー /etc/opt/IBM/tsamp/sam/cfg がない場合は、以下を使用してそれを作成します。

   ```
   # /bin/mkdir -p /etc/opt/IBM/tsamp/sam/cfg
   ```

   次に適切な許可を設定します。

   ```
   # /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. sam.policies パッケージを使用する場合に必要な任意の調整: インストール・パッケージ sam.policies には、さまざまなアプリケーション用の既製のポリシーが用意されています。このパッケージは、 IBM Integrated Service Management Library からダウンロードできます。
10. sa_admin 役割を持つユーザーがこれらの既製のポリシーをセットアップできるようにするため、すべてのノードへの sam.policies パッケージのインストール後、/usr/sbin/rsct/sapolicies ディレクトリーの許可および所有権を変更する必要があります。

```
# chmod -R 2775 /usr/sbin/rsct/sapolicies
# chgrp -R sagroup /usr/sbin/rsct/sapolicies
```

ステップを正常に完了すると、ローカル・ユーザー ernie および bert は、リソースに対する開始および停止要求の発行などの System Automation for Multiplatforms の操作可能タスクを実行でき、ローカル・ユーザー bert は、ポリシーの定義および変更などの System Automation for Multiplatforms の管理用タスクも実行できます。

RSCT レベル 2.5.4.0 以上を使用する非 root ユーザーのデフォルトの許可の変更

RSCT レベル 2.5.4.0 (AIX 6 および Linux) 以降では、リソースをリストするコマンドの実行を非 root ユーザーに許可しないようにする変更が導入されました。 新規ドメインが作成される 場合は、適切な許可が自動的に構成されます。

既存のドメインをこの RSCT レベルに マイグレーションする場合、lssam や lsrg -m などのコマンドを実行する適切な許可は、非 root ユーザーに対して自動的に構成されません。 以下のようにご使用の RSCT レベルに応じて適切なアクションを選択して、構成を調整してください。

RSCT レベルが 2.5.5.2 (AIX 6 および Linux) 以上の場合:
暗黙的に構成を調整する別のドメインを作成します。 新しいドメインを開始しないでください。後で取り外すことができます。

それ以外の場合 (つまり RSCT レベルが 2.4.13.2 より低い場合):
以下のコマンドを使用して、 ユーザー root としてすべてのノードで構成を調整します。

1. ファイル /usr/sbin/rsct/cfg/ctsec_map.global を編集して、 次の内容が存在しない場合は、この内容を追加します。

```
unix:*@*=clusteruser
```

2. ファイル /tmp/addacl を作成し、以下の内容を追加します。

```
DEFAULT
   none:clusteruser * r
```

3. 次のコマンドを実行して、acl ファイルを調整します。

```
/usr/sbin/rsct/install/bin/chrmcacl -a < /tmp/addacl
```

4. ctrmc サブシステムをリフレッシュして、変更を有効にします。

```
refresh -s ctrmc
```

これで、以前の RSCT レベル同様、非 root ユーザーが lssam や lsrg -m などのコマンドを使用できるようになりました。

非ルート・セキュリティー・セットアップの制限

このタスクについて

以下のリストは、非ルート・セキュリティー・セットアップの制限の要約です。

- 通常のユーザーは、RMC Resource Manager のトレース・ファイルの内容を表示できません (例えば、IBM.RecoveryRMd デーモンのトレース)。

  すべての RMC Resource Manager デーモンは、RMC フレームワーク・ライブラリー・ユーティリティーを使用して、/var/ct/<cluster> ディレクトリーの下に、トレース・ファイルおよびコア・イメージを作成します。これらのリソース・マネージャーは、**/usr/bin/startsrc** コマンドを使用して、スーパーユーザー (ユーザー ID root) によってのみ開始できるので、作成されるファイルは、ユーザー ID root に属します。

  すべての非ルート・ユーザーは、**/usr/sbin/rsct/bin/ctsnap** コマンドを使用してデバッグおよびトレース情報を収集することはできません。

  非ルート・ユーザーが、トレース・データまたは ctsnap デバッグ・データ、あるいはその両方を収集できるようにするには、これらのユーザーおよびコマンドに "sudo" のようなメカニズムをインプリメントする必要があります。
- 以下のコマンドは、root 権限を持っている場合のみ始動することができます。これは、これらのコマンドが、ログ・ファイルが root 権限で保守されている場合のみ正しく機能する Tivoli ロギングを使用するためです。
  - **sampolicy** コマンド。
  - エンドツーエンド自動化アダプターを開始するための **samadapter** コマンド。
  - ライセンスをインストールまたはアップグレードする **samlicm** コマンド。
- ACL オブジェクトの細分度は、リソースではなくリソース・クラスに基づいています。 つまり、通常のユーザーは、リソース・クラスのリソースの変更を認可される場合も、されない場合もありますが、リソース・ベースの許可を認可または否認することはできません。例えば、データベース管理者に、データベース・リソースのみの権限を与えることはできません。
- "sa_operator" 役割は、リソースの属性値を変更して、リソースを変更できます。 これは、System Automation for Multiplatforms 要求を出すのに必要な "s" 許可の結果です。 この役割を持つユーザーは、「s」許可なしにいかなる有効なタスクも実行できません。「s」許可があれば、属性の設定および変更を行えます。

以下の表に、代表的な System Automation for Multiplatforms タスクの実行に必要な役割または権限を示します。

表 *35. System Automation for Multiplatforms* タスクを実行する許可および役割

操作	**権限**	**役割**	**アクセス権**
製品および製品ライセンスのインストール	ルート	システム管理者	System Automation for Multiplatforms および製品ライセンスのインストールおよびアップグレード
クラスター管理	ルート / sa_admin	システム管理者/ System Automation for Multiplatforms 管理者	クラスターおよび個々の RMC Resource Manager の定義、開始、停止、およびモニター
リソース定義および System Automation for Multiplatforms のポリシー定義	ルート / sa_admin	システム管理者/ System Automation for Multiplatforms 管理者	リソースの定義、除去、変更、および自動化ポリシーのセットアップ

表 35. *System Automation for Multiplatforms* タスクを実行する許可および役割 (続き)

操作	権限	役割	アクセス権
自動化操作	ルート / sa_admin / sa_operator	システム管理者 / System Automation for Multiplatforms 管理者およびオペレーター	「オンライン」および「オフライン」要求の発行、ならびにリソース・グループおよび個々のリソースのリセットおよびモニター
問題判別用のトレースおよびデバッグ・データの収集	ルート	システム管理者	すべてのシステムおよびアプリケーション・トレース (ログ) ファイルへのアクセス (制限のリストを参照)
セキュリティーのセットアップ	ルート	システム管理者	このセクションで説明するセキュリティー・セットアップの定義、変更、および除去
アダプター・セットアップ	ルート / sa_admin	システム管理者/ System Automation for Multiplatforms 管理者	エンドツーエンド自動化の構成の定義、変更、および除去

SSL を使用したエンドツーエンド自動化アダプターへの接続の保護

System Automation Application Manager エンドツーエンド自動化サーバーと System Automation for Multiplatforms エンドツーエンド自動化アダプターとの間の通信用に、ご使用の環境内で Secure Socket Layer (SSL) を構成します。

このタスクについて

このトピックでは、System Automation Application Manager サーバーとエンドツーエンド自動化アダプターの間の接続を保護する方法を説明します。System Automation Application Manager サーバーと自動化アダプターの間の接続は、両方向通信で、すべての照会およびアクションは、SSL 暗号化によって保護されます。 EIF イベントの自動化アダプターから System Automation Application Manager サーバーへの送信は保護されません。この接続の保護について詳しくは、*IBM Tivoli System Automation Application Manager Installation and Configuration Guide* を参照してください。

SSL 公開鍵および秘密鍵を使用した鍵ストアおよびトラストストアの生成

このタスクについて

以下のファイルを生成します。

- **トラストストア**: Application Manager と FLA アダプター用の公開鍵を含みます。
- **Application Manager 鍵ストア:** Application Manager 用の秘密鍵を含みます。
- **アダプター鍵ストア**: アダプターごとに 1 つ生成します。 FLA アダプター用の秘密鍵を含みます。

129 ページの図 20 に関連コンポーネント、ファイルおよびファイルを生成する手順の概要を示します。以降で、オペレーション・コンソール という用語は System Automation Application Manager オペレーション・コンソールを意味します。

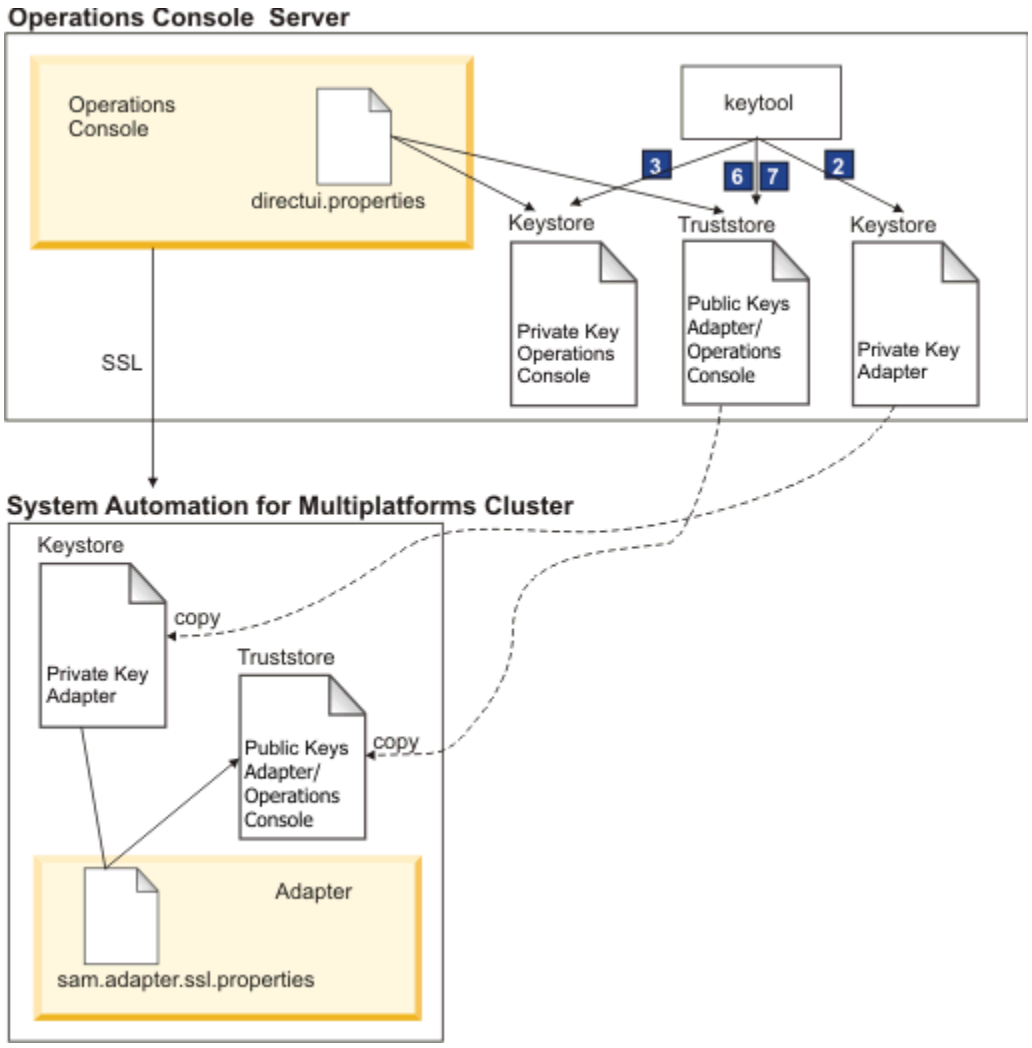


図 *20. SSL* を使用した鍵ストアおよびトラストストアの生成

以下の手順を実行してトラストストアおよび鍵ストアを生成します。鍵は、デフォルトの有効期間が 9125 に設定されているため、25 年後に有効期限が切れます。パスフレーズは 6 文字以上にしてください。 手順の番号は 129 ページの図 20 の番号に関係します。使用されている値は、サンプル値またはデフォルト値です。

1. **変数の設定:**

```
# 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
# keys will expire in 25 years
KEY_VALIDITY_DAYS=9125
# passphrase at least 6 characters
PASSPHRASE=passphrase
```

2. **自動化アダプター用の公開鍵および秘密鍵を使用した鍵ストアの生成:**

```
${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. **オペレーション・コンソール用の公開鍵および秘密鍵を使用した鍵ストアの生成:**

```
{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. **自動化アダプター用の公開鍵を使用した証明書ファイルのエクスポート:**

```
${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. **オペレーション・コンソール用の公開鍵を使用した証明書ファイルのエクスポート:**

```
${JAVA_KEYTOOL} -export -alias eezoperationsconsole ¥
          -file "${OC_CONFIG_DIR}/ssl/eezoperationsconsole.cer" -storepass ${PASSPHRASE} ¥
          -keystore "${OC_CONFIG_DIR}/ssl/sam.ssl.operationsconsole.keystore.jks"
```

6. **許可された鍵のトラストストアの生成および自動化アダプター用の公開鍵を使用した証明書のインポート:**

```
${JAVA_KEYTOOL} -import -noprompt -alias samadapter ¥
          -file "${OC_CONFIG_DIR}/ssl/samadapter.cer" -storepass ${PASSPHRASE} ¥
          -keystore "${OC_CONFIG_DIR}/ssl/sam.ssl.authorizedkeys.truststore.jks"
```

7. **許可された鍵のトラストストアの生成およびオペレーション・コンソール用の公開鍵を使用した証明書のインポート:**

```
{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. **自動化アダプター用の証明書ファイルを削除します。 この証明書ファイルは、実行時には必要ではありません。**

```
rm ${OC_CONFIG_DIR}/ssl/samadapter.cer
```

9. **オペレーション・コンソール用の証明書ファイルを削除します。 この証明書ファイルは、実行時には必要ではありません。**

```
rm ${OC_CONFIG_DIR}/ssl/samoperationsconsole.cer
```

自動化アダプター構成での SSL セキュリティーの使用可能化

このタスクについて

自動化アダプター構成で SSL セキュリティーを使用可能にするには、以下の手順を実行します。

1. **許可された鍵のトラストストア・ファイルを IBM Tivoli System Automation for Multiplatforms クラスターのすべてのノードにコピーします。**

```
scp ${OC_CONFIG_DIR}/ssl/sam.ssl.authorizedkeys.truststore.jks ¥
    root@<adapter-nodename>:/etc/opt/IBM/tsamp/eez/cfg/ssl/sam.ssl.authorizedkeys.truststore.jks
```

2. **アダプターの鍵ストア・ファイルを IBM Tivoli System Automation for Multiplatforms クラスターのすべてのノードにコピーします。**

```
cp ${OC_CONFIG_DIR}/ssl/sam.ssl.adapter.keystore.jks ¥
    root@<adapter-nodename>:/etc/opt/IBM/tsamp/sam/cfg/ssl/sam.ssl.adapter.keystore.jks
```

3. **構成ユーティリティーを開始します。**

   コマンド `cfgsamadapter` を入力してください。

4. **パラメーターを指定します。**

構成ダイアログのメインウィンドウで、「**構成**」をクリックします。「**セキュリティー**」タブで以下のパラメーターを指定します (79 ページの『「セキュリティー」タブ』を参照)。 以下の値はサンプル値です。

- トラストストア: `/etc/opt/IBM/tsamp/sam/cfg/ssl/sam.ssl.authorizedkeys.truststore.jks`
- 鍵ストア: `/etc/opt/IBM/tsamp/sam/cfg/ssl/sam.ssl.adapter.keystore.jks`
- 鍵ストアのパスワード: `passphrase`
- 証明書の別名: `samadapter`

「**保存**」をクリックして構成変更を保管します。

5. 構成ダイアログのメインウィンドウで、「**複製**」をクリックします。この構成ファイルをこの SSL 構成を含む IBM Tivoli System Automation for Multiplatforms クラスターのクラスターの別のノードに複製します。
6. 自動化アダプターの制御に使用する `samadapter` コマンドを使用して、自動化アダプターを再始動します。これにより、SSL 構成がアクティブになります。
7. System Automation Application Manager サーバー を再始動し、SSL 構成をアクティブ化します。

   以下のコマンドを使用して、System Automation Application Manager サーバーを手動で開始または停止します。

   開始
   ```
   /opt/IBM/WebSphere/AppServer/bin/startServer.sh server1
   ```
   停止
   ```
   /opt/IBM/WebSphere/AppServer/bin/stopServer.sh server1
   ```
   注 : System Automation Application Manager サーバーを停止するには、WebSphere Application Server の管理ユーザー ID とパスワードが必要です。

IBM Support Assistant の使用

以下は英語のみの対応となります。IBM Support Assistant は、任意のワークステーションにインストールできる、フリーのスタンドアロン・アプリケーションです。IBM Support Assistant を使用することで、製品、サポート、および教育リソースを検索する時間が節約され、問題管理レコード (PMR) または Electronic Tracking Record (ETR) を開く必要がある場合に 情報を収集するために役立ちます。これらのレコードは問題の追跡に使用できます。

次に、ご使用の IBM 製品に対応する製品固有のプラグイン・モジュールをインストール して、このアプリケーションを機能強化できます。Tivoli System Automation for Multiplatforms 用の製品固有プラグインは、以下のリソースを提供します。

- サポート・リンク
- 教育リンク
- 問題管理レポートを送信する機能
- トレース収集機能

IBM Support Assistant および Tivoli System Automation for Multiplatforms プラグインのインストール

IBM Support Assistant V 4.1 をインストールするには、以下のステップを実行します。

- IBM Support Assistant Web サイトにアクセスします。

  ```
  www.ibm.com/software/support/isa/
  ```

- ご使用のプラットフォームに対応するインストール・パッケージをダウンロードします。IBM のユーザー ID (例えば、MySupport または developerWorks® ユーザー ID) およびパスワードを使用してサインインする必要があることに注意してください。IBM ユーザー ID をお持ちでない場合は、登録処理 (無料) を完了することにより入手できます。
- インストール・パッケージを一時ディレクトリーに解凍します。
- インストール・パッケージに含まれている「*Installation and Troubleshooting Guide*」の指示に従って、IBM Support Assistant をインストールします。

Tivoli System Automation for Multiplatforms のプラグインをインストールするには、以下の手順を実行します。

1. IBM Support Assistant アプリケーションを始動します。IBM Support Assistant は、システムに構成されているデフォルトの Web ブラウザーに表示される Web アプリケーションです。
2. IBM Support Assistant 内の「**アップデーター(Updater)**」タブをクリックします。
3. 「**新規製品およびツール (New Products and Tools)**」タブをクリックします。製品ファミリーごとにプラグイン・モジュールがリストされます。
4. 「**Tivoli**」 > 「**Tivoli Tivoli System Automation for Multiplatforms** 」 を選択します。
5. インストールする機能を選択し、「**インストール**」をクリックします。ライセンス情報および使用法の説明を必ずお読みください。
6. IBM Support Assistant を再始動します。

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、 サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。 本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、 またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の 製品、プログラム、またはサービスを使用することができます。 ただし、IBM 以外の製品とプログラムの操作またはサービスの 評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を 保有している場合があります。本書の提供は、お客様にこれらの特許権について 実施権を許諾することを意味するものではありません。 実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒 103-8510
東京都中央区日本橋箱崎町 19 番 21 号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムと その他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
Mail Station P300
2455 South Road
Poughkeepsie New York 12601-5400
U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用すること ができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定の プログラム契約の契約条項、IBM プログラムのご使用条件、 またはそれと同等の条項に基づいて、IBM より提供されます。

以下の保証は、国または地域の法律に沿わない場合は、適用されません。 IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、 商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含む すべての明示もしくは黙示の保証責任を負わないものとします。 国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、 強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。 本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、 改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものでは ありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。 それらの Web サイトは、お客様の責任でご使用ください。

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は 表示されない場合があります。

商標

- IBM、IBM ロゴおよび ibm.com は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、ibm.com/trademark をご覧ください。
- Adobe、Adobe ロゴ、PostScript、PostScript ロゴは、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。
- Microsoft、Windows、および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。
- Java およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の商標または登録商標です。
- Linux は、Linus Torvalds の米国およびその他の国における登録商標です。
- Red Hat およびすべての Red Hat ベースの商標は、Red Hat, Inc. の米国およびその他の国における商標または登録商標です。
- UNIX は The Open Group の米国およびその他の国における登録商標です。

索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

[ア行]

[カ行]

[サ行]

[タ行]

[ナ行]

[ハ行]

[マ行]

[ラ行]

A

D

E

I

L

N

R

S

T

V

X

Z

[特殊文字]

プログラム番号:　5724-M00

SA88-7249-05